



**CYBER DEFENSE**  
MAGAZINE

**eMAGAZINE**

## IN THIS EDITION

*Election Integrity Is A Moving Target, But  
It's Essential to Pursue*

*Acronis Cyber Readiness Report*

*COVID Impact on MSSPs*

*Cyber-Attacks Are the New Norm and  
Ransomware Is on The Rise*

*...and much more...*

**OCTOBER 2020**

**MORE INSIDE!**

# CONTENTS

Welcome to CDM's October 2020 Issue-----	7
<b><i>Election Integrity Is A Moving Target, But It's Essential to Pursue</i></b> -----	25
By Craig Hinkley, Chief Executive Officer, WhiteHat Security, a wholly-owned, independent subsidiary of NTT Ltd.	
<b><i>Acronis Cyber Readiness Report</i></b> -----	29
By Peter Hale, Sr. Content Manager, Acronis	
<b><i>Centrify Study Lifts the Hood on Cybersecurity Policy and Threat Challenges During COVID-19</i></b> -----	35
By Andy Heather, VP and managing director - EMEA, Centrify	
<b><i>Are Your Corporate Networks Ready for An Impending 'Return to Work' Cyber Attack?</i></b> -----	38
By Stephen Burke, Cyber Risk Aware CEO & Founder	
<b><i>COVID Impact on MSSPs</i></b> -----	41
By Tristan Hinsley, Cybersecurity Expert, TDI Security	
<b><i>The Four Insights Network Metadata Can Reveal About Your Compromise Level</i></b> -----	43
By Ricardo Villadiego, CEO of Lumu	
<b><i>Business Email Compromise - Why Is It Dangerous and How to Avoid It</i></b> -----	47
By Elena Georgescu, Communication & PR Officer at Heimdal™ Security	
<b><i>Cyber-Attacks Are the New Norm and Ransomware Is on The Rise</i></b> -----	52
By Ehab Halablab, Regional Sales Director – Middle East at A10 Networks	
<b><i>One Year on From Whatsapp Hack- What's Changed?</i></b> -----	55
By Nicole Allen, Marketing Executive, SaltDNA	
<b><i>Years of IoT Hacking, But What Have We Actually Learned?</i></b> -----	58
By Brad Ree, CTO, ioXt Alliance	
<b><i>Building Trust: The Path to True Security Synergy Between Appsec And Developers</i></b> -----	61
By Matias Madou, co-founder and CTO, Secure Code Warrior	
<b><i>3 Steps to Reimagine Your AppSec Program</i></b> -----	65
By Jake Reynolds, Product Manager at NetSPI and Nabil Hannan, Managing Director at NetSPI	

<b><i>Cyber Security Patent Lawsuits on The Rise and The Need for Shared Innovation in Cyber Security --</i></b>	<b>70</b>
By Keith Bergelt, CEO of Open Invention Network (OIN)	
<b><i>The Challenges of Industrial 3D NAND-----</i></b>	<b>74</b>
By Roger Griesemer, General Manager Memory Solutions, Swissbit AG and Ulrich Brandt, Technical Director Marketing, Swissbit AG	
<b><i>How Can CISOs Work with CMOs to Secure Social Media?-----</i></b>	<b>82</b>
By Otavio Freire, CTO & Co-Founder, SafeGuard Cyber	
<b><i>Why Deepfakes Will Threaten the Future of Digital Communications -----</i></b>	<b>86</b>
By Steve Durbin, Managing Director, Information Security Forum	
<b><i>5 Steps to Ensure IoT Security Amidst CMMC Compliance -----</i></b>	<b>89</b>
By Mike Raymond, Federal Sales Manager, Ordr	
<b><i>Under the SASE Hood: Key Components to Delivering Frictionless, Cloud-Native Security-----</i></b>	<b>93</b>
By Kaushik Narayan, CTO Cloud Business Unit, McAfee	
<b><i>The Limitations of SASE and Zero Trust-----</i></b>	<b>97</b>
By Jayant Shukla, CTO and Co-Founder, K2 Cyber Security	
<b><i>Measuring Cybersecurity Systems Durability -----</i></b>	<b>101</b>
By Joseph Kirkpatrick, President, Kirkpatrick Price	
<b><i>Defending Ever Expanding Networks and IT Systems-----</i></b>	<b>103</b>
By Trevor Pott, Product Marketing Director, Juniper Networks	
<b><i>Reducing ‘Cyber-security Engineer Burnout’ -----</i></b>	<b>107</b>
By Tim Bloomer, a Sales Engineer at AlgoSec	
<b><i>How to Avoid or Remove Mac Malware -----</i></b>	<b>110</b>
By Emma Brighton, a contributor to Cyber Experts and Cybers Guards.	
<b><i>How To Protect Your Self-Driving Car From Potential Cyber Threats -----</i></b>	<b>114</b>
By Okonkwo Noble, travel enthusiast, Writer, and Electrical Electronics Engineer, Limo services U.S.A	
<b><i>The Impact Of Blockchain &amp; Crypto On Cyber Security -----</i></b>	<b>118</b>
By Jesús Cedeño, Senior Editor, cryptocurrenciesociety.co -----	

***The Serverless Security Machine ----- 124***

By Art Sturdevant, Director of Operations, Censys

***Why Endpoint Protection Should Be a Security Priority ----- 127***

By JG Heithcock, General Manager of Retrospect, Inc., a StorCentric Company

***Psychological Operations in A Modern Landscape ----- 130***

By Milica D. Djekic



@MILIEFSKY

## From the Publisher...



OUR NEWEST PLATFORM ENTERING ITS SIXTH MONTH: PLEASE VISIT [CYBERDEFENSEWEBINARS.COM](https://cyberdefensewebinars.com)

Dear Friends,

Many years ago, only a few of us had modems at home. We were excited to do telecommuting at 28.8k per second – that was fast, in the early days of the internet.

In fact, telecommuting has not been that popular. Most companies have a majority of their employees working at the headquarters or a branch office. However, we've now been hit with a plague – COVID-19 and at a time almost all humans on the planet – billions of us have high speed internet connectivity and on average at least 3 personal devices on the internet – our cell phone, tablets, laptops and desktops.

Now, given the global “shutdown” a few major changes have come to society. The first, is that we now have 100% of company staff having worked from home for at least the first half of the year. Folks are starting to go back to work but we'll still see huge numbers working remotely in the coming years.

This has opened a new door – we're now, in real-time, testing the edges of cloud security, testing scalability of personal and corporate virtual private networks (VPNs) and remote desktop software as well as video conferencing software, en masse.

The effects of COVID-19 on nearly all enterprises which depend on cyberspace for their operations are growing. The actionable intelligence Cyber Defense Magazine provides is the first and best means of meeting these challenges. On that note, checkout our new [Cyber Defense Webinars site](https://cyberdefensewebinars.com) to enjoy contactless expert content.

In addition to the relevant articles in the October issue, we are pleased to continue providing the powerful combination of monthly eMagazines, daily updates, and features on the Cyber Defense Magazine home page, and webinars featuring national and international experts on topics of current interest. Warmest regards,

*Gary S. Miliefsky*

Gary S. Miliefsky, CISSP®, fmdHS  
CEO, Cyber Defense Media Group  
Publisher, Cyber Defense Magazine



*P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly*



**InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE InfoSec information.**

## From the International Editor-in-Chief...

As in past months, the principal international challenges in the world of cybersecurity have centered on issues of varying standards for information security.

Most recently, the inconsistencies and conflicts appear to focus on differing privacy requirements among various jurisdictions.

It may be instructive to remember the legendary French soldier Nicolas Chauvin, who is noted for his message of extreme nationalism and for whom the term "chauvinism" was coined.

While it's not in our brief to take positions for or against national policy, we can only encourage cooperation and compatibility among nations on cybersecurity and privacy matters.

We can but hope that in our world of cybersecurity and privacy, there may be room for both national and global interests.

On that note, please keep an eye on our [WWW.CYBERDEFENSEAWARDS.COM](http://WWW.CYBERDEFENSEAWARDS.COM) site for upcoming Global InfoSec Awards opening up for nominations, very soon.

To our faithful readers, we thank you,  
Pierluigi Paganini  
International Editor-in-Chief



**@CYBERDEFENSEMAG**

## CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

### PRESIDENT & CO-FOUNDER

Stevin Miliefsky

[stevinv@cyberdefensemagazine.com](mailto:stevinv@cyberdefensemagazine.com)

### INTERNATIONAL EDITOR-IN-CHIEF & CO-FOUNDER

Pierluigi Paganini, CEH

[Pierluigi.paganini@cyberdefensemagazine.com](mailto:Pierluigi.paganini@cyberdefensemagazine.com)

### US EDITOR-IN-CHIEF

Yan Ross, JD

[Yan.Ross@cyberdefensemadiagroup.com](mailto:Yan.Ross@cyberdefensemadiagroup.com)

### ADVERTISING

Marketing Team

[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

### CONTACT US:

Cyber Defense Magazine

Toll Free: 1-833-844-9468

International: +1-603-280-4451

SKYPE: cyber.defense

<http://www.cyberdefensemagazine.com>

Copyright © 2020, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (a Steven G. Samuels LLC d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001  
EIN: 454-18-8465, DUNS# 078358935.  
All rights reserved worldwide.

### PUBLISHER

**Gary S. Miliefsky, CISSP®**

Learn more about our founder & publisher at:

<http://www.cyberdefensemagazine.com/about-our-founder/>

## 8 YEARS OF EXCELLENCE!

Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

**[CYBERDEFENSEMEDIAGROUP.COM](http://CYBERDEFENSEMEDIAGROUP.COM)**  
**[MAGAZINE](#)   [TV](#)   [RADIO](#)   [AWARDS](#)**  
**[WEBINARS](#)**

# Welcome to CDM's October 2020 Issue

## From the U.S. Editor-in-Chief

In the October issue of Cyber Defense Magazine, we are pleased to bring our readers over two dozen new and relevant articles with actionable information on cybersecurity trends and practices, provided by our valued contributors.

We start with the most pressing of the COVID-19 issues, cover high-altitude views of the cyber landscape, and then drill down into granular presentations on specific concerns we all face. May I recommend your perusal of the Table of Contents, and select those articles of most direct relevance to your own activities.

One trend I'd like to emphasize, as we focus on the presence (or absence) of a "new normal," is the likelihood that many (if not most) of the workers who now work from home, as opposed to the organization's HQ, will never go back. They may even migrate from W-2 employee to freelancer status on a permanent basis.

One logical implication of this trend takes notice of more and greater remote cybersecurity challenges, meaning that freelancers with robust security will have a competitive advantage over those who don't!

There will, of course, continue to be States like California, which mandates W-2 employee in many situations. As I mentioned last month, HIPAA and HITECH, may require health care administrative workers to be treated as third party business associates, with their own independent set of security and privacy requirements.

With that perspective, we are pleased to present the October 2020 issue of Cyber Defense Magazine.

Wishing you all success in your cyber security endeavors,

Yan Ross

US Editor-in-Chief  
Cyber Defense Magazine

### About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & US Editor-in-Chief for Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him via his e-mail address at [yan.ross@cyberdefensemediagroup.com](mailto:yan.ross@cyberdefensemediagroup.com)





# SPONSORS



# **CYBER DEFENSE MEDIA GROUP**

WHERE INFOSEC KNOWLEDGE IS POWER

**Rise above the noise,  
take your Infosec story to the moon and back!  
Only with Cyber Defense Media Group**



[www.cyberdefensetv.com](http://www.cyberdefensetv.com)  
[www.cyberdefenseradio.com](http://www.cyberdefenseradio.com)  
[www.cyberdefenseawards.com](http://www.cyberdefenseawards.com)  
[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)



**Lucio Frega, Threat Researcher**  
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

#### About the Author/Disclosure



Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.

  
MALWARE  
YARA

PREDICT

  
HUNT



# CYBERSECURITY KNOWLEDGE. WHEN YOU NEED IT.

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

[rsaconference.com/cyberdefense-2020](https://rsaconference.com/cyberdefense-2020)

# Stony Lonesome Group

MISSION FOCUSED INVESTING

EST 2011



Founder & Managing Partner

# SEAN DRAKE



***“At Stony Lonesome Group, we believe that Freedom Is Not Free and we do not take it for granted. SLG is a pioneer and thought leader in Mission Focused Investing protecting American Exceptionalism and National Security by investing in a vital areas of Cybersecurity, Big Data Analytics, and Artificial Intelligence. ”***

**Sean Drake**

Managing Partner

Stony Lonesome Group LLC

203-247-2479

[www.stonylonesomegroupllc.com](http://www.stonylonesomegroupllc.com)



# By the time an attacker tastes the difference, their presence is known.



"Attacker mistakes are made when they cannot distinguish real from fake."

Tony Cole, CTO Attivo Networks

## DECEPTION-BASED THREAT DETECTION

Detecting threats needs to be comprehensive, however it doesn't have to be complicated. Designed for simplicity, Attivo Networks brings uncertainty to the mind of the attacker, redirecting them away from the target assets and providing defenders with high-fidelity alerting that is backed with actionable attack and forensic data on malicious activity and insider policy violations.

**Attivo**  
NETWORKS  
Deceive. Detect. Defend.

Learn more at [attivonetworks.com/ebook](https://attivonetworks.com/ebook)

# Setting the Standard

## in Cyber Defense Training & Education

Transform your cyber defense capabilities with customized training. Regent's Institute for Cybersecurity will help you develop your workforce credentials, manage your cyber risks and defend your assets.

CORPORATE | GOVERNMENT | MILITARY | EDUCATION



Powerful Hyper-Realistic Range Simulation



Industry Certifications



Executive & Senior Leadership Cyber Workshops



Associate, Bachelor's & Master's Programs



Regent's B.S. in Cybersecurity has received NSA and DHS designation.

Learn More

[regent.edu/cyber](https://regent.edu/cyber) | 757.352.4590



**REGENT**  
UNIVERSITY

Institute for  
Cybersecurity

# OneTrust

## Privacy Management Software

## World's #1 Most Widely Used Privacy Management Software

### For Privacy, Security & Third-Party Compliance

Solutions to Comply with the CCPA, GDPR & Global Privacy Laws & Security Frameworks



#### Privacy Program Management:

- Maturity & Planning: Compliance Reporting Scorecard
- Program Benchmarking: Comparison Against Peers
- DataGuidance Research: Regulatory Tracking Portal
- Assessment Automation: PIAs, DPIAs & Info Security



#### Marketing & Privacy UX

- Cookie Compliance: Website Scanning & Consent
- Mobile App Compliance: App Scanning & Consent
- Universal Consent: Consent Receipts & Analytics
- Preference Management: End User Preference Center
- Consumer & Subject Requests: Intake to Fulfillment
- Policy & Notice: Centrally Host, Track & Update



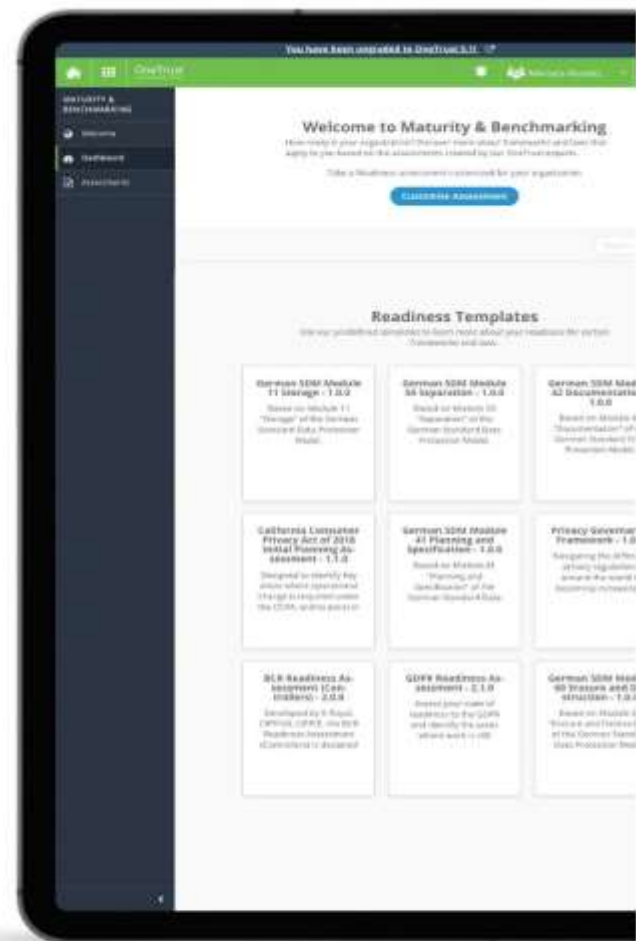
#### Third-Party Risk Management

- Vendorpedia Management: Assessment & Lifecycle
- Vendorpedia Risk Exchange: Security & Privacy Risks
- Vendorpedia Contracts: Contract Scanning & Analytics
- Vendorpedia Monitoring: Privacy & Security Threats
- Vendor Chasing Services: Managed Chasing Services



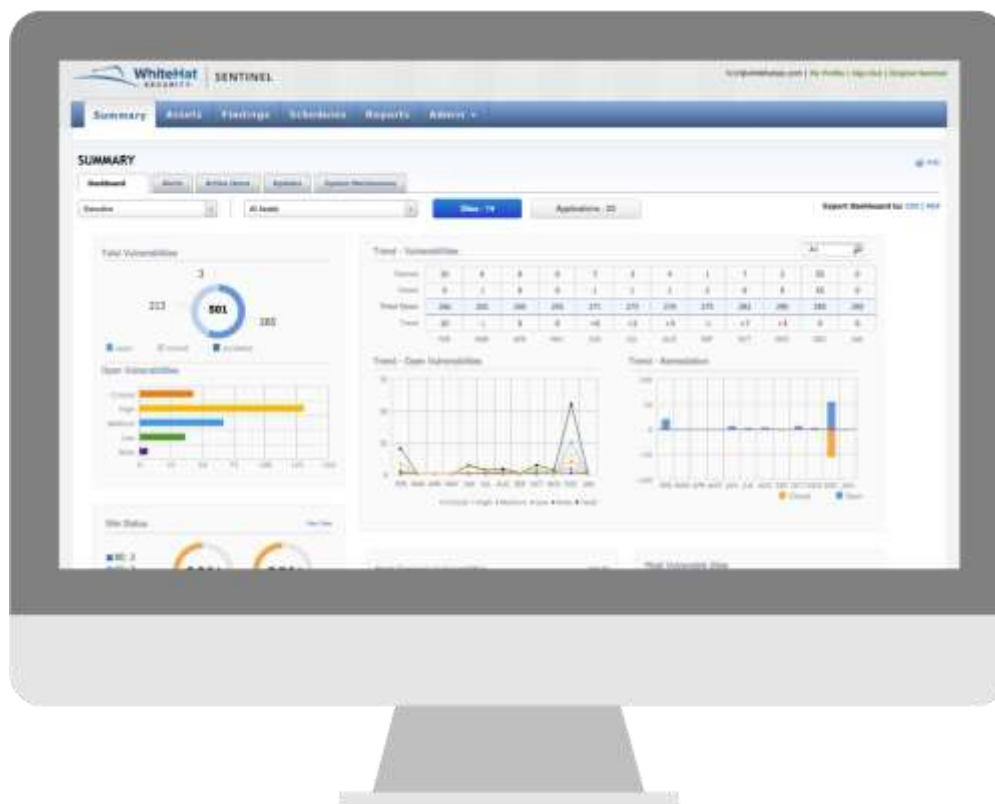
#### Incident & Breach Response

- Incident & Breach Response: Intake & Lifecycle Management
- DatabreachPedia Guidance: Built-in guidance from 300 laws



GET STARTED TODAY | [ONETRUST.COM/FREE-EDITION](https://onetrust.com/free-edition)

LEARN MORE ABOUT ONETRUST | [REQUEST A DEMO | ONETRUST.COM](https://onetrust.com)



***Your website could be vulnerable to outside attacks.*** Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With this trial you will get:

An evaluation of the security of one of your organization's websites

Application security guidance from security engineers in WhiteHat's Threat Research Center

Full access to Sentinel's web-based interface, offering the ability to review and generate reports as well as share findings with internal developers and security management

A customized review and complimentary final executive and technical report

[Click here](https://www.whitehatsec.com/info/security-check/) to sign up at this URL: <https://www.whitehatsec.com/info/security-check/>

***PLEASE NOTE: Trial participation is subject to qualification.***

# Detect and prevent breaches at wire speed

Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.



## Proven capability

Trend Micro TippingPoint:

"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:

"Recommended" Breach Detection System 4 years in a row and 100% detection rate

## Industry leading threat intelligence



Please get in touch:

Bharat Mistry, Principal Security Strategist  
Bharat\_mistry@trendmicro.co.uk

[www.trendmicro.co.uk/xgen-cyber](http://www.trendmicro.co.uk/xgen-cyber)

©2018 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro i-ball logo are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.



# Now More Than Ever, You Need To Be Connecting With



Customers



Influencers



Media

**At Vrge Strategies,** we've been making connections that businesses build around for more than a decade.

Cybersecurity companies (from VC-funded startups to the Fortune 500) and global nonprofits count on us every day to deliver results that lead, influence, as well as spark conversations and new business.

Isn't it time you maximized the value of your **strategic communications?**

**Come talk to us,  
we'd love to connect.**

Email Adam Benson  
adam@vrge.us  
or visit us at  
[www.vrge.us/cybersecurity](http://www.vrge.us/cybersecurity)

**vrge**

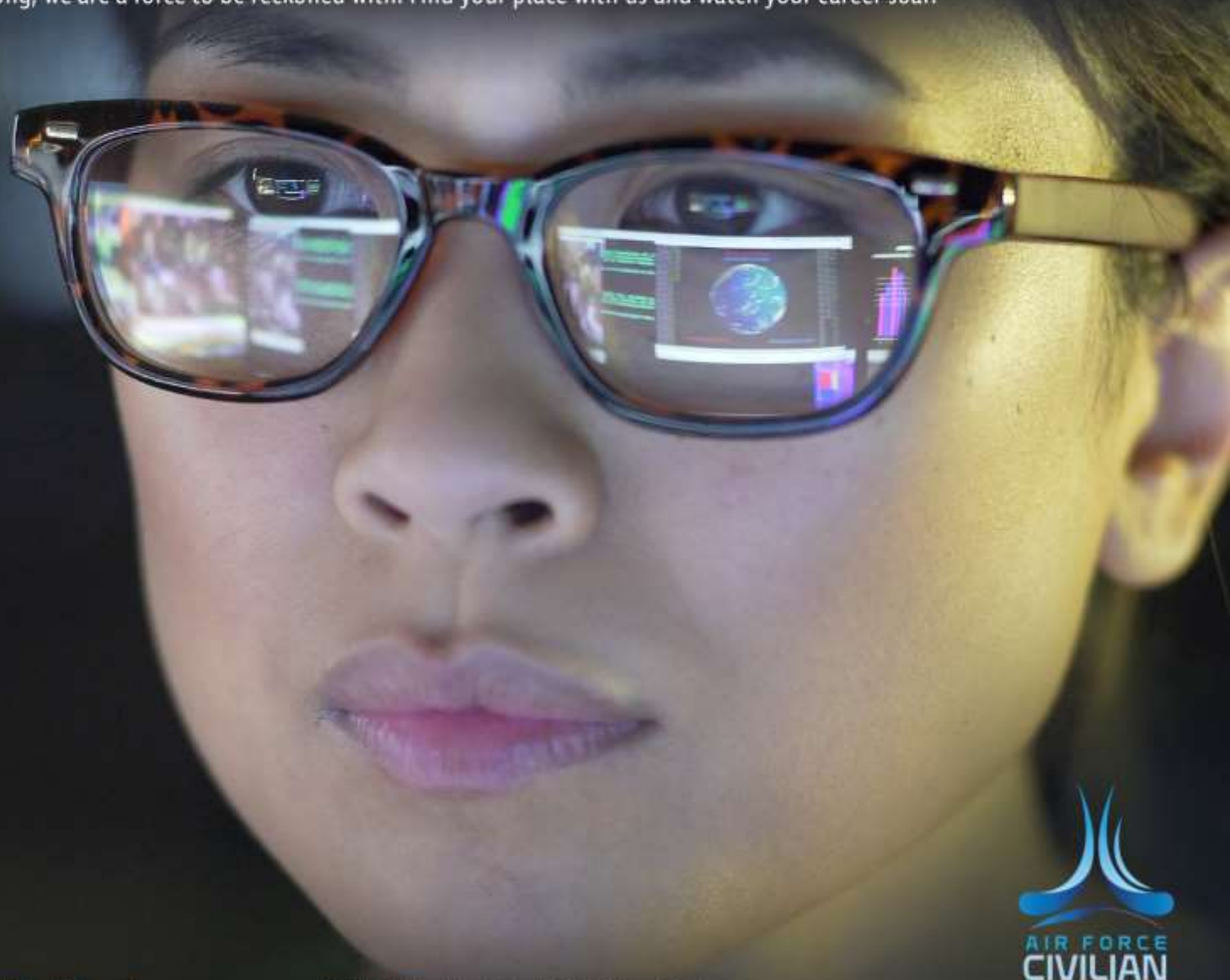
Navigate the Politics  
of Disruption

# WORK ON THE FRONT LINES PROTECTING AMERICAN INTERESTS

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working to safeguard Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll find a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.



**AFCivilianCareers.com/CYBER | #ItsACivilianThing**

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.



# Database Cyber Security Guard

**Don't be the next data breach. Equifax paid \$575 million, British Airways \$230 million and Marriott \$124 million in fines.**

**Prevents confidential data theft by Hackers, Rogue Insiders, Phishing Emails, 3rd Party Cyber Risks, Dev Ops Exploits and SQL Injection Attacks.**

## Product Features

- **Detects Informix, MariaDB, MySQL, Oracle, SQL Server and Sybase data theft within milliseconds and shuts down Hackers immediately.**
- **Advanced SQL Behavioral Analysis of the database query activity learns the normal query patterns and detects database data theft.**
- **View all suspicious database activity and attempted data theft.**
- **Supports key GDPR compliance requirements. Non-intrusive detection of data theft. Runs on a network tap or proxy server.**

**Get a FREE COPY now.**

[www.DontBeBreached.com/Free](http://www.DontBeBreached.com/Free)



**"NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"

-David DeWalt

Managing Director and Founder NightDragon Security

### **ADVISE**

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

### **INVEST**

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

### **ACCELERATE**

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

[www.nightdragon.com](http://www.nightdragon.com)

# Two Years Later

## NotPetya's Game-Changing Lessons for Cybersecurity and Collective Defense

In early Summer 2017, the highly destructive NotPetya malware appeared and spread with devastating efficiency across data systems and architectures worldwide. The attack not only shattered records for speed and destruction, but also served as a wake up call for security professionals to up their game on cyberdefense. Here are key lessons learned from NotPetya, and how those lessons continue to shape today's leading practices in cybersecurity.

### LESSON 1

Malware is increasingly designed to disrupt business operations in the physical world.

NOTPETYA CREATED AN UNPRECEDENTED

**\$10 billion**  
IN DAMAGE WORLDWIDE<sup>1</sup>



**How NotPetya changed the game** — Unlike ransomware and other profit-driven attacks, NotPetya was built simply to destroy.



**How the cybersecurity industry is adapting** — NotPetya has taught today's security teams to assume destruction is a potential goal, appreciate the elevated risk and then act accordingly.

### LESSON 2

NotPetya raised the speed limit for modern cyber attacks.

NOTPETYA SPREAD TO MORE THAN

**64 countries**  
IN JUST THE FIRST  
**24 hours<sup>2</sup>**



**How NotPetya changed the game** — NotPetya was built for speed, with code designed to proliferate automatically, rapidly and indiscriminately.



**How the cybersecurity industry is adapting** — Cyberdefenses today should ideally use near-real time network traffic analysis and behavioral analytics to rapidly catch new forms of attacks that perpetually outdated signature-based systems would miss.

### LESSON 3

The worst attacks take lateral movement to the extreme — across all organizational and industry barriers.

THE FAR-FLUNG INDUSTRIES AFFECTED BY NOTPETYA INCLUDE shipping, pharmaceuticals, banking, advertising, energy AND OTHER MAJOR SECTORS<sup>1</sup>



**How NotPetya changed the game** — NotPetya's spread was not only fast, but also far and wide — with cross-sector damage at major organizations like Maersk, FedEx and others. NotPetya was also patch-resistant, vacuuming up credentials on infected targets for use later as workarounds on protected servers.



**How the cybersecurity industry is adapting** — Companies must assume the when, not if, mindset to penetration and lateral movement, and embrace collective defense and threat information sharing — across entire industries and even between many different sectors.

### LESSON 4

NotPetya shows the limits of attribution.

CYBERATTACK ATTRIBUTION IS GETTING MORE COMPLEX, WITH AT LEAST 10 variations OF NATION-STATE RESPONSIBILITY<sup>2</sup>



**How NotPetya changed the game** — While Russia is generally blamed for NotPetya,<sup>3</sup> the attribution is less critical, given the indiscriminate nature of the attack and increased "collective offense" between criminal groups and nation-states sharing tactics and targets.<sup>4</sup>



**How the cybersecurity industry is adapting** — Security teams must meet threat actor's collective offense approach with collective defense — working with peers to share threat information and identified attack techniques.

<sup>1</sup> <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

<sup>2</sup> <https://www.securityweek.com/petyanotpetya-what-we-know-first-24-hours>

<sup>3</sup> <https://www.securityweek.com/notpetya-attack-costs-big-companies-millions>

<sup>4</sup> <https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/>

<sup>5</sup> <https://hackerone.com/white-paper-aurety-download/>

<sup>6</sup> [https://www.atlanticcouncil.org/images/files/publication\\_pdfs/803/022212\\_ACUS\\_NaIResponsibilityCyber.PDF](https://www.atlanticcouncil.org/images/files/publication_pdfs/803/022212_ACUS_NaIResponsibilityCyber.PDF)

A hand holding a black pen is positioned over a spiral-bound notebook on a wooden desk. To the left of the notebook is a white computer keyboard. The background is a blurred office setting with a bookshelf. A blue, glowing digital network overlay with interconnected lines and nodes is superimposed on the right side of the image. The word "ARTICLES" is written in large, bold, black capital letters across the center of the image.

# ARTICLES



## Election Integrity Is A Moving Target, But It's Essential to Pursue

*Measures to improve voting security need to start long before election day itself*

**By Craig Hinkley, Chief Executive Officer, WhiteHat Security, a wholly-owned, independent subsidiary of NTT Ltd.**

U.S. election security shouldn't be a controversial issue. But it is. Although there are legitimate quarrels over partisan election districting and attempts at voter suppression, the integrity of the balloting process itself, with only minor exceptions, has been upheld in election after election at virtually every level of government.

Two developments have thrown that record of integrity off the track. One direction comes from the White House's accusations that an election that relies heavily on paper mail-in ballots is corrupt. The other course involves the growing use of electronic technologies such as voter registration files, voting machines, ballot counters, and election reporting systems – all of which, at least in theory, are potentially vulnerable to hacking.

Ransomware extortion, denial of service attacks and personal data abuse from voter registration records are all possibilities, so voters are understandably concerned.

Members of Congress – all of whom are elected through that same process – have their concerns. As a result, during 2018 and 2019, the federal government allocated \$805M to states to upgrade election security. Almost all of it – 90 percent – went to new voting machines and other cybersecurity projects for the elections<sup>1</sup>. Predictably, though, many observers felt that there still wasn't enough money to safeguard registration databases, tabulate votes, conduct post-election audits, and secure better voting machines – all of which are key to election integrity.

## Brain hacking

Of course, there is merit to some of these complaints; the processes and technologies involved in voting must be adequately funded and made as tamper-resistant as possible. Yet it is also essential to keep in mind that hacking the balloting system is only one path to corrupting an election.

Another, which has also received considerable attention, comes from hacking the voters themselves – presenting them with misinformation, propaganda, half-truths, and outright lies that taint their thought processes and influence their voting behavior.

As recently as September 1, *The New York Times* reported that the FBI had given Facebook a warning: the Russian group which interfered in the 2016 presidential election was at it again, this time using a network of fake accounts and a website set up to look like a left-wing news site. Yet that Russian group is only one of many organizations, each with its own agenda, using deception to influence the election<sup>2</sup>

At the end of the day, once all the campaigning and crusading and propagandizing has concluded, the electoral system's final test comes down to the balloting process itself. Did the winning candidates receive the votes they claimed? Were individual voters systematically disenfranchised?

## Nuts and bolts

The voting procedures and equipment that Americans use are so decentralized that no single solution will work everywhere to satisfy the system's many critics. There are 50 states, more than 3,000 counties, and 8,800 election districts in the United States. Most of them bring their own unique histories involving polling place procedures, staffing, and balloting equipment to the voting process.

---

<sup>1</sup> [https://www.darkreading.com/risk/electoin-security-2020-how-we-should-allocate-\\$425m-in-funding-/a/d-id/1336885](https://www.darkreading.com/risk/electoin-security-2020-how-we-should-allocate-$425m-in-funding-/a/d-id/1336885)

<sup>2</sup> <https://www.straitstimes.com/world/united-states/pro-russia-actors-pushing-more-fake-news-as-us-election-nears>

Such staggering levels of fragmentation are scary and almost certainly contain an assortment of security risks. Yet a 2018 bill introduced in the U.S. Senate to strengthen the voting process, called the Protecting American Votes and Elections Act failed to receive bipartisan support<sup>3</sup>.

In 2017, the Department of Homeland Security (DHS) designated the nation's election infrastructure as a critical subsector. It was reported to be working with the federal Election Assistance Commission, offering technical services including cybersecurity hygiene scans, vulnerability assessments and incident response assistance upon request. But the DHS's resources are simply not enough to support a robust national effort.

A valuable approach to the issue includes clarifying the responsibilities of all those involved, reconciling any conflicting perspectives, establishing clear cybersecurity policies; providing education to voters, candidates and election officials, implementing technology that provides visibility into the system and putting an incident response plan in place.

Also, hire a regional security consultant to oversee the process. Have them create a customized election security model, patterned after those used in other critical infrastructures.

Implementing application testing protocols such as SAST, DAST, and SCA to ensure the voting machine software works right might make sense. And remaining vigilant about the risks of using third-party companies for development or security is always a good idea.

An all-in effort to upgrade our security needs to happen since no single voting district can do it all by themselves. Establishing a rock-solid plan now is critical to the future of our elections. Trusted partnerships and industry cooperation will drive us forward in the digital world safely. Protecting the credibility of America's election systems is essential.

---

<sup>3</sup> <https://www.darkreading.com/vulnerabilities---threats/8-steps-toward-safer-elections/d/d-id/1332400>

## About the Author



### **Craig Hinkley - Chief Executive Officer**

Craig Hinkley joined WhiteHat Security as CEO in early 2015, bringing more than 20 years of executive leadership in the technology sector to this role. Craig is driving a customer-centric focus throughout the company and has broadened WhiteHat's global brand and visibility beyond the application security space and security buyer, to the world of the development organization and a DevSecOps approach to application development.

Prior to joining WhiteHat Security, Craig served as vice president and general manager of the LogLogic business unit for TIBCO Software. In that role, he was responsible for global field sales and operations, client technical services, engineering, research and development, product design, and product management. Before TIBCO, he served as the general manager at Hewlett-Packard for the HP Networking Business in the Americas. Earlier in his career, Craig held positions at Cisco Systems Inc. and Bank of America. He earned a bachelor's degree in Information Technology from the Swinburne University of Technology in Australia.

Craig can be reached on Twitter at @CraigHinkley and at our company website <https://www.whitehatsec.com/>.



## Acronis Cyber Readiness Report

*Pandemic reveals cybersecurity gaps, need for new solutions*

By Peter Hale, Sr. Content Manager, Acronis

As businesses around the world reacted to the COVID-19 pandemic, many had to address new risks to their infrastructure, endpoints, and mission-critical data. The shift to remote work alone introduced a range of new challenges – from closing security gaps with new technology to educating now-remote employees to avoid phishing attacks to strengthening the protection of third-party apps needed to work from home.

The newly released [Acronis Cyber Readiness Report](#) takes a close look at how prepared organizations were to adapt to the pandemic's impact on their IT operations and cybersecurity posture. In preparing the report, Acronis surveyed 3,400 companies and remote workers from around the world during June and July 2020.

In the end, the findings showed that organizations continue to struggle to protect their data and infrastructure against the new challenges of the remote work landscape.

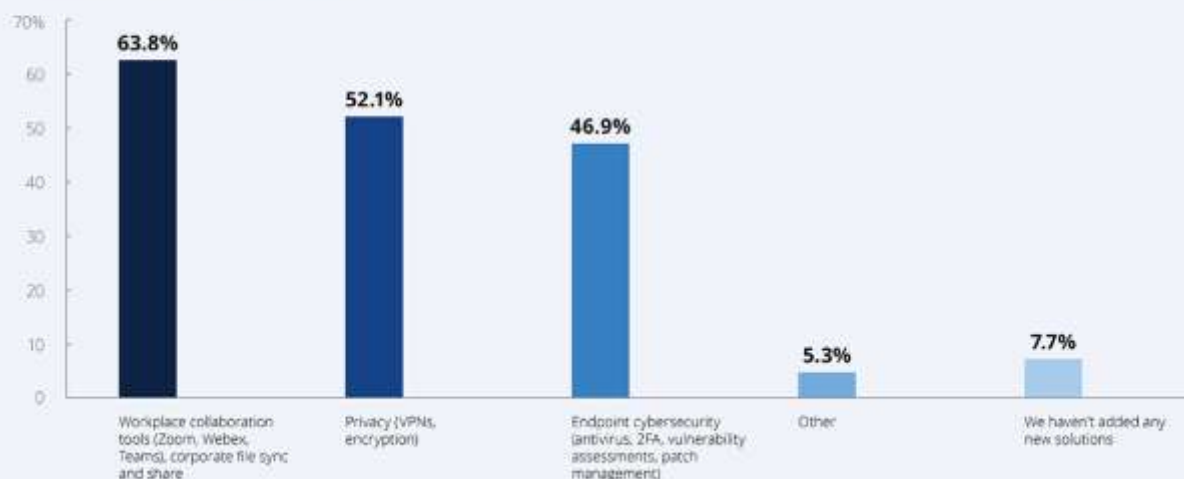
The report also underscored how new solutions are required – with 92% of surveyed companies reporting they had to adopt new technologies to enable remote work, including workplace collaboration tools, privacy solutions, and endpoint cybersecurity.

That revelation that modern cyber protection solutions are needed comes on the same day that [Acronis Cyber Protect 15](#), which addresses the concerns revealed in the report and which has been [available in beta since June](#), is released for general availability.

## 92% of global organizations have had to adopt new technologies in order to switch to remote work

Q2. Did you adopt any new technologies to help enable/manage/secure employees working from home?

Acronis  
Cyber Readiness  
Report 2020



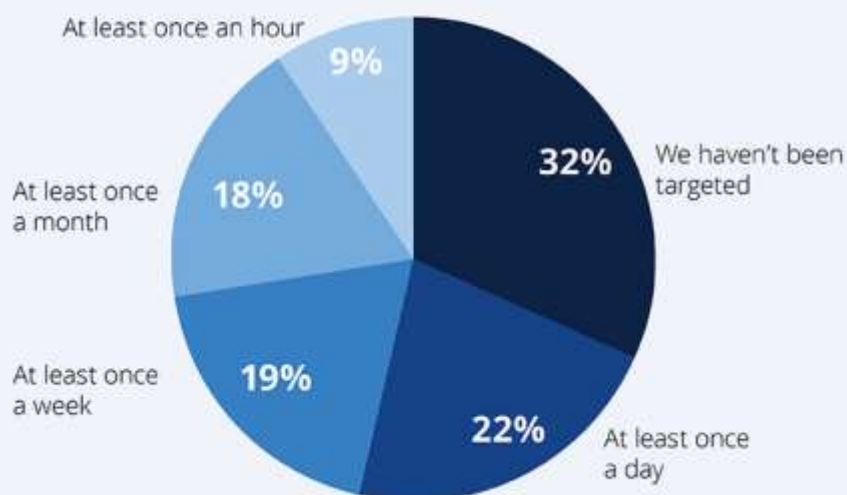
The Acronis Cyber Readiness Report reveals that as hackers target remote workers, phishing, distributed denial of service (DDoS), and videoconferencing attacks are the most common tactics used.

### 31% of companies reporting daily cyberattacks

Malware attacks such as ransomware also have increased during the pandemic, with half (50%) of all surveyed companies reporting they are targeted at least once a week. This includes small companies as well as large, such as the leading GPS manufacturer that allegedly paid \$10 million in a WastedLocker ransomware attack.

## 31% of global companies are attacked at least once a day. India reported nearly twice as many attacks as any other country

Q4. How often has your company been targeted by a cyberattack in the past three months?



What's stunning is how many cyberattacks have been getting past outdated solutions. Our global network of Acronis Cyber Protection Operating Centers (CPOCs) found that 35% of customer endpoints were exposed to malware attacks that were still getting through before the deployment of Acronis Cyber Protect.

The good news for organizations is that testing by independent cybersecurity labs such as [AV-Test](#) and [Virus Bulletin](#) shows that Acronis Cyber Protect's antimalware detects 100% of malware attacks with zero false positives. If the GPS manufacturer had Acronis Cyber Protect, it would never have paid a \$10 million ransom.

In fact, based on the current cyberattack rate, the unique integration of backup and cybersecurity enables Acronis Cyber Protect to prevent an estimated \$150 million in direct losses for its customers each year.

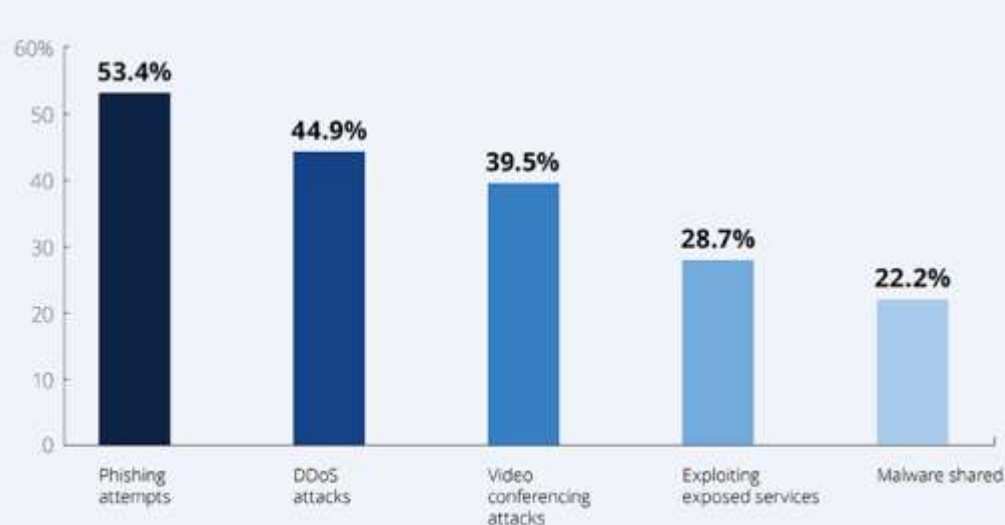
### 39% of companies experienced videoconferencing attacks

As a result of the pandemic lockdown, 69% remote workers necessarily rely on apps like Zoom, Cisco Webex, and Microsoft Teams to collaborate with colleagues, communicate with partners and vendors, or to meet with customers and prospects. Cybercriminals have been taking advantage of that reliance: 39% of companies experienced videoconferencing attacks in the past three months

In fact, Cisco recently revealed a vulnerability in its Webex app that could allow attackers to open, read, and steal potentially valuable or damaging content.

## 39% of companies have encountered videoconferencing attacks. India, Switzerland, Canada, and the UK most affected

Q5. What types of cyberattacks has your organization encountered in the past three months?



Closing the vulnerabilities and potential exploits in these necessary third-party apps is critical. Thankfully, Acronis Cyber Protect 15 strengthens the cybersecurity of these apps. In fact, Acronis Cyber Protect prevented code execution exploits in Webex before it was patched by Cisco.

### 2% of companies consider URL filtering

[Phishing attacks](#) are occurring at historic levels, which is not surprising since the report found that only 2% of companies consider URL filtering when evaluating a cybersecurity solution.

That oversight leaves remote workers vulnerable to phishing sites – Acronis CPOCs discovered that approximately 10% of users clicked on malicious websites in May, June, and July.

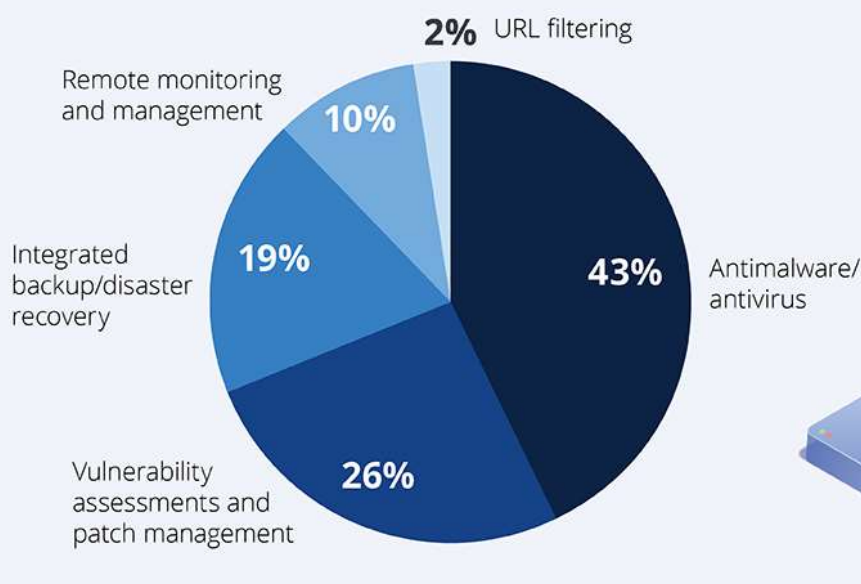
### Modern requirements for cyber protection

These Acronis findings and external research illustrate why organizations need a cyber protection solution that reduces complexity and improves security to support remote work environments, and the solution must be cost-effective to address the scale of remote workers.

“The cyberthreat landscape has changed dramatically during the past few years, and in the last six months in particular. Traditional stand-alone antivirus and backup solutions are unable to protect against modern cyberthreats,” said Serguei “SB” Belousov, founder and CEO of Acronis. “Organizations that modernize their stack with integrated data protection and cybersecurity not only gain greater security, they lower their costs and improve efficiencies. The automation and streamlined management of Acronis

## Only 2% of companies prioritizing a URL filtering feature – no wonder phishing attacks are at a peak

Q6. Which features do you prioritize most when choosing/operating a corporate cyber protection solution?



Cyber Protect 15 means any business can decrease their risk, avoid downtime, and increase their IT team's productivity."

With Acronis Cyber Protect 15's unique integration of data protection and next-generation cybersecurity capabilities – including AI-based behavioral detection that stops zero-day attacks, URL filtering, vulnerability assessments, videoconference protection, and automated patch management – organizations protect against modern cyberthreats while ensuring they can recover their data and systems faster than any other solution.

The integration and automation of Acronis Cyber Protect 15 provide unique performance benefits as well. By leveraging backup data, the AI-based threat detection engine improves its detection rates and avoids false-positives. This enables Acronis' next-gen antimalware technology to deliver a 100% detection rate with zero false positives in testing by independent cybersecurity labs such as [AV-Test](#) and [Virus Bulletin](#), and earned the solution [Frost & Sullivan's 2020 New Product Innovation Award](#) for Data Protection in North America.

### Benefits of cyber protection

The single solution approach of Acronis Cyber Protect removes the complexity and risks associated with non-integrated solutions. There is one agent, which improves systems performance, eliminates conflicts, and increases stability; one management interface, which streamlines administration and reporting tasks; and one license to manage.

The ability to unify multiple protection technologies into one solution also decreases the time an IT team needs to learn, deploy, and maintain the solution. With Acronis Cyber Protect, everything is managed via a single pane of glass, which enables the organization to streamline management, cut unnecessary administrative time, and lower the total cost of ownership (TCO).

### Final thought

The Acronis Cyber Readiness Report includes tremendous insights from both the IT managers trying to secure their organizations and the remote workers who are on the frontlines of these challenges. To read all of the findings, [download the Acronis Cyber Readiness Report](#).

With 88% of the remote workers surveyed by Acronis expecting to work from home to some extent even after the pandemic ends, ensuring their protection and cybersecurity will require the kind of integration and automation only found in Acronis Cyber Protect 15.

Organizations that are looking to eliminate the complexity while increasing their cybersecurity posture can learn more about Acronis Cyber Protect 15 [here](#). They can also test drive the solution for 30 days as well.

### About the Author



My name is Peter Hale and I am the Senior Content Manager at Acronis and I am responsible for supervising and coaching members of our Content Marketing team focused on inbound and outbound development of Acronis's messaging.

Peter can be reached online at [linkedin.com/in/peterhale2](https://www.linkedin.com/in/peterhale2) and at our company website [acronis.com](https://www.acronis.com).



## Centrify Study Lifts the Hood on Cybersecurity Policy and Threat Challenges During COVID-19

Recent study shows increased breaches in cybersecurity led nearly 40% of UK business decision makers to dismiss staff members since the start of the pandemic

By Andy Heather, VP and managing director - EMEA, Centrify

A recent study of U.K.-based IT security professionals unveiled that 39% of local business decision makers have admitted to dismissing staff members due to a breach of company cybersecurity policy since the start of the COVID-19 outbreak.

In addition, two-thirds (65%) of companies have made substantial changes to their cybersecurity policy in response to the pandemic and forced remote work shift. Despite this, 58% agreed that employees are more likely to try and circumvent company security practices when working from home – indicating a fundamental flaw in the execution of security measures in a remote-working model.

In addition, 46% of those surveyed have already noted an increase of phishing attacks since implementing a policy of widespread remote working.

## Work-from-home Security Trends

In an effort to combat poor security practice from employees, 57% of business decision makers revealed that they are currently implementing more measures to securely authenticate employees. Such measures include biometric data checks, such as fingerprint and facial recognition technology, and other multi-factor authentication steps when gaining access to certain applications, files and accounts.

In addition, more than two-thirds (70%) of British businesses are using multi-factor authentication (MFA) and a virtual private network (VPN) to manage the security risks posed by the increase of remote work.

Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more known identity confirmations (such as a password and a code texted to their known phone number, a hardware key and biometric confirmation like a fingerprint scan, etc.). A VPN, on the other hand, extends a private network across a public network, allowing internet users to protect their location and stay anonymous.

Finally, more than half (55%) of businesses already have, or plan to formally ban staff from using personal devices to work from home.

## Many Businesses Skeptical About Increased Security Protocols

Despite the cybersecurity policy issues and threat increases, 43% of individuals believe upping cybersecurity protocols for remote workers will have a negative impact on workplace productivity. Similarly, almost half of the individuals (49%) preferred to remove extra authentication steps for basic apps and data in the workplace, as they felt it adds unnecessary time to procedures.

## A Potential Compromise

As a potential alternative or middle ground, 60% of U.K. businesses claim to support biometric data – such as fingerprint or facial recognition identification factors supported by the FIDO2 specification for passwordless authentication – as a suitable replacement to more time-intensive multi-factor authentication to increase productivity. Furthermore, two-thirds (66%) agree that they would feel more secure using fingerprint or facial recognition ID as opposed to a traditional password.

## What Does the Data Tell Us?

It's clear that businesses recognize the risks posed by increased remote working during this difficult time, with the majority opting for multi-factor authentication solutions to verify every user and protect company data. What's troubling is the other 30% who are not using MFA, which is a security best practice.

Every organization wants to ensure productivity for remote workers, but it cannot come at the expense of proper security. They need to weigh the risks they are facing with these heightened threats very carefully and take any and all measures available to ensure access is granted only to authentic users.

This is especially important for privileged access by IT administrators, many of whom are outsourced third parties with broad entitlements and less restrictive controls. It's worth requiring the extra few seconds for these users to properly authenticate their identities. As the data indicates, many organizations are looking at more modern factors of authentication such as biometrics that can both increase security and productivity.

## We are the Weakest Links

With more people than ever working from home and left to their own devices, it's inevitable that some will find security workarounds, such as using personal laptops and not changing passwords, in order to maximize productivity. It's also possible that the changes in security procedures are not being communicated well to employees, and many are practicing unsafe internet usage without even realizing.

The reality is the weakest link in any organization continues to be the human element. Combatting this issue starts from the top. CIOs and business decision makers must implement strict and transparent, cloud enabled and identity-centric security solutions. This will allow companies to quickly and safely deploy scalable security privileged access management measures, which make it impossible for an employee to access company networks, applications and data, unless they are following correct procedures.

### About the Author



Andy is the VP and managing director - EMEA at Centrify. He has over 25 years of IT experience in sales, sales management, engineering, and professional services. At HP Andy was responsible for leading the EMEA sales organization for HP Data security. Previously Andy was VP Sales for EMEA at Voltage Security and has held a number of senior sales management roles at Tripwire, Affiniti, Opsware, NetApp, Sun Microsystems, IBM and HP. Andy can be reached at our company website <https://www.centrify.com>.



## Are Your Corporate Networks Ready for An Impending 'Return to Work' Cyber Attack?

**As employees rejoin the network, cyber risks are heightened. Why it's important to have essential security measures in place before it's too late.**

By Stephen Burke, Cyber Risk Aware CEO & Founder

As the new normal starts to take shape and businesses gradually open their doors to the returning workforce, a fundamental question to any IT department is whether adequate security measures are in place to protect the corporate network from an influx of looming cyber security risks.

When lockdown dispersed the nation into a remote workforce earlier this year, few businesses were fully equipped to issue company devices with regularly patched antivirus security at such short notice. The IT departments did their best to equip all teams with whatever was available to enable a 'working from home' environment. With employees now set to rejoin the workplace, there is an abundance of insecure hardware about to hit the corporate network, a cyber security bomb about to go off, threatening to explode confidential data out to an eagerly awaiting cyber attack.

The average cost of a data breach in 2019 was \$184k for a medium-sized business and \$715k for a large organisation. These cyber criminals target the vulnerable areas within a business. They are aware of changing employee circumstances and know how to best theme attacks to maximise effectiveness. We have seen this through the increased phishing attacks around Covid-19 and working from home for example. Google data revealed a 350% surge in active phishing websites during the coronavirus pandemic. Phishing attacks are more sophisticated than ever, and they continually evolve and adapt.

With a re-emerging 'out of sight' remote workforce, there are huge, potentially detrimental unknowns, about to come to the fore. Devices used remotely most likely have confidential data stored on the system. It should be anticipated that other household members have used the same devices possibly having installed insecure software or visited insecure websites. There is no guarantee these computers have been maintained and patched over recent months. Do CISOs feel they can trust these devices to rejoin the corporate network?

With every employee having access to 17 million files on average, CISOs need to be prepared for the heightened security risks as employees return to the workplace. We already know that **over 90% of data breaches are caused by human error**. It is therefore imperative that businesses tackle the issue of cyber security at the root cause - the people within the organisation.

CISOs within business are best placed to ensure risk assessments are carried out before their networks are fully exposed:

- Do you know where employees have shared corporate data and under which accounts?
- Was data shared via a public cloud environment such as google drive, one drive, dropbox?

These are essential questions to determine the level of security risk to any business, to ensure GDPR compliance is maintained and corporate data is safe.

- Have company devices been shared across other household members? If so, are all passwords protected?
- Has any new software been installed or removed? Were any security warnings received from anti-virus software?
- Have any sensitive and confidential files been printed or disposed of at home?

Before devices are reconnected to the corporate network, assessments need to be undertaken, networks need to be monitored, and most essentially, the people within the business need cybersecurity awareness training and support. **It is the people who pose the greatest business risk**. They send and receive data all day every day, through a multitude of access points. If left untrained, they are the easiest target and can unwittingly expose the entire network, regardless of technological defences that may be in play. If trained and supported, employees are the greatest line of defence a company can have - a **Human Firewall**.

Cybersecurity awareness comes in many forms, but for optimum effectiveness, is it best to combine interactive cybersecurity awareness training content with a software solution that works hand in hand with your company's IT infrastructure. Cyber Risk Aware offers "real time" intervention training, which identifies where employees are making mistakes and sends focused training material to help improve their behaviours, saving both money and time. **Building a Human Firewall is the biggest defence against cybercrime.**

### About the Author



Stephen founded Cyber Risk Aware in 2016, after a career spanning over 20 years in technology and security specialising as a CISO. In that time, he found that most if not all security incidents are caused by human error at all levels in an organisation, no matter how good the technical defences were. Stephen founded Cyber Risk aware with the mission of making a genuine difference and helping companies and users at home from being victims of cybercrime. Specialities:

Security Education and Awareness Programs, Cyber Insurance, Network Security, Data Governance and Security, Malware Investigator and Incident Response, Risk Management, Security Behavior Analytics. Security Architecture, Heuristic Security, Security Audit, Digital Forensics, Penetration Testing, Encryption, Wireless security, Security management, Database as a Service, Internal Cloud Design, SAN Design, RDBMS Virtualisation and Consolidation, Disaster Recovery

<https://www.cyberriskaware.com/>

Email: [info@cyberriskaware.com](mailto:info@cyberriskaware.com)

LinkedIn: [linkedin.com/company/cyber-risk-aware](https://www.linkedin.com/company/cyber-risk-aware)

Twitter: [@cyberriskaware](https://twitter.com/cyberriskaware)



## COVID Impact on MSSPs

by Tristan Hinsley, Cybersecurity Expert, TDI Security

Given the remote nature of most Managed Security Service Providers' (MSSPs) business operations, most would imagine they would be well positioned to deal with a near-nationwide work-from-home workplace transition, and for the most part that's true. However, while some say that their transition for [their own employees to remote work](#) was quick and effective, MSSPs have also had to shift their existing security services to better protect their customers' more geographically distributed workforce. This comes with its own challenges depending on the scale of the changes needed to accommodate remote work, but for MSSPs who have large clients with demanding IT security needs it could be a monumental task.

### The Impact of Remote Work on MSSPs

Due to the nature of the business operations of most MSSPs, remote work comes naturally as most of their services are provided remotely even in pre-pandemic times. This places MSSPs in a particularly advantageous position compared to other segments of the market during challenging times, because it allows for faster response to rapid shifts in the industry. But this doesn't mean that MSSPs are completely immune to the shift; because they are responsible for securing their client's infrastructure, many MSSPs are struggling with establishing secure remote work protocols for their clients in a timely manner. This aspect is particularly troublesome when you consider that an [IBM survey](#) of over two thousand respondents found that 52% of remote employees are using personal laptops to conduct work activities. Securing non-organizationally owned endpoints is particularly difficult, and insecure personal devices operating on an insecure personal network handling organizational data is never a good place to be for a security team.

## Market Uncertainty for MSSPs

The other looming issue for MSSPs is the economic impact of the pandemic. While the full economic damage from the nationwide lockdown is still relatively unknown, many organizations are being cautious with their short-term projections. With so much market uncertainty, many organizations are hoping for the best but planning for the worst. Gartner has predicted that [global IT spending will decline by around 8%](#) overall in 2020, and that security spending specifically will drop from the initially projected 8.7% increase in spending down to a [2.4% increase](#). Other industry voices such as CxO Advisor for Cyber Strategy [John Hellickson](#) opines that, “We’re a bit early to see an industrywide trend on cybersecurity budgets due to COVID-19, but at this time, many security teams have had their allocated budgets put on hold or reduced altogether, as businesses adjust to revenue shortfalls.” If businesses are limiting spending in anticipation of reduced revenue, MSSPs may find reduced demand for their products moving forward. Small and medium size businesses may be most impacted by the economic fallout, as organizations cut back on cybersecurity spending while large cybersecurity firms already have existing contracts and brand recognition.

## Conclusion

While security consulting firms are largely placed in a better position to weather the storm than other industries, many will still feel the impact in one way or another. Whether it be by reduced security spending and revenues, the hurdles of securing a remote workforce, or increased risk as cybercriminals ramp up efforts to compromise key remote employees; security firms and MSSPs in particular may be in for a rough ride in coming months. Market uncertainty is always a stressful time, because even in the best of times it can be hard to tell whether a given decision is the right one. To make the right decisions as an MSSP requires maximizing market knowledge, organizational visibility, and complete understanding of their clients' needs. Make sure you have the right knowledge and tools to provide the best results for your clients.

### About the Author



Tristan Hinsley is a Cybersecurity expert at TDI Security and Undergraduate Student at George Mason University studying Information Security. In his time at TDI, Tristan has gained experience in NIST 800-171 Compliance and Auditing, as well as a number of tangentially related areas.

Tristan can be reached online at: [Tristan.hinsley@tdisecurity.com](mailto:Tristan.hinsley@tdisecurity.com) and at our company website <https://www.tdisecurity.com/> & <https://cnsight.io/>



# The Power of Metadata

## The Four Insights Network Metadata Can Reveal About Your Compromise Level

*Why Network Metadata is an Underappreciated and Undervalued Threat Intelligence Resource*

By Ricardo Villadiego, CEO of Lumu

Modern security teams are not unlike the tenacious forensic investigators featured on many popular network television shows. In order to determine ‘who done it’ they must piece together small and seemingly unrelated strains of evidence.

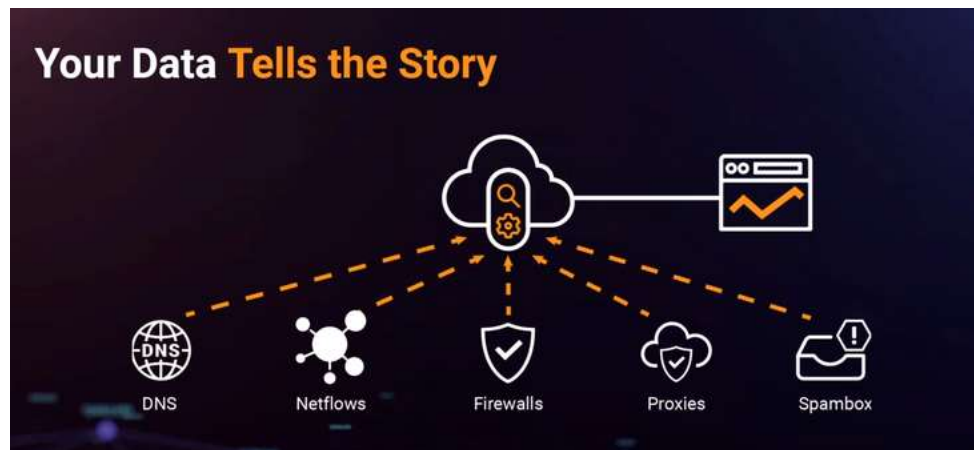
However, unlike a TV investigator, the vast majority of security teams today are often unaware that a malicious incident has even occurred -- which is why according to IBM, it takes the average enterprise almost 200 days to even recognize the fact that they’ve been breached in the first place.

Which is why security analysts are taking a closer look at network metadata which represents one of the most underutilized and overlooked sources of threat intelligence. For an attacker to successfully exfiltrate data from a network, the attacker must use the network itself to move the data. No matter how stealthy an attacker might be, traces of network metadata will invariably be left behind.

The sheer volume of metadata generated by the network is staggering and comes in a variety of forms, from DNS queries and firewall or proxy access logs to even lowly spam messages – the metadata attached to each one of these sources represents a pixel of threat intelligence. Just as an isolated pixel in a digital image by itself won’t tell you very much, once you collect, correlate and organize all these

pixels, a picture will begin to come into focus – one that can help answer the most important question for today's cybersecurity practitioner: have we been compromised?

What follows are four distinct insights that network metadata that can help you definitively answer this question.



## Four Insights Generated by Network Metadata

### Insight 1: DNS Metadata Can Verify an Adversary is Communicating with Your Infrastructure

The Domain Naming System (DNS) is the phonebook of the Internet, providing a distributed and hierarchical naming system for the devices, services and resources -- without it, there is no Internet. More than 90% of our daily usage of the internet involves DNS queries, hence it's a gold mine to assess whether or not a device is interacting with adversarial infrastructure.

Once a device is successfully compromised, the first thing it will typically do is attempt to resolve a domain that belongs to the adversary and if successful, the conclusion is self-evident: your organization has been compromised.

Analysis of DNS metadata can also be used to detect other telltale compromise indicators such as domain spoofing and unresolved IP addresses. One aspect where analyzing DNS metadata can be particularly useful is in identifying Domain Generating Algorithms (DGAs) which threat actors regularly employ to dynamically generate and activate random domains from which they can orchestrate and obscure their attacks.

Blocking malicious DNS requests is a logical first step, however the ultimate goal should be to eliminate the residual compromise from the device that triggered the initial blocked DNS request. Otherwise, a compromised device will continuously trigger malicious DNS requests generated by the DGA until it succeeds in connecting to its Command & Control master console.

## **Insight 2:** Proxy and Firewall Log Metadata Can Be Used to Visualize Compromise Connection Points

If an attacker does not use domain infrastructure to communicate with compromised infrastructure, their only other option is to use an IP address. In this case instance, the traces of adversarial contact will lie in the access logs of firewalls or proxies, which when analyzed and correlated with other network metadata components, can help connect the dots between a constellation of compromised devices.

For instance, many of the most persistent strains of malware will automatically scan a network looking for accessible hosts from which to escalate their privileges and in response, the firewall will either block or drop the connection. When the firewall drops a lot of different connections from a single source host that's usually a pretty good indication that an intruder is already inside and scanning the network to identify lateral openings.

In most instances, the adversary will opt to use DNS because it provides the attacker with greater flexibility and can persist undetected for a longer period of time. However, if an attacker is deprived of this option they will instead default to an IP-based communication method, making it all the more important to incorporate this source of metadata.

## **Insight 3:** Analyzing Netflow Metadata Can Illuminate How an Attacker is Moving Across the Network

Once an attacker has gained a foothold in the network, they must then use the network itself to move laterally in order to achieve the goal: the exfiltration or encryption of host data. During this crucial phase of an attack, specific and distinct types of network traffic are being generated, leaving the attacker vulnerable to discovery.

However, because the network is a noisy place, identifying and isolating these markers can be especially tricky. Analyzing netflow metadata can provide important clues as to how they are traversing the network, providing network defenders with valuable insight into how and at which point an attacker is attempting to escalate privileges or propagate their payload.

## **Insight 4:** There's More than Spam in Your Spambox

Your email spambox is more than just a receptacle of junk emails and phishing lures. By identifying the machines that are contacting the spam infrastructure based on the metadata from the spambox itself can tell us a great deal about other malicious activities that might be related to the same organization -- especially if a phishing link was the initial point of incursion.

Correlating metadata from the spambox with other network metadata elements can also help identify compromised endpoints which can be mapped back to individual users, providing incident responders and forensic teams with a vehicle to trace the route of a compromise, update its heuristics to improve detection of future threats, and ultimately limit its impact.

Stopping spam is a good first step, however, analyzing it is better as it can tell you who and how your organization is being attacked.

The age old maxim, 'the whole is greater than the sum of its parts' has become a popular refrain for technology leaders looking to cultivate a holistic ethos. However, when it comes to seeing the big picture of your network, you must be able to see all of those individual parts to understand the whole picture. The real power of network metadata becomes fully realized when you are able to fully assess and integrate all of these discrete parts – only then will you be able to transform them into something that's both actionable and meaningful.

### About the Author



Ricardo Villadiego is the founder and CEO of Lumu. A seasoned entrepreneur and visionary technology leader focused on cybersecurity, Ricardo has spent the last 20 years working to solve some of the most prevalent cybersecurity challenges organizations face. Prior to Lumu, Ricardo founded Easy Solutions, a global organization focused on the prevention and detection of electronic fraud which was part of an \$2.8 billion acquisition by Cyxtera Technologies, where Ricardo led their cybersecurity business unit. Ricardo has also held various leadership positions at IBM, Internet Security Systems and Unisys Corporation. He is an Electrical Engineer, avid reader, relentlessly curious, technology enthusiast, who currently lives in South Florida with his family.

Ricardo can be reached online at [rvilladiego@lumu.io](mailto:rvilladiego@lumu.io) or you can follow him on Twitter at <https://twitter.com/rvilladiego> and at our company website: <http://www.lumu.io>



## Business Email Compromise - Why Is It Dangerous and How to Avoid It

By Elena Georgescu, Communication & PR Officer at Heimdal™ Security

When talking about business email compromise, we cannot omit to mention two aspects: technology and money. Technology is the engine that moves humanity forward, allowing us to conquer new horizons and money, whether we like to admit it or not, is the fuel that makes this technologic progress possible. In cybersecurity though, there are people that care more about money than evolution, using technology to their own benefit. Such is the case for business email compromise attacks, one of the most financially damaging online crimes.

Business email compromise/email account compromise/man-in-the-email is a type of cyber attack in which a criminal hacks into an email account and impersonates the real owner in order to gain financial

benefits from the company, its customers, partners and/or employees by tricking them into sending money or sensitive data.

## How do hackers get access to your e-mail?

### By spoofing an email account or website

One of the main B.E.C. tactics is to use slight variations on legitimate addresses to fool victims into thinking fake accounts are authentic - like dan.kelley@examplecompany.com versus dan.kelly@examplecompany.com.

### By sending spearphishing emails

Spearphishing emails look like they're from a trustworthy person, but they only trick victims into revealing sensitive information, allowing criminals access to company accounts, calendars and valuable data.

### By using malware

When orchestrating a BEC attack, hackers might also use malicious software to infiltrate into company networks, get access to email threads and then sending messages that would not raise any questions.

### By using social engineering

It's not uncommon for cybercriminals to use employees existing social habits against them. They might call or send an email stressing the urgency of the matter, usually at the end of the business day or week. This is not always the case, though, since they might also try to blend in, establish a conversation, build a friendly relationship and then ask for sensitive information at a later date.



## **B.E.C. history and attacks**

Business Email Compromise attacks have been on the FBI's radar since 2013. The scammers are believed to be members of African, Eastern European and Middle East organised crime groups. High-level executives and people working in the finance department from companies of all sizes are the most likely targets of cybercriminals.

The Austrian aerospace firm FACC AG, the Dublin Zoo and Save the Children USA are only three of the business email compromise attack's victims.

Back in 2016, FACC AG, a major designer and manufacturer of aircraft components and systems, with a client base that includes Boeing, Airbus, Rolls-Royce, Siemens SAS and Mitsubishi Heavy Industries, lost €50 million in a business email compromise incident which also got their CEO fired. The criminal activities were executed from the outside of the company. The Austrian Criminal Investigation Department was immediately announced and investigated the attack.

Save the Children USA fell victim to a B.E.C. attack in 2017, when hackers got access to an employee's email account and used it to make a profit of \$1m by pretending the money was needed to pay for health centre solar panels in Pakistan. Unfortunately, attacks on charities are not rare and this incident with Save the Children USA is not singular.

That same year, the Dublin Zoo lost nearly €600.000 due to a business email compromise attack. The incident was immediately reported to the Garda National Economic Crime Bureau and Ireland's national police service.

## **What can you do to prevent a business email compromise attack?**

When it comes to preventing B.E.C. methods, there are both online and offline tactics that can be used.

### **1. Protect your systems**

It's highly important to use a good firewall and a good antivirus that can regularly scan your devices in order to prevent malware infections. It's equally important to keep your systems updated - pay attention to security alerts and deploy security patches. Don't forget to enable spam filters and block all access to suspicious websites and make sure you have a good password management policy for all your email accounts. Last but not least, take care of your passwords - they should include numbers, symbols, capital and lower-case letters.

## 2. Make vigilance your second nature

This vigilance should come in several forms, especially when it comes to “urgent” payment requests:

- look very carefully at the email address of the sender - usually compromised email addresses have only one different letter in comparison to the original ones.
- if you receive an email including a change of payment method or bank account, do not reply directly to that email - always contact the payment recipient through another means of communication to verify the authenticity of the claim.
- get used to also verify the authenticity of the websites that may appear in the received emails - always hover your mouse over links before clicking them and make sure that their URL includes HTTPS.
- it would also be recommended to pay attention to how you handle sensitive data at home, not only at work, since you never know who might be watching you - don't post private information on social media, use different passwords for every account and shred all confidential documents.

## 3. Know the usual B.E.C. scenarios

The main tactics that hackers use to perpetrate B.E.C. scams are: a false sense of urgency, a trick domain name and impersonation of a vendor. All of them, especially the last one, imply emails that seem very legitimate. Usually, in the case of vendor impersonation, the domain name is genuine, the transaction seems legitimate and has even proper documentation, but the payments would be directed to an account that the hackers control.

### What should you do if, despite all the precautions, you become a victim of a B.E.C. attack?

- alert your bank about the fraudulent transaction - they should immediately try to recall the funds. It is possible to get your money back within 24-48h after the attack.
- gather all the transaction's documentation and the emails or invoices you received and report the incident as soon as possible to the local police, identifying it as “Business Email Compromise” or “BEC”.
- think about consulting a lawyer in the country where the money was deposited.
- prosecute an internal review to see what happened, who was involved and what processes allowed the attack to happen.

## Conclusively...

Business email compromise attacks are so dangerous because they target not only electronic systems, but also the human factor - they rely on someone being gullible enough and tricked into sending money. Good cybersecurity education and excellent software solutions (for your endpoints, network and email) are the only ways to work your way around cybercriminals' malicious intents.

### About the Author



Elena Georgescu is a Communication and PR Officer at Heimdal™ Security, a leading European provider of cloud-based cybersecurity solutions. At Heimdal™, she combines her passion for reading and writing with her desire to make a positive impact on the world - through education. Elena can be reached online at <https://www.linkedin.com/in/elenafeliciageorgescu/> and at the Heimdal™ Security's website - <https://heimdalsecurity.com/en/>.



# Cyber-Attacks Are the New Norm and Ransomware Is on The Rise

By Ehab Halablab, Regional Sales Director – Middle East at A10 Networks

Last year ransomware made a comeback, as worldwide mobile operators made aggressive strides in the transformation to 5G, and GDPR achieved its first full year of implementation. The industry saw some of the largest fines ever given for massive data breaches experienced by enterprises. As the spike in demand for ransomware-as-a-service tools in underground forums, coupled with the anonymity offered by the dark web, the surge in these types of cyberthreats should not be a surprise.

This year ransomware will continue to garner more international attention as a host of the not new, like the continued rash of DDoS attacks on government entities and cloud and gaming services, to the new and emerging.

## Growth of ransomware

One reason for ransomware attacks gaining widespread popularity is because they now can be launched even against smaller players. Even a small amount of data can be used to hold an entire organisation, city or even country for ransom. The trend of attacks levied against global cities and governments will only continue to grow.

Below I can share three new strains of ransomware types introduced:

*Modular or multi-levelled/layered ransomware* and *malware* attacks will become the norm as this evasion technique becomes more prevalent. Modular attacks use multiple trojans and viruses to start the attack before the actual malware or ransomware is eventually downloaded and launched. 70 percent of all malware attacks will use encryption to evade security measures (encrypted malware attacks)

It is no surprise that cyber security skills gap will keep on widening. As a result, security teams will struggle with creating fool-proof policies and leveraging the full potential of their security investments.

### Slow Adoption of new Encryption Standards

Although TLS 1.3 was ratified by the Internet Engineering Taskforce in August of 2018, we won't see widespread or mainstream adoption: less than 10 percent of websites worldwide will start using TLS 1.3. TLS 1.2 will remain relevant, and therefore will remain the leading TLS version in use globally since it has not been compromised yet, it supports PFS, and the industry is generally slow when it comes to adopting new standards. Conversely, Elliptical-curve cryptology (ECC) ciphers will see more than 80 percent adoption as older ciphers, such as RSA ciphers, are disappearing.

### Decryption: It's not a Choice Any Longer

TLS decryption will become mainstream as more attacks leverage encryption for infection and data breaches. Since decryption remains a compute-intensive process, firewall performance degradation will remain higher than 50 percent and most enterprises will continue to overpay for SSL decryption due to lack of skills within the security teams. To mitigate firewall performance challenges and lack of skilled staff, enterprises will have to adopt dedicated decryption solutions as a more efficient option as next-generation firewalls (NGFWs) continue to polish their on-board decryption capabilities.

Cyber-attacks are now the new norm. Each year brings new threats, data breaches and operational challenges, ensuing that businesses, governments and consumers must always be on its toes. With the transformation to 5G mobile networks and the dramatic rise in IoT, by both consumers and businesses, the potential for massive and widespread cyber threats expands exponentially. Let's hope that organizations, as well as security vendors, focus on better understanding the security needs of the industry, and invest in solutions and policies that would give them a better chance at defending against the ever-evolving cyber threat landscape.

## About the Author



Ehab is the Regional Sales Director for Gulf, Levant and Egypt at A10 Networks. Prior to joining A10 Networks, Ehab started his career at Naizak Distribution, managing Riverbed and Opnet business. He later moved into the role as Regional Sales Manager at Sophos Middle East, where he built an amazing team and significantly grew the business. For 4 years Ehab was the Territory Sales Manager at Symantec/Bluecoat managing Enterprise BFSI business in the UAE. He also worked as Regional Channel Sales Manager at Bluecoat and A10 Networks to build the channel team and program covering the Middle East and North Africa. Ehab has more than 14 years of success in business Development & Regional sales with technology expertise in the IT Security, Services, cloud & IT industries.

Ehab can be reached online at (ehalablab@a10networks.com) and at our company website <https://www.a10networks.com/>

# ONE YEAR ON FROM WHATSAPP HACK

what's changed?



## One Year on From Whatsapp Hack- What's Changed?

In 2019, WhatsApp was hacked using sophisticated NSO spyware, Pegasus, used to spy on iOS WhatsApp users' phones.

By Nicole Allen, Marketing Executive, SaltDNA

### One year on from WhatsApp Hack - What's changed?

In May 2019, [SaltDNA published a blog](#) about the latest WhatsApp security vulnerability which was made public on the 13th May 2019. It was in reference to the sophisticated NSO spyware, Pegasus, being used to spy on unsuspecting iOS WhatsApp users' phones by recording phone calls, opening messages and controlling the phones microphone and camera. Since this incident WhatsApp has sued the NSO Group, claiming that the cyber attack violated US laws, including the Computer Fraud and Abuse Act (CFAA). This case is ongoing and it is unclear how it will be resolved.

That is not the end of the problem. Just a month after the incident in May 2019 there was a security hack which allowed a hacker to transform an audio call into a video call, without the victim knowing. According to [The Independent](#), researchers from cyber security firm, Symantec, uncovered the '[Media File Jacking](#)' vulnerability. [Android](#) users were now the main targets for this attack. Such a vulnerability gave hackers the ability to ["misuse and manipulate sensitive information, for personal gain or to wreak havoc."](#)

According to [The Financial Times](#), since 2019, there has been a severe escalation in the number of WhatsApp security flaws. With 2 billion users and an open and unrestricted user base, WhatsApp is still the most popular chat app in the world. Consumers are not worried about well documented security flaws - except maybe for those (prosumers) using it for sensitive business communications. For these CISOs

of these users, the [increasing number of bugs, trojans, flaws and hacks](#) is becoming more and more difficult to ignore. Does the obvious ease-of-use outweigh the risk?

In January 2020, WhatsApp was put at the forefront of the news again, when [The Guardian](#) released an article stating that Amazon Founder, [Jeff Bezos](#), believed that an encryption message sent to him from the Saudi Arabian Crown Prince, [Mohammed Bin Salman](#) injected malicious software onto his phone.

Not surprisingly, it has been revealed that while WhatsApp has typically been the main communication channel for MP's, world leaders and business moguls, the [European Commission](#) has stated that *'WhatsApp should not be the app of choice'* for those who want to keep their communications private. This decision comes a month after the [United Nations](#) claimed that ever since the May 2019 security vulnerability, officials have been barred from using WhatsApp due to security fears.

### Then came COVID-19...

The main impact of the global pandemic has been the disappearance of business travel and the closure of many work offices for long periods. Effective remote working requires frequent communication through smartphones, laptops, tablets and maybe even the odd landline call! There has obviously been a massive increase in the use of real-time communication apps to try to fill the gap in face-to-face meetings. However, there is a good reason why a lot of these meetings would normally take place in person, namely, the sensitivity of the subject matter. With the existence of security flaws associated with WhatsApp and other consumer messaging applications, organisations which deal with sensitive content must be more aware of the risks associated with using these applications.

WhatsApp is a consumer app and by definition the end user is in control of how they use the system. WhatsApp has no concept of a corporate admin portal to configure security settings nor does it have a reporting function to ensure compliance.

As a large number of decision makers within organisations are now being forced to work from home, the continued use of consumer messaging applications poses a great risk for these organisations due to the inherent insecurity of the systems.

The fact remains a year later, that organisations which deal with sensitive business, government or client information should not use consumer apps to share information. By choosing a closed system, such as SaltDNA, organisations are protected against the risk of critical and private data being compromised.

[SaltDNA](#) understands that encryption is simply not enough to secure data. SaltDNA offers a highly secure platform which provides the same convenient user experience as consumer apps, but in a safer and more secure manner, enabling the customer to have full, centralised control of the system at all times. SaltDNA

is the best armour organisations have to protect trade secrets and other sensitive, strategic and proprietary information. Especially during these uncertain times when nearly all communication is taking place via mobile phones. SaltDNA offers a software solution that is more than a secure mobile app: it also offers a web-based management platform that allows for the dynamic provisioning of secure mobile voice and text communications.

To find out more information about the award winning SaltDNA secure communications platform or to avail from a free trial, please contact our team on [info@saltdna.com](mailto:info@saltdna.com).

## About SaltDNA

SaltDNA is a multi-award winning cyber security company providing a fully enterprise-managed software solution giving absolute privacy in mobile communications. It is easy to deploy and uses multi-layered encryption techniques to meet the highest of security standards. SaltDNA offers 'Peace of Mind' for Organisations who value their privacy, by giving them complete control and secure communications, to protect their trusted relationships and stay safe. SaltDNA is headquartered in Belfast, N. Ireland, for more information visit [www.saltdna.com](http://www.saltdna.com).

## About the Author



Nicole Allen, Marketing Executive at SaltDNA. Nicole completed her university placement year with SaltDNA, as part of her degree studying Communication, Advertising and Marketing at University of Ulster. Nicole worked alongside her degree part time during her final year and recently started full time with the company having completed her placement year with SaltDNA in 2018/19.

Nicole can be reached online at ([LINKEDIN](#), [TWITTER](#) or by emailing [nicole.allen@saltdna.com](mailto:nicole.allen@saltdna.com)) and at our company website <https://saltdna.com/>.



## Years of IoT Hacking, But What Have We Actually Learned?

By Brad Ree, CTO, ioXt Alliance

Since the inception of the Internet of Things (IoT) in 1999, connected devices have been integrated into nearly every industry, from retail to automotive and healthcare. In fact, there are estimated to be 50 billion connected devices in 2020, and this number is only expected to grow exponentially. While these devices provide many benefits, they have also been prime targets of cyber attacks due to the vast amount of sensitive data being shared. There are numerous examples throughout the years of device manufacturers and companies that have fallen victim to these attacks - all resulting in them spending a significant amount of time, money and resources to restore their reputation and regain the trust of their customers.

One notable example in the healthcare industry is the Medtronic insulin pump hack. Medtronic, a manufacturer of healthcare devices, made an insulin pump that was able to be remotely accessed by caregivers or medical professionals to monitor and control the pumps to diabetic patients from a distance. Hackers figured out a way to gain access and control the devices from their mobile phones, which could have potentially caused a deadly outcome. This flaw impacted over 4,000 patients and was eventually recalled by Medtronic and the FDA and taken off the market, but patients remained equipped with the old devices and the brand reputation of Medtronic took a hit.

Despite companies taking precautions to prevent attacks after seeing others across industries fall victim to them, hackers continue to adapt and find loopholes and vulnerabilities in security systems to exploit. What's more, industry stakeholders are aware companies need to prioritize IoT security, however the

motivation to uphold these standards isn't always there because they are rushing to get the next innovative products on the shelves. After we have seen countless examples of hacks, has the industry actually learned anything from them or will they not adapt and keep repeating the same mistakes that cause the hacks?

### **An evolving industry and present dangers**

Over the years, there has been a misalignment in the IoT industry due to the highly competitive nature to be the first to come out with the next best device. As a result, manufacturers race to get products to the market as quickly as possible, oftentimes skipping out on critical security measures. This, combined with the need to maintain the device security over the product's lifetime, creates more risks and problematic factors for security.

Additionally, connected devices are becoming more widespread across industries, which has opened the door for experts outside of IT and technology to enter the IoT world, despite not fully understanding the industry and risks that come with it. Healthcare, appliance and automotive professionals have thrown their hat in the connected device ring to adapt their products to keep up with the demand for innovation, but don't completely understand the nuances behind strong security. Because making connected devices is now easier than it once was, there is a higher risk of potential vulnerabilities, giving hackers more opportunities to cause damage.

The increased use of WiFi is also another factor that has evolved which can pose problems to IoT devices and make them vulnerable to hacks. WiFi access used to be a large expense, but has evolved to be a low-cost implementation - making it more widely used for manufacturers. While convenient, WiFi has a large bandwidth, compared to Bluetooth, and can allow for hackers to easily gain access to a device. For instance, a WiFi connected doorbell doesn't require the bandwidth of WiFi and is actually more vulnerable being connected to it. If the device was connected with Bluetooth instead, a hacker would need to be in a much closer proximity to the doorbell to access it, increasing the risk of being caught and making the device more difficult to hack.

### **Lessons learned**

Though companies and manufacturers are aware that there are precautions to prevent attacks and other security issues, old practices that don't work are being repeated and basic recommended guidelines for device security are still not being followed. Security should be accepted from device inception and not added in at the end of manufacturing to fully protect the end-users from hacks. Engineers who think, "Why would someone want to do that?" and ignore those "what if they do" questions, are leaving vulnerabilities to be exploited and putting the company at risk. By not addressing these questions, security professionals are now facing not if, but when the next attack will come.

One common issue in the industry is a lack of standards that has caused technology companies to repeatedly make the same security mistakes. But certain third-party organizations are working to directly change this narrative, introducing and enforcing global security standards and certification programs. The

companies that are partnering with these kinds of alliances and accepting and adopting globally recognized IoT security standards have greater visibility into the products they are manufacturing and distributing and the confirmation that what end-users purchase can be deemed cyber safe. While this can help further mitigate security issues and future hacks from the start, much of onus is on manufacturers to actually lead the charge.

Over the years, IoT attacks have also taught us that hackers will continue to expose holes in devices and exploit data from end-users, and as the industry grows, the future of connected devices will only become more integrated into our daily lives. It's more important than ever that manufacturers ensure that their devices are secure, not only to avoid attacks, but also to prevent being the next security case study or leading headline in the news. These hacks could have more than financial implications and could take months or even years to rectify. For companies and industries looking to innovate their products, implementing security standards and taking measures from the start will ensure the safety of devices, help evolve the industry as a whole and will save tech companies time, money and major headaches down the road.

#### About the Author



Brad Ree is chief technology officer of ioXt. In this role, he leads ioXt's security products supporting the ioXt Alliance. Brad holds over 25 patents and is the former security advisor chair for Zigbee. He has developed communication systems for AT&T, General Electric, and Arris. Before joining ioXt, Brad was vice president of IoT security at Verimatrix, where he led the development of blockchain solutions for ecosystem operators. He is highly versed in many IoT protocols and their associated security models.

<https://www.ioxtalliance.org/>



## Building Trust: The Path to True Security Synergy Between Appsec And Developers

By Matias Madou, co-founder and CTO, Secure Code Warrior

A relationship that is built on the shaky foundations of mistrust is, well, best approached with low expectations. Sadly, this can be the state of the working relationship between developers and the AppSec team within an organization. Generally frosty and marred by a tendency to get in each other's way, the situation is not ideal and leads to poor outcomes in a world of high-risk dependencies on technology.

Developers thrive on problem-solving, building features, and showing creativity in their work. AppSec, on the other hand, has the unenviable task of finding security bugs in their code, bouncing it back for fixes, and providing audits and reports that spoil the shine on the engineer's pet projects. It's not fair to put the blame solely on developers -- security is not their priority or part of their KPIs -- nor can the overworked AppSec team be penalized for simply doing their job. However, for cybersecurity best practices, and better security outcomes at the organizational level, they really need to start playing nice.

And it all starts with trust.

### AppSec's "bad guy" image stands in the way of DevSecOps harmony.

If your only interactions with someone come when they are pointing out where you've gone wrong, chances are good that their input won't be looked upon favorably.

Rarely seen unless there is a problem, the negative connotations of the security team's presence tend to cause some friction. The relationship has been fractured for quite some time, with developers seeing the AppSec team as blockers to their creativity, process, and punctual shipping of features, while AppSec grows very weary of continually pointing out common security bugs that have existed (as has their remedy) for decades.

With increasingly impossible deadlines, under-resourced teams, and a strong desire to avoid rework, developers would often wait until the last possible moment to ship their code, making the window of opportunity for AppSec review and intervention as small as possible. A dysfunctional process, and it has an unacceptable impact of increasing cybersecurity risk to the organization.

For security specialists, it's a case of "don't shoot the messenger" - after all, their job is to find bugs and report them so they can be remediated - nothing personal. The sticking point is that they can often make recommendations that are not the best fit for the company's technology stack, so can be seen as largely unhelpful in the bigger picture of in-house software development.

The notion of AppSec as the villain is counterintuitive for most development methodologies, but for DevSecOps, it's a disaster. The gold standard has moved well beyond Waterfall, Agile, and even DevOps, into a process that sees security as a shared responsibility from the very beginning of the SDLC as vital.

For DevSecOps to work, software engineers need to be given a reason to care about security, and that comes from understanding why it's so important for them to do their part in securing the world's software. Security specialists who make the effort to extend the olive branch, work with development managers to meet the team's needs, and take on more of a mentoring role in nurturing security awareness tend to see long-term benefits from their efforts... and they spend slightly less time tearing their hair out over yet another XSS error.

### **Developers need to be enabled to deliver better secure coding outcomes.**

When it comes to learning secure coding during tertiary education, for many engineers, it's non-existent. And it's not because they were all busy playing beer pong and WoW - it's simply not part of most computer science and IT degrees.

To that end, on-the-job training is often the first exposure a developer will get to the art of software security, and it rarely sets their world on fire. Hours of boring videos are a common training method, as are "tick-the-box" compliance exercises that are far too infrequent to have any real impact on teaching developers how to code securely, or make any headway in reducing common vulnerabilities in an organization's software.

Both the AppSec team and the development cohort are crazy-busy, so any training should be meaningful, engaging, and hands-on. Speaking from a development background, we love to solve problems and get on the tools, so most static training just passes us by while we concentrate on something more pressing (or, let's be honest, interesting).

AppSec specialists are in a place of influence, and they can forge a long-term, win-win situation by advocating for developers' best interests. Seeking out viable training that is job-relevant, and delivered in their preferred languages and frameworks, is a huge step towards shifting the needle and inspiring a grassroots, positive security culture within an organization. We have tried the same thing for decades, and clearly, the "one size fits all" training approach doesn't work. By helping to deliver the right tools and

knowledge to developers, they can successfully upskill in secure coding, act with a heightened sense of security awareness, and produce a higher standard of code.

### Efforts to get on the same page must come from both sides.

It's easy for people with different goals to misunderstand each other, or, at worst, become somewhat distrustful. AppSec has the goal of keeping up with the onslaught of code being churned out, and finding any security issues that may lead to data being compromised, unauthorized access, and malicious attacks that have the potential to destroy positive customer sentiment for years.

Developers, among other things, build features to deadline. They are tasked with making software functional and beautiful, and being the creators of unique digital experiences that keep customers loyal. They've already got a lot to juggle, and pitching them a curveball in the shape of responsibility for security is a daunting prospect. It's seen as AppSec's problem to secure the code, and while that was somewhat

achievable in the 90s (you know, before our cars could be hacked, and our entire lives could be carried around in a pocket supercomputer called a smartphone) there is simply too much code and not enough people to run it through the security gauntlet.

With a healthy dose of empathy, plus the enablement to make security a priority from the very beginning of the software creation process, AppSec and developers can see ways to align their goals. After all, a positive security culture depends on it, and security-aware developers are the secret ingredient to stopping common vulnerabilities, even with an ever-widening cybersecurity skills shortage.

### Mutual respect for time has immense benefits.

Like I said before, everyone is super-busy when it comes to making magic (a.k.a. amazing software) happen. Developers will need allocated work time to do viable, hands-on training that builds their secure coding skills, and any training program should be hyper-relevant by design.

AppSec has their time wasted by fixing the same OWASP Top 10 vulnerabilities over and over again, and developers have theirs whittled away with low-engagement exercises that reinforce the idea in their minds that security is a chore.

Curated learning experiences are vital, and they help to cut to the chase through contextual, bite-sized delivery of relevant training, right at the moment it is needed.

By curating a custom secure coding course that is tailored to desired outcomes and in-house learning pathways, the developer's time and workflow is being respected, while at the same time working towards a measurable reduction of vulnerabilities and cybersecurity risks for the business. It is a quick win in the quest to end soft rivalries, and move forward into the cybersecurity wild west as a united front.

*Secure Code Warrior's latest contextual learning feature, Courses, is available now.*

## About the Author

Matias Madou, Ph.D. is a security expert, researcher, and CTO and co-founder of Secure Code Warrior. When he is away from his desk, he serves as an instructor for advanced application security training courses and regularly speaks at global conferences including RSA Conference, Black Hat, DefCon, BSIMM, OWASP AppSec, and BruCon. He also loves a Fortnite battle or two (or three, or four... ).

Matias can be reached online via:

Twitter: <https://twitter.com/mmadou>

LinkedIn: <https://www.linkedin.com/in/matiasmadou/>

Blog: <https://insights.securecodewarrior.com/author/matias/>

Company website: <https://www.securecodewarrior.com>





## 3 Steps to Reimagine Your AppSec Program

By Jake Reynolds, Product Manager at NetSPI and Nabil Hannan, Managing Director at NetSPI

With Continuous Integration/Continuous Deployment (CI/CD) increasingly becoming the backbone of the modern DevOps environment, it's more important than ever for engineering and security teams to detect and address vulnerabilities early in the fast-paced software development life cycle (SDLC) process. This is particularly true at a time where the rate of deployment for telehealth software is growing exponentially, the usage of cloud-based software and solutions is high due to the shift to remote work, contact tracing software programs bring up privacy and security concerns, and software and applications are being used in nearly *everything* we do today. As such, there is an ever-increasing need for organizations to take another look at their application security (AppSec) strategies to ensure applications are not left vulnerable to cyberattacks. Here are three steps to get started:

### Step 1: Identify Existing Barriers to AppSec Success

Even now there remains outdated and immature AppSec programs. Many organizations tend to perform vulnerability testing in an ad-hoc, reactive manner, typically driven by some type of security incident, by compliance requirements or a client's request. Add to that, with the plethora of vulnerability testing and discovery tools available from multiple vendors, almost every organization struggles with content overload and tool management which ultimately leads to inefficiencies and ineffective AppSec programs.

In many cases, vulnerabilities aren't tracked or managed anywhere centrally, but instead lengthy reports are emailed back and forth amongst development teams to digest and consequently there's no easy way to measure an organization's risk posture. The overarching barrier to AppSec success? A lack of using data properly to make informed decisions.

To effectively adopt a reimagined, proactive AppSec program, there needs to be a formalized, data-driven program that defines and guides how an organization implements application security. As a starting point, engineering and security teams will benefit from an understanding of traditional and emerging application vulnerability discovery tools and techniques.

## Step 2: Expand and Understand Your Options for Vulnerability Discovery

To catch security flaws early in the SDLC process, the *traditional* application vulnerability discovery techniques most commonly used are Static Analysis Security Testing (SAST) with Manual Secure Code Review or Dynamic Application Security Testing (DAST) with Manual Penetration Testing. Most organizations use these techniques to some extent, and when it comes to managing open source software risk, many organizations just manually manage and inventory a list of their open source usage. New and *emerging* technologies like Interactive Application Security Testing (IAST), Real-time Application Self Protection (RASP) and Software Composition Analysis (SCA) are quickly gaining popularity and changing how organizations look for security vulnerabilities in their applications.

There are many different vulnerability discovery tool options to consider, with pros and cons to each. Here's a guide to better understanding your options:

## SAST & DAST

### Technology Considerations in Vulnerability Discovery

Even though the technique of analysis is vastly different when deploying SAST (for source code error) and DAST (for running applications) technologies, a lot of the challenges that they pose to organizations to adopt and deploy are similar. Additionally, they both require manual setup and configuration to start yielding valuable results. Both DAST and SAST aid in finding the vulnerabilities that matter – DAST gives quick and thorough coverage of the most common vulnerabilities such as OWASP Top 10 and SAST does a deeper analysis and looks for vulnerabilities at the source code level.

## IAST

IAST is gaining popularity quickly and is a rising star amongst security discovery techniques. Because it is instrumented into running the application on the server side, it can report issues that are truly exploitable, which results in the IAST tool reporting little to no false positive vulnerabilities.

## RASP

RASP is a technique, as the name suggests, that isn't really intended for vulnerability discovery, but more for attack prevention. Ultimately, RASP is an additional layer of protection to protect an application from common attacks similar to how Web Application Firewalls protect an application from attacks.

## SCA

When identifying and managing open source risk, SCA techniques have evolved and are being adopted widely. SCA tools allow organizations to create a bill of materials and inventory all open source software components and their corresponding versions that are being used in applications as a means to notify developers if known vulnerabilities are reported.

A final note on the tools: SAST, DAST and IAST all detect new vulnerabilities; SCA only reports on known threats.



### Step 3: Focus on Infrastructure to Improve Efficiency

A critical component of an organization's AppSec program is the infrastructure built around vulnerability management, tracking, reporting, and remediation. Consideration should be given to implementing the most efficient and effective infrastructure to manage AppSec programs holistically, for many beneficial reasons including faster remediation and better reporting.

When analyzing vulnerability discovery techniques, it quickly becomes apparent that they are not all created equal in terms of integration and reporting. Some have a consolidated system (DAST running through Jira, for example), but unfortunately, there are still many other components and data sources in an AppSec program that can result in inefficiencies, lack of automation, and unmanageable amounts of noise. And when it comes to the vulnerability reports? Many times, the results across testing platforms are supplied in hundreds of pages-long PDFs, are not deduplicated or consolidated, and there is no system of record for the organization. This results in inefficiencies, no master plan, more staff time, and lost context related to the vulnerabilities. Ideally, an AppSec program should deliver all data behind a single infrastructure platform that foregoes the reams of paper and allows for immediate remediation and access to historical data to track the progress of the AppSec program over time.

To further build a solid AppSec infrastructure, consider these strategic pillars:

- Adopt a centralized vulnerability infrastructure management system to record and manage all AppSec activities, one that can house vulnerabilities in a manner that provides insights into trends and analyzes for better security initiatives
- Integrate technology into the process, as appropriate, that ingests disparate data sources for noise reduction and provides more global context and intelligence around the vulnerabilities
- Manage the entire secure SDLC, centered around engagements for project management focus; Enable automation to assign people to strategic tasks/activities

It's a reality that many organizations struggle with the breadth of their testing coverage. Engineering and security teams lack the time or financial resources to adequately test all of the applications and systems in their environment – and they can't remediate all the vulnerabilities from each test. According to [Gartner](#), once a company discloses a vulnerability and releases a patch, it takes 15 days before an exploit appears in the wild. And clearly a lot can happen in 15 days in the world of cyber defense.

An effective, reimagined AppSec program includes being able to manage manual penetration testing and secure code review augmented with automated vulnerability discovery tools that are deployed at various phases of the SDLC process. Penetration Testing as a Service (PTaaS) provides our customers with tests when they need them. Release-based testing is gaining popularity and PTaaS allows organizations to consume the appropriate level of testing at the appropriate time.

Ultimately, a reimagined AppSec program will improve vulnerability ingestion, correlation, and enrichment, and will bring increased speed to remediation to organizations. These program improvements will undoubtedly enhance reporting around vulnerabilities (and the positive results in thwarting an attack) to leadership to optimize AppSec programs even further.

## About the Authors



Jake Reynolds is a Product Manager at NetSPI. He is responsible for leading the product strategy for Resolve, NetSPI's vulnerability management and orchestration platform. Previous to his current role, Jake was a Principal Security Consultant helping lead internal R&D and application penetration testing services at NetSPI. Jake can be reached at [jake.reynolds@netspi.com](mailto:jake.reynolds@netspi.com), on Twitter and LinkedIn ([@JReynoldsDev](https://twitter.com/JReynoldsDev)) and via the NetSPI website <https://www.netspi.com/contact-us/>.

Nabil Hannan is a Managing Director at NetSPI. He leads the company's consulting practice, focusing on helping clients solve their cyber security assessment, and threat & vulnerability management needs. His background is around building and improving effective software security initiatives, with deep expertise in the financial services sector. He has over 13 years of experience in cyber security consulting from his tenure at Cigital/Synopsys Software Integrity Group, where he has identified, scoped, and delivered on software security projects. Nabil has also worked as a Product Manager at Research In Motion/BlackBerry and has managed several flagship initiatives and projects through the full software development life cycle. Nabil can be reached at [nabil.hannan@netspi.com](mailto:nabil.hannan@netspi.com), on Twitter ([@NabilHannan](https://twitter.com/NabilHannan)), on LinkedIn ([@nhannan](https://www.linkedin.com/in/nhannan)) and via the NetSPI website <https://www.netspi.com/contact-us/>.



## Alternative graphic for discovery techniques:





## Cyber Security Patent Lawsuits on The Rise and The Need for Shared Innovation in Cyber Security

By Keith Bergelt, CEO of Open Invention Network (OIN)

According to the FBI's Internet Crime Complaint Centre, by June of 2020, daily digital crime in the U.S. had risen by 75%, since the start of the stay-at-home restrictions generated by the COVID-19 pandemic. The U.S. Federal Trade Commission reports that by June 30<sup>th</sup>, it had received almost 140,000 reports since the start of the year, nearly as many as it received for all of 2019. Interpol's cyber-crime division, reports that as the pandemic continued, criminal networks have increasingly shifted their targets to big companies, governments and critical infrastructure, away from individuals and small businesses.

Gartner estimates that businesses on average spend 5% to 8% of their overall technology budget on cybersecurity. As of June 2020, it predicts a 33.3% increase in spending on cloud security, over 2019. Other areas seeing growth are data security at 7.2%, application security at 6.2%, identity access management and infrastructure protection. By the end of 2020, these estimates may turn out to be low considering that businesses are increasingly employing remote working, which may require additional cybersecurity spending to protect their systems adequately.

A Cybersecurity Ventures report issued in late-2017, states that cybercrime damage is estimated to reach \$6 trillion annually by 2021. Due to the convergence of an escalation in the number of security

vulnerabilities, an increase in hacker capabilities and tools as well as the GDPR legislation enacted in the European Union, the estimated costs due to cybercrime may be conservative.

In order to meet the cybersecurity challenges of tomorrow, information security companies and governments must invest and rapidly deploy new, innovative systems. A potential impediment is the growth of cybersecurity technology-related intellectual property lawsuits.

### **Cyber Security Patent Lawsuits on the Rise and The Need for Shared Innovation in Cyber Security**

The expected growth in the security software industry has the potential to be significantly disrupted and its innovation impaired by patent lawsuits. With the industry's growing market size, many aggressive entrants, and an open source software model that is fast becoming the standard way of moving innovation forward, there is a potential for established vendors to look to impair these growth drivers through the use of intellectual property.

In mid-January of 2020, Zscaler agreed to pay \$15 million to settle all patent infringement lawsuits filed by Symantec, just three months after Broadcom purchased Symantec's enterprise security business. The settlement amount is just under five percent of Zscaler's annual sales.

Finjan Holdings Inc., a security technology company turned Patent Assertion Entity (PAE), has been the most litigious actor in the cybersecurity market. They have successfully sued for awards and licensing fees from Symantec, FireEye and Sophos, among others. In October of 2020, a Finjan lawsuit will proceed to trial asserting five U.S. Patents against Cisco. Finjan has pending patent infringement lawsuits against Palo Alto Networks, ESET, SonicWall, Check Point, Rapid7, Fortinet, Qualys and Trustwave/SingTel, relating to more than 15 patents.

### **Open Source is Driving Innovation Across the Business Spectrum**

Open source is a leading technology in smart cars, IoT platforms, blockchain technologies and cybersecurity software projects. Today, open source code is so effective and cost efficient that it is used in more than 90 percent of all commercially available software. In fact, it is impossible to catalog all of the daily touch points the average person has with an open source-powered product, or service. Growth in security open source software (OSS) projects, like all manner of OSS development and usage, is growing at a rapid pace due to the innovations the community consistently achieves.

While it has experienced exponential growth, the successful proliferation of open source in cybersecurity technology as well as banking networks, mobile devices, telecom networks, smart cars, cloud computing and blockchain platforms, among others, was not always a foregone conclusion. In 2003, there was an intellectual property (IP)-based attack on Linux, the most important and prolific OSS project.

## Fostering Patent Non-Aggression in Core Cybersecurity Technology

While the claims underlying the litigation ultimately were found to be without merit in the court proceeding, it was a wakeup call to several IP-savvy companies as to the potential negative impact of patent aggression on the growth of Linux and OSS projects. IBM, Red Hat and SUSE (then Novell) coordinated an effort with Sony, Philips and NEC to architect and implement a solution designed to create a “patent no-fly zone” around the core of Linux, called the Linux System. The organization is charged with administering this patent no-fly zone, utilizing a free license to require participant companies to forebear litigation and cross-license patents in the core of Linux and adjacent OSS. In the 15 years since its formation, the organization has grown into the largest patent non-aggression community in history with an excess of 3,300 participant companies that own upwards of 2.5 million patents and applications.

In addition to administering the highly successful royalty-free free license, the organization has been one of the most active users of the America Invents Act's pre-issuance submission program and through its actions prevented the grant of hundreds of patent applications with overly broad claims that, if issued as submitted, would have threatened Linux technology and products for years to come. This community-based organization also routinely uses its central role as guardian of patent freedom in the open source community to gather critical prior art to neutralize Linux-related litigation and pre-litigation patent assertions. In some cases, it has taken the extraordinary measure of forward deploying key assets from its defensive patent portfolio of more than 1,300 patents and applications to companies at risk or in litigation for the purpose of allowing these companies to better defend themselves from patent antagonists with often far larger patent portfolios and deeper pockets seeking to slow or stall the progress of Linux.

Given the current environment and trends, the cybersecurity industry will increasingly be an investor in technology, and it will be a significant driver of technological innovation. The organization and community will continue to evolve to include core open source technology in the Linux System and thereby insulate its members from patent risk in technologies and markets where OSS is adopted. As the threat landscape morphs and new patent challenges arise from the ranks of operating companies and PAEs, the community will remain vigilant in acting to ensure fewer poor quality patents are issued, more poor quality granted patents are invalidated and the community of companies pledging patent non-aggression in the core of Linux and adjacent open source technology grows.

In order for the creativity and inventive capacities of the hundreds of thousands of people developing around cybersecurity technology to be realized, it is vital that patent non-aggression in the core is safeguarded. Companies and individuals seeking to support patent non-aggression in cybersecurity systems should participate as members of this community by becoming signatories of OIN's free license and, in so doing, commit to the onward sustainability of the collaborative model of innovation that is central to open source.

## About the Author



Keith Bergelt is the CEO of Open Invention Network (OIN), the largest patent non-aggression community in history, created to support freedom of action in Linux as a key element of open source software. Funded by Google, IBM, NEC, Philips, Sony, SUSE and Toyota, OIN has more than 3,300 community members and owns more than 1,300 global patents and applications. The OIN patent license and member cross-licenses are available royalty-free to any party that joins the OIN community.



## The Challenges of Industrial 3D NAND

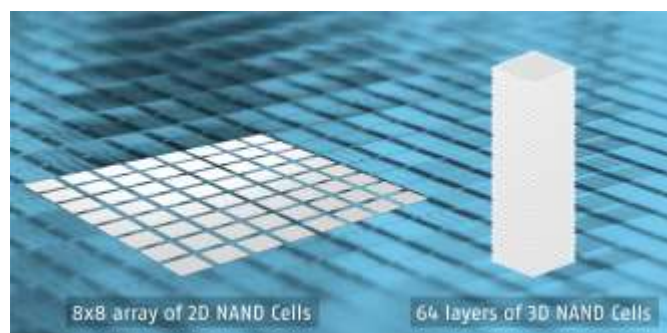
By Roger Griesemer, General Manager Memory Solutions, Swissbit AG and  
Ulrich Brandt, Technical Director Marketing, Swissbit AG

3D NAND is a popular topic on websites, in magazines, in advertisements and at conferences. In the discussion surrounding 3D NAND, there is one common theme: it has a promising future. Within a few years, the technology has evolved from the original 32 layers, increasing first to 48, then to 64. 3D NAND currently has 96 layers. This will continue to grow, with the next generation, only a few months away from release, set to contain 128 layers.

Vertical stacking was the perfect solution to the increase in miniaturization of components, heightened risks and rising costs. Sub 10nm NAND was deemed unachievable, both commercially and technologically.

The market saw a significant drop in the cost of SSDs and storage cards. This was caused by a combination of reduced manufacturing of stacks in excess of 64 layers and an oversupply driven by higher chip capacities. The 3D cell had a larger capacity, thanks to a superior physical build over the 2D

cell. This made way for the introduction of QLC products; 4 bits per cell with 16 voltage levels that need to be distinguished reliably. Designs with 5 bits per cell (PLC = Penta Level Cell) are already being developed.



### 64 cell comparison between 2D & 3D NAND

It's safe to say that 3D NAND has conquered the storage world and is very well positioned. This is particularly the case for consumer or enterprise SSDs that typically sit within well-ventilated systems.

However, what happens if you use a consumer 3D NAND SSD for atypical industrial application? Those that are within tight vent-less systems and often used outdoors and subjected to frequent and extreme temperature variations? Those applications that need to log data from a multitude of sensors with a high data rate of small transfers? How does 3D NAND meet these requirements?

Let us start with a few common statements about 3D NAND:

- 3D NAND is more reliable than 2D NAND
- 3D NAND is faster than 2D NAND
- 3D NAND is cheaper than 2D NAND

The last statement is unquestionably accurate given the current 3D NAND designs. Afterall, that's exactly what NAND manufacturers wanted to achieve with their billions of dollars of investments into the technology. The other two statements require a little more insight.

### Is 3D NAND more reliable than 2D NAND?

It is often suggested that 3D NAND is more reliable than 2D NAND because the active area of the cell and the size of the storage plate is significantly greater in 3D NAND. The cell in 2D NAND is comprised of a small flat area; whereas the cell in 3D NAND wraps around the bitline, allowing for more charge to accumulate. In 3D NAND, electrical interference from adjacent cells could be reduced and the signal to noise voltage ratio improved; this all sounds promising. This advantage, however, was used to achieve greater bits per cell and cost reductions and not necessarily increased reliability.

2D NAND MLC technology typically has an endurance of 3000 program/erase cycles, meaning each block can be erased and reprogrammed 3000 times, before the cell degrades so far that its storage capability of one year can no longer be guaranteed.

3D NAND should achieve a higher number of program/erase cycles. However, typically, only 3D TLC NAND versions are offered. Cell capacity improvements have been used to increase bits-per-cell, and as a result, 3D NAND also offers 3000 program/erase cycles identical to 2D NAND. This was only achieved incidentally through various modifications, particularly regarding error correction.

Whilst the 2D NAND's 3000 program/erase cycles are reached with a simple 40-bit per 1KiB BCH error correction, 3D NAND requires at least a 120-bit error correction to be able to match the 3000 cycles. This is a new process called LDPC, that requires a lot more check bits, and therefore more silicon area in the controller and more computing time of the correction firmware. This is especially the case when the number of faulty bits increases towards the end of life. Older controllers do not have the required resources and therefore won't work with 3D NAND.

With the new 3D NAND technology, new error mechanisms have appeared in the Flash. Consequently, new firmware functions such as Block RAID, are now required. This feature prevents failure of an entire block which previously was neither possible nor necessary.

Without this feature, system failures can occur in the range of up to 1000 DPPM (1000 failures per million devices). This is acceptable for consumer products and block RAID is usually not implemented. However, such an error rate is not acceptable for industrial products.

Here, the correction of block failures is mandatory and requires great efforts both in the firmware and in the provision of greater redundancy. The feature protects customers from unexpected failures in the field. With error rates at 1000 DPPM level, potential risks cannot be discovered during normal qualifications. Customers must rely on the SSD manufacturer to have taken all necessary measures to minimize field failures.



**Swissbit X-75m2 Industrial M.2 SATA Solid State Drive (SSD) module available in storage capacities from 30GB to 960GB that deploys 3D NAND technology and AES256 encryption.**

The advantage of block repair, however, also comes at a price: additional memory is required to save parity information. This increases the Write Amplification Factor (WAF), which in turn reduces the lifespan of the SSD. The larger the WAF, the lower the life expectancy. For this reason, many consumer products avoid this feature. Industrial SSDs on the other hand, need block RAID or an equivalent error handling, making them more complex and resulting in a significantly higher qualification effort.

## Cross-temperature

A further aspect of 3D technology is its behavior during temperature changes, otherwise referred to by its technical term, cross-temperature.

With 2D NAND, conformity of all cells was defined by the optical lithography's accuracy. A reasonable assumption is that the cell properties of all cells in an array were identical. Whilst the cells did not have a high capacity, they were at least equal within a page.

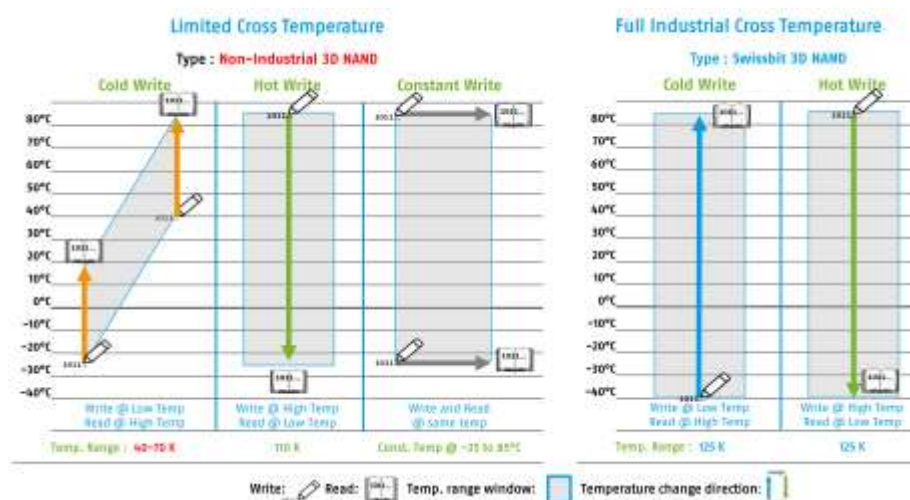
Whilst 3D NAND has much better cell properties, it's also characterized by much higher variations.

Let's picture a 3D NAND bitline as a tiny hole that is etched through 64 layers. Ideally, the hole would be the same size at the top layer as it is at the bottom of the stack. However, the reality is very different: the top layer has a much larger diameter than the bottom, resulting in completely different cell capacity and voltage thresholds. All 64 cells between the top and bottom layers belong to the same bitline and the same voltage detector. As a result, voltage levels within this bitline vary greatly and must be permanently compensated. Now add in temperature variations, and the work of the detector becomes very difficult. For example, when writing at low temperatures and reading at high temperatures, the voltage ratio is completely different than when the order is reversed.

Generally speaking, all extreme temperatures are critical for 3D NAND. Operation below  $-10^{\circ}\text{C}$  or at  $85^{\circ}\text{C}$  will cause read problems by shifting the voltage level. If there is further interference due to intensive reading or a power failure, data loss is inevitable.

For standard consumer 3D NAND flash, the permitted fluctuation between the write and read temperature is about 45 to 50 Kelvin (K). This means, for example, you can write at  $20^{\circ}\text{C}$  and read at  $65^{\circ}\text{C}$ , which is sufficient for consumer products.

In contrast, industrial applications with a specified ambient temperature operating range between  $-40^{\circ}\text{C}$  to  $50^{\circ}\text{C}$  easily reach an SSD temperature range between  $-40^{\circ}\text{C}$  and  $85^{\circ}\text{C}$ . This is 125K cross-temperature and 2.5 times the range of a consumer drive, which will most likely fail under these conditions.



## Cross temperature behavior

Very few specially tuned 3D NAND products that meet these specifications are available on the market. They are more expensive but offer safety against data loss.

3D NAND offers a higher reliability on an individual cell level than 2D NAND, but the high stack-up and transition to TLC negates any performance improvements, thereby requiring additional mechanisms to match the reliability of 2D NAND. Only by implementing the correct NAND can industrial-grade products be manufactured.

## Speed characteristics

It is true that 3D NAND technology offers a faster Write speed than 2D NAND. This is because all three bits of the 3D cell can be written in a single process step. In contrast, 2D NAND requires two programming steps to write each bit - first the lower (fast) bit followed by the upper bit in a separate programming step.

Whilst each individual step is faster in 2D NAND, 3D NAND is faster in the total time that it takes to write 3 pages (3 bits).

What if there aren't three pages readily available for writing? This can often be the case with random writes of small data packages. In this case, the addition of dummy pages is needed to fill the 3 bits. Writing with dummy pages reduces the effective data rate compared to 2D NAND.

DRAM cache is often used as a counter measure to be able to collect pages over a longer period of time in order to write three information pages at a time. This makes the SSD more expensive. In addition, the controller needs enough buffer space for three pages, which older controllers don't offer.

A common solution is to use a small portion of the memory as an SLC cache. The write performance is very high at the beginning. As soon as the cache is full, 3 pages from the pSLC area are converted into a TLC page. Once this process begins, the drive slows down significantly. Each new data transfer causes pSLC pages to be converted into TLC. Another option is to use the complete memory in pSLC mode to begin with. The cache in this instance is much larger than in the previous case. 1/3 of the drive capacity is available as fast storage. Additional capacity requirements kickstart the conversion process from pSLC to TLC.

Benchmark tests are often based on small storage capacities and are usually carried out with "Fresh out of the box (FOB) = as yet unused" SSDs. Here, the complete SLC cache is still available and impressive measurements can be taken. Over the lifetime, the performance drops down to a fraction of the specified values.

A third solution is called 'TLC direct'. Here, the SLC cache is not used and programming is performed as a one-step process. As previously mentioned, a DRAM is needed for the process to work efficiently. Even then, the top speed is reduced compared to the SLC caching option. However, the performance remains largely constant over the entire service life.

As can be seen from the above descriptions, speed is not necessarily constant when using a memory drive. Impressive specifications do not mean that they are maintained as the drive is filled.

For industrial applications, performance consistency is more important than maximum performance. For this, the firmware needs to be optimized according to the application requirements. Drives for industrial applications are finetuned for constant data rates and long service life.

## Endurance

The endurance of 2D NAND drives was measured relatively easily by letting the required test run for an extended period of time. Then, with the use of tools, the number of internally and externally written pages was determined (the term for this ratio is WAF) and finally the expected possible Terabytes written (TBW) extrapolated.

With 3D NAND, many new aspects influence the endurance of the drive. Essentially, the more flash that is written internally as a result of an external data transfer, the lower the expected TBW.

Endurance is reduced by:

- Block RAID, as additional pages are needed for parity
- SLC Cache, because each logical page will be written at least twice in the flash
- DRAM-less drives, often requiring dummy page writes.

Endurance is often also influenced by:

- The memory size effectively used by the benchmark
- Preconditioning of the drive (FOB vs already written)
- The benchmark profile (small vs large block size, use of TRIM, flush cache).

In summary, the endurance of SSDs with 3D NAND flash is comparatively lower than a drive with 2D MLC, even though both NAND components are specified with 3000 erase cycles. Consumers are more interested in cost per GB than cost per TBW. For industrial drives that operate for many years in the field, the cost per TBW is much more important than the initial purchase price of the drive.

## Error correction

As already mentioned, 3D NAND needs a much higher number of bits for error correction.

120-bit LDPC is needed instead of 40-bit BCH.

Initially this may not appear to be so important. However, the consequences are a lot more complex. Going from 40-bit BCH to 120-bit BCH would require not just a 3-fold, but more than a 10-fold bigger chip surface area. This is not only very expensive but also difficult to achieve.

The solution is a new code procedure, initially used in 2D TLC: LDPC (low density parity check). Only a few bits are used for the checksum generation, but this requires so-called soft information from the NAND. Instead of getting all the correction information with a simple read, three read accesses are now needed to repair a maximum of 120 faulty bits. While a small number of bit errors can be corrected by the LDPC hardware, the controller needs software algorithms when the number of errors is higher. As a consequence, the memory slows significantly when the bit error rate increases, due to aging. In fact, significantly slower than with 2D NAND.

### **New controllers – new features**

One improvement that has resulted from the additional requirements demanded from modern 3D NAND controllers is End-to-End data path protection, or E2E DP. In older controllers the internal RAM for the page buffers, the data path between the different units and the DRAM content were not protected against bit fails (for example as a result of radiation or alpha particles).

Undetected data corruption poses a high risk because it can lead to incorrect settings or wrong results. An undetected single bit fail could cause significant financial or even physical damage were it to happen with bank transactions, medical treatments or robot control.

The latest controllers protect all data paths with parities. All buffer areas and DRAM content are secured by ECC (Error Correction Code).

Errors no longer go undetected, and in most cases rejecting and repeating a write command or marking the read data as defective can prevent further processing of the incorrect data.

### **Conclusion**

For industrial SSD's, the firmware and NAND architecture need to be fine-tuned to achieve high endurance, consistent performance and stable operation within the industrial temperature range.

The sacrifices to be made are a limitation in top performance and higher purchase prices. The advantages, however, are robust products with low life cycle costs due to the greater endurance and reliability.

Swissbit has more than 20 years' experience in designing products for industrial applications and offers a variety of drives that are optimized for endurance, life cycle costs and robustness.

## About the Authors

### Roger Griesemer



Roger Griesemer is a proven electronics industry expert who joined Swissbit AG in 2003 and helped to shape the company during its startup years. He was appointed General Manager of the Memory Solutions division in July 2019. Roger's contributions as Head of Product Management and Business Unit Manager were instrumental in establishing the company as the only European provider of real industrial products and solutions for data storage.

Roger can be reached online at [security@swissbit.com](mailto:security@swissbit.com) and at the company website <http://www.swissbit.com/>

### Ulrich Brandt

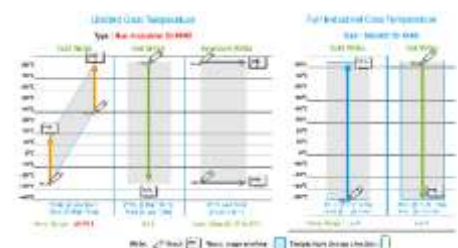
Ulrich Brandt is Director Technical Marketing at Swissbit AG. With more than thirty years of experience in memory architecture, DRAM chip design, application engineering and technical marketing, he was until recently responsible for the DRAM business unit at Swissbit. He holds a master's degree (Dipl.Ing.) in electrical engineering from the Technical University in Braunschweig, Germany.

Ulrich can be reached online at [security@swissbit.com](mailto:security@swissbit.com) and at the company website <http://www.swissbit.com/>



### 64 cell comparison between 2D & 3D NAND

### Cross temperature behavior.



### Swissbit X-75m2 module



## How Can CISOs Work with CMOs to Secure Social Media?

By Otavio Freire, CTO & Co-Founder, SafeGuard Cyber

Recent reports indicate that [over half of the global population now uses social media](#) – up 10.5% on last year's 3.5 billion users. For businesses, being able to engage with customers and users on social media is no longer a side strategy. It is an absolute must.

However, unlike email, social media lacks a robust security system. Social media channels exist outside traditional cybersecurity architecture, and are vulnerable to a range of dangerous [digital risks](#). And here's the real challenge: Despite this risk, CISOs don't own these channels. Typically, the marketing department does. Even though executive leaders, spokespeople, and brand reputation are all at risk on social media, marketing usually doesn't prioritize security. It isn't their job.

How can CISOs effectively work with their CMOs to protect social media assets, so that everyone benefits? By offering a clear picture of the risks, and communicating the benefits of security in such a way that collaboration becomes a no-brainer. Social media security isn't only a defensive initiative. It drives revenue and growth. Once this is understood, organizational buy-in is far easier to acquire.

## Social Media Has No Security Infrastructure

Decades ago, when email began to be broadly adopted by large organizations, security threats evolved. By the [early 2000s](#), software vendors entered the market to help businesses secure their email channels. Today, email security is a [\\$3B industry](#), but it took nearly a decade for solutions to catch up to the risks.

Social media protection is currently caught in a similar security gap. Brands and companies have only been seriously leveraging social media for a few years – and the cybersecurity industry is yet to catch up. The massive adoption of cloud SaaS and mobile apps to streamline communication and improve the customer experience has created a new gap between the developing threats and the security infrastructure. Solutions are emerging, but they never appear as quickly – or in as well-formed a fashion – as CISOs require.

Because social media channels live outside the traditional security perimeter, IT teams are deprived of visibility. Bad actors know this, and they are circling. A [study](#) involving 1.2 billion social media interactions found that 53% of all social media logins were fraudulent, and 25% of new accounts were fake. Even popular celebrities on Twitter [aren't safe](#).

This is why [73%](#) of cybersecurity professionals say that web-based threats are far harder to deal with than their email counterparts, and 80% think that attacks launched via Facebook pose serious threats to their organizations. What's more, brand threat intelligence is increasingly becoming part of the CISOs overall risk management responsibility. The threats are legion: social engineering, spear-phishing, account impersonation, sophisticated profile hijacking, insider threats, and more.

## COVID-19 Complications

Remote work mandates during lockdowns [accelerated enterprise adoption and use](#) of social media platforms. This expanded the attack surface, creating huge risk exposure for the enterprise. Cyber criminals and nation state actors are targeting people where they are, relatively unprotected. These attacks include (but are not limited to) infiltrating collaboration platforms, and [phishing employees with malware-laced files or conducting espionage on LinkedIn](#) and even WhatsApp.

## Bringing Marketing Onboard

If CISOs don't own social media channels, how can they repel these threats? By showing the departments that do own social media that social media security is about more than security. The following questions should be posed to CMOs:

- Would you like to guarantee that your products and services are accurately represented online?
- Would you like proper visibility of malicious actors on the dark web?
- If rules and policies could ensure security, compliance and visibility on social media channels, would you be able to increase productivity without increasing headcount?

- Would you benefit from securely enabling the executive team and recruiters to communicate effectively on channels like LinkedIn?

The answer to these questions will, of course, be yes! And once marketing realizes that the right security tool will help drive outreach and growth, a win-win is created. In terms of securing social media, everyone now has skin in the game.

What kind of software will ensure that the whole organization is satisfied? Social media security software needs to be lightweight, and not get in the way of the user. Social media tools are now crucial to operations, so any cybersecurity software cannot make them any trickier to use. If this happens, employees will find a way to sidestep the software, and sales and marketing will be irked.

As well as being invisible to the user, social media protection needs to be automated. The fact is that, with the volume and velocity of digital communications being what they are, people cannot be trusted to protect themselves. [Human error featured in 95% of all security breaches](#), according to a study by IBM. Enterprises can train employees in cybersecurity best practices to keep them vigilant and responsive to possible threats, but this will never be enough. CISOs need to lean on AI and ML.

Above all, social media protection needs to meet the platforms where they are: in the cloud. Only cloud-based defense can stymie attacks at the app level, and stop them from moving laterally into endpoints and onto enterprise networks. An effective platform should offer:

- *Comprehensive Visibility*

Security teams need to be able to find and onboard all authorized social accounts. They need the ability to inspect messaging for malicious content, track new connection requests, and archive account activity.

- *Threat Detection*

All social media accounts need to be monitored around the clock for suspicious activity and correspondence. All files, attachments and links must be automatically scanned for malware, and connections must be evaluated for known or potential bad actors.

- *Incident Response*

Malware and other threatening content must be immediately quarantined, in real-time, at the app level. IOC notification details should be sent to SOC/SIEM for evaluation, and social attacks need to be correlated with EDR.

Social media platforms are only going to become more central to enterprises. In line, bad actors are going to get more sophisticated, COVID-19 is going to continue to exacerbate things, and the security stakes

are going to continue to rise. CISOs need to communicate this reality to their CMOs in a way that brings them onboard. Once marketing realizes that real security can drive growth and revenue, bringing in the right software will become a priority for the whole organization.

#### About the Author



As the President, CTO and Co-Founder of SafeGuard Cyber, Otavio Freire is responsible for the development and continuous innovation of SafeGuard Cyber's enterprise platform. He has rich experience in social media applications, internet commerce and IT serving the pharmaceutical, financial services, high-tech, and government verticals. Mr. Freire has a BS in Civil Engineering, an MS in Management Information Systems and an MBA from the University of Virginia Darden School of Business, where he currently serves as a visiting executive lecturer. Otavio can be reached online via [LinkedIn](#) and at our [company website](#).



## Why Deepfakes Will Threaten the Future of Digital Communications

By Steve Durbin, Managing Director, Information Security Forum

Advanced deepfakes of high-profile individuals or executives will soon threaten to undermine digital communications, spreading highly credible fake news and misinformation. Deepfakes will appear with alarming frequency and realism, accelerating and turbocharging social engineering attacks.

The underlying Artificial Intelligence (AI) technology will be used to manipulate both video and audio, enabling attackers to accurately impersonate individuals. As attackers use increasingly sophisticated deepfakes they will cause serious financial damage, manipulating public opinion with fake videos and images to manipulate financial markets, promote political agendas or gain competitive advantage. Severe

reputational damage will be caused when executives or high-profile individuals have their identities compromised.

Organizations and individuals will face new security challenges beyond anything they have dealt with before. Nation states, activists and hacking groups will use deepfakes to spread disinformation on scale, leaving individuals and organizations unable to distinguish fact from fiction, truth from lies.

### Deepfakes Lead to Deep Trouble

The advancements and increasing availability of AI technologies will enable attackers to create highly realistic digital copies of executives in real-time, by superimposing facial structures and using vocal patterns to mimic real voices. As deepfake technologies become more believable, many organizations will be impacted by this new, highly convincing threat. Organizations using poor quality audio and video streaming services will find it particularly challenging to identify this threat, as the imperfections in even the most simplistic deepfakes will go unnoticed.

Early generation deepfakes have already been used to replicate the audio and visual likeness of public figures, such as politicians, celebrities and CEOs. The likelihood of these unsophisticated examples is low, with viewers being able to tell when a video is authentic or fake. However, the development of deepfakes is progressing quickly, with the first case of AI assisted voice phishing (vishing) – social engineering using an automated voice – used to perform a high-profile scam in early 2019. Attackers replicating the voice of an energy company's CEO were able to convince individuals within the organization to transfer \$243,000 to a fake supplier. The attackers used social engineering techniques to trick an employee into calling the CEO and, as the voice on the other end of the phone sounded exactly like the CEO, the employee went ahead with the transfer.

While the manipulation of images has a considerable history, often used as propaganda in times of conflict, the easy availability of digital tools, the highly realistic nature of the doctored content, and the existence of new media channels to distribute misinformation have turned deepfakes into a viable attack mechanism. With a growing number of important government elections taking place in the coming months, the impact of deepfakes is likely to far exceed that of existing 'fake news'.

As deepfakes become more common and the technology behind them becomes cheaper and more widely available, it will raise major concerns around the likelihood of attackers targeting organizations for financial gain, blackmail or defamation. Not only do popular mobile applications such as Snapchat and Zao allow individuals to create deepfake content with ease, attackers will be able to buy and sell highly convincing deepfake technologies or services on the dark web and use bots to generate fake content on social media.

While deepfakes have already begun to cause considerable concern in the media, the speed at which this technology moves will inevitably result in negative impacts to targeted organizations. Traditional attempts to identify and counter defamation will be unable to deal with the sophistication of deepfakes. Established forms of communication will be questioned, as the real becomes indistinguishable from the fake and trust erodes further in an already fractured world.

## Preparation Begins Now

Organizations need to enhance current technical security controls to mitigate against the threat of deepfakes to the business. Training and awareness will also need revamping with special attention paid to this highly believable threat.

In the short term, organizations should incorporate an understanding of deepfakes into the security awareness program and run an executive-level awareness program focusing on deepfakes.

In the long term, enhance or invest in identity controls and content management products to protect against deepfakes. Review authorization processes for financial transactions in the context of deepfakes. Finally, monitor deepfake activities in related industry sectors.

### About the Author

Steve Durbin is Managing Director of the Information Security Forum (ISF). His main areas of focus include strategy, information technology, cyber security, digitalization and the emerging security threat landscape across both the corporate and personal environments. Steve can be reached online at @stevedurbin and at our company website [www.securityforum.org](http://www.securityforum.org).





## 5 Steps to Ensure IoT Security Amidst CMMC Compliance

By Mike Raymond, Federal Sales Manager, Ord

Cyber threats against the U.S. and the Department of Defense (DoD) are very real, and efforts related to the department's Cybersecurity Maturity Model Certification (CMMC), released earlier this year, [are underway](#) to mitigate risks that affect the DoD and its contractors.

CMMC is meant to help more organizations fix low rates of compliance with NIST 800-171, the standard written to protect controlled, unclassified information (CUI), and it will become a requirement designed to permit only businesses with a valid certification to bid on and win contracts with the US Government. CMMC is a tiered model with the potential to impact every business in the [Defense Industrial Base](#) (DIB).

DoD contractors will soon be evaluated against this maturity model, which contains seventeen capability domains, each one encompassing a different area of [security baked into the DoD supply chain](#), adding a lot to the mix.

## IoT/OT security is a big piece of the pie

[CMMC](#) was created to help organizations understand the complexity and breadth of achieving a true security posture and to help mitigate security failures that have plagued contractors in the past.

Modern exploits and attacks usually cross IT/OT infrastructures at some point as everything is “connected” these days. This means that without IoT visibility and accountability, the entire network is potentially threatened, and CMMC auditors are very aware of that fact.

The good news is that the majority of CMMC domains apply to IoT network devices, as with asset discovery, threat detection, and incident response. These are part of any intelligent and comprehensive response package and securing IoT and other connected devices is an integral part of CMMC requirements.

The capability domains outlined in CMMC ([version 1](#)) are very broad and entail everything from physical security and personnel security, to asset management and any other applicable security control that the government can think of.

## 5 steps to ensure device security and compliance

As CMMC covers a lot of territory, it's critical that any organization wanting to compete and win lucrative contracts heed the call to ensure they consider their IoT/OT security vulnerabilities, as well as their other security controls and programs.

Below are five basic steps and considerations that can help set organizations on the right track to achieving CMMC compliance - specifically related to IoT/OT network devices - and ensure proactive accountability with the government.

### 1) Visibility is a crucial first step

You can't defend what you can't see, and you can't protect the enterprise if you don't know the totality of devices in your network. And because embedded IoT/ICS devices often do not support agents and may not be visible to IT teams or tools, it's impossible to prioritize risks, detect active threats already operating in an environment, or prove that a security posture is strong enough and doing its job.

All of those things are key to CMMC compliance across a variety of domains.

### 2) Understand device behavior

CMMC focuses on building a stronger cybersecurity posture in DoD supply chain contractors, requiring organizations to detail how they have built a strong overall approach for securing all network connected

devices. Part of having a sound security posture is to make sure that all devices only communicate with the internet as intended by mapping communications patterns and baselining device behavior.

### 3) Identify vulnerabilities

Key CMMC requirements focus on identifying and addressing vulnerabilities across all devices and infrastructure components. For networks with IoT/OT devices, that could mean common vulnerabilities and exposures, malfunctioning devices, or the presence of unauthorized ports or rogue applications.

CMMC requires the ability to detect and prioritize vulnerabilities, so there is a need to understand the risk profile for these devices and to identify anomalous behaviors such as a rogue or infected device communicating to a bad domain.

### 4) Leverage analytics

IoT and device threats are different from those targeting legacy IT systems and endpoints. Because of this gap in security, an organization may be required to incorporate IoT and device aware analytics to detect abnormal machine behavior that could help identify an attack.

Enhanced analytics also provide organizations with insights into device utilization to inform budgetary and maintenance decisions, allowing for better management of capital resources.

### 5) Prepare for audits

Like every other federal certification requirement, a third party is going to audit organizations for compliance, including IoT devices, device security controls, and asset inventory. To minimize the time and costs, it's imperative to have an accurate inventory and full visibility of every asset - including IoT devices - before an audit takes place.

Automation is essential to ensuring your CMMC compliance program remains accurate, ongoing, and up-to-date. With automation, organizations that need to meet CMMC requirements can quickly discover and categorize each device connected to the network. They can also easily understand device functions and behaviors, as well as devise effective segmentation policies for securing all of these devices. Automation eliminates human error, leading to better operational processes to address IoT device adds, moves, and changes.

## About the Author



Mike Raymond leads the [Ordr](#) Federal program and has over 25 years of experience working with the government and its agencies to secure their most valuable assets. Based out of Washington D.C., he previously held leadership positions with A10, Riverbed, Cisco, and IBM. Mike has a passion for developing emerging cybersecurity companies in the Federal market. Mike also Co-founded “No Boundaries,” a 501c3 non-profit assisting combat wounded veterans. Mike can be reached online via [LinkedIn](#) and through the Ordr website, [www.ordr.net](http://www.ordr.net).



## Under the SASE Hood: Key Components to Delivering Frictionless, Cloud-Native Security

*Under the SASE Hood: Key Components to Delivering Frictionless, Cloud-Native Security*

By Kaushik Narayan, CTO Cloud Business Unit, McAfee

While cloud services deliver on promised savings and convenience, they still remain a challenge to implement securely – as a recent study found that [76 percent of security professionals still find it difficult to maintain secure configurations in the cloud](#). How is it that something so beneficial can still present such a challenge for today's leaders?

One reason is that the enterprise perimeter has not only expanded, but also pushed the service edge to anywhere business takes you - or employees choose to go. Consequently, many organizations must up level how they protect cloud-based applications and data. Gartner recommends a Continuous Adaptive Risk & Trust Assessment (CARTA) strategy implemented in a [Secure Access Service Edge](#) (SASE) framework to secure the use of cloud applications.

Gartner predicts that [by 2024, at least 40 percent of enterprises will have explicit strategies to adopt SASE frameworks](#). The key business goal of SASE is to protect applications and data in the cloud by building a pervasive edge to safeguard against unwarranted or unapproved access. In turn, the business benefits of SASE are numerous. In addition to increased agility to meet new demands, a SASE solution can eliminate the need for organizations to scramble to implement new cloud services securely,

potentially opening the business to threats. Organizations can instead apply consistent data protection and threat prevention policies across their entire spectrum of cloud services, along with the devices and physical sites that access them.

### Building a seamless, integrated and secure network

Organizations no longer have the liberty, time or resources to research and ultimately implement disparate security tools and solutions for their network. As enterprise workforces continue to operate remotely across the globe, the dispersion of data is promised to increase even more. Maintaining control is of utmost importance as businesses struggle to meet revenue and keep operations moving forward - they may not have the time, funds or resources to combat a threat or breach.

By combining the components of a Cloud Access Security Broker (CASB), next-gen Secure Web Gateway (SWG), and data loss protection (DLP) technologies, organizations can ensure coverage over distinct control points that deliver a pervasive edge.

- A **CASB** can provide direct visibility and control over cloud-native interactions that are impossible to broker via a network/man-in-the-middle approach. This not only includes real-time data and threat protection for assets in the cloud, but also on-demand scanning to identify both sensitive data and malware. This can include files and messages in applications like Microsoft Teams and structured data objects in business applications like salesforce.com, ServiceNow, Workday, and more.
- A **SWG** establishes proxy-based visibility and control over web traffic, offering deep awareness of cloud activity and data interactions. This keeps users safe from accidental data loss or malware and delivers the most advanced threat protection against ransomware, polymorphic malware and other advanced attacks. Because proxy-based SWGs terminate traffic for inspection before sending it to its final destination, they also make an ideal orchestration point for seamlessly layering in new sophisticated threat protection technologies like remote browser isolation.
- A common **DLP** engine provides device-to-cloud visibility and control over sensitive data on personal or managed devices as well as data residing, transacted or transiting in the cloud. Data classifications are set once and shared across all enforcement points for devices, network, and the cloud.

### Enhancing safeguards with SASE

While important, SASE protection needs to be extended beyond user-to-cloud security – otherwise known as “front door” controls. Data and threats also need to be protected across “side doors” in the cloud – namely interconnected cloud applications and services. Finally, protection needs to be extended to control and management plane “back doors” within the cloud.

SASE provides yet another reassurance here, allowing for continuous and real-time evaluation of risks and data policies.

- **Connected application control** can enable your architecture to discover (and in turn authorize or deny) 3<sup>rd</sup> party marketplace applications or home-grown applications connected to each other via API. For instance, if a sales vice president were to connect and integrate Clari, a sales forecasting mobile application, to Salesforce.com and then pull the Salesforce.com data into Clari, SASE architecture can discover all such app-to-app connections and have granular policies around what scope of access should be allowed.
- **SaaS Cloud Security Posture Management (CSPM)** allows SASE architecture to assess and manage the native security configuration of your SaaS provider to avoid any mistakes or oversights in your deployment. Specifically, Microsoft Office 365 has more than 200 individual configuration settings that need to be evaluated for an appropriate enterprise security posture. For example, the default sharing permissions on SharePoint make shared links available to anyone in the world and never expire.
- **Sharing and collaboration control** permits SASE to control the transaction flow of sensitive data being shared inappropriately between users within the organization or external collaborators when using popular collaboration platforms such as Microsoft OneDrive, Microsoft Teams, Slack, and more.

## The Future for SASE

Long promised, cloud transformation is catching on at a time when enterprises increasingly rely upon cloud services to support their expanding distributed workforce. As organizations continue to rely on cloud-services to keep remote employees both connected and secure, leaders need a framework that can deliver on both fronts in the most frictionless and seamless way possible.

SASE delivers the framework needed to support remote workers, cloud adoption, and all the ways that risk is introduced in the modern, distributed network. Enterprises should look to the market for efficiency-driving consolidation in areas of synergy, such as data and threat prevention in a SASE framework, to secure their cloud transformation.

## About the Author

Kaushik Narayan is responsible for McAfee Cloud BU's technology vision and software architecture. Kaushik joined McAfee in January 2018 with the acquisition of Skyhigh Networks, the leading cloud access security broker (CASB) company where he was co-founder and CTO. He brings over 18 years of experience driving technology and architecture strategy for enterprise-class products.

Kaushik has been working in the network security and management space for sixteen years and a large part of that at Cisco systems where his last stint was as the Principal Engineer responsible for the Identity Services Engine product, which won the Cisco Pioneer Technology award. Kaushik helped drive key technology initiatives within Cisco in the areas of Policy Management, Cloud Centric Networking and Network Automation. He has filed several patents and has also been an active member at the IETF, where he is responsible for multiple RFCs.

Kaushik holds a Bachelor of Science in Electrical Engineering from Pune University and an MS in Management Systems from BITS Pilani. Kaushik can be reached online on LinkedIn and at our company website, <https://www.mcafee.com/blogs/author/kaushik-narayan/>





## The Limitations of SASE and Zero Trust

By Jayant Shukla, CTO and Co-Founder, K2 Cyber Security

Over the past several years, two industry buzz terms have really started to gain traction. [SASE \(Secure Access Service Edge\)](#) was a hot topic at this year's RSA in San Francisco and [Zero Trust](#) has been around a bit longer. As cyber attacks continue to increase and organizations continue to move to the cloud, both SASE and Zero Trust frameworks offer a way to give organizations additional security to their applications and data. Both frameworks focus on making sure that only verified and authenticated users should have access to assets in the cloud, and conversely, making sure unauthorized and unrecognized users have essentially zero access. However, SASE and Zero Trust are not a panacea for every network and application security need.

### Where SASE and Zero Trust Work

SASE and Zero Trust are ideal for applications that have migrated to the cloud, where the organization knows who the users will be and can identify and authenticate them. These applications are typically restricted to employees, third party contractors, and employees of partner organizations. These applications and their associated data have the benefit of being able to identify who the users are and use these new frameworks to make sure only these identified users have access to the applications.

### Where SASE and Zero Trust Miss the Mark

While SASE and Zero Trust work well for applications where it's easy to identify valid users, these frameworks fail to address two specific areas of concern. First, there are many applications and

workloads that must be left open and available to everyone on the internet. Retail and real estate are two prime examples. How many of us browse and comparison shop before we make an online purchase?

What would happen if we had to sign in and be authenticated just to take a look around? Likewise, most new house hunters take multiple virtual tours, usually anonymously, before they decide to take the next step with an agent. Validation and authorization typically are not possible for these open applications. Security needs to be addressed through a different approach than zero trust.

Open and freely accessible applications and workloads need higher levels of protection than those that already have been secured through layers of identity access security, especially as vulnerabilities can exist in any application or workload. It is especially important that these web applications are protected during runtime, when the applications are most targeted by cyber criminals. Static testing tools may miss vulnerabilities that only exist with the interaction of components during runtime.

### Even Valid Users Pose a Risk

In addition to the requirement for protection for open systems where identity is not possible, even authenticated users can pose risks. For the typical website, it doesn't take much for a cyber criminal to register an account on a site, or for cyber criminals to purchase credentials on the dark web and use valid credentials to attempt to hack a website. The security in place needs to monitor the activity of the web application and its activity on the web server, regardless of whether the end-user has been identified, authenticated, or authorized.

The real issue here is that no matter how much security you implement to regulate access based on identity, there will always be parts of the typical web application that are exposed to the entire world. And with no guarantee that you found all the vulnerabilities in your proprietary code during the development and QA cycle, or in the 3rd party and open source code you're using in your application, organizations need a defense-in-depth solution that includes effective advanced runtime security to protect the organization's assets in the cloud.

### Web Application Firewalls Alone are not Enough

There is sometimes a [mistaken belief that having perimeter security, like a Web Application Firewall \(WAF\) is sufficient for protecting a web application](#). Perimeter security may protect inbound and outbound traffic to the application, but it does not monitor the activity happening directly on the web application server itself or between application servers sitting behind the WAF. If a WAF misses an attack (like in the Capital One or Equifax attacks), then there's no way for the WAF to prevent any further damage on application servers behind the WAF, or to see the damage the cybercriminal is causing on the application server itself.

### NIST Recognizes the Need for Application Security

Application security on the application server (also known as [Runtime Application Self-Protection or RASP](#)) is [now recognized as a requirement by NIST](#) (National Institute of Standards and Technologies) for web application security as part of their recommended application security standards framework SP 800-53 in the latest draft revision. As part of the same updates, NIST also added a requirement for IAST

(Interactive Application Security Testing) as part of the same application security framework. It is a significant change to see NIST acknowledge these deficits to application security in the NIST application security framework.

With reports like the annual Verizon Data Breach Incident Report continuing to highlight web application vulnerabilities as the top reason for breaches, RASP as a requirement is needed more than ever. NIST's new guidance underscores that it is more important than ever for organizations to have a runtime security solution that validates the application execution and alerts to attacks in real time during the actual runtime of the application.

### DevSecOps also Needs Security Framework Attention

Another area in which both SASE and Zero Trust fail to fully address an organization's security requirements is [DevSecOps](#), the move to implement and test security earlier during the development of the application before it goes live. The enormous pressure to bring applications to market as quickly as possible creates tension with the security teams charged with protecting the organization's infrastructure and the application development team. Security needs to be a significant part of the framework during development, as well as in production.

Finding and remediating application security vulnerabilities before the application goes to production can help prevent breaches, and also help cut down on the lengthier and costlier remediation times that seem inevitable once an application has already gone to production. We have already seen during this COVID-19 pandemic that [many organizations are moving their applications more quickly to the cloud](#), and one by-product of this acceleration is often missed opportunities to test for vulnerabilities and security issues in the application code during development.

### Adding Security Focus During Development

There are several other specific security areas an organization should remember to focus on during the development process in addition to the basic requirements of SAST, DAST and IAST scanning and the guidelines for coding with security in mind.

1. Developers need to remember to look at data security holistically, meaning they need to remember to look at the bigger picture, keeping in mind all the components that touch the data and how they interact, and whether there are security risks in the way they hand off data from one part of the application to another.
2. Organizations also need to look at the security of their APIs, as it is another way that data can be accessed.
3. For those applications that are protected by identity and access, make sure strong authorization and authentication methods are incorporated securely
4. The most important reminder, incorporate vulnerability and penetration testing throughout the development lifecycle.

## Security is more than just SASE or Zero Trust

Even if you've decided to embrace SASE or Zero Trust as your security framework, be sure to recognize the limitations of these frameworks. Organizations need to make sure they have security incorporated throughout the application lifecycle in both development and in production.

Security needs to be implemented for applications in different layers, including directly on the application server to ensure you are protecting your most valuable assets in the cloud, regardless of whether these applications are protected by identity and access management tools that provide a zero trust framework.

Finally, the updated NIST guidelines are a great reminder to look at the latest technologies for application security, both RASP and IAST, and consider adding these to your organization's application security framework.

### About the Author



Jayant Shukla is the CTO and Co-Founder of K2 Cyber Security. Jayant is passionate about developing the next generation tools and technologies for securing modern compute infrastructure and breaking the perpetual catchup game resulting from advanced attacks and zero-day exploits. Prior to K2, Jayant was the founder of Trlokom, where he pioneered protection of applications using sandboxes and developed SpyWALL, the first commercial sandbox for the web browser. At Trlokom he also built the first solution for end-to-end secure communications between clients through multiple gateways and network address translation. Jayant holds a BS from IIT Mumbai and MS/PhD from Carnegie Mellon University.



## Measuring Cybersecurity Systems Durability

By Joseph Kirkpatrick, President, Kirkpatrick Price

Developing sound cybersecurity systems is a complex, multi-faceted task— but a crucial one. Not only do these systems help businesses meet their regulatory requirements, but they are intended to help the business succeed. Many businesses focus on the required aspects and simply forget that cybersecurity efforts are meant to achieve and support business objectives.

So, you've built in cybersecurity practices to your business structure. But once you've architected a cybersecurity system, how do you tell if it's resilient and effective? How do you know if it's working, before you find out the hard way that it's not?

### What Do Attackers Want?

The goal of a cyberattack is typically to steal the data you are responsible for or to take control of your systems. Have you ever considered how much your data is worth to a hacker? According to Symantec's 2019 Internet Security Threat Report, hackers can earn \$1-\$15 for groups of hacked email accounts, \$10-\$20 for certain hotel loyalty accounts, \$0.10-\$1.50 for stolen identities, \$0.10-\$35 for stolen medical records, and \$30-\$100 for a full ID.

While they're making money off of the hack, what will it cost your business? That depends on how quickly you identify and contain the data breach, who you will need to report to, what systems you will need to fix, and if you owe your customers anything. Think about Capital One's 2019 breach; when their cloud migration went wrong and the data of 100 million individuals was exposed, it cost them \$80 million in fines alone.

How can your organization develop and measure durable cybersecurity systems to avoid the consequences of a data breach?

### 3 Measurements for Durability and Resilience

Building a durable and resilient cybersecurity system that can stand up against attackers comes down to being proactive instead of reactive. When you can anticipate what your attackers are going to do and where they will strike, you're in a winning position.

I'm not asking you to overcomplicate or overdesign your cybersecurity systems – not at all. Mastering the basics may be effective enough for your organization. But there are three signposts for assessing if your cybersecurity systems are durable and resilient enough.

1. **Becoming Data-Centric:** When you implement cybersecurity practices at the data level, it makes it much more difficult to attack instead of difficult to defend. It means you're doing everything possible to cut the attacker off from the moment they begin the attack.
2. **Minimize Security Incidents:** If a security incident does happen, you need to minimize the impact that it will have.
3. **Continued Operations:** Accenture defines cyber resilience as the ability to continuously deliver your intended outcome despite adverse cyber events. When your Business Continuity Plan incorporates and addresses your cybersecurity systems, it will enable you to operate despite a security incident.

The NIST Cybersecurity Framework is an industry standard for learning how to measure your cybersecurity systems' durability through five steps: identify, protect, detect, respond, and recover. That Framework will be a great resource for developing innovative cybersecurity systems for new areas like IoT, mobile, and the cloud.

#### About the Author

Joseph Kirkpatrick is the President of [Kirkpatrick Price](https://kirkpatrickprice.com/). Kirkpatrick Price is a licensed CPA firm, PCI QSA, and HITRUST CSF Assessor, and most commonly provides advice on SOC 1, SOC 2, HIPAA, HITRUST CSF, PCI DSS, GDPR, ISO 27001, FISMA, and penetration testing. Joseph can be reached online on [LinkedIn](#) or at his company's website <https://kirkpatrickprice.com/>





# Defending Ever Expanding Networks and IT Systems

*Architecture at Scale is Needed*

By Trevor Pott, Product Marketing Director, Juniper Networks

How many systems must an information security professional defend? For most people, the numbers involved are abstract concepts. We think we understand them, but when confronted with them in a tangible form, we are constantly surprised by how much our perception differs from reality. Today even the smallest enterprises operate at scales that are simply beyond our ability as humans to truly comprehend.

There's a considerable gap in capability between small business IT and enterprise IT. For example, it is entirely feasible – and even reasonable – to meet all of a small organization's file storage needs using a bare-bones secure cloud storage provider like Sync.

It would be rank madness to do this for an organization with 10,000 employees. When you get to the scale of a military, there are strong arguments to be made that, if used as the organization's only storage solution, such an approach would constitute criminal negligence.

Scale matters. As scale increases, inevitably, so does complexity. There is no getting around this.

So how many systems must an information security professional defend? All of them. Given the scale of our increasingly interconnected world, that's quite the problem.

### **The evolution of network management and automation**

In the beginning, we managed everything by hand. Each system on our networks was a pet, loved and cared for, unique amongst all other systems. Eventually, the number of systems under management became too large for this approach to management, and so administrators turned to scripting. Common tasks were automated. Each administrator could manage a larger number of systems.

Eventually, people who had a large number of scripts packaged them into the first IT management applications, and manual IT gave way to management centralization. Scripting and #CommandLineLife was replaced by policies, profiles and templates. The number of systems a single administrator could manage exploded, and this is where most organizations are today.

Unfortunately, that scale thing keeps coming back 'round again. Despite the management magnification capabilities afforded administrators by today's policy-driven management applications, larger organizations are hitting very real scaling problems. 100% of administrator time is being tied up with policies, profiles and templates. Worse, in many cases the relevant IT teams are already at their maximum size: adding staff does little to increase the number of systems that can be managed.

### **Holistic architect wanted**

If there is one thing I would like every single network defender to keep in mind for the next decade, it is that there is no network edge anymore. The days of hunkering down behind our perimeters are long past.

"Hybrid IT" and "multicloud" – including all flavors of modifying buzzwords – is no longer novel. It is simply how IT is done today. A single organization's IT can span multiple infrastructures. On-premises IT blends neatly into infrastructure, software and services provided by multiple public cloud providers, while edge computing has quietly become an ordinary fact of life that we don't even pay much attention to anymore.

That dispersed, complex vision of a modern network exists without even beginning the conversation about mobile and remote workers, IoT, or the intricacies of interdependence that exist both upstream to our supply chain, and in the provisioning of IT to downstream customers. Unfortunately, in many ways, we are our own worst enemy, and we – both as IT practitioners and as vendors – create many of the security problems that will haunt us in the coming years.

Our innate need to categorize, to segment and to simplify may well be looked upon as the security threat of the 2020s. Our need to keep bringing complexity down to something we can fit in our brains stands in

the way of making holistic architectural – and thus security – decisions about the implementation of IT across these many and varied infrastructures.

### Think outside the network

The persistence of a siloed mentality, complete with an insistence on treating network segments as though they had perimeters (and as though those perimeters mattered) consistently limits our thinking. This puts us at risk. The compromise of the most minor system can lead to the compromise of significantly more important systems, and an inability to think holistically will ultimately lead to compromise.

Consider, for example, the caching of credentials. In many cases, merely logging into a system with administrative credentials once (and then forgetting to wipe the cache) is enough to leave a copy of those credentials on the system in question. That cache can be exploited by attackers to then compromise other systems that are part of the network and which share those credentials.

In this manner the compromise of a small edge node located on the other side of the world could result in a devastating compromise of central databases. What's worse, these sorts of compromises happen not because anyone along the chain of responsibility between those two systems does anything wrong, but because their areas of responsibility were so disconnected that the security implications of how doing something to A would affect B were never even considered.

### Machines managing machines managing machines...

This is the challenge of the 2020s. In order to cope with perpetually increasing scale we must begin to turn the definition and daily management of policies, profiles and templates over to machines. Machine Learning (ML), Artificial Intelligence (AI), and other Bulk Data Computational Analysis (BDCA) tools are a must.

Initially, these tools will make suggestions, and automate very simple tasks - the sort of things we're seeing from AIOps vendors today. But this is only the beginning; in order for the networks of tomorrow to even be possible, virtually everything that IT administrators do today must be done by BDCA tools without any form of human input.

This is not about replacing IT personnel. It isn't about an attempt to save money. The problems we're running up against are the limits of human capability.

Humans can only hold so many things in working memory at a time. Call it a RAM limit, if you will. We can only conceive of so many nodes on a network. We can only wrap our minds around so many permissions interactions. Enterprise networks are already bigger than we can fit in our brains, and that means we are running up against human limits in terms of even being able to architect these networks, let alone defend them.

For security to be effective, it needs to be holistically integrated into network architecture decisions. Network and security are inseparable, and the challenge of the next 10 years is going to be redesigning how we represent these networks for human consumption, and how we translate human-scale architectural and security decisions into the practical application of configuration for a literally incomprehensible number of systems that, even for small businesses, can span the entire globe.

Vendors will build – are building – AIs to take on the day-to-day. This, while fantastically difficult, is still the easy part. The hard part is convincing organizations – and certainly individual administrators within those organizations – to give AIs that kind of power. The jump from basic BDCA tools and suggest-o-tron ML agents all the way to AIs which make judgment calls about which policies to craft and apply is, psychologically at least, a pretty big deal. To say nothing of the legal and regulatory implications.

In the end, the latest strains of malware or who is hacking whom is not the problem. The problem – the real problem – is architecture at scale. What is needed are the tools to take the intelligent, experienced, and capable IT staff that organizations already have and empower them to operate at that level. The robots can handle the rest.

#### About the Author



Trevor Pott is the Product Marketing Director for Juniper Networks. He shares all the ways that Juniper's technologies can help organizations of all sizes defend their data, meet regulatory requirements, and advance the organization's own goals while doing so.

<https://www.juniper.net/us/en/>



## Reducing ‘Cyber-security Engineer Burnout’

*A first-hand experience of the workload challenges security engineers face, and how their employers can help to address them*

By Tim Bloomer, a Sales Engineer at AlgoSec

I’m sure we’ve all read about the global cyber-security skills shortage, but even so, the numbers are worth repeating. It’s [estimated](#) there are over 4 million openings that are not being filled – which is over a million more than 12 months previously. What’s more, the [cyber-security unemployment rate is at 0%](#). It seems that cyber-security professionals can get hired pretty much as quickly, or as often as they want. But that leads to the question: do they *want* to stay in the industry?

The latest Chartered Institute of Information Security’s [Security Profession 2019/2020 report](#) paints a bleaker picture. It found that 54% of IT security professionals had either left a job due to overwork or burnout or had a colleague who did. It also showed the potential causes of burnout and its consequences. Security budgets are not keeping pace with the rising threat level – and when security teams are stretched

during holidays or busy periods, 64% said their businesses simply 'hope to cope' with fewer resources when necessary, whilst 51% would let routine or non-critical tasks slip.

I have first-hand experience in the cyber-security trenches of working long hours, all the time. My wife would call me around 5:00 pm every day to remind me that it was time to come home. But it really wasn't the end of the working day for me. I simply looked for when I would have an opening at work big enough for me to drive home and open my laptop so that I could continue working. I did this for over 3 years, working 80 to 100 hours every week. That was my 'normal' 40 – 50 hours in the office, plus another 40 – 50 hours in a data center during maintenance windows, or working from home. It's only when I look back that I realize they were very stressful times, which impacted my time with the family as well as my performance level at work.

So why does burn-out happen? Here are a few of the contributing factors to the crazy hours and intense workload, based on my own experiences.

- **Unrealistic expectations** – every company seems to have projects based on perceived timelines. You might say that you can stand up an application (for example, a VM instance, networking, documentation, configuration, connectivity, etc.) in 3 weeks. This allows for everyone to work 'normal' hours and do their due diligence. However, most of the time, that 3 weeks was condensed into a week or less based on external factors outside of our control.
- **Understaffing** – with the “do more with less” mentality that companies have lately, we seem to all be understaffed. That doesn't mean the workload decreases, it only means our pressure increases and more hours and duties are added to your day. This has been made worse during the Covid-19 pandemic, with the huge changes enforced to organizations' networks to support mass remote working.
- **Doing more than one job** – when your co-workers leave the company, you often have to pick up the workload with your remaining co-workers while they look for a replacement. Numerous companies either do not open that position up for a replacement or only open it to a junior position even if it's the most senior person to leave.
- **Mental health** – often this is overlooked. Cyber-security engineers are under enormous amount of pressure to protect the company's assets and keep the business running. If everything goes well, no one notices; but if it doesn't go well, *everybody* notices. The stress has a lasting effect on us. I, personally, lost two people to suicide, a friend and a co-worker. While I cannot prove that was the reason, I can tell you that my friend definitely felt the pressure.

Now I know not everyone will burn out and walk away, or switch jobs. But how do you reduce that burnout rate, while maintaining your organizations' security demands and standards? This is where automation of security processes, such as planning and making changes to existing applications or provisioning new applications, comes in.

There's a common misconception that automation has a negative impact, because it replaces people. In cyber-security, however, the opposite is true – automation takes away the tedious manual 'grunt' work of making business-as-usual configuration changes, combing through security logs, and paper-based audit preparations. Looking at my bullet points on burnout above, here's how automation can help in each case:

- **Unrealistic expectations** – automation helps engineers and their employers make changes to migrate or provision an application in a few minutes, rather than taking days or weeks. There's no risk of manual errors or configuration mistakes. And because it logs every step of every change, automation even ensures that all the paperwork is done without complaining – speeding up processes and making the business more agile.
- **Understaffing** – automation removes the need for staff to research and review every change needed, as the solution flags any needs or exceptions. Automation also reduces the reliance on veteran experts and tribal knowledge, because the solution documents everything, helping to cover times when staff are on holiday or have left the company.
- **Doing more than one job** – you may still have to do more than one job, but at least you'll have a smart, automated assistant to help you get jobs done faster.
- **Mental health** – cyber-security engineers love to learn new technologies and implement solutions they know will help their organization in the long run. Using automation is a major step-change in helping organizations streamline and accelerate change processes, and in helping the staff responsible for implementing them. However, this should also be supported by other measures from the organization to help engineers achieve a better work/life balance.

In conclusion, automation solutions can deliver a true win/win, improving the organization's cyber-security posture while also helping its cyber-security staff with their workload, retaining their skills and increasing their motivation.

### About the Author

Tim Bloomer, a Sales Engineer at AlgoSec. He has more than 20 years' experience in developing and delivering complex solutions in diverse environments, working across both pre-sales and post-sales.

Tim can be reached at our company website [www.algosec.com](http://www.algosec.com)





## How to Avoid or Remove Mac Malware

*Today, Macs are more prone to hacking attacks than PCs. In this article, you'll find useful tips on how to detect malware on your computer and get rid of it.*

By Emma Brighton, a contributor to Cyber Experts and Cybers Guards.

If you still believe that [Macs never get viruses](#), we regret to inform you that this information is outdated and doesn't correspond to the reality. It's true that Apple computers are much better protected from malware than their PC counterparts. Nevertheless, Kaspersky's Lab experts claim that approximately 10% of the world's Macs are affected by a fake Adobe Flash Player updater that is actually malware in disguise. MacDefender malware became such a widespread problem that Apple Support dedicated a special section to it in its online guide. In this article, you will find useful tips on how to identify and erase malware from your Mac before it causes any considerable harm.

### The Definition of Malware

Malware is the generic term for all the software that you did not install on purpose and had no intention to use. The most common categories of malware are apps and programs that perform the following operations:

- Download items without asking for permission first
- Lock the screen of your computer
- Sneak your confidential information
- Allow hacker to seize remote control of your device
- Misappropriate administrator privileges
- Use your computer as a shadow bot
- Disguise themselves as legit software

The so-called "potentially unwanted programs" are currently the most widespread type of malware. On average, each Mac becomes a target for 11 of them. PCs, meanwhile, count 5.8 threats on average per each device.

### How to Identify that Your Computer is Affected by Malware

These are the most evident symptoms that signalize about the presence of malware:

- You notice numerous ads everywhere, not necessarily in your browser
- The computer freezes too often and reboots for no reason
- Unwanted apps download and launch automatically
- Programs update themselves suspiciously frequently, even though you did not enable such an option

If you spot any of these eccentricities, run an antivirus scan immediately.

### Where Could I Contract Malware

Hackers often mislead naive users by disguising malware as useful apps such as browser extensions, file extractors, multimedia players, plugins, codecs or even antiviruses. For this reason, you should download files exclusively from their developers' sites or from legal shops. BitTorrent, pirate sources and third-party sites spread malware en masse. And, of course, unknown attachments to emails from suspicious senders often contain harmful programs that install themselves on your Mac discreetly.

### How to Cure Your Computer

To get rid of the problem manually, type "[Activity Monitor](#)" in the Launchpad. Find the troublesome app in the Processes and quite the process by clicking the "x" button. Then return to the Applications folder, relocate the malware item to the trash bin and empty the bin. After that, restart the system.

This approach has two drawbacks. First, it helps only when you know precisely which app is the culprit. Second, the erased malware might have left traces all over the memory of your device, so the same problem might arise again pretty quickly. To prevent such a scenario, install a powerful antivirus.

## The Functionality of Antiviruses

Modern antiviruses are able to detect hundreds of threats, including viruses, malware, phishing attacks, cryptocurrency miners and so on. After you install such an app, please update it regularly so that it is able to track all new hacking inventions. If malware has already infected your computer, the antivirus will deeply scan all the system, identify unwanted items and delete them, leaving no dangerous traces behind.

But most important, such software will detect malware before it targets you and ward off its potential attacks. Antiviruses of the latest generation are proactive programs that not only clean your device of the harmful components but also free its disk space and boost its productivity.

One essential step that you might need to manually is [to delete all of your browser extensions](#) and then reinstall the useful ones one by one. Advertising malware often disguises itself as helpful extensions for diverse purposes.

## What to Do If the Mac Still Doesn't Function Properly

If your antivirus is out of date or you resorted only to manual cleaning, your device might keep breaking down even after you erase the questionable items. In this case, try the subsequent measures:

1. Log out of the account you are currently using and log into a new one. Then, do a full system cleanup.
2. Save all the necessary files on an external hard drive or cloud storage and restore the computer with the help of the Time Machine. This will bring the device back to the moment when it was still not infected.
3. Install the freshest versions of all your apps and programs plus the latest operating system.

Even if you are not a geek, you can complete all of these tasks yourself relying on step-by-step instructions from the internet.

## Preventive Measures

Once your Mac is safe and sound, try to stick to precautionary measures while surfing the web next time:

1. Cover your webcam
2. Replace passwords with passphrases and save them in a credible password manager
3. Enable anonymous mode in your browser
4. [Create a bootable SD card](#) for emergency cases
5. When the system starts a dialogue, don't agree recklessly. Read attentively all the dialogue boxes before pressing OK

Also, learn to tell the real antivirus alerts from the fake ones. It might happen so that you see a pop-up window or a browser page with a warning. It tells you that your device is infected by malware that can be cured exclusively by some advanced antivirus. You hurry to purchase this antivirus following the link from the pop-up window — and this is how hackers get hold of your payment credentials. That's why you should install only the regular notifications from your antivirus.

## Conclusions

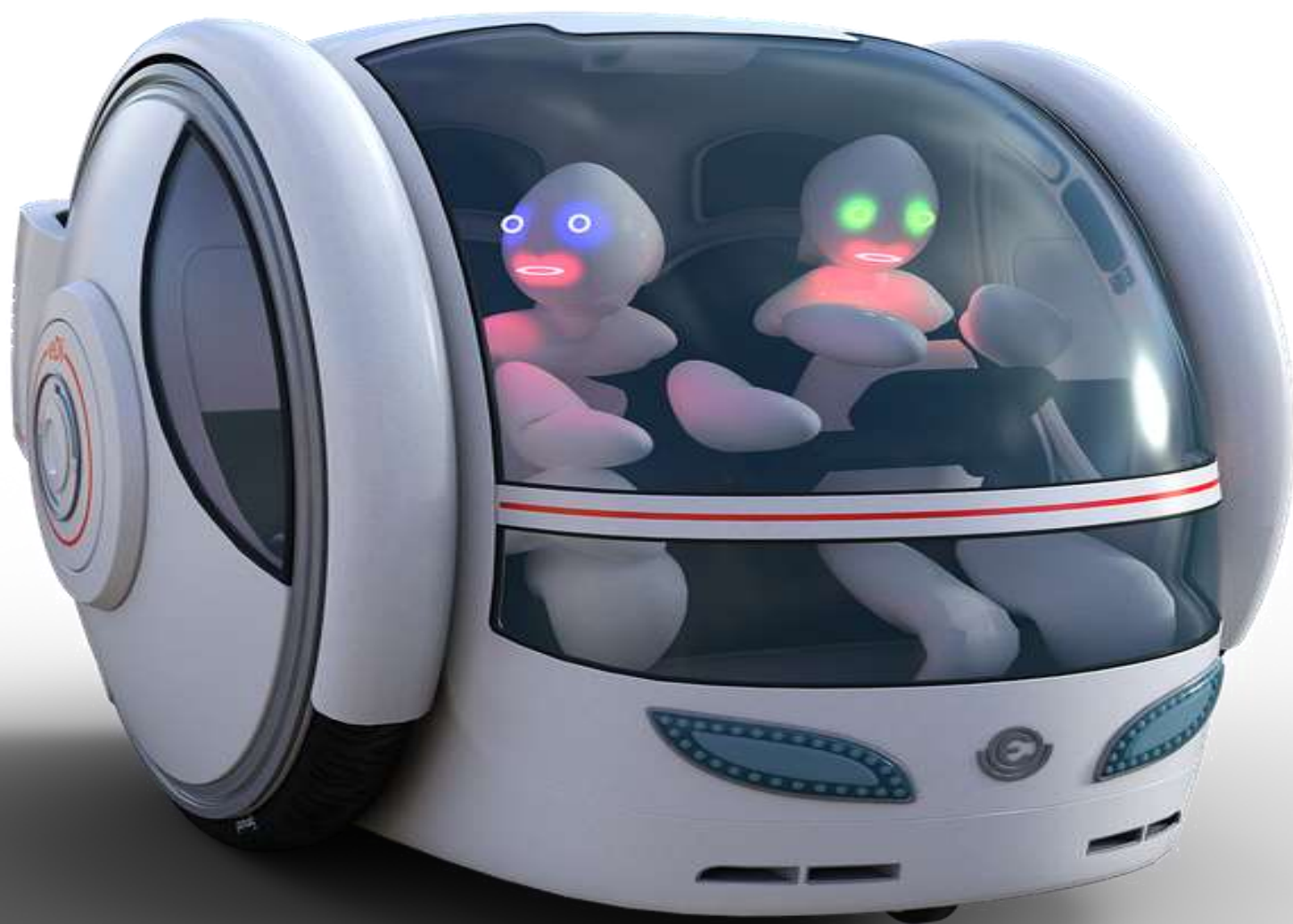
Hopefully, the information from this review came in handy and now you know how to detect malware and get rid of it. The most crucial tips are to never download pirated content or legit content from unknown sources, regularly run malware scans and to keep your antivirus enabled. Today, malware targets Macs more often than PCs, so you should keep vigilant and systematically upgrade your software.

### About the Author



Emma Brighton is a cybersecurity enthusiast and Mac aficionado. She's passionate about covering topics like Mac cybersecurity, Mac tips & hacks, Mac's how-to guides. He is a contributor to Cyber Experts and Cybers Guards.

Email: [emma.brighton986@gmail.com](mailto:emma.brighton986@gmail.com)



# How To Protect Your Self-Driving Car From Potential Cyber Threats

## Automotive Cyber Threats

By Okonkwo Noble, travel enthusiast, Writer, and Electrical Electronics Engineer, Limo services U.S.A

With the increasing reliance on technology in most global economic sectors, the transportation industry has experienced paradigm shifts like never before. The constant struggle for the topmost position concerning innovation in the automobile industry has led to the emergence of self-driving cars and electric vehicles.

These represent only a fraction of the effects of technology on the industry, perhaps, the most notable effects.

[Self-driving cars](#) are exactly what the name suggests—also referred to as autonomous vehicles, driverless vehicles, or robot cars. Self-driving vehicles use sensors, radars, GPS, and other technological platforms to commute effectively with little to no human intervention.

Thanks to these platforms, humans have been able to unlock a whole new level of comfort and exquisiteness. Depending on the automation level, we never have to worry about stress and fatigue, which are products of long drives.

### Why Self-driving cars are important

The [year 2020](#) was set to be the year for mass-deployment self-driving cars by most automotive giants. Tesla had tried to grab a huge market share by attempting a large scale release two (2) years [earlier \(2018\)](#). However, that did not exactly work out.

What makes these cars so important, and why is every significant player in the automotive industry giving this much attention to these driverless vehicles?

While driving has indeed proven therapeutic for some, most of us would prefer extra minutes to take a final look at the document from last night, or perhaps a few minutes nap while on a commute to class. Self-driving cars come with juicy pros regardless of pundit views.

For example, self-driving cars have proven to be an effective means of reducing road accidents. The resultant effect, a reduced number of casualties. Most car accidents are resultant effects of human error. Therefore, it only makes sense that technology, which is less susceptible to mistakes, be used instead to mitigate these unfortunate occurrences.



These cars use [ADS technology](#) to ensure road safety and to alert drivers of potential dangers. Self-driving cars also help to reduce traffic congestions and are widely acknowledged for being eco-friendly. They help to reduce environmental pollution by reducing car emissions since most of these vehicles are electric.

## Self-driving cars and cybersecurity

While self-driving vehicles boast of multiple advantages, as with most innovations, it brings forth its own set of challenges. One of the major problems has to do with cyber threats.

Since self-driving cars use the Internet of Things (IoT), software algorithms, IoT connectivity, and other technology-dependent on the Internet, they are highly susceptible to cyber threats. They are essentially internet cars, and all the security challenges faced by internet users equally apply to them.

## Protecting your self-driving car from potential Cyber-threats

Completely disregarding the importance of self-driving vehicles due to their potentially high susceptibility to cyber threats may be likened to throwing the baby along with the bathwater.

While it is true that with increased technology comes increased risks of cyber threats, it's possible to mitigate cybercrimes by implementing preventive measures.

The first step towards protecting your self-driving car from potential cyber threats is by keeping your passwords safe. You may need to activate features such as two-factor authentication to mitigate the risks of cyber threats further.

Automated cars, like your personal computers, are personalized and are made to be accessed by authorized individuals only. One easy way for hackers to perpetuate their criminal activities is to get a hold of your passwords.



To ensure that you're not giving cybercriminals easy access to your automated vehicle, be sure not to share your passwords with anyone. Also, ensure that your passwords are strong enough by meeting the [minimum suggested password length](#) and combination suggestions.

Another way to protect your self-driving car from potential Cyber threats is by purchasing your automated cars from credible sources. Some manufacturers are known to take cybersecurity more seriously than others. These manufacturers will provide all the necessary security apparatus to curb cyber threats.

It's always important to understand the values that drive your car manufacturer, and ensure that all security measures to forestall cybercrimes against your car are made available by the manufacturer. Also, regularly update the applications (OTA) on your automated car system as frequently as required. The new updates usually come with increased and updated security measures to frustrate cybercriminals' activities.

The use of dedicated short-range secured communication channels (DSRC) also reduces the risk of cyber threats. However, this poses certain challenges since the encryption of the data would result in additional production/maintenance costs.

## Conclusion

It's important to note that cyber threats cannot cease to exist. They can only reduce. Therefore, all self-driving car users are encouraged to actively lookout for potential cyber threats and report any successful threats to the relevant authorities.

## About the Author

Okonkwo Noble understands the need for sustainable travel. He is a foremost travel enthusiast, Electrical Electronic Engineer, and adventurer. He also volunteers as a part-time English teacher for Internally displaced children.

He's a writer for [Limo Services USA](https://limoservicesusa.com/).

Okonkwo can be reached online at our company website <https://limoservicesusa.com/>





## The Impact Of Blockchain & Crypto On Cyber Security

By Jesús Cedeño, Senior Editor, [cryptocoinsociety.com](http://cryptocoinsociety.com)

These days many people (especially if they're more or less tech-oriented) have heard about cryptocurrencies and blockchains. Even if they don't fully understand these terms, think that Bitcoin is the only cryptocurrency or only know that blockchains are the "thing that makes Bitcoin work", they have heard or read about these terms. Cryptocurrencies have their supporters and detractors, but they are reshaping the world of finance. Blockchain technology is also having an impact on many sectors, not limited to that of cryptocurrencies themselves. Blockchain applications are being developed for education, trade and other areas. But what about cyber security? What is the impact of blockchains and cryptocurrencies on cyber security? Read along to find out more about what's going on in this sector.

### Just what is a Blockchain?

Let's start by explaining what a blockchain is to make sure we're all on the same page. We probably all know what a ledger is. Ledgers have been around for millennia as records of transactions. Some examples of ledgers in the modern world are the accounting logs that all businesses keep. Blockchains are, at their core, ledgers. So what makes them different?

Unlike a business's accounting ledger, which is usually stored in a single, secure location, blockchains are *distributed* ledgers. This means that there are many copies of the ledger stored on many computers

across a network. And the blockchain itself has ways of assuring that all copies of the ledger are identical to each other. This keeps the information stored on the blockchain immutable and protected from crashes, attacks or other after-the-fact modifications.

The anonymous, secure nature of blockchains has had both positive and negative impacts on cybersecurity. Let's take a look at both.

### Blockchains and Cyber Security: The bad

Although cryptocurrencies are far from the only application for blockchain technology, they were the first successful implementation of blockchains. Specifically, Bitcoin was the first such implementation. Bitcoin offered users a secure, reliable, anonymous way to transfer funds. And anonymity was the first major factor that drew many users to Bitcoin.

Of course, any normal, law-abiding, by-the-book citizen anywhere in the world can have perfectly valid reasons for wanting to make anonymous financial transactions. Personal security can be one of them; if you have a lot of money, you don't necessarily want everybody around you to know that. But the flip side of anonymity is that it is also desirable for illegal purposes. In the early years of Bitcoin, many black market sites like Silk Road would accept payments only in Bitcoin. In more recent years, cryptocurrencies are increasingly being used as forms of payment in ransomware attacks. In these cases, anonymity means that identifying and prosecuting the ones responsible is extremely difficult. Cryptocurrencies have also made money laundering easier.

This downside of cryptocurrencies' anonymity is the reason why many exchanges are being forced to comply with KYC policies if they want to keep operating. So, each user on these exchanges is being asked to provide proof of identity and/or residency to use the exchange's service. Even localbitcoins, a long-time haven for anonymous Bitcoin transactions, has recently started applying KYC.

Of course, there are many services that you can currently use to protect your personal data and enhance your cyber security and that don't work with blockchain technology. But these systems have a drawback... they are centralized services, meaning that they are hosted on a particular server. This makes the security systems *themselves* targets for hackers and other ill-intentioned people that want access to your data. Though far from a security system, Facebook is a good example of what can happen. In October 2018 a hack on Facebook's servers exposed personal data on over 30 million accounts.

### Blockchains and Cyber Security: The Good

Looking at the bad things just mentioned above, you can probably notice something important. These downsides are really related to cryptocurrencies (or, more specifically, the ways some people have chosen to use them) and *not* to blockchains themselves. There are three features in blockchains that can make them useful for cybersecurity: decentralization, immutability, and transparency.

In a decentralized system, by definition, there is no single main server. All information is shared between all the participants in the system. These are the *nodes* that host the blockchain. New nodes can be installed at any time, but it means downloading the entire ledger so every node has the exact same information. Besides sharing the same information, the nodes work together to ensure that the data is intact; unchanged (here's where the immutability feature comes in). If there is no single server and all

nodes are constantly verifying the information, this makes the system very secure. A potential hacker that wanted to alter any data would have to hack most of the nodes in the blockchain *at the same time*. This is near-impossible.

Having the data spread out over many nodes also improves availability. Since there is no single server, then saturation because a lot of people are trying to read the data at the same time is less likely and decreases, even more, when new nodes come online.

Transparency is something that can be seen as an advantage or a disadvantage, depending on the situation. All transactions on a blockchain are publicly visible, meaning that the data on the blockchain isn't usually encrypted. If you go to a Bitcoin blockchain explorer like [btc.com](https://btc.com), you can see every transaction that has ever occurred on that blockchain. For example, you could see that on August 30<sup>th</sup>, 2020, at 12:35, 0.13098231 BTC was sent from the wallet address 33ACizvWTKqBGCKFdM2DEhVRp4qxeWcBPw to wallet address 13UsFi8MnqmgxBU31T9uWA5ocXLZkeNPQy. The transaction is visible to all. We just don't know who owns those wallets. For all we know, it could be a user sending Bitcoin from his personal wallet to an exchange wallet.

Even though the data isn't usually encrypted, that doesn't mean it *can't*. Some blockchains are designed to encrypt the data, and data can also be encrypted by an app before storing it.

So blockchains offer an available, secure, hack-proof way to store data. And this can be used to improve cybersecurity in several ways. Let's take a look at some of the possibilities.

## Blockchains and Cyber Security: What's being done now?

So there are a lot of *theoretical* benefits of using blockchains for enhancing cybersecurity. But it's not just on paper. There are five key aspects of cybersecurity that are exploring the benefits of blockchains right now:

### 1. Safer DNS

If you aren't too into the technical aspects of the web, you probably don't realize that the addresses for all the websites you visit, like Facebook, Wikipedia, Google, The New York Times, etc. are actually IP numbers like 207.86.123.34. But can you imagine browsing the web like that? Having to remember the IP numbers for all the websites you visit regularly (instead of easy website names like [www.google.com](https://www.google.com)) would be too much of a hassle. That's where Domain Name Servers (DNS) come in. When you type [www.cyberdefensemagazine.com](https://www.cyberdefensemagazine.com), your computer asks a DNS where to go. The DNS knows the IP number for the site and directs your browser where you want to go. Imagine what can happen if someone hacks the DNS. They can alter it so that when you type in an address, you will be redirected to some other site. They can make you enter your bank information at a site that looks just like your bank's website but is actually under their control. They can make whole websites unavailable for hours or days at a time. These are what are known as DNS attacks or Denial of Service (DoS) attacks.

If the DNS data were stored on a blockchain instead of specific servers, that would make these kinds of attacks near impossible. This is something that is already being looked into. DoS attacks are a big problem in cybersecurity, but their days just might be numbered.

## 2. Secure Private Messaging

Instant messaging is great. Apps that let you send messages, audio, photos, and videos instantly, or even make voice or video calls to anywhere in the world have completely changed the way we communicate with each other. But this improvement came with an initial cost: data security. There were many cases of stolen data in the early years of instant messaging platforms like WhatsApp. While it is true that some apps like Telegram and WhatsApp itself have implemented end-to-end encryption to secure user's data, other services are looking to blockchains for enhancing security and create a framework that would even make cross-platform messaging possible. Users can even be rewarded with crypto tokens for using these apps. SENSE chat and FortKnoxter are some of these early, blockchain-based instant messengers.

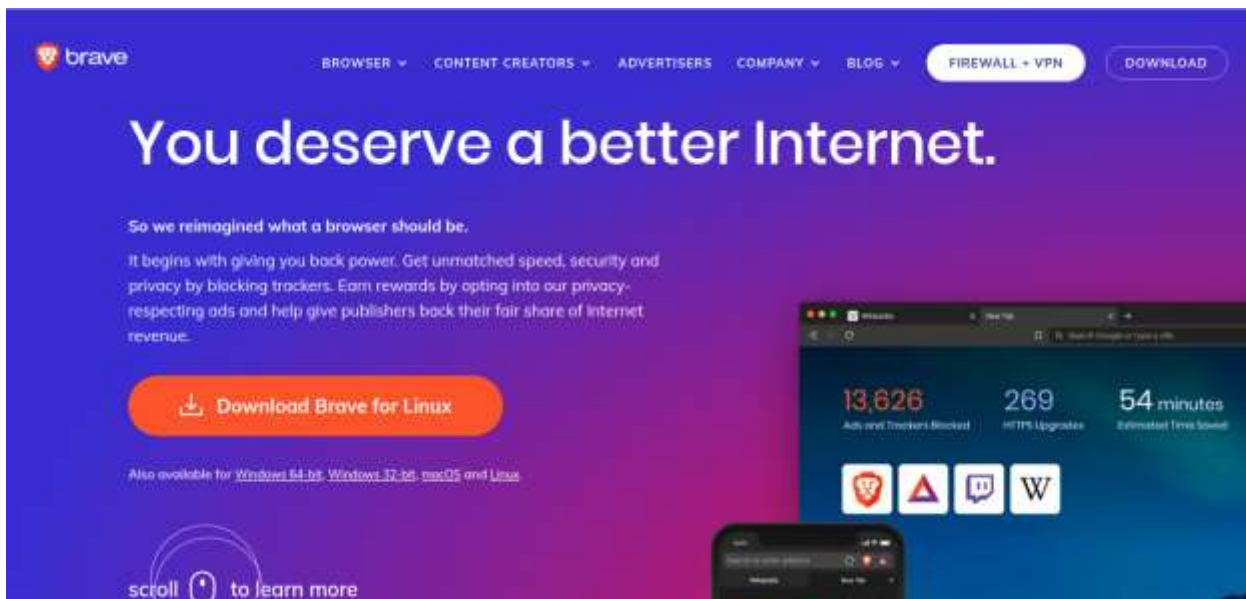
## 3. Decentralized Data Storage

Having online backups of your personal data can be a life-saver. If your computer ever crashes, needs to be formatted, is stolen, or simply goes toes-up because of an electrical failure, your cloud storage is there for you. Just stop for a second and think about what potentially valuable information is in your Dropbox or OneDrive account. I know of a fellow crypto enthusiast (who honestly has more enthusiasm than technical know-how) that used to keep his private wallet keys in *unencrypted* text documents on OneDrive. Businesses can store sensitive information about *millions* of clients. Losing that information would be a disaster. But these data storage services are all centralized, meaning that a hacker knows where the information is stored, and those servers are highly attractive targets.

There are projects in development, like the Apollo Data Cloud, that use blockchains to ensure the security of the information stored in them. The data isn't usually stored on the blockchain itself, but spread out over many storage nodes using protocols like the InterPlanetary File System (IPFS). This way there is no single entry point to the data and each file is split into pieces that can be on any node. This makes it a lot harder for anyone to break into your valuable personal information.

## 4. Safer, More Fair Web Browsing

If you're a casual web browser, you're probably not aware of how much valuable information you're actually sending out. Your web browser keeps track of your history, including what you do after you visit a particular site. Websites use trackers to know what kind of ads you click on and which ones you don't; what pages you stay on longer and which ones you barely glance at before moving on. This is all valuable information that companies can sell. There's also the issue of rewarding content creators. Have you ever visited a web site and wished there was a way to tip the content creator directly. Maybe it's a new YouTuber that still doesn't have enough followers or views to start receiving rewards directly from Google but is putting out good content. If so, you might want to check out Brave browser. It's a more private browser with built-in tracker blocking and that enables tipping via the Basic Attention Token (BAT) cryptocurrency. You can read more about it in this [Brave Browser review](#).



## 5. Safer “Smarts”

These days, the internet isn't only on our computers or smartphones and tablets. Each day there are more "smart" devices. Now we can have smart TVs, refrigerators, air conditioners, washers, toasters and a lot of other things. I'm pretty sure smart pencils and pens aren't too far away at this point. This is what is known, very appropriately, as the "Internet of Things", or IoT. While these IoT devices can bring a lot of benefits, they also bring risks. There's no way of knowing if the manufacturer of your new smart toaster is taking the trouble of making it secure enough. And each device connected to the internet is a potential entry point for hackers, so if one of them managed to hack your toaster, they could then have access to your whole network.

Implementing IoT blockchains could help make smart devices a lot "smarter". The blockchain could continuously monitor all the nodes and learn what behaviour is expected from each device. So if your microwave suddenly starts asking for the feed from your smart camera, this suspicious activity could be shut down without having to send a request to any security server.

## In Conclusion...

Cryptocurrencies have somewhat of a bad rep in certain circles. Lots of people don't understand them and lots of governments don't trust them. To be fair, there are some valid reasons for that mistrust. But those reasons are related to the way some people have used cryptocurrencies for many kinds of scams and money laundering and not to the cryptocurrencies themselves. And they certainly don't apply to the blockchain technology behind them. Blockchains can be used for a lot of things and they can certainly become a major force for enhancing cyber security. The main advantage of blockchains as applied to security systems is their decentralized, self-verifying nature. With no single point of entry and needing to compromise possibly hundreds or thousands of nodes at the same time, hacking blockchain-based

security systems is nearly impossible. The potential impact of blockchains and cryptocurrencies on cyber security is huge and I, for one, am excited to see what the near future will bring. How about you? What excites you most about blockchain-based security systems? What concerns you most?

#### About the author



Jesús Cedeño is the senior editor of Crypto Coin Society. He is a doctor turned cryptocurrency and blockchain enthusiast who loves sharing his thoughts on everything crypto, blockchain, and decentralized technology related in an attempt to help simplify the subject matter in order to make it more accessible to the masses. Jesús can be reached on LinkedIn (<https://www.linkedin.com/in/jesuscedeno73/>) and at our company website <https://www.cryptocoinsociety.com/author/jesuscedeno/>.



## The Serverless Security Machine

By Art Sturdevant, Director of Operations, Censys

Servers are bullshit. They require constant maintenance, monitoring and tweaking. As a security practitioner, regardless of where your team lands on the org chart, you're being charged with securing an ever-evolving landscape against all internal and external threats. The time required just to keep basic services functioning is daunting and now, you're probably working even harder to secure and protect your remote workforce, all while working from home. While the amount of time required to evaluate and respond to threats is constantly increasing, security budgets, personnel, and tooling are not being adjusted at the same rate or are only adjusted in response to a particular threat or incident.

Given that time is at such a premium, why is your team still deploying infrastructure that requires constant supervision? With all these demands on your team, now is the time to move to a serverless infrastructure.

Traditional servers are great in that they can be provisioned and run forever, but unless the server is under constant load, you're likely wasting money and resources managing it. Teams are using all kinds of complex tools to deploy new servers, apply configurations, update users, and apply security patches and still, there are servers that live outside of these tools or silently lose connectivity, never to be

managed again. Every time a new server is deployed, you're really managing three different problems -- server updates, software updates, and code updates.

Server updates can be risky, which is why large organizations employ a CAB to approve changes and security updates. Teams schedule downtime or work to deploy across zones without interruption, but because these changes apply to the entire operating system and are likely not authored by your team, it can be difficult to anticipate how the change will affect the service you're trying to manage and even tougher to debug.

Software updates are easier to manage and are likely better understood since the code was written by a team you know. If you're already familiar with CI/CD models, then you might already be well suited to the serverless lifestyle. Code changes go in, peers review the changes, and the code is deployed in a seamless fashion. It may not always be that flawless, but debugging code you wrote is almost always easier than debugging operating system changes or behaviors.

By moving to a serverless architecture, you're removing all the issues around software and security updates, system breaches, user provisioning, system health monitoring and more. These issues are no longer your team's problem because you're only responsible for deploying code that runs. All of the system updates and application updates used to run the code are maintained behind the scenes.

Moving to a serverless architecture doesn't have to be "all or nothing" in order to maximize your time investment. For example, a good first step might be to evaluate the servers in your environment that only perform one task or those that are heavily underutilized. A good sign that you've identified a solid candidate is when you find a service/server that is performing a very event-driven task such as a server that collects and ships logs from various SaaS services or systems. If the service operates on a schedule or cron job - you've got a perfect first candidate!

Most users start by moving to a containerized version of their code. Docker is a popular tool and is available on nearly all platforms. Once you've containerized your code, simply deploy it to a docker host, or a cloud service capable of running containers. Every major cloud provider has support for running containers in production environments.

If you're looking for something that is truly serverless, consider evaluating a cloud provider's "Function as a Service" (FaaS) offering. These come with a slight learning curve but also a lot of great features including a deployment model that is easier than containers. FaaS is a model to deploy code (think a python script) and to run it over and over in response to an event. A common scenario might be to fire a chat notification if a storage bucket becomes public, or to update TLS certificates on specific hosts as they near expiration. A serverless architecture can allow your team to quickly deploy proof of concept applications, or full blown applications to manage all corners of your security program.

Although serverless assets can and often do reduce the administrative burden of managing servers, there are some limitations to be aware of as you adopt this new model.

- *Potential Learning Curve:* Containerization and FaaS both require a new skillset. If for no other reason than to get deployment working in a seamless fashion from your Continuous Integration/Continuous Deployment tool. Once your team understands the requirements to deploy a service, this is a very repeatable process. Deploying your first serverless project is likely an afternoon project for you or your team.
- *Additional Expense:* Misconfigurations can result in higher costs than a traditional virtual appliance in the cloud. However, even at the increased expense, consider that your team doesn't need to manage updates, security patches, or worry about attackers compromising the server. It is a good idea to understand cloud pricing models before automating these tasks to avoid a surprise at the end of the month. Functions should be designed to read each word in the book, not each letter and not the whole book either.
- *Increased Latency:* Depending on the cloud provider, FaaS and containerized services could result in increased latency because of the "cold start time". However, once the service is started up, running a second or hundredth service should be fairly quick.
- *Task Timeouts:* Most cloud providers limit the amount of time a FaaS task can run before it is terminated. A common timeout is between 30 seconds and 15 minutes. If you have a long-running task, you might want to consider breaking it into smaller tasks or moving to containerization since container deployments do not have the same timeout limitations.
- *Updates Require Redeployments:* To update containers with new code or new software packages, you'll need to redeploy the container to the cloud. If you're updating a FaaS function, you'll just need to redeploy the code. While this might seem like a headache, if you update and deploy using CI/CD tools, this is actually pretty straightforward. Most clouds allow you to deploy with a canary model - meaning you can direct some traffic to your new code and some to your old code and keep adjusting until you're confident that you haven't introduced any unexpected problems.

Help your security team alleviate the administrative burdens of managing servers by moving to a fully serverless infrastructure. It may seem daunting at first, but once you have a couple of services or workflows moved over, you'll wonder why you didn't make the move sooner.

### About the Author

Art Sturdevant is the Director of Operations at Censys. An Information Security professional with over 15 years experience, Art maintains a passion for open-source projects, entrepreneurship, and the outdoors. Before joining Censys in 2019, he was a Sr. Security Engineer for Duo Security and is also a graduate of Central Michigan University where he graduated with honors with a Bachelor of Science in Business Administration. To learn more about Censys, visit [censys.io](https://censys.io) or email Art at [art@censys.io](mailto:art@censys.io).





# ENDPOINT SECURITY

## Why Endpoint Protection Should Be a Security Priority

Understanding common endpoint protection mistakes will better prepare your business to combat cyber threats

By JG Heithcock, General Manager of [Retrospect, Inc.](#), a StorCentric Company

For many small to medium-sized businesses (SMB), focusing on security can be a costly endeavor. SMBs generally can't afford the luxury of implementing a high-end security suite to protect their vital data and infrastructure, let alone react to a cyber attack that occurs due to a lax system of protection. While your business might run on servers, your employees move the business forward on endpoints, which include laptops, desktops, tablets and virtual environments. It's easy to take those desktops and laptops for granted, until something happens and you realize the need for data insurance to prevent downtime, data loss and the expenses they incur. The list below explains a few reasons behind common endpoint mistakes and how to avoid them.

### You're Using a File Hosting Program Such as Dropbox

File hosting programs, such as Dropbox, Google Drive and Sharepoint, are great tools for business synchronization. These programs might also seem like great backup systems, until the endpoint is lost.

Your employees are focused on completing their tasks and as a result, don't always ensure every necessary file is saved to the file management system. Employees may start working in a document that is saved to their desktop or personal drive before uploading it to the shared system, waiting until the document is ready for review or collaboration. Waiting to add files prevents sending multiple notifications every time a change is made and allows the employee to work on the document without interjection. While the employee's reasons for waiting to add a document to a shared drive are well-intended, this can present problems in the long run.

When a set of documents goes missing, the business loses time and money spent recreating or recovering the set of documents, not to mention the downtime spent recreating the user's personalized environment. Working to reverse the effects of missing documents can take anywhere between a few hours to a few days, ultimately costing the business for having to shift priorities and fall behind on other tasks. At the end of the day, Dropbox and its contemporaries are file syncing tools that should not be used for endpoint protection.

### **Your Imaging Tools Need a Backup Solution**

The purpose of imaging tools is to help users quickly deploy a complete environment to a set of endpoints. With a single image, every environment has the necessary updates and applications without having to manually manage every instance.

Using endpoints for web-based applications and work, or editing documents that live on your server might make sense. However, if your workforce has personalized environments or does local work, it makes your business prone to losing work and increases the opportunity for downtime. Reimaging might only take an hour, but recreating work or personalizing an environment takes days, sometimes weeks.

In order to prevent downtime or energy spent recreating personalized work environments, it is crucial to invest in a backup solution that works well in tandem with imaging tools. You can use the base image as the template and then protect only the user's folder where work and application settings are stored. When something does happen, you can reimage then restore without worrying about lost work and experiencing minimal downtime.

### **NAS Folders Should be Used for Document Sharing, Not Data Protection**

A Network Attached Storage (NAS) shared folder serves as an excellent tool for keeping your business running on-premise and in sync. Similar to Dropbox and Google Drive, NAS folders are often treated as a backup system however, a NAS shared folder is a file storage tool, not a data protection strategy.

Rather than relying on NAS folders for your backup strategy, use them to share work between users and ensure employees have access to each other's work, taking advantage of the quick access they provide on your local network.

## Invest Now to Save Time and Money Later

For SMBs focused on sales and keeping the business running, security and data backup are often seen as a distraction and are left behind, despite the fact that maintaining each is essential to keeping a business afloat.

Being short on time is an unavoidable reality for SMBs. Larger businesses can absorb disruption, but downtime and lost data can leave a small business struggling to survive. If you are the owner of a SMB, it would be wise to invest time in a backup solution to protect your endpoint upfront, avoiding time spent on disaster recovery later. When you think about it, if you lose some or all of your data, you'll spend time focusing on ways to recover it, rather than spending precious time on growing your business. You have insurance for your car, your house, your health and your business. Your data deserves insurance, too.

Businesses should also consider making an investment in quality backup solutions that fit their unique needs as early as possible. Many cloud-based backup solutions operate on subscription-based payment models for their 'as-a-service' offerings, which helps with flexibility and scalability. By allocating money towards a backup solution from the first day, businesses will be better protected against ransomware, natural disasters and human error, all of which can yield high costs to the business and determine the survival rate of a SMB. By investing time in research and drafting a budget, SMBs can find the right solutions priced for their needs.

### About the Author



JG Heithcock is the general manager of [Retrospect, Inc.](https://www.retrospect.com/), a StorCentric Company. He has 18 years experience in the storage and backup industry. JG was the User Experience Architect at WildPackets (now Savvius) before coming back to recruit and manage the Engineering team for Retrospect at EMC. JG was one of the founding members of Retrospect, Inc, and is now General Manager at Retrospect under the StorCentric family. JG can be reached online at <https://twitter.com/jgheithcock> and at our company website <https://www.retrospect.com/>.



## Psychological Operations in A Modern Landscape

By Milica D. Djekic

In the current time, people are talking about many issues and opinions. They use the internet and the other media to share their thoughts, opinions and perspectives. The trouble is once launched news in the media space can become accepted as fact, rather than just someone's personal belief. The people always consume some form of news, and there is no a single day without reading the stories on the web or watching the favorite political TV follow-up. Before anyone accepts the truth of such content, that person should know that only a human stands behind it. A similar case is with war propaganda when, let's say, the terrorists produce plenty of embarrassing campaigns. Those individuals doing so are also subject to some weaknesses and they are not in fact superior to the rest of us – they simply use some tactics that can impact our psyche and mind.

It's not the rare case that someone reading some story or listening to some recordings could feel some negative emotion such as fear. The ultimate goal of the terrorists is to spread the fear and make people believe they are beaten before anyone even fired a weapon. The fact is those sorts of psychological operations could lead to a mental health crisis, and if anyone is influenced by so much web content or media news that person could experience a serious problem. The bad guys would use this way to approach us and even if they are sending an email or contacting someone through social networks – they are definitely creating the picture they want us to see. It's just human nature to feel insecure if anyone targets our fears to leave us without that peace of mind. This could be critical returning the peace of mind and inner balance.

The main aim the bad guys want to accomplish is to instill distrust about our reality, lives and the entire legal system. Many would say that nowadays we live in a “zero trust” world; that claim could wake up our

paranoia and make us believe there is no space to develop the strong and positive relationship with anyone. The common people used to live their lives in a predictable manner, but this new time could bring us the spirits from the past that would remind us how harsh and merciless some persons can be. In our opinion, there are apparently a lot of conspiracy theories that would suggest to us that someone who deeply cares for us wants to hurt us instead. That's one more reason to feel scared and impact your natural need for security. The bad guys would depend on such findings and they would literally play that card.

If we lose our sense of being secure we can start developing our animal instincts that would suggest us it's time to fight to survive. In other words, the psychological campaigns could increase the level of aggressiveness and frustration amongst the common people. That's what the terrorists want! It would appear this new horrifying time has caught us unprepared and we still need more space to develop the resilience to face the entire situation. Apparently, many of us are not fully aware of what is going on and that seriously affects our rationality and the ability to find and rely on accurate information. Throughout history, it's known that the timing and accurate information can decide the winner and the victory in any battle, which in turn provides many advantages and benefits to the winners. It seems it's time to win the hard battle and it's important to always get aware that the good guys are on our side always being ready to protect us!

### About The Author



**Milica D. Djekic** is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book "The Internet of Things: Concept, Applications and Security" being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the [Australian Cyber Security Magazine](#) since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.



# EVENTS



CYBERSEC

Europe's Digital Decade  
has started.

Let's get **#Together**  
to cyber secure it.

**REGISTER NOW**

CYBERSEC

THIS YEAR

The most unique CYBERSEC Season created so far  
Carefully designed binge-conferencing format.

Are you ready to stand

**#TOGETHER**  
AGAINST ADVERSARIAL INTERNET?

Spectacular  
Insightful  
Thrilling

28-30 SEPTEMBER 2020 **ONLINE**



# CYBER SECURITY

FOR CRITICAL ASSETS | EUROPE

6th - 7th October 2020

— Virtual Event —

FREE with code:

CDMVIP

Join Us Online at Cyber Security for Critical Assets European Summit This October

The 7th annual Cyber Security for Critical Assets Summit brings together 100's of IT & OT security leaders from across the Oil & Gas, Energy, Utility, Power, Water, Mining, Healthcare & Chemical industries for 2-days of insight building and expert knowledge exchange on 6th - 7th October. Join us online to hone your skills in areas including:

- Steps to ensuring business continuity during the COVID-19 pandemic
- Transforming your cyber security strategy to keep up with Industry 4.0
- Modelling an OT SOC
- Incident response and disaster recovery for critical systems
- Addressing the human element of cyber security
- Designing, operating and managing risks to ICS and their assets
- Governance in OT environments
- And, more!



Speakers include CISOs, VPs, Heads of IT & OT Security at: Maersk, Ofgem, Iberdola, NATS, Ansaldo Energia and more...



Andy Powell  
CISO  
Maersk



Cristian Cucu  
CIO  
Nuclearelectrica



Mark Chaplin  
Principal  
Information Security Forum



Sandra Heissenberger  
CISO  
City of Vienna



Marc Samson  
CISO  
ENGIE Services BeLux



Stuart Okin  
Head of Security Privacy  
& Resilience  
Ofgem



João Domingues Agostinho  
Cyber Security Chairman  
Trans Adriatic Pipeline



Claudio Bolla  
Group Information Security  
Director  
INEOS



Mikael Vingaard  
Specialist Industrial Security  
Danish Energy Agency



Andrew Coding  
Information and Cyber  
Security Manager  
NATS

This is a one-of-a-kind opportunity for critical infrastructure leaders across Europe, to come together and safeguard their assets. View the agenda and secure your place for FREE using the discount code: CDMVIP at: [europe.cs4ca.com](https://europe.cs4ca.com)

# ISAF | CyberSecurity

## 9<sup>th</sup> International Cyber Security, Information & Network Security Exhibition

OCTOBER 08<sup>th</sup>-11<sup>th</sup>, 2020

Istanbul Expo Center (İFM) - Türkiye



[www.isaffuari.com](http://www.isaffuari.com)

T. +90 212 503 32 32 - [marmara@marmarafuar.com.tr](mailto:marmara@marmarafuar.com.tr)

**MARMARA**  
TANITIM FUARCILIK  
[www.marmarafuar.com.tr](http://www.marmarafuar.com.tr)

[/marmarafuar](https://www.instagram.com/marmarafuar)

[/isafexhibition](https://www.facebook.com/isafexhibition)

[/company/marmara-fuar](https://www.linkedin.com/company/marmara-fuar)

# CYBER SECURITY FOR CRITICAL MANUFACTURING | USA MANUSEC

October 13th-14th 2020

— Virtual Event —

FREE with code:

CDMVIP

Join Us Online at Cyber Security for Manufacturing USA Summit This October!

Cyber Security for Critical Manufacturing Summit launches online this October, uniting 100's of manufacturing security leaders from America's: **Transport, FMCG, Food & Beverage, Machinery, Chemical, Pharmaceutical & Automotive** industries.

The agenda boasts an A-list speaker line-up as well as an educational edge that reveals the most up-to-date insights for mitigating risks and safeguarding critical manufacturing processes. Join us online to hone your skills in areas including:

- Managing cyber risks in the era of smart production
- Launching an OT security operations centre
- Overcoming the challenges of network design and security in manufacturing environments
- Building high-performing security teams
- Employing a Strategic Approach to Managing Shared Supply Chain Risks
- Developing, implementing and testing OT disaster recovery plans
- And, more!

**CPD  
CERTIFIED**  
The CPD Certification  
Service

Speakers include CISOs, VPs of IT & OT Security, Heads of Automation at **Pepsico, GSK, Nexteer, Kraft Heinz, Tesla Motors...**



Arun DeSouza  
CISO  
Nexteer



Arvin Verma  
Cyber Risk Management  
Specialist  
Pepsico



Lisa Tuttle  
CISO  
SPX Corporation



Michael Elmore  
VP OT Security  
GSK



Chandra Brown  
CEO  
MxD



Imail Guneydas  
Cyber Security  
Assurance Manager  
Tesla Motors



Ricardo Lafosse  
CISO  
Kraft Heinz



Yanko Gerdjikov  
Regional Security Lead  
Nestlé



Brandi Johnson  
Sr. Manager Cyber Risk  
Management  
Toyota



Scott Reynolds  
Manager Industrial  
Security  
Johns Manville

This is a one-of-a-kind opportunity for manufacturing security leaders across USA, to come together and safeguard their assets. View the agenda and [secure your place for FREE](#) using the discount code: **CDMVIP** at: [usa.manusecevent.com](https://usa.manusecevent.com)

**THE INDUSTRY'S LARGEST  
INDEPENDENT AI GOVERNMENT EVENT**

2nd Annual

# aiworld | GOVERNMENT VIRTUAL

OCTOBER 28-30, 2020

**1,100+**  
ATTENDEES

**120+**  
SPEAKERS

**85+**  
SPONSORS

**50+**  
CONFERENCE  
SESSIONS

Save 20% with  
discount code CDM2020

**Accelerating Innovation in the Public Sector**

AI World Government provides a comprehensive three-day forum to educate and inform public sector agencies on proven strategies and tactics to successfully deploy AI and cognitive technologies.

**[AIWorldGov.com](https://AIWorldGov.com)**

# QUBIT CONFERENCE **SOFIA** 2020

3<sup>rd</sup> Cybersecurity Community Event

**29**OCTOBER/ SOFIA,  
BULGARIA

## CALL FOR SPEAKERS IS OPEN!

### We are looking for:

- new speakers with original, innovative and creative topic and session outline
- real-life stories, strategies and mind opening ideas, case studies that Conference Attendees can apply to their jobs

### Speakers should focus on the main Conference Streams:

Threat intelligence | Cloud security | Disaster recovery  
Secure team cooperation

**SUBMIT YOUR PROPOSAL**



Excellent speakers



Educational session



News & networking



Practical workshops





# EURONAVAL

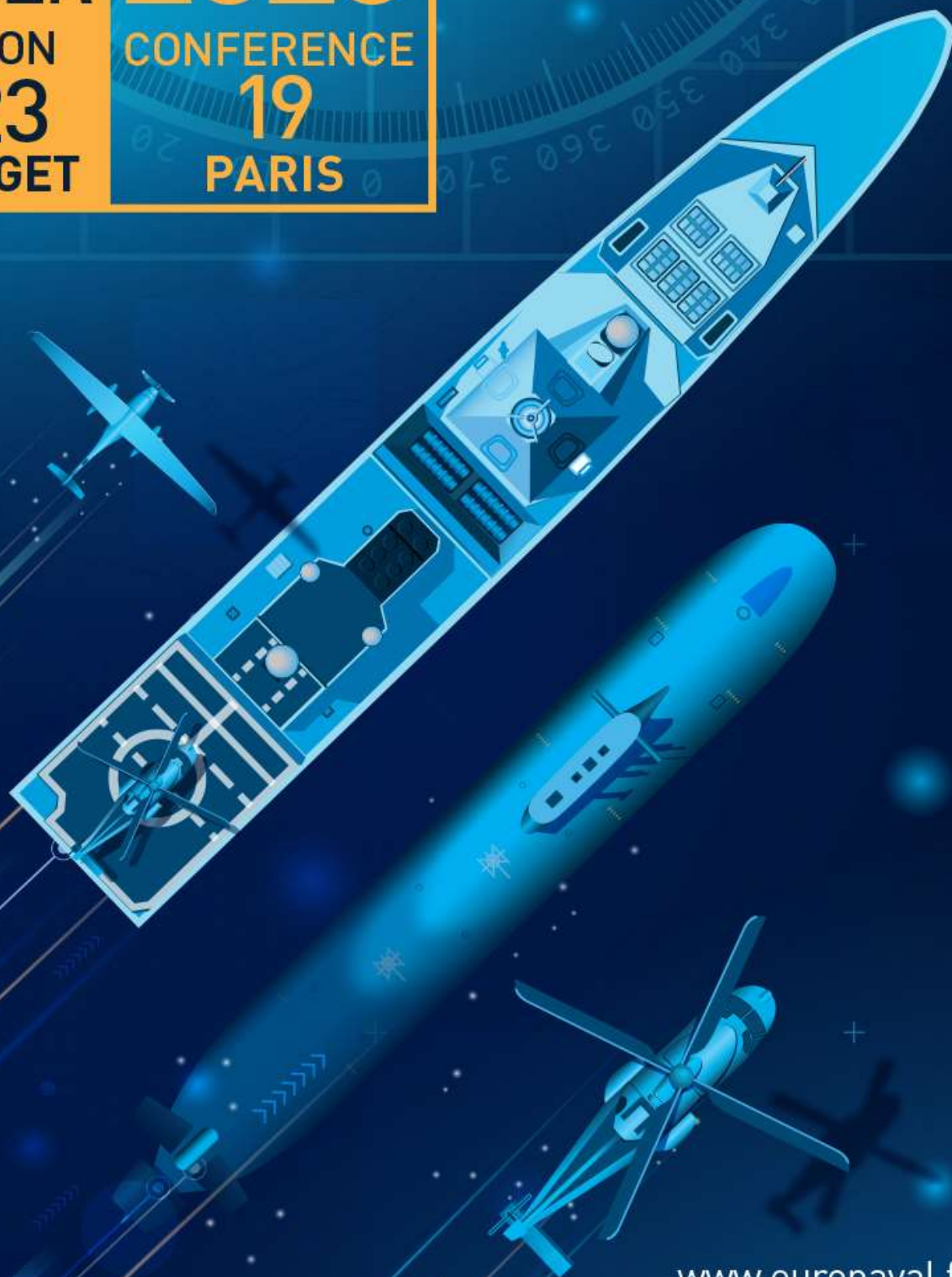
THE WORLD NAVAL DEFENCE EXHIBITION

**OCTOBER**

EXHIBITION  
**20/23**  
LE BOURGET

**2020**

CONFERENCE  
**19**  
PARIS



[www.euronaval.fr](http://www.euronaval.fr)

# **5<sup>th</sup> BRAND PROTECTION CONGRESS**



**09 - 10 November  
2020  
Kuala Lumpur, Malaysia**



## ***Experience:***

- *Our unique and inspiring program*
- *Countless networking opportunities.*
- *Remarkable one-to-one meeting sessions.*
- *The congenial gathering of distinguished industry leaders*
- *The Magnificent petronas twin towers & shoppers paradise that is Kuala Lumpur , Malaysia.*

# **6<sup>th</sup> BRAND PROTECTION CONGRESS**




**02 - 03 December  
2020  
Nice, France**





## ***Experience:***

- *Our unique and inspiring program*
- *Countless networking opportunities.*
- *Remarkable one-to-one meeting sessions.*
- *The congenial gathering of distinguished industry leaders*
- *The fabulous beaches, beautiful coastline and fantastic architecture of Nice, France.*



 [www.egyptdefenceexpo.com](http://www.egyptdefenceexpo.com)

 [@egyptdefenceexpo](https://twitter.com/egyptdefenceexpo)

 [/egyptdefenceexpo](https://www.facebook.com/egyptdefenceexpo)

 [@visitedex](https://twitter.com/visitedex)

 [#edex2020](https://twitter.com/visitedex)

## THE 2<sup>ND</sup> EDITION OF EGYPT'S ONLY INTERNATIONAL DEFENCE EXHIBITION

EGYPT INTERNATIONAL EXHIBITION CENTRE  
7-10 DECEMBER 2020

 **400 +**  
EXHIBITORS

 **30,000 +**  
VISITORS

 **FULLY-HOSTED VIP**  
DELEGATION PROGRAMME

Media Partner

Supported by

Organised by





# CYBERSECURITY KNOWLEDGE. WHEN YOU NEED IT.

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

[rsaconference.com/cyberdefense-2020](https://rsaconference.com/cyberdefense-2020)

# HELP PROTECT AMERICAN INTERESTS IN CYBERSPACE

Air Force Civilian Service (AFCS) has hundreds of civilian cyber security and IT professionals working on the front lines safeguarding Air Force facilities, vital intelligence, and digital assets. We're looking for the best and brightest to help us stay ahead of this ongoing threat.

In fact, AFCS is currently hiring cyber security specialists, information technology specialists, information security specialists, software developers, software engineers, computer scientists, and computer engineers. These are challenging and rewarding positions that put you at the heart of our mission in cyberspace. Our systems are some of the most complex in the world, and we need the best in the business to keep our infrastructure and digital information secure.

Consider AFCS. You'll find a supportive and inclusive workplace, where excellence is rewarded, and work-life balance is a priority. Factor in great benefits and you'll see why AFCS is a place where you can excel. At 170,000 strong, we are a force to be reckoned with. Find your place with us and watch your career soar.

**AFCivilianCareers.com/CYBER | #ItsACivilianThing**

Equal Opportunity Employer. U.S. Citizenship required. Must be of legal working age.



# You don't need to be next in line for a data breach.

Put on your thinking hat and step into the shoes of a hacker.

Cyber incidents are on the rise. While most organizations play defense--creating plans that tell them what to secure and how to react if their security settings fail--it's not enough to respond to a data breach.

What if you looked at cybersecurity from a different point of view?

In our guide, "How to Think Like a Hacker and Secure Your Data," you'll discover how to go on offense with your data by:

- Diving into modern data breach statistics
- Exploring hacking terminology and techniques
- Walking through seven strategies for data protection

***Are you ready to put yourself in the shoes of a hacker?***

Visit [\*\*https://www.goanywhere.com/think-like-a-hacker\*\*](https://www.goanywhere.com/think-like-a-hacker) to get a free copy of our cybersecurity guide.



**GO ANYWHERE®**  
Managed File Transfer





DATA PROTECTION WORLD FORUM

PRIVACY | TRUST | RISK | SECURITY

CDM

CYBER DEFENSE MAGAZINE

the magazine devoted to the security professionals

**Rowena Fell**

Global and EMEA Risk Assurance  
Operations Leader - Ernst & Young

**Flavius Plesu**

Head of Information Security  
Bank of Ireland UK

**Steve Wright**

Data Privacy and Information  
Security Officer - John Lewis

**Marloes Pomp**

Head of Blockchain Projects  
Dutch Government



**SEE THESE SPEAKERS FOR FREE**

*Use our code 'CYBERMAGFREE'*

**#CYBERBYTE**  
**@ROSSOWESQ**



## Meet Our Publisher: Gary S. Miliefsky, CISSP, fmDHS

**“Amazing Keynote”**

**“Best Speaker on the Hacking Stage”**

**“Most Entertaining and Engaging”**



Gary has been keynoting cyber security events throughout the year. He's also been a moderator, a panelist and has numerous upcoming events throughout the year.

If you are looking for a cybersecurity expert who can make the difference from a nice event to a stellar conference, look no further email [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)



# CYBER DEFENSE TV

## INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here...we've launched [CyberDefense.TV](https://www.cyberdefense.tv)

At least a dozen exceptional interviews rolling out each month starting this summer...

Market leaders, innovators, CEO hot seat interviews and much more.

A new division of Cyber Defense Media Group and sister to Cyber Defense Magazine.

### The Interviews

These anticipated "CEO Hotseat" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by **Gary Miketasy**. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2019 CYBER DEFENSE MAGAZINE. All Rights Reserved. [www.cyberdefense.tv](https://www.cyberdefense.tv)

## Free Monthly Cyber Defense eMagazine Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. [Click here](#) to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

[By signing up, you'll always be in the loop with CDM.](#)

---

Copyright (C) 2020, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

All rights reserved worldwide. Copyright © 2020, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at [marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)

### **Cyber Defense Magazine**

276 Fifth Avenue, Suite 704, New York, NY 1000  
EIN: 454-18-8465, DUNS# 078358935.  
All rights reserved worldwide.  
[marketing@cyberdefensemagazine.com](mailto:marketing@cyberdefensemagazine.com)  
[www.cyberdefensemagazine.com](http://www.cyberdefensemagazine.com)

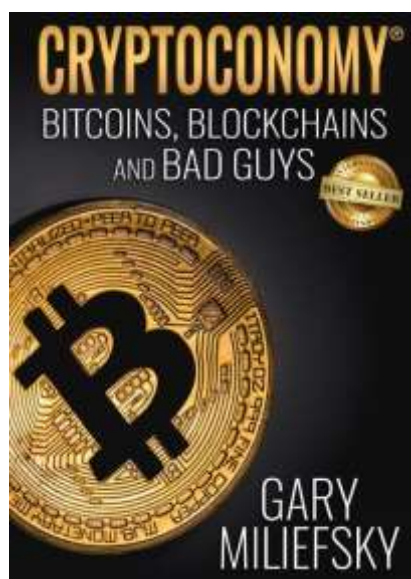
### **NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)**

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 10/02/2020

# TRILLIONS ARE AT STAKE

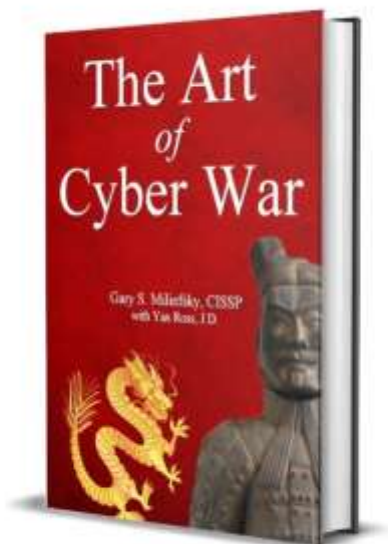
**No 1 INTERNATIONAL BESTSELLER IN FOUR CATEGORIES**

Released:



<https://www.amazon.com/Cryptoeconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH>

In Development:





**PWN YOUR  
CYBER RISK**

GROUNDBREAKING  
**COMPANY**  
APPLICATION SECURITY

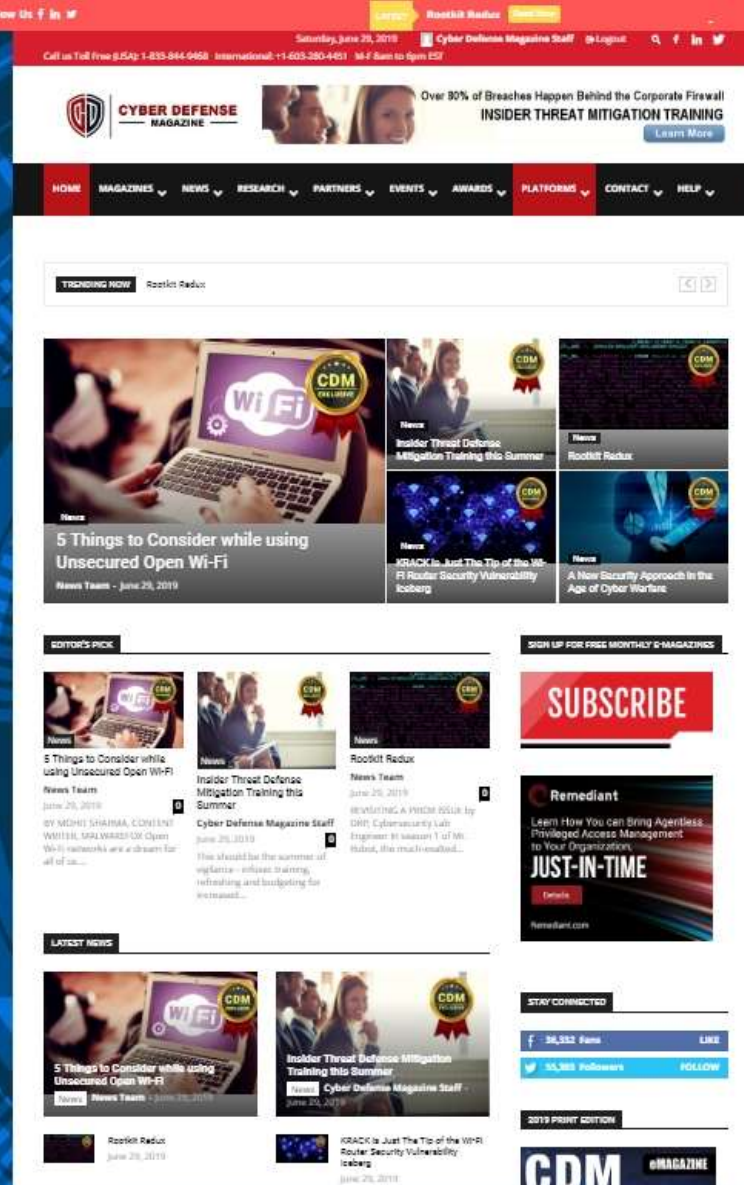
**CYBER DEFENSE MAGAZINE**

2019

**BEST  
PRODUCT**  
VULNERABILITY  
MANAGEMENT

**CYBER DEFENSE MAGAZINE**

2019



## 8 Years in The Making...

***Thank You to our Loyal Subscribers!***

We've Completely Rebuilt [CyberDefenseMagazine.com](http://CyberDefenseMagazine.com) - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're shooting for 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and [CyberDefenseMagazine.com](http://CyberDefenseMagazine.com) up and running as an array of live mirror sites.

***Millions of monthly readers and new platforms coming...***

**JUNE 2-4, 2020**

David L. Lawrence Convention Center | Pittsburgh, PA

# SMART MANUFACTURING EXPERIENCE

## the path to the connected world of manufacturing

### Greater Connectivity = Greater Need for Cybersecurity Solutions

- **Thousands of buyers.** Engage with qualified attendees searching for the best ways to secure their data and their business
- **Exclusive opportunity.** Only open to companies that can demonstrate a connection/application to smart manufacturing
- **Active participants.** Demonstrate your solutions and educate manufacturers on the most effective methods to safeguard their valuable data

### The Event is Focused on These Transformative Technologies:

- |                                                   |                                       |
|---------------------------------------------------|---------------------------------------|
| • Cybersecurity                                   | • Automation & Robotics               |
| • Additive Manufacturing (AM) & 3D Printing       | • Data Analytics                      |
| • Artificial Intelligence/Machine Learning        | • Industrial IoT (Internet of Things) |
| • Augmented Reality (AR) and Virtual Reality (VR) | • Workforce Transformation            |



### Be Part of the Experience!

Call **800.733.3976** or visit [smartmanufacturingexperience.com](https://smartmanufacturingexperience.com)



## Celebrating Over 15 Years of Cybersecurity Operations Excellence



**At Herjavec Group, information security is what we do.**

You may know me from making deals on television, but my passion lies in innovating technology - yes, cybersecurity.

Over 15 years ago we started the business selling commercial firewalls to IT buyers. Over time we've seen a monumental shift towards what we are all familiar with - the cybercrime epidemic. Now our customers are challenged to address compliance requirements, incident response plans, nation state threats, security awareness, malware detection...the list goes on. In response, we have advanced our cyber capabilities and attracted world class talent.

Today, Herjavec Group is a global leader in cybersecurity with expertise in comprehensive security services including **Managed Security Services** (SOC Operations, Threat Detection, Security Technology Engineering) & **Professional Services** (Advisory Services, Identity Services, Technology Implementation, Threat Management & Incident Response). Herjavec Group is over 300 people strong, with offices and Security Operations Centers across the United States, United Kingdom, Canada and India. At Herjavec Group, we realize that in cybersecurity change is constant, but we are driven by a steadfast goal: to make enterprises around the world more secure.

To your success,

**Robert Herjavec**  
Black Unicorn Awards Judge  
Star of ABC's Shark Tank  
Founder & CEO of Herjavec Group

### Recognized Industry-Wide

**MOST INNOVATIVE  
IAM PROVIDER**



**SECURITY SERVICES  
LEADER**



**LEADER IN MANAGED  
SECURITY SERVICES**



**SECURITY COMPANY  
OF THE YEAR**



**#1  
ON THE**



**TOP 10  
ON THE**



# CDM

**CYBER DEFENSE MAGAZINE**

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

## eMAGAZINE

[www.cyberdefenseemagazine.com](http://www.cyberdefenseemagazine.com)

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert



**ALWAYS FREE  
NO STRINGS ATTACHED**



# CYBERSECURITY KNOWLEDGE. WHEN YOU NEED IT.

Ensuring the security of your organization is always challenging, even in the best of times.

We created an **online resource center** to help you find the answers you may be looking for. It includes relevant content such as interviews with CISOs dealing with today's realities, preventing ransomware attacks, tips on how to improve your virtual presenting skills, and much, much more.

Browse our specially curated resources today, and keep checking back as new information is added regularly.

[rsaconference.com/cyberdefense-2020](https://rsaconference.com/cyberdefense-2020)



**Lucio Frega, Threat Researcher**  
Deutsche Telekom - Cyber Threat Intelligence

DTAG-CTI (Deutsche Telekom - Cyber Threat Intelligence) protects clients against cyber-attacks worldwide.

Like us, the adversaries too have cyber-experts. They continuously enhance their malware attacks with stealth and anti-forensics capabilities. This increases our overall risk and also the cost of detection and remediation.

For example, repacked malware strains evade endpoint's protection, fluxed C2s bypass SIEM, and obfuscations fool reversing.

We can cope with this in spite of the high cost. However, it all amounts to nothing if, by the time a defense is erected, the attack has reshaped and shifted direction again, turning those defenses obsolete.

We in DTAG-CTI have erected predictive defenses using malware's code-similarity.

This predictive layer goes beyond network activity, behavior, metadata and state-of-the-art technologies. We match binaries using Cythereal's automatically generated YARA rules, unearthing previously unseen strains despite reshuffling, repacking, and other evasions. These predictive defenses nail the malware "in the bud," before it has had a chance to spread or even to report to its C2.

As an extra value, these early detections also empower early identification. We learn from the start who is against us and hunt for associations regardless of their obfuscated binaries, dissimilar metadata, IOCs, and payloads.

Together with the professionalism and commitment of our teams and partners, we have found in the expertise, dedication, and engagement of Cythereal a very powerful and astounding ally that brings threat hunting and cyber-defense to a superior level.

#### About the Author/Disclosure



Lucio Frega is a computer forensic examiner certified by IACIS (International Association of Computer Investigative Specialists). He has over 40 years of worldwide experience in IT/OT security in Banks, Pharma, Telcos and the energy sector. Lucio is not affiliated with Cythereal. His comments are not to be construed as the official posture of any stakeholder but himself.



**cythereal.com**



**\* with help from writers  
and friends all over the Globe.**