[+] (IN)SECUREMagazine

12 | 2018
ISSUE 60

Building strategies

RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

Stop here for all the cybersecurity intel you need.

Wondering how to pull ahead of dangerous adversaries? Or throw off advanced threats?

Get the answers at RSA Conference 2019, March 4 – 8.

- Interactive demos from LookingGlass, UnifyID, ZeroFOX and 600+ more exhibitors
- Hands-on tutorials, trainings and on-point conversations you won't find anywhere else
- Sharp and relevant keynotes from cybersecurity's most celebrated experts as well as some special celebrity guests
- 550+ sessions and seminars addressing a range of timely issues and themes

Register today to secure your spot at RSAC 2019—but hurry, passes and savings will go fast.

Learn more: **www.rsaconference.com/helpnet-us19**

Follow us: **#RSAC**

Table of contents

Contributors

EDWARD AMOROSO, CEO, TAG Cyber
JONATHAN BOHRER, CFO, Abacus Group
MARK BOWER, CRO, Egress Software
ANDREW GINTER, Vice President of Industrial Security, Waterfall Security
SEAN MASON, Director of Threat Management and Incident Response, Cisco
JOSH MAYFIELD, Director of Security Strategy, Absolute
GADI NAOR, CTO, Alcide
VLATKO KOŠTURJAK, Security Researcher
SEAN WALLS, Vice President, Eurofins Cyber Security

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz
Editor in Chief
mzorz@helpnetsecurity.com

Zeljka Zorz
Managing Editor
zzorz@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

How to make the CFO your best cybersecurity friend

AUTHOR_ Jonathan Bohrer, CFO, Abacus Group

I'm bad dinner company. As the CFO of a cloud technology provider, I like to speak about finance and cybersecurity, two topics that are likely to put my dinner guests to sleep. However, both topics are extremely important in today's business world and are inextricably linked. Good cybersecurity is expensive, and bad cybersecurity is, well… even more expensive.

If you are not a cybergeek, it can be very difficult to tell the difference between the good stuff and the bad stuff, until something bad happens.

+ It's very important to be able to clearly illustrate the ROI of any cybersecurity project to your CFO so he or she can rationalize the level of spending that good security requires.

Allow me to explain what information CFOs are looking for before they write the check.

Spend more on cyber policy management and less on high-end CapEx

I'm often amazed at the amount of capital expended on high-end security appliances, with little thought of how those tools will be managed once installed. Essentially, this is what CFOs call "ROI." We see this often when we migrate clients onto our platform – we see so much technology go to the junk heap because of over-purchasing.

This is not to say that all of the bells and whistles included in these offerings are not potentially useful and protective, but without a fully qualified pilot in the cockpit to operate and navigate all of the functionality, much of it ends up unused, or worse yet misused, resulting in false positives and corresponding organizational inefficiencies.

CFOs would rather see fewer CapEx dollars spent on cyber investments, offset by more dollars spent

on qualified professionals and organizational structure to manage those investments. Ultimately, this will yield a higher ROI.

If you are outsourcing your cloud services and security, it's important to assess whether the provider has the financial and technical wherewithal to purchase the full menu of high-end appliances and, more importantly, employ a small army of engineers to properly and efficiently manage these devices on behalf of its clients.

Understand that your CFO looks at cybersecurity spending like corporate insurance

Cybersecurity investments often behave in a similar way to corporate insurance policies, although I think we can agree that these days we are much more likely to have a data breach than a fire or earthquake. Just like with insurance, cyber investments are money spent to protect against an unlikely-to-happen threat. However slim, we can't take that chance so we allocate scarce dollars to protect or compensate us should the worst occur.

When we buy insurance, we make trade-off decisions because to completely insure our business against every event would cost us more than we make in revenue. The same goes for cyber tools - a technologist could literally spend the entire P&L on protecting against cyber attacks. So we must be selective.

> CISOs beware: CFOs look at cyber spending as they do insurance, which is to say probabilistically. This is quite different from a technologist's approach, which is to put as much firepower between the company and potential harm as possible.

Your CFO wants you to identify different types of cyber investments that might cover the same risks, or even be covered by implementing better policy. The already crowded space of vendors selling fear grows larger every day. Many of the technologies they are selling overlap with other technology that may already be in place. Make sure that your technology/security team can clearly articulate to the CFO what the various cyber investments are meant to defend against, and how they interact with one another. Provide the CFO with a protocol for purchasing cyber defenses that follow a standard for the who, what, why, where, how, and how much for every solution you recommend. The blanket statement "because it will make us safer" is unacceptable

given the dollars at stake, and should not be cause for the CFO to write a blank check.

More and more companies are spending significant dollars to protect against hackers. If you are one of these companies and you also spend dollars on cyber E&O insurance, consider approaching your carrier or broker for a discount. Much like being a non-smoker may reduce your health insurance premiums, so should having a robust cybersecurity program reduce your corporate premiums.

Make cybersecurity work for your HR managers

+ Be sure to illustrate to your CFO how useful cyber tools can be across the firm, thereby increasing utility and ROI.

Many people think that cybersecurity is a bunch of expensive appliances and intrusion detection software, and sometimes this is true. But the biggest mistake that firms make is to invest in these tools and then let them sit exclusively under the purview of the technology team, or worse yet, installed with no hands-on management at all.

While these tools generally have a passive role, scanning or waiting for an event before leaping into action, the data that they analyze can be extremely useful to other areas of your company - if translated, summarized and communicated to the right people. An example of this is web filtering through an advanced firewall. Ostensibly, the purpose is to prevent employees from accessing sites with malicious potential. But in the course of scanning and blocking these sites, firewalls collect information on traffic to all of the other sites that employees are visiting. Thus, if presented clearly to an HR manager, this data could result in useful business intelligence around employee productivity. Trust me, the employee juggling seven fantasy football teams is not a great contributor to your firm.

Review: Specops Password Policy

AUTHOR_Vlatko Košturjak, Security Researcher

All who work in the information security industry agree that passwords are one of the worst security nightmares of the modern information security age. Having weak passwords - even as part of a multi-factor authentication scheme - degrades the security posture of an organization.

Unfortunately, as passwords scale well, they are still present in practically every organization and even central authentication places like Active Directory.

There are multiple security controls, even in core operating systems, which should prevent users from choosing weak passwords, but we all know the limits of those security controls in production. Most of the passwords in many Active Directory password dumps are cracked in mere days, which is time enough to foil password change requirements in any organization.

Some 17 years ago Specops Software took on the challenge of developing authentication tools for

the Microsoft ecosystem. This review focuses on Specops Password Policy, their flagship tool for preventing Active Directory users from choosing weak passwords.

Installation

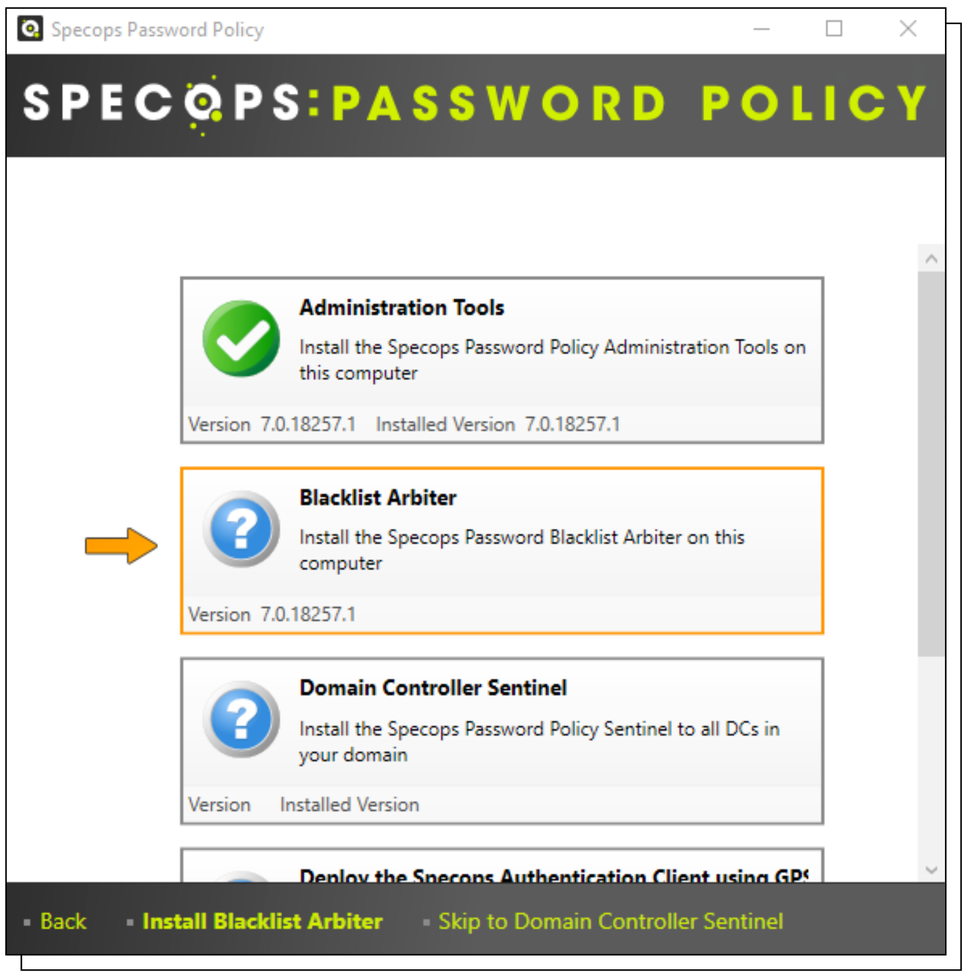
Specops Password Policy works by extending the functionality of Group Policy with more password strength options and fine-grained password policies.

The core component consists of three parts: the Specops Password Policy Sentinel (Domain Controller Sentinel), the Specops Authentication Client, and the Specops Password Policy Administration Tools.

The Administration tool can be installed on any computer that is part of the Active Directory domain, and it will be used to administer Specops Password Policy. The Domain Controller Sentinel should be installed on every domain controller.

The Specops Authentication Client is an optional component that is meant to be installed on every host that is part of a domain if you want to display the password policy rules when a user fails to meet the policy criteria when changing their password. The Client also notifies users when their passwords are about to expire.

INSTALLATION STEPS ARE EASY TO FOLLOW



If you are looking to get more serious about password security, there are also optional components. Blacklist Arbiter is the most interesting of those, as it notifies users if a password is found in a list of leaked passwords and prevents them from using it.

Since the solution works with user passwords on Active Directory, you'll need to have domain administrator rights in order to install it and make it work as intended. Although it has many components that should be installed on different servers, the wizard-like installer makes installing them a breeze.

A test of the installation process on a simple Active Directory domain revealed that all the components, including optional ones, can be installed in less than 15 minutes by following instructions provided by the installer. The installer even helps with the installation of the Specops Authentication Client on domain hosts using GPSI.

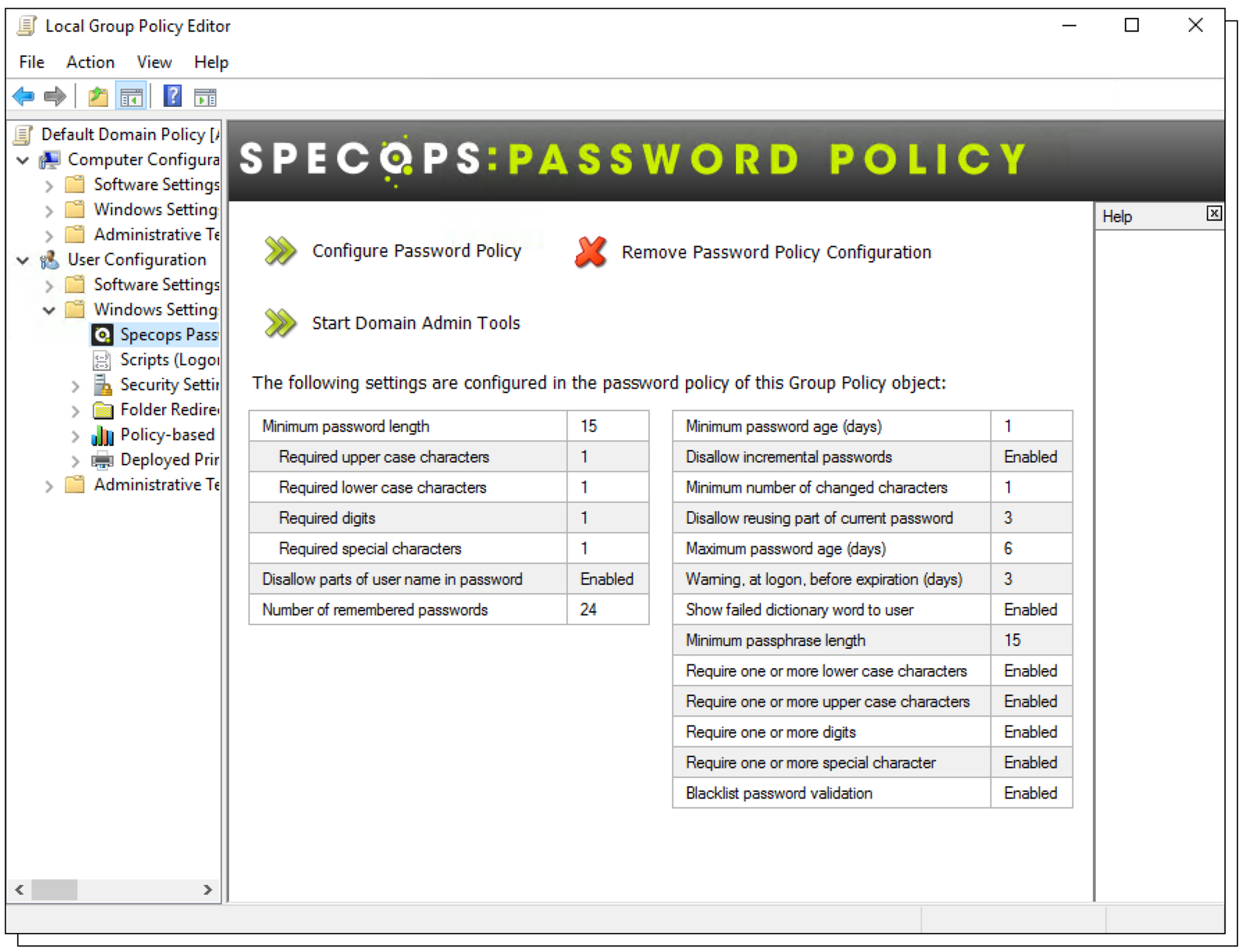
To try the solution out, I have installed a test Active Directory domain in the Amazon cloud with several testing servers as part of the domain, and I have populated users with different privileges and roles with a test script. I have also customized password expiry periods and passwords of the different users.

Use

Once the solution is installed, you (the administrator) will spend most of the time working with the Administration tool, which is used to tweak all the settings and enforce password policies. It is the administrative front-end for all the installed components.

When you open the Administration tool, on the left side you'll see most of the configuration settings listed by category or tool. They allow you to target any GPO level, group, user with specific password and passphrase requirements.

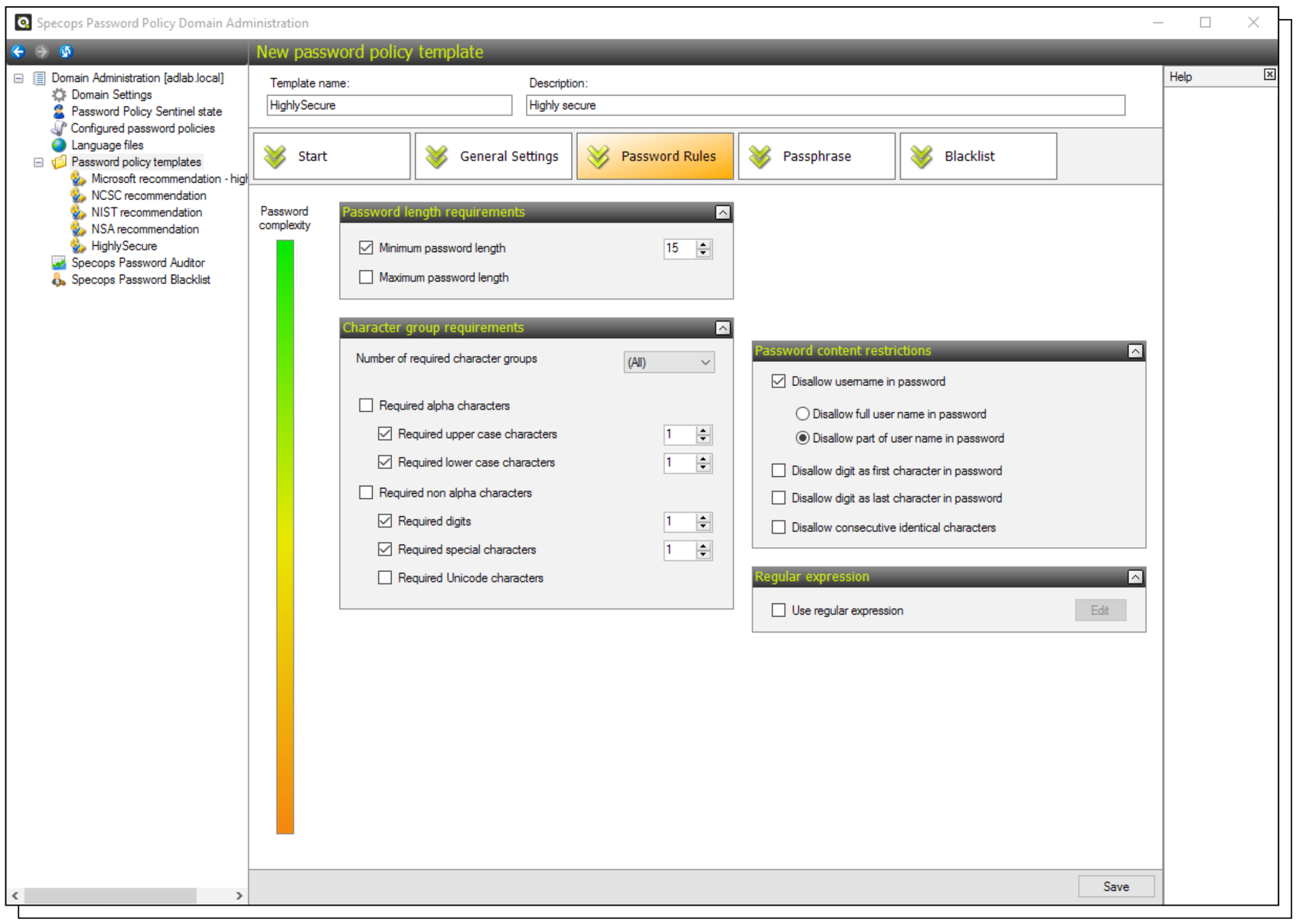
SPECOPS PASSWORD POLICY IN LOCAL GROUP POLICY EDITOR



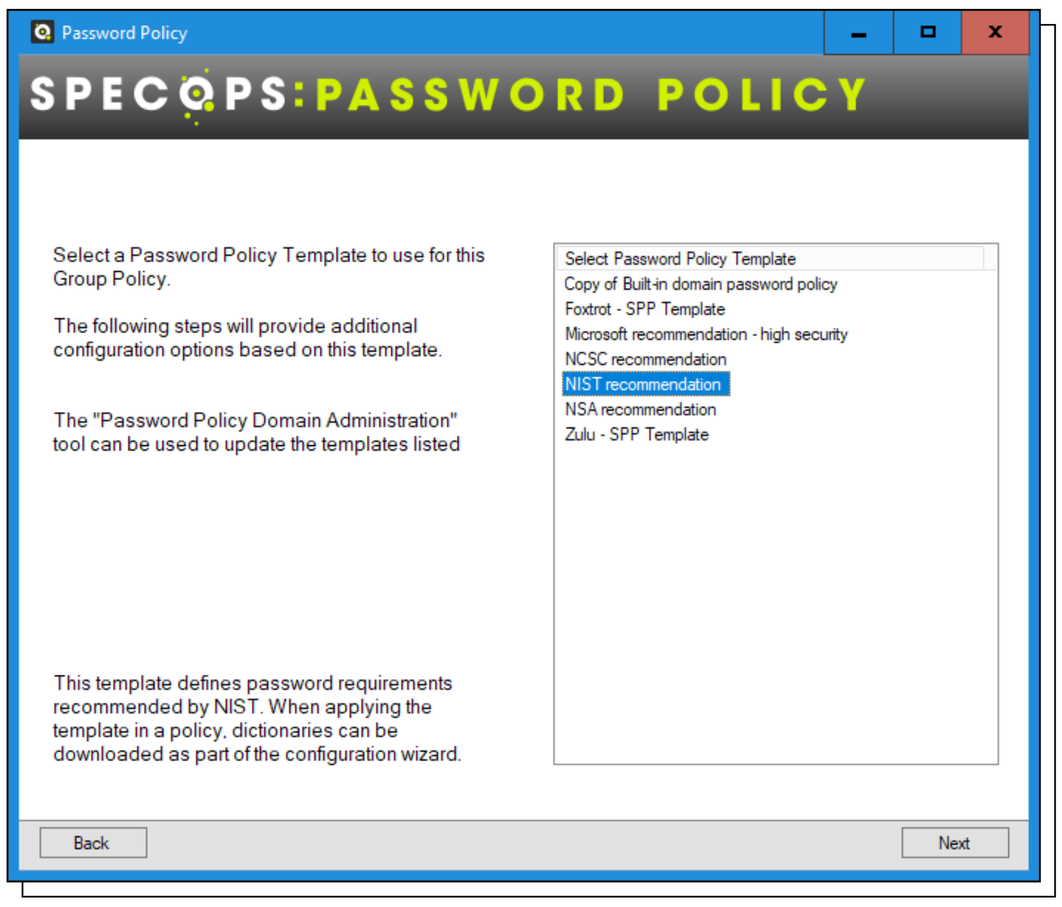
+ Specops Password Policy also comes with password policy templates for Microsoft, NCSC, NIST and NSA recommendations.

If you need something specific, a new password and passphrase policy template can be made with a few mouse clicks.

CREATING HIGHLY SECURE CUSTOM PASSWORD POLICY



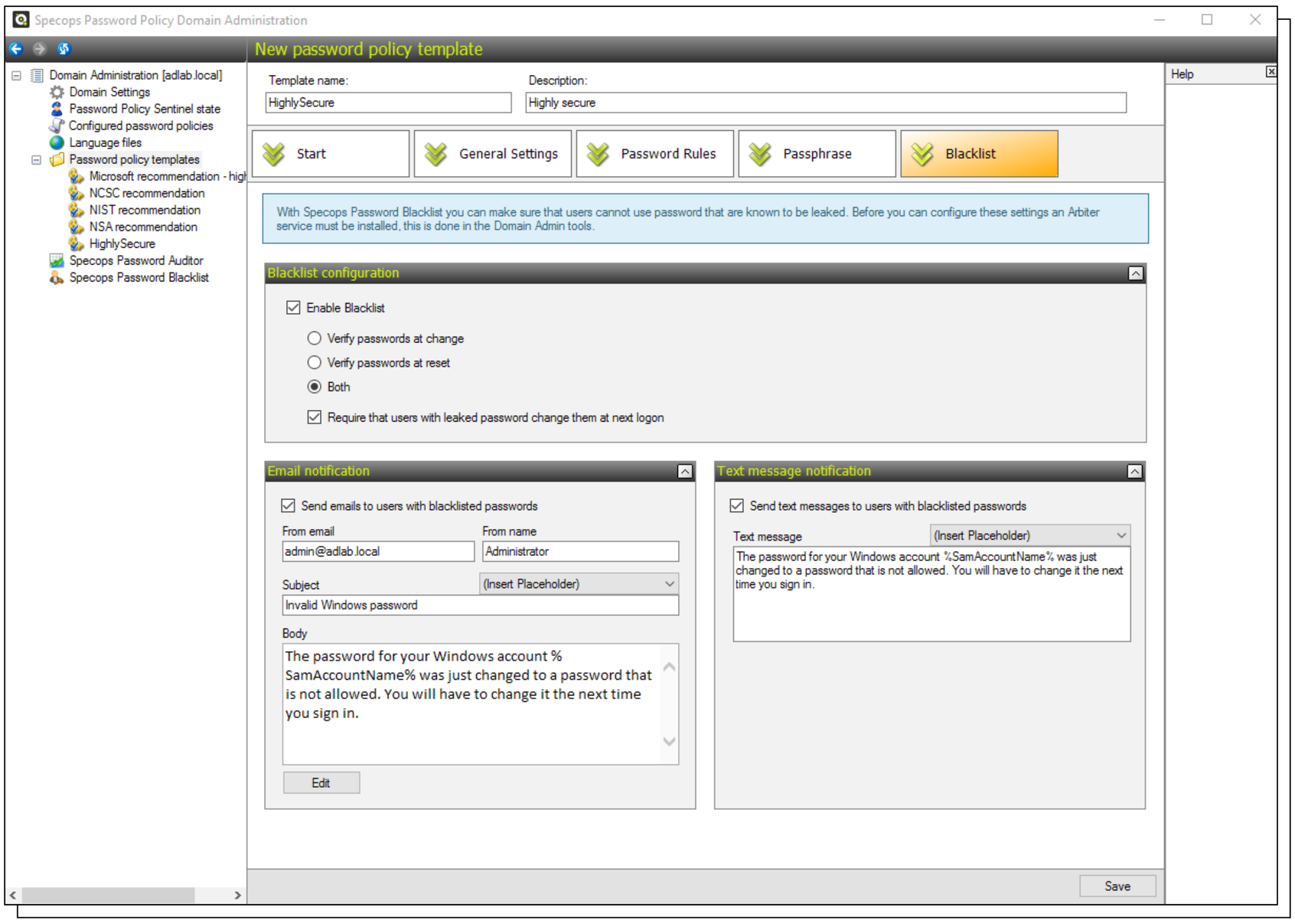
ONCE A TEMPLATE IS SELECTED, YOU WILL BE PRESENTED ADDITIONAL CONFIGURATION OPTIONS THAT ALLOW YOU TO CREATE A LIST OF DISALLOWED WORDS, DOWNLOAD DICTIONARY AND SET MAXIMUM PASSWORD AGE FOR USERS AFFECTED BY THE POLICY



If you want to enforce strong password policies, there's a Blacklist feature that allows you to block and notify users if the password they've chosen is found in a list of leaked passwords.

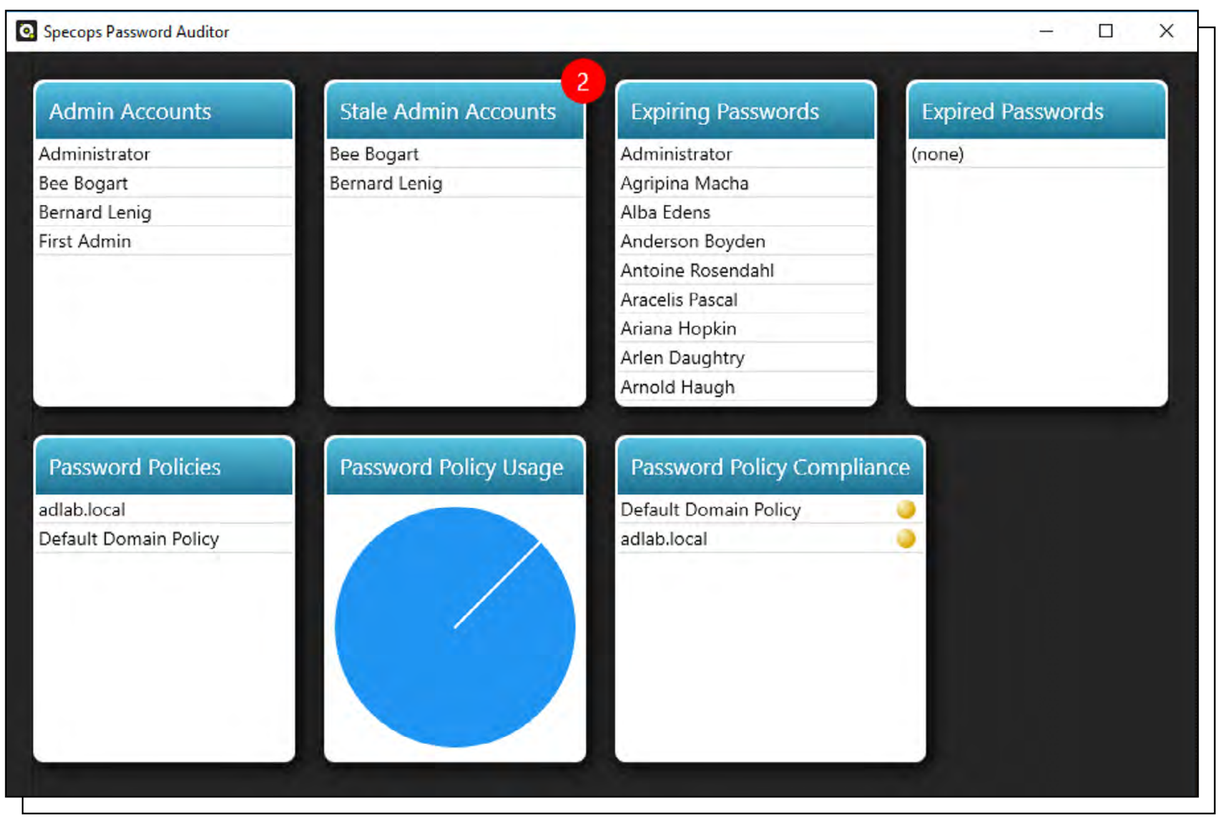
It works by querying the Specops cloud service, and you need to get a customer unique API key from Specops in order to enable it. The Blacklist Cloud API hosts an extensive and up-to-date list of leaked passwords.
Only the first few characters of the password's bcrypt hash are sent to the cloud, as sending the complete hash would be a security nightmare. The small added risk of enabling the feature is nullified by the increased security that comes with preventing users from using leaked passwords (a low-hanging fruit for attackers).

CONFIGURATION OF BLACKLIST PART OF THE PASSWORD POLICY



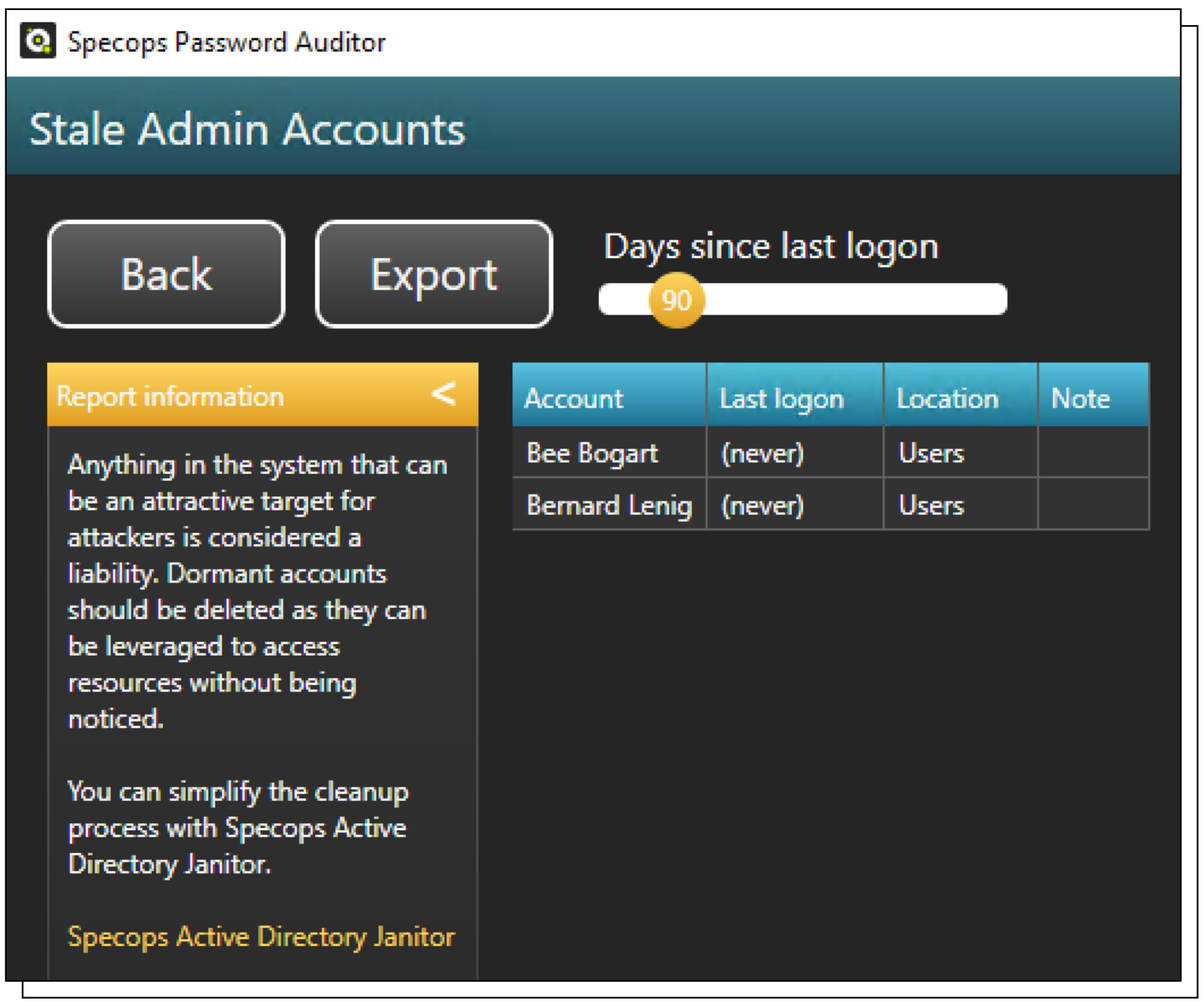
The Specops Password Auditor is another interesting tool that comes with Specops Password Policy. It scans user passwords in the specified Active Directory domain and reports expired and soon-to-expire passwords. (This should not be confused with account expirations.)

PASSWORD AUDITOR RESULTS SUMMARY



The Auditor reports stale admin accounts, used password policies and shows the password policy compliance status. You can drill down in each item in the summary overview. You can also export the whole list to a CSV file for further processing.

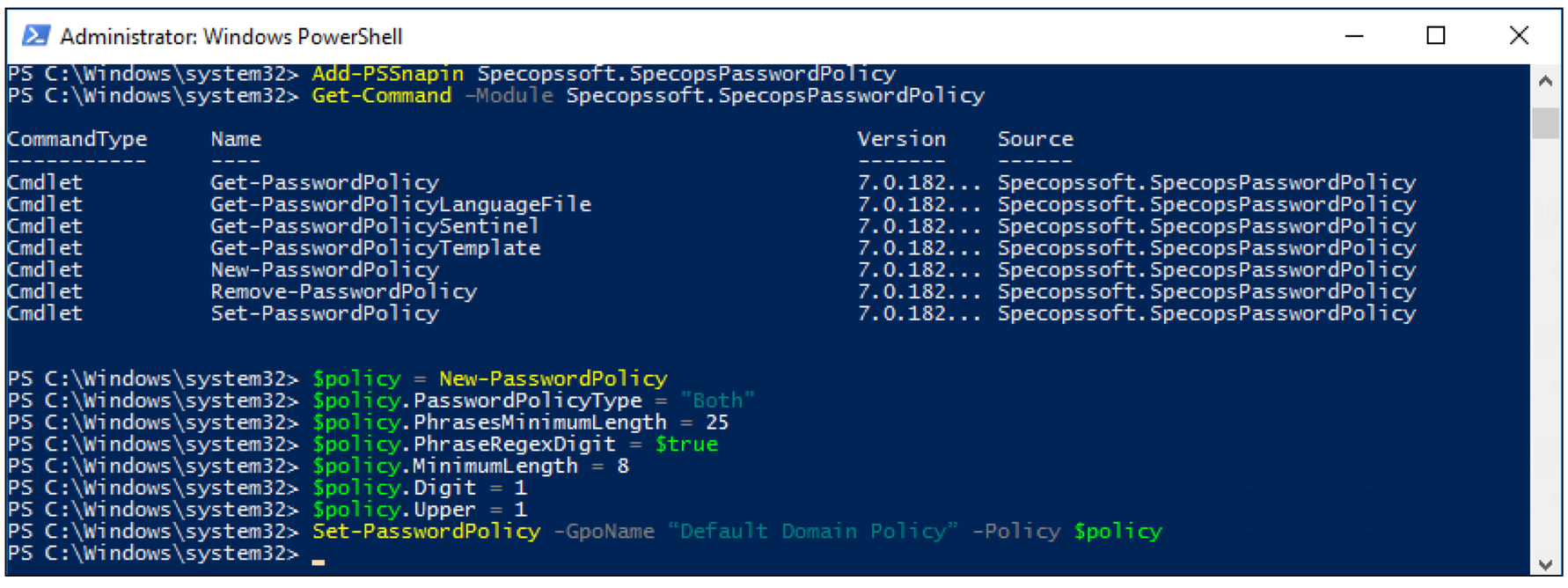
PASSWORD AUDITOR REPORT ON STALE ADMIN ACCOUNT



Those who prefer using Windows PowerShell for administering of Active Directory will be happy to know that it is possible to manage Specops Password Policy by using PowerShell cmdlets.

Specops-related cmdlets are focused on managing password policies, so it is possible to create, list, delete and set password policy for both passwords and passphrases. You just need to Register the Specops Password Policy Powershell snapin and then you can start using it.

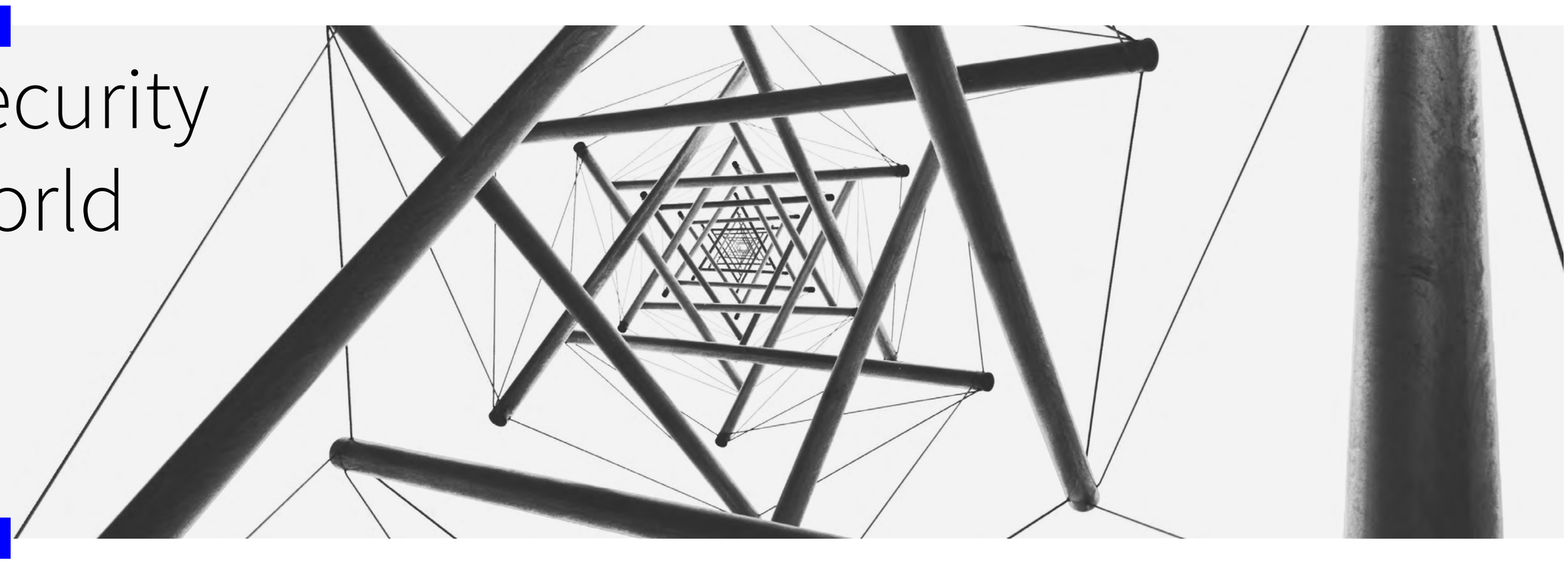
SPECOPS PASSWORD POLICY POWERSHELL CMDLETS



Final thoughts

If you are looking to strengthen passwords in Active Directory, you should definitely consider using Specops Password Policy. It's easy and intuitive to use, and works as advertised.

Security world



Cloud interoperability and app mobility outrank cost and security for primary hybrid cloud benefits

Enterprises plan to increase hybrid cloud usage, with 91% stating hybrid cloud as the ideal IT model, but only 18% stating they have that model today, according to Nutanix. Application mobility across any cloud is a top priority for 97% of respondents, with 88% of respondents saying it would “solve a lot of my problems.”

IT decision makers ranked matching applications to the right cloud environment as a critical capability, and 35% of organizations using public clouds overspent their annual budget. When asked to rank the primary benefits of hybrid cloud, interoperability between cloud types (23%) and the ability to move applications back and forth between clouds (16%) outranked cost (6%) and security (5%) as the primary benefits.

In roles centered on agility and digital transformation, IT teams understand that runtime environments for enterprise apps change constantly. Respondents indicated a need for greater orchestration and application mobility across cloud environments, as they seek flexibility to move apps to the “right” cloud on a more dynamic basis. Shadow IT practices that circumvent enterprise IT teams are posing a significant challenge to forecasting and controlling public cloud spend with well over half of respondents (57%) reporting one or more incidents of shadow IT.

Consumers can’t shake risky security habits

Despite almost half of U.S. consumers (49 percent) believing their security habits make them vulnerable to information fraud or identity theft, 51 percent admit to reusing passwords/PINs across multiple accounts such as email, computer log in, phone passcode, and bank accounts, according to Shred-it.

Consumers are not only putting their digital security at risk, but their habits toward physical information security also make them vulnerable to fraud or identity theft. While 17 percent are concerned that they could fall victim to a physical security breach, 27 percent admit they do not shred paper or physical documents containing sensitive information before throwing them away.

Organizations unable to achieve business resilience against cyber threats

The Resilience Gap study, which surveyed over 4,000 business decision makers across the United States, United Kingdom, France, Germany and Japan found that while 96% of the global business decision makers believe that making technology resilient to business disruptions should be core to their firm's wider business strategy, the reality is very different. In fact, only 54% of respondents claim that it definitely is.

Despite 96% of respondents claiming that business resilience is important to their organization, several barriers to achieving business resilience remain, with clear challenges between internal organizational structures and access to the right skills and technology.

Over a third (34%) blame their organization's growing complexity, while, one fifth (20%) blame siloed business units. Looking to their team and tools, a third (33%) say the issue lies with the hackers being more sophisticated than IT teams, 21% claim that they don't have the skills needed within the company to accurately detect cyber breaches in real-time and almost a quarter (24%) claim that poor visibility of entry points is the biggest barrier to business resilience.

Demand for cybersecurity professionals continues to accelerate

Employer demand for cybersecurity professionals across the United State continues to accelerate, according to new data published on CyberSeek, created by CompTIA and Burning Glass Technologies through a grant awarded by NIST.

U.S. employers in the private and public sectors posted an estimated 313,735 job openings for cybersecurity workers between September 2017 and August 2018. That's in addition to the 715,000+ cybersecurity workers currently employed around the country.

"Increasingly, governments and businesses are working to build better defense against cyber attacks, but training programs are simply not producing enough cybersecurity talent to keep up with demand and to keep data-driven enterprises safe," noted Matthew Sigelman, CEO of Burning Glass Technologies.

Despite the rise in security awareness, employees' poor security habits are getting worse

Despite an increased focus on cybersecurity awareness in the workplace, employees' poor cybersecurity habits are getting worse, compounded by the speed and complexity of the digital transformation.

Of the 1,600 global employees Vanson Bourne surveyed, 75% of respondents admitted to reusing passwords across accounts, including work and personal.

Organizations are at varying stages of the digital transformation, and that evolution has presented an increasingly complex IT environment to manage securely. Yet the survey findings points to a workforce who are less committed to security best practices. This has not only introduced more risk, but also a sense of frustration between the IT team trying to secure and enable the business and users who want to work more efficiently.

Reported breaches in the first 9 months of 2018 exposed 3.6 billion records

There have been 3,676 publicly disclosed data compromise events from the beginning of the year through September 30. Breach activity continues at a consistent pace for 2018, which although significant in level, will likely not reach the numbers we saw in 2017, according to the 2018 Q3 Data Breach QuickView report by Risk Based Security.

“The number of reported breaches shows some improvement compared to 2017 and the number of records exposed has dropped dramatically,” said Inga Goddijn, Executive Vice President for Risk Based Security. “However, an improvement from 2017 is only part of the story, since 2018 is on track to have the second most reported breaches and the third most records exposed since 2005. Despite the decrease from 2017, the overall trend continues to be more breaches and more mega breaches impacting tens of millions, if not hundreds of millions, of records at once.”

Employees aren’t taking the proper steps to keep information safe while traveling

ObserveIT surveyed more than 1,000 U.S. employees ages 18 to 65+ who have traveled with corporate devices in the past year and found that the majority are putting connectivity and efficiency above security, and using public Wi-Fi and unauthorized devices to access work email and/or files on the go.

While they may not have malicious intent, the negligent actions of employees caused 64 percent of all insider threat incidents in the past 12 months (Ponemon Institute). And, though breaches caused by accidental insiders can happen at any time, there’s heightened risk when employees are outside the office, using public workspaces or personal devices to remain connected.

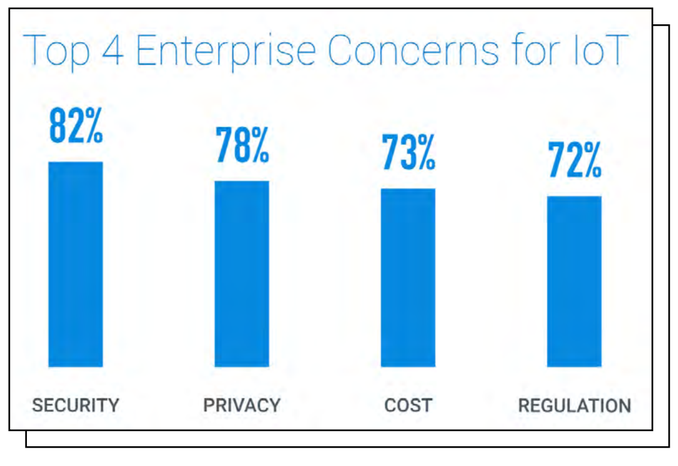
The survey confirms that employees are, in fact, jeopardizing corporate information while they’re traveling, and employers aren’t doing enough to mitigate these risks.

IoT related security missteps cost enterprises millions

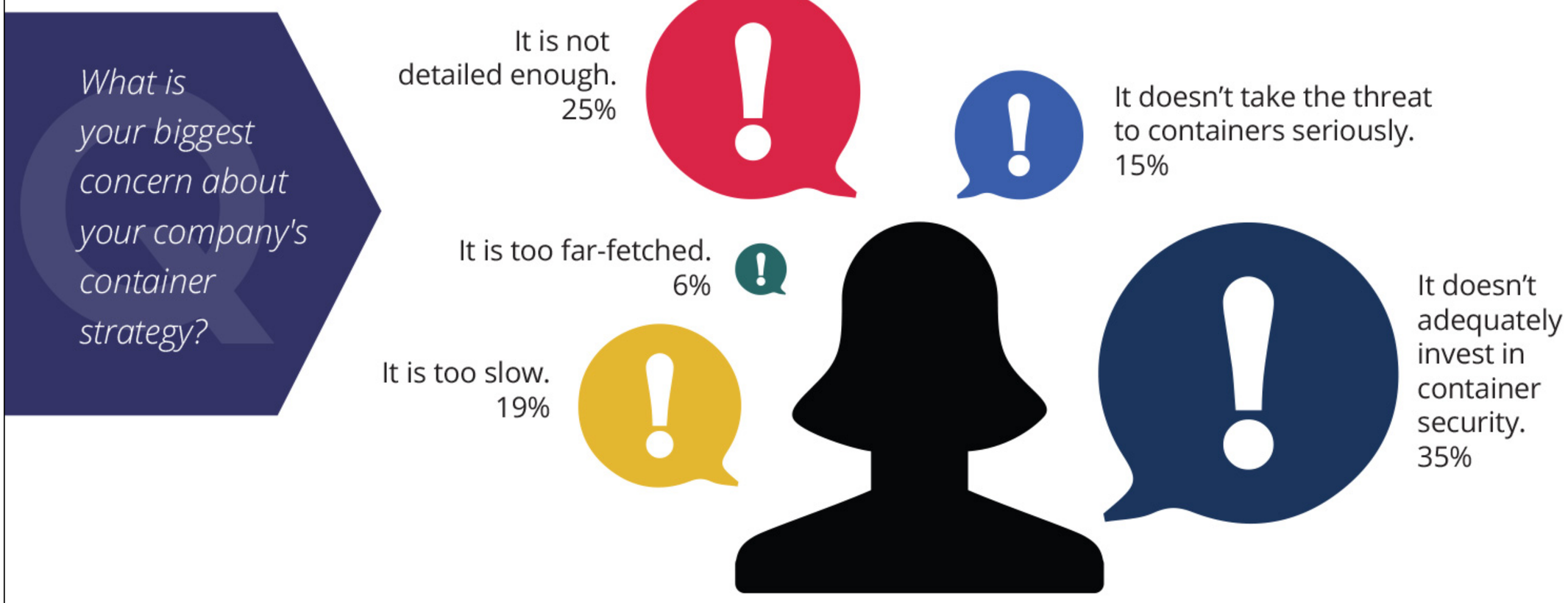
Enterprises have begun sustaining significant monetary losses stemming from the lack of good practices as they move forward with incorporating the IoT into their business models, according to a new study from DigiCert.

Among companies surveyed that are struggling the most with IoT security, 25 percent reported IoT security-related losses of at least $34 million in the last two years.

These findings come amid a ramping up of IoT focus within the typical organization. Eighty-three percent of respondents indicated that IoT is extremely important to them currently, while 92 percent said they anticipate IoT to be extremely important to their respective organizations within two years.



Container strategies don’t take security seriously enough



Most organizations do not feel prepared to adequately secure cloud-native applications, despite the surging adoption of containers and Kubernetes, according to a recent survey by StackRox.

Notable findings:

- More than a third of organizations with concerns about their container strategy worry that their strategies don’t adequately address container security
- An additional 15 percent believe their strategies don’t take seriously enough the threat to containers and Kubernetes deployments
- More than one-third of respondents haven’t started or are just creating their security strategy plans.

Digging into the sources of concern over container security, survey respondents focused on misconfigurations and runtime security as their primary sources of concern:

- Fifty-four percent of respondents said risks driven by misconfigurations and accidental exposures is their primary concern
- A near majority of respondents, 44 percent, indicated that runtime (vs. build and deploy) is the phase they are most concerned about from a security perspective.

Post implementation, GDPR costs higher than expected

A Versasec survey examining the global impact of the General Data Protection Regulation (GDPR) nearly six months after its roll-out shows the privacy regulation costs more to implement than many had anticipated, and that non-EU companies are adopting similar regulations in anticipation of stronger customer privacy rules in their own locations.

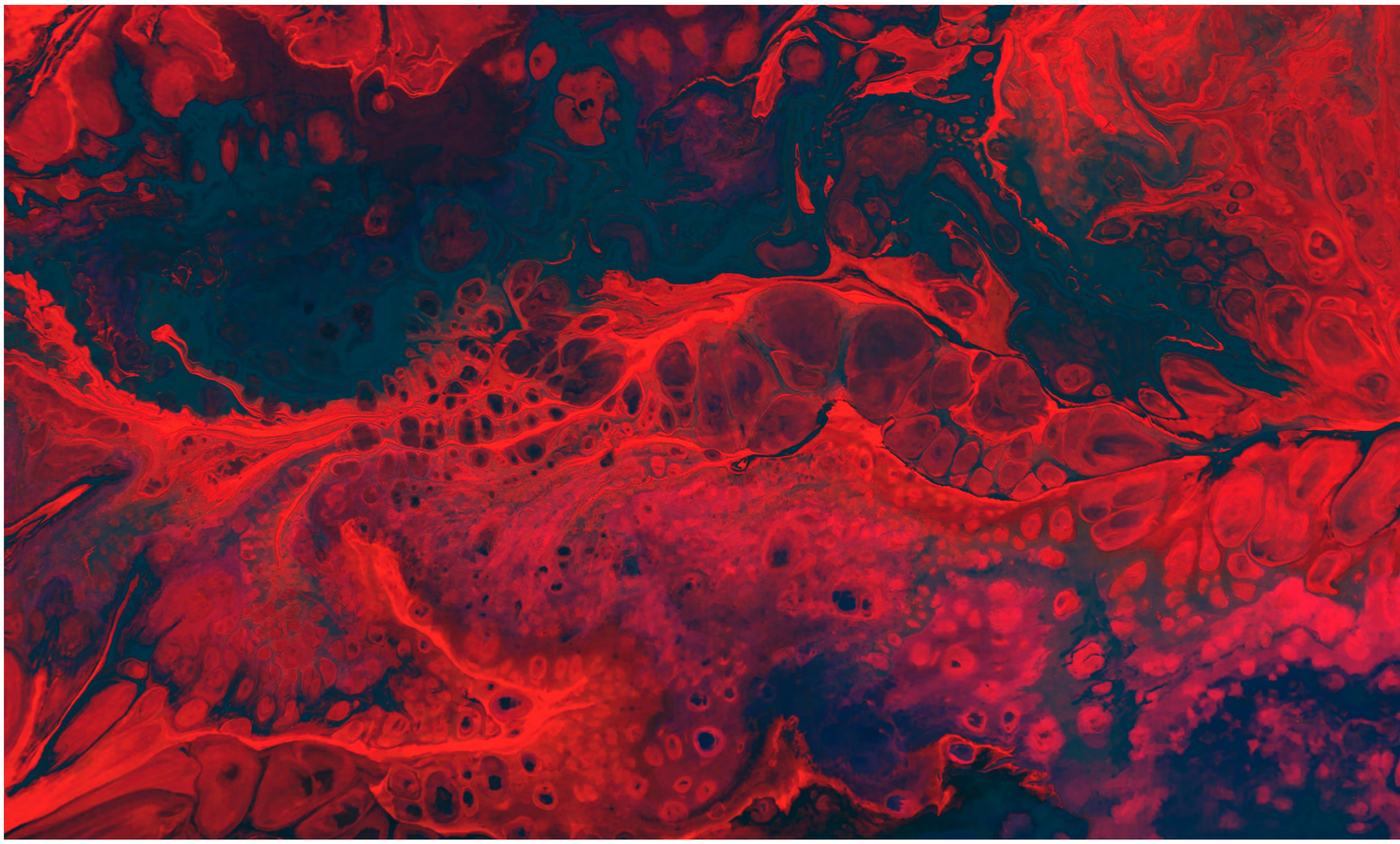
Though the survey showed a generally positive response to GDPR, 41 percent of respondents said their companies paid more than they had anticipated for compliance with the regulation. Another 41 percent said they were successful in keeping their costs on budget, and 18 percent said it cost them less to implement than they had expected.

Companies said their challenges centered around educating internal employees (27 percent), not having enough resources to complete the implementation (23 percent), communicating with customers (20 percent) and addressing technical issues in a timely manner (20 percent).

Cyber attacks ranked as top risk in Europe, North America, East Asia and the Pacific

There are significant differences in risk perceptions across the eight regions covered in the World Economic Forum's Regional Risks for Doing Business report. Over 12,000 executives highlighted concerns ranging from economic to political, societal and technological. Unemployment, failure of national governance and energy price shocks were among the top worries of executives across various regions.

Cyber attacks are the number one risk in Europe, East Asia and the Pacific, and North America. This points to growing concerns about technological risks – cyber attacks were the top risk in two regions, according to the 2017 survey (East Asia and the Pacific and North America), and only one region in 2016 (North America).



Break out of malware myopia by focusing on the fundamentals

AUTHOR_ Josh Mayfield, Director of Security Strategy, Absolute

Organizations today suffer from malware myopia, a condition characterized by threat-centric security programs and caused by the ease of imagining a takedown by malicious code. Malware myopia is a mental bug; a defect in reasoning that scrambles people's judgment. If asked point-blank, few would say that malware is an existential threat.

To be sure, it is vital to acknowledge that an attacker only has to be "right" once, and given eye-catching headlines surrounding new forms of malware, it's only natural to conclude that a narrow focus on these threats is simply responsible stewardship. A recent study showed the use of fileless malware now represents 42 out of 1,000 (4.2%) endpoint attacks, raising fears and distorting our evaluation of the risk.

+ To anchor our security programs to objective risk rather than subjective fear, we must turn our gaze inward and analyze our own cyber hygiene

The ability to understand and prioritize cyber hygiene is the cure for overestimating malware's impact, because it provides a statistically derived understanding that works as an antidote for malware myopia. For the purposes of this piece, I'll define cyber hygiene as a composition of controls, protective technology and behaviors that make up the character of a computing environment able to withstand cyber risks. First, let's see what keeps us from putting our attention on cyber hygiene.

A matter of incentives

The fundamental truth behind malware myopia is that all malware requires a vulnerability or an exposure. But there's often an execution gap when it comes to prioritizing cyber hygiene to uncover those weaknesses. A top reason for this execution gap is a lack of incentive. Unlike sexy, Hollywood depictions of the cyber realm, cyber hygiene looks nothing like a scene out of Minority Report. The work devoted to strong cyber hygiene does not have the same appeal as AI, robots, successful implementations of fileless antimalware or GPU crypto-blocking. The action movie visions of grandeur can lure us away from what really contributes to cyber resilience: incremental improvements of cyber hygiene.

Thomas Edison once quipped, "The reason most people miss opportunity is because it comes dressed in overalls and looks like hard work." Unfortunately, the accoutrements of cyber hygiene are also stained and worn, veiling the fact that it's the best way to protect data, devices, apps and users.

> Because of its relatively low appeal, cyber hygiene often doesn't create an irresistible urge to pursue it, but this aversion can be overcome.

By utilizing management by objectives (MBO) and tying bonuses to measured improvement in cyber hygiene, managers can encourage employees to focus on the basics.

Entropy

While incorporating incentives adds a boost to a renewed focus on cyber hygiene, there is an endogenous reason for the struggle. The second law of thermodynamics tells us that everything in the universe goes from order to disorder (entropy). For example, if you build a sand castle on the beach and return the next day, there's a very small chance it'll still be standing. There's a high chance of a child knocking it over or the tide's waters washing it away. There are far more ways for things to go wrong than for them to go right. This order dissipation applies to IT resources as well. Without direct action, entropy will degrade configurations, security controls, application resilience or data protection. They will, inevitably, move toward disorder. Couple entropy with a lack of incentive and you get invisible influences that keep us from achieving strong security hygiene.

Environmental evolution

Environmental evolution can lead to a breakdown of the basics, as well. New technology, processes and user demands have changed the makeup of IT resources and mandates. When confronted with mutations on the attack surface and generational turnover within the user population, it's easy to see how IT teams are unable to spend time sustaining the gains of cyber hygiene. That's not to say anyone is relinquishing responsibility, but rather that they can't be in two places at once. When IT teams are dealing with a new environment or implementing digital transformation, it's only natural for entropy to erode the hard-won gains of cyber hygiene.

These reasons for the execution gap may seem disconcerting and even fatalistic, but don't throw your hands up just yet.

We can make extraordinary progress if we foster an environment where knowledge is unleashed to guide decisions, taking to heart the words of the physicist David Deutsche, “Anything that is not prohibited by natural law is achievable given the right knowledge.” For companies looking to close the execution gap, here are a few steps to prioritize.

1_Baseline your current cyber hygiene and break apart its defining attributes: To establish a baseline and forge strong cyber hygiene, start with asset intelligence—an intimate awareness of what makes up your IT environment. Then form red teams to identify and assess risks, test assumptions and reveal the security blind spots for your organization. Give red teams full autonomy and listen to their findings. It’s better to have them discover your blind spots than someone with less benevolent intentions.

2_Monitor key metrics and tie incentives to them: To make cyber hygiene more attractive, tie incentives to the metrics that indicate cyber hygiene’s direction. A key metric is what I like to refer to as the endpoint hygiene index, a composite of true/false measures to see when resources drift from desired hygiene. Reward IT security teams for keeping the hygiene index above an agreed upon threshold. Two other key metrics to monitor include indicators of exposure (IOE), artifacts signifying the susceptibility to compromise, and the window of vulnerability (WoV), the average time it takes to mitigate IOEs. Align team incentives to performance against these variables and be honest about where you stand.

3_Automate actions that toggle the attributes to restore hygiene: After breaking apart your cyber hygiene’s defining attributes and tying incentives to key metrics, you should automate key functions. Is encryption disabled? Automate its restoration. Is there unauthorized software? Automate its removal. Using automation will enable IT security teams to catch any drifts away from the desired state and pull resources back to squeaky clean hygiene.

While these steps are a solid start to getting organizations on the right track, security teams must first acknowledge their need for a cyber hygiene scrub. Embarrassment and shame often overshadow action, as security teams are reticent to admit that they don’t diligently practice the foundations. If they don’t see it, they have plausible deniability - it’s human nature.

However, in the world of cybersecurity, we must forego childhood warnings and go looking for trouble.

By paying attention to cyber hygiene and staying committed to maintaining it, we prevent malware myopia from taking root. When malware has no place to sprout, it becomes inert and our fears about it can be better aligned with its objective risk. This gives security teams the power minimize the likelihood of cybercriminals catching them disarmed when they arrive at the proverbial castle.

A VISIBILITY PLATFORM THAT **SCALES** WITH YOUR NETWORK

BRIDGE THE GAP between today's high speed networks and your existing performance, monitoring and security tools.

INCREASE TOOL ROI by optimizing your existing deployments and feeding them 100% of relevant data in real-time.

DEPLOY SEAMLESSLY without the need for engineers, manage traffic from a single-pane management interface and expand at will.

Discover the four core dimensions of network visibility with your free white paper:
www.networkcritical.com/whitepaper-4d-visibility

Network Critical
The Window to your Network™

Securing our future in the age of IoT

AUTHOR_Sean Walls, Vice President, Eurofins Cyber Security

It is estimated that, by 2025, more than 80 billion devices will be connected to the Internet. This rapidly expanding attack surface will become the greatest cybersecurity risk since the emergence of the Internet itself. This threat arises not only from the lack of security built into these systems, but also the tendency to neglect them from a security management and hardening perspective, creating easy targets for compromise. Therefore, the solution to this complex problem needs to adequately address both of these fundamental issues: secure design and secure management.

How to develop secure IoT devices

Designing secure IoT devices requires intent and careful consideration from the beginning of the development process. Security should be part of every stage of development, beginning with the planning phase. This is the perfect time to consider the protection mechanisms required to address

security concerns in a way that is proportionate to the critically and sensitivity of the device being created.

Having a security standard to follow would help ensure consistency and interoperability of IoT devices, while simplifying the integration and management of these systems.

Unfortunately, one of the fundamental weaknesses facing this industry is a lack of agreed upon standards for security and communication.

However, there are emerging standards from the IEEE-SA (Institute of Electrical and Electronics Engineers Standards Association) and the ITU (United Nations' specialized agency for information and communication technologies) that address communication aspects, as well as UL standards focusing on the software security of network-connected devices. It is likely that these standardization issues will be resolved in the near future; however, until then manufacturers should leverage these de facto standards to guide their design and manufacturing decisions.

When purchasing IoT devices, it is important to choose a manufacturer that aligns with security standards and industry best practices. This will ensure that the systems you are implementing will not inject unnecessary risk into your enterprise. Standards certify that products are designed with adequate security and also ensure that they are maintained with vulnerability management processes in place, thus guaranteeing your product will remain secure throughout its usable life. Performing due diligence when selecting a device is the first step to maintaining a secure IoT environment.

IoT design best practices to look for when selecting a device

1_Documentation

It's important to ensure that the product is adequately documented from a design and functionality perspective, but also from a security standpoint. Confirm that user manuals and configuration guides that address security features and functionality are available.

2_Access, authentication and authorization

Restricting access is critical, and a device's defense front line. Ensure that adequate controls, such as access control lists, user and administrative management, permissions, and role-based access, can be configured.

3_Remote communication

The device should provide secure remote and administrative access (e.g., via HTTPS). Additionally, Wi-Fi and Bluetooth need to be securable via adequate authentication mechanisms and encryption algorithms.

4_Data protection

Many IoT devices collect, store and transmit sensitive data. It is, therefore, important that adequate controls can be implemented to protect that data in transit and at rest. This may require encryption capabilities.

5_Risk and vulnerability management

It's important to ensure that manufacturers regularly assess risk levels and addresses critical vulnerabilities in a timely fashion. Security and software update notices should be issued promptly, and patches or workarounds must be made available within a reasonable timeframe.

6_Software security

Manufacturers should ensure software is tested against know vulnerabilities, such as the OWSAP Top 10, prior to release and after major software updates.

Securing and managing IoT devices in production

IoT devices must be integrated into the enterprise without injecting unnecessary risk.

This requires an organization to adopt policies and processes for managing and maintaining IoT devices, much the same way they would with other assets in their enterprise. Securing these devices often starts with defined procurement, staging, and implementation processes, which will ensure only secure devices are acquired, adequately hardened, and managed securely while in use.

IoT security best practices for deployment to production

1_Procurement process

It's important to create a standardized approach to follow when selecting IoT devices, so that the manufacturer and the device are adequately vetted prior to purchase.

2_IoT device policies

Organizations should amend their network security policies to ensure they address the configuration and management of

IoT devices. This will improve accountability and consistency throughout the organization and ensure IoT devices are implemented in a way that brings maximum benefit to the business, with minimal risk.

3_Hardening process

IoT devices should be adequately secured to minimize risk. Be sure to follow your organization's hardening process prior to deployment. Below are examples of some best practices:

- Remove or disable unused services
- Change OEM passwords
- Use strong passwords
- Enable adequate logging and auditing
- Install endpoint protection
- Update software and install the latest patches

4_Implementation process

Moving an IoT device to the production environment should follow proper design, testing, and configuration practices, which may include:

- Network segmentation
- Security and integration testing
- Configuring devices according to corporate security and configuration standards
- Implementing adequate identity and access management controls

5_Production management

Once a device is deployed, it's important to maintain it in a secure manner. This may include, but is not limited to:

- Following approved change management processes
- Limiting administrative access
- Implementing patch management processes
- Monitoring for vulnerabilities through regular testing and the review of the manufacturer's security notifications
- Adequate monitoring and alerting
- Developing and testing incident response capabilities
- Secure communications for administrative access and the transmission of sensitive data

6_Asset management

In order to protect your enterprise, it's important to know what assets are on your network.

This requires processes be in place to:

- Identify assets on the network
- Monitor an asset's configuration state and security posture
- Assign asset owners and custodians
- Document the criticality of each asset

7_Access management

It's important to restrict access using the principles of least privilege and need-to-know, not only with traditional IT management but also with IoT devices. Centralized authentication should be used whenever possible, along with robust authentication mechanisms such as strong passwords, certificates, or multi-factor authentication.

8_Vulnerability management

IoT devices should be included in an organization's vulnerability management program. These systems should be regularly tested for vulnerabilities, and remediation actions taken in accordance with corporate risk and vulnerability management policies.

9_Data protection and regulatory compliance

When sensitive data is collected, stored, or transmitted by IoT devices, it's important to ensure this data is protected in accordance with corporate and regulatory compliance requirements. Understanding these requirements and how they translate into the management of IoT systems is vital. Ensuring sensitive data is protected at rest and in transit is only the beginning. Other requirements may include access monitoring, file integrity checking, data inventory management controls, and data retention and destruction policies.

Conclusion

IoT technologies will bring many benefits to society and business, but those advantages will only be realized if we understand the risks and take intentional steps to mitigate and resolve those dangers.

Ensuring manufacturers design IoT devices with security in mind is the first step, but it is equally important to manage and maintain them in a secure manner. Remember, security is holistic in nature and requires cooperation from all stakeholders, both manufacturers and end users.

Blind spots and how to see them: Observability in a serverless environment

AUTHOR_Gadi Naor, CTO, Alcide

Companies embracing DevOps and cloud to fuel digital transformation are increasingly turning to serverless computing, also known as “functions-as-a-service” (FaaS), to shift resource-intensive operational duties away from developers to cloud providers.

According to the Cloud Native Computing Foundation, the use of serverless technology is surging, up 22 percent since December 2017, with 26 percent of organizations planning to deploy within the next 12 to 18 months to maximize operational efficiencies and enable application developers to focus on their core job functions, i.e., writing code.

Yet relinquishing infrastructure control to the provider creates a new set of risks for both development and security teams, including several major blind spots that traditional security toolsets are not able to capture:

Ownership confusion

Many organizations run serverless-based applications in conjunction with other types of workloads, like containers or virtual machines.

+ Each added element introduces a new layer of complexity to the environment.

Additionally, since serverless functions are constantly processing data flowing from numerous sources, organizations can quickly lose track of who is responsible for securing which of these many moving parts.

And as input sources and data streams multiply and the environment becomes more complicated by the day, so too does the overall attack surface. In a serverless environment, while the infrastructure attack surface is reduced, the application attack surface remains as vulnerable as applications deployed on your own VMs or containers.

Yet as a fairly new technology, many development and security teams do not fully understand the unique security risks serverless architectures present – let alone how to adequately control and prevent them.

Over-privileged functions and users abound

In serverless environments each application is comprised of many specific functions. Each of these functions requires a level of access to perform what it needs to do. All too often, however, functions are assigned full permissions so they don't slow down workflow. This introduces significant security risk, as unauthenticated internal users and outside attackers may be able to compromise functions with elevated access, manipulate application flow and take unauthorized actions.

Establishing function-level segmentation with strong identity access management policies is critical.

+ If the serverless environment requires access to a virtual private cloud, it's also important to enforce least privilege principles to ensure users have the minimal level of access necessary to perform their intended functions.

A set-it-and-forget-it approach is sure to fail. Once these security policies are solidly in place, organizations must continuously monitor functions as they are deployed to quickly identify suspicious in- or out-bound traffic between networks and other anomalies, to protect against advanced attacks that transcend traditional protection layers.

Insecure storage of secrets

Most applications require secrets: API keys, access credentials, tokens, passwords, and so on. It's a common and dangerous practice for developers to simply store these secrets and access keys in plain text configuration files, or in environment variables. This is low-hanging fruit for savvy attackers.

To avoid these risks and stay in compliance, all of the credentials within function codes should be stored in-memory and accessed through a secret store. If, for some reason, the function requires the use of a long-lived secret, secrets should be encrypted. The cloud provider's key management service can be leveraged to manage, maintain and retrieve these secrets automatically.

An incomplete picture

Since serverless is typically only part of an organization's unique cloud strategy, security teams often struggle to maintain a full and accurate view of their security posture across their public and private cloud data center meshes – from serverless and containers to third-party services. That's because each workload provider follows its own security frameworks, making it nearly impossible for organizations to manage and control each piece of the puzzle. In such dynamic and disparate environments, organizations need a more practical, uniform and automated way to enforce and manage security policies and efficiently control various cloud-native services, infrastructure and environments.

The third-party problem

Serverless functions often rely on third-party services and software, such as APIs, open-source packages and libraries. Without an intelligent, automated way to discover, continuously scrutinize and control these third-party services, organizations open the door to potential vulnerabilities that can pave the way for exploit and data loss.

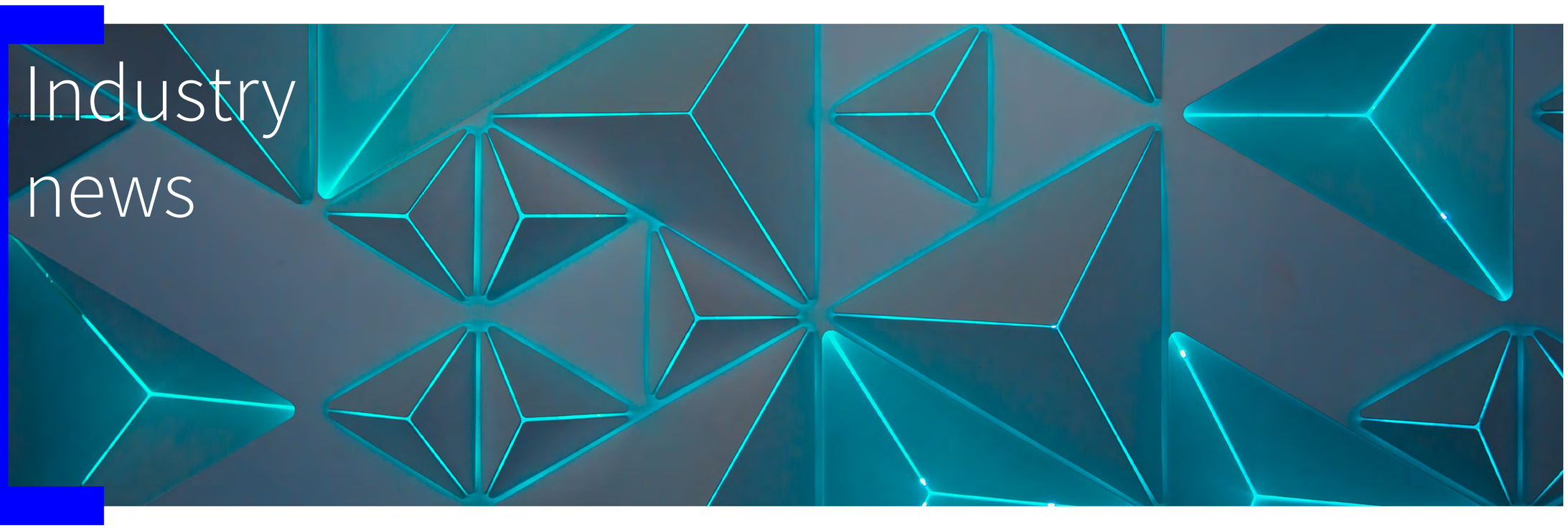
Legacy and shared security tools have limits

Legacy security tools designed for data centers compound this serverless security and observability dilemma.

Traditional firewall and endpoint protection tools and even cloud security groups lack the app-aware, fine-grained controls and advanced anomaly detection mechanisms necessary to detect and prevent advanced attacks. Further, cloud providers offer limited threat detection coverage since they are blind to network-based attacks such as DNS exfiltration, spoofing and lateral movement. As such, enterprises need the extra layer of network protection not currently made available by leading providers such as AWS, Google and Azure.

While it's tempting to equate serverless with less security responsibility for your organization, the shared responsibility model still holds true. But this doesn't mean that organizations must trade speed and agility for security. By following best practices for securing serverless environments and utilizing cloud-native tools that simplify and unify cloud operations protection, organizations can have it all as they continue their digital transformation journey with confidence.

Industry news



DFLabs open framework enables integration of SOAR and security tools

DFLabs launched a new version of the IncMan SOAR platform that provides an open integration framework for customizing and adding new automated integrations between security tools and IncMan SOAR, without the need for complex coding. This capability enables security teams to add and orchestrate new functions between IncMan SOAR and third party products in order to address requirements and workflows.

Organizations can now extend the existing IncMan SOAR product integrations with new functions they require. For example, an enterprise using a vulnerability assessment tool may want to exclude a legacy application from being scanned due to concerns it may cause unexpected failures.

New additions to RSA Conference Advisory Board bring wealth of industry knowledge

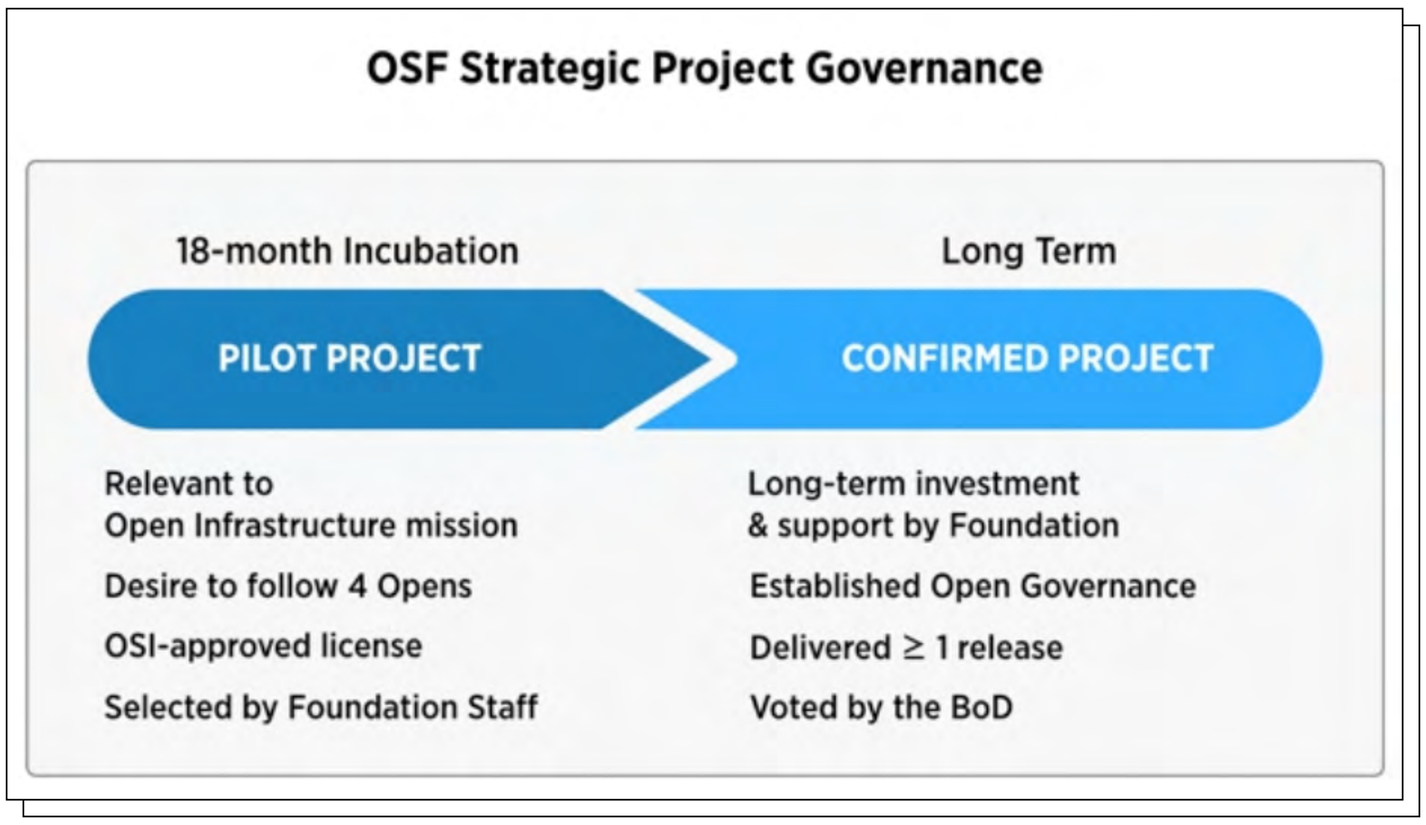
RSA Conference announced the addition of nine new members to its Advisory Board for a total of 16 members across a wide array of positions in the industry. This expansion falls under the governance pillar of the new diversity and inclusion initiative.

The RSA Conference Advisory Board is designed to assist in driving an impartial, yet informed dialogue on the rapidly evolving information security industry. It extends the influence of Conference by providing insight into trends and breaking news in the information security industry on behalf of the Conference, as well as offering guidance into overall program development.

ISACA refreshes COBIT framework to address latest business technology trends and standards

ISACA released its first update to the COBIT framework in nearly seven years. The new version, COBIT 2019, will come in four phases and will include focus areas reflecting trends and priorities in technology (e.g., DevOps, cybersecurity), updates aligned with the latest industry standards, and a design guide that provides flexibility and guidance to help organizations tailor a governance system to their needs.

OpenStack Foundation board expands mission to host new open source projects



The board of directors of the OpenStack Foundation (OSF) adopted a resolution advancing a new governance framework supporting the organization's investment in emerging use cases for OpenStack and open infrastructure.

These include continuous integration and continuous delivery (CI/CD), container infrastructure, edge computing, datacenter and, newly added, artificial intelligence/machine learning (AI/ML). The board resolution authorizes the officers of the OSF to select and incubate Pilot projects.

BehavioSec announces authentication features and patents Behavioral Biometrics Platform

BehavioSec released a series of new features to its BehavioSec Behavioral Biometrics Platform (Version 5.0) giving banks, fintech firms, retailers and cloud service providers authentication defenses against costly account hijacking and fraud committed with stolen passwords and other credentials.

BehavioSec's software platform defending Web portals, storefronts and mobile apps can now detect suspicious use of attack obfuscation techniques, including the use of virtual private networks (VPNs) and TOR-routed traffic during login attempts and sessions.

Offensive Security redesigns Exploit Database

Offensive Security's Exploit Database is the collection of exploits on the Internet. EDB is a repository for exploits and proof-of-concepts, rather than advisories, making it a valuable resource for those who need actionable data right away. The update to EDB includes a redesign to improve the speed and accuracy of searches. This includes an all-new user interface, making it easier for testers and researchers to access the data they want, when they want it. For example, in the new version of EDB, it only takes two clicks to search and filter for remote exploits targeting the Windows platform. Prior to the redesign, this took at least five clicks to accomplish.

IBM to acquire Red Hat for $34 billion

IBM and Red Hat announced have reached a definitive agreement under which IBM will acquire all of the issued and outstanding common shares of Red Hat for $190.00 per share in cash, representing a total enterprise value of approximately $34 billion.

With this acquisition, IBM will remain committed to Red Hat's open governance, open source contributions, participation in the open source community and development model, and fostering its widespread developer ecosystem. In addition, IBM and Red Hat will remain committed to the continued freedom of open source, via such efforts as Patent Promise, GPL Cooperation Commitment, the Open Invention Network and the LOT Network.

NTT Security adds botnet infrastructure detection to Managed Security Services

NTT Security has developed a new network analytics technology to detect and defend NTT Group's Managed Security Services (MSS) customers from attacks launched on botnet infrastructures. The new network flow data analysis uses machine learning and scalable streaming analytics – developed in partnership with NTT Group companies – and pulls data from NTT's global network infrastructure, which provides visibility into the world's internet traffic.

The Linux Foundation launches Ceph Foundation to advance open source storage

The Linux Foundation and over 30 global technology leaders are forming a new foundation to support the Ceph open source project community. The Ceph project develops a unified distributed storage system providing applications with object, block, and file system interfaces.

Ceph is used by cloud providers and enterprises around the world, including financial institutions (Bloomberg, Fidelity), cloud service providers (Rackspace, Linode), academic and government institutions (Massachusetts Open Cloud), telecommunications infrastructure providers (Deutsche Telekom), auto manufacturers (BMW), software solution providers (SAP, Salesforce), and many more.

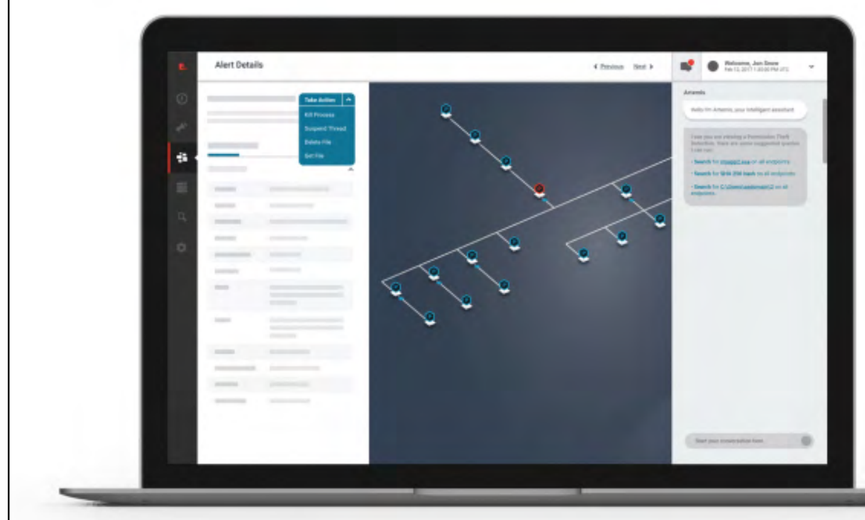
Symantec acquires Javelin Networks and Appthority

Symantec acquired Javelin Networks, a company that offers software technology to defend enterprises against Active Directory-based attacks.

Microsoft Active Directory (AD) services have become a popular target for attackers, who use AD reconnaissance to discover the users, servers and computers in an enterprise network and then move laterally across the network using this information to carry out multi-stage attacks.

Appthority's technology qill Symantec customers the ability to analyze mobile apps for both malicious capabilities and unsafe and unwanted behaviors, such as vulnerabilities, risk of sensitive data loss, and privacy-invasive actions.

Endgame introduces Total Attack Lookback for incident review

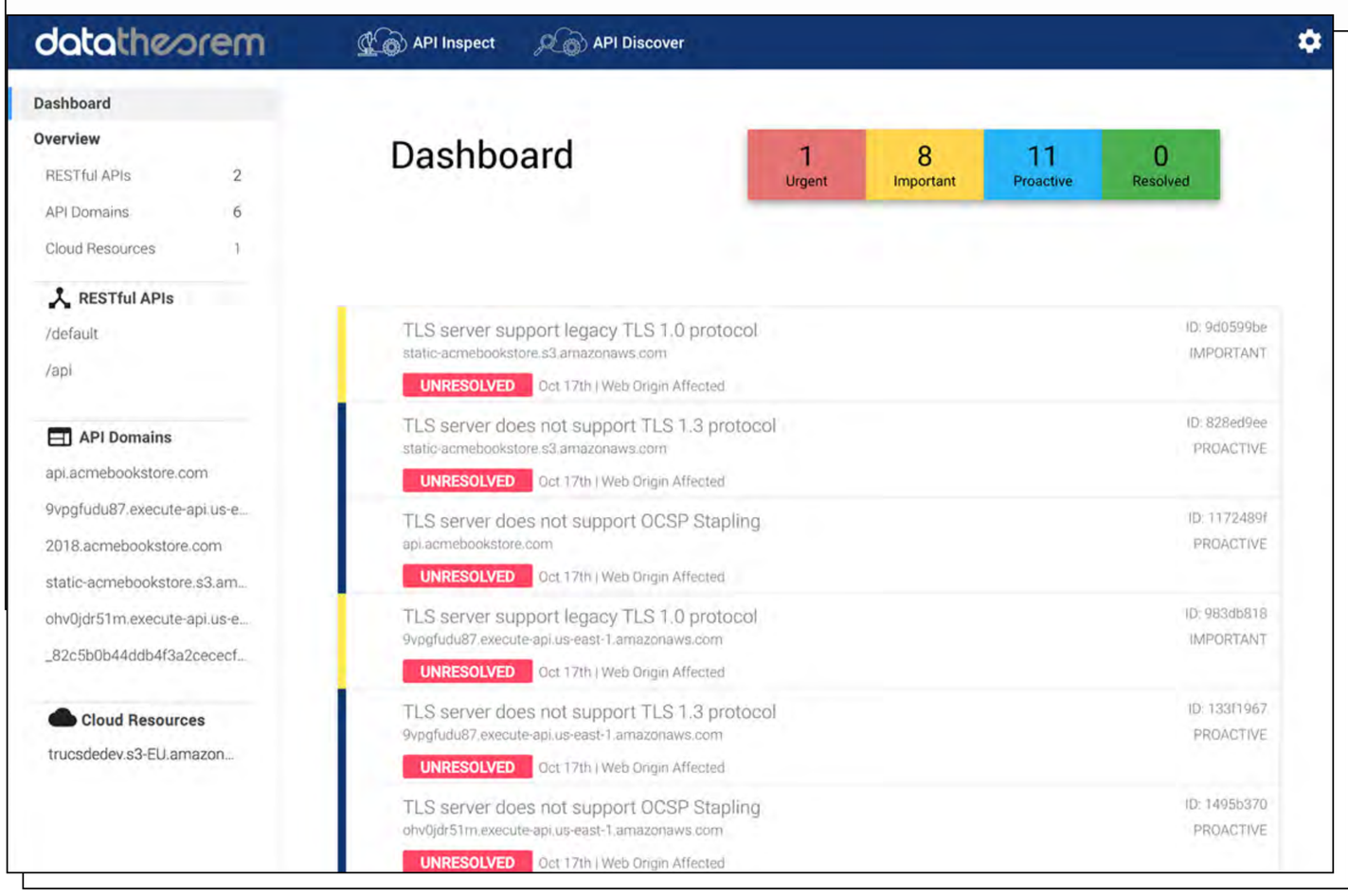


Endgame has made critical threat intelligence data available to all customers free of charge through Total Attack Lookback – the forensic review feature to exceed average adversary dwell time.

Endgame Total Attack Lookback provides a record of operating system events, to ensure assessment of the origin and extent of an attack, meet notification requirements, and minimize exposure to compliance and regulatory violations.

Data Theorem introduces automated API discovery and security inspection solution

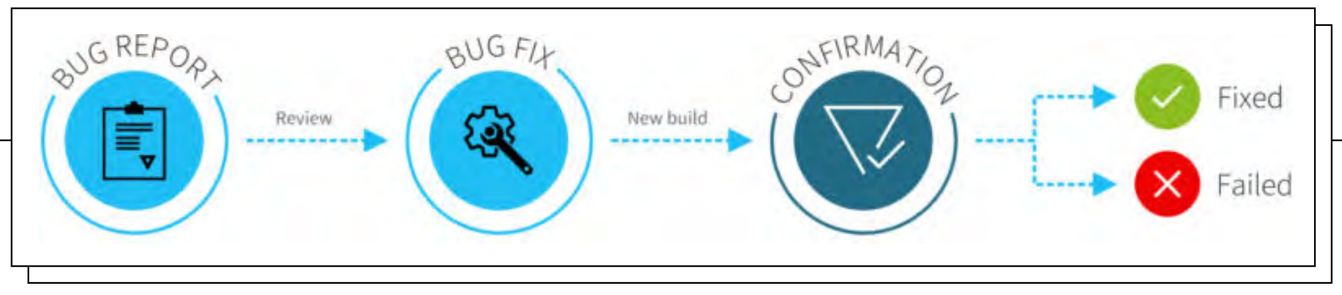
Data Theorem introduced the industry's first automated API discovery and security inspection solution aimed at addressing API security threats introduced by today's enterprise serverless and microservices applications, including Shadow APIs.
With this launch, users can automate API discovery and security inspection seamlessly into their DevOps practices and continuous integration/ continuous delivery (CI/CD) processes to protect any modern application.



Test IO introduces Bug Fix Confirmation, leveraging network of software testers to verify bug fixes

Verifying resolution of bugs is a standard step in the software development cycle and a bottleneck in release processes. It is troublesome for companies whose development teams have prioritized automated testing and have fewer QA people on staff manually testing their software.

Test IO's new Bug Fix Confirmation product enables test IO's network of testers to take on this task and supply feedback so that teams can maintain focus on fixing bugs, rather than checking them.



ISACA to update CISA exam in 2019

ISACA's Certified Information Systems Auditor (CISA) certification is being updated in 2019 to reflect the industry trends impacting the IT audit profession. Updated CISA review materials and training courses will be offered beginning in March 2019 to prepare candidates for the new version of the exam, which will take effect in June 2019.

While the five domains that comprise the CISA exam change will remain similar in 2019, the exam weighting will change, including emphasis on protection of information assets – a growing industry challenge.

For Xerox Chief Information Security Officer Dr. Alissa Johnson, human ingenuity, partnerships and automation are the answer to most security problems the company has encountered and might encounter in the future.

“The future is an amalgamation of many futures, shaped by privacy policies, breaches, all types of threats and cybersecurity responses. Changes in any of these change the trajectory of the future,” she explains. “We try to comprehend all of the possible futures and to prepare for them. There are no real shortcuts. I wish there were, but there aren’t.”

So, the company gets ready for the unknown by championing a multi-layered approach to security, whereby one layer can serve as a safety net for the others.

> There are no real shortcuts to most security problems

AUTHOR_Zeljka Zorz, Managing Editor, (IN)SECURE Magazine

Cybersecurity insurance shouldn't replace defense

One of the security layers that every enterprise should maintain to optimize their security is cybersecurity insurance. But while having it makes good sense, relying on it as a replacement for sound security practices does not.

"Diverting more funds into cybersecurity insurance instead of bolstering defenses increases the likelihood of a breach. More to the point, though, insurance payments can't make up for all of the damage done by a cyberattack," she points out.

"When customers' personal data is stolen, businesses can lose trust. When trade secrets and pricing become available to competitors, reputations and brands can be weakened and business can be lost. Fixing the problem can be a big drain on time as well as money. And make no mistake, the costs are high."

The various security layers are meant to complement one another.

"Expecting that one layer to replace or compensate for a lower investment in another is shortsighted," she opines.

Defending against APTs

Dr. Johnson was, at one point, the Deputy CIO for the White House. Today her two overarching goals are ensuring the security of the Xerox corporate infrastructure and all the products they sell that connect to the Internet.

To defend the company's infrastructure against advanced persistent threats, the company employs advanced, persistent defense built on intrusion prevention, compromised device detection, documents and data detection, and external partnerships.

For intrusion detection they rely on solutions such as internal firewalls, user access solutions, and authentication and whitelisting technology from McAfee. To detect compromised devices they employ measures such as firmware verification.

They keep personal and confidential information safe through capabilities such as secure print and encryption features. Finally, they work with compliance testing organizations and security industry leaders to enhance and protect devices with the latest security standards.

"By partnering with cybersecurity leaders, we gain expertise that complements our own, and by automating we ensure that our routine security monitoring is fault-proof while freeing our best minds to work on our toughest problems," she notes.

"In the process, we are establishing and nurturing an infrastructure and culture that is ready to preempt and respond to any and all threats, now and in the future. We bring that same mentality to our customers and our partners, sharing with them the data security lessons we have learned on the front lines of protecting our printers, scanners and other connected office equipment."

Dealing with the cybersecurity skills shortage

According to reliable estimates, 70 percent of jobs in the cybersecurity field will go unfilled by 2022.

Xerox's answer to expanding security needs and insufficient labor is, again, automation and partnerships.

"Automation because talent needs to be pulled away from babysitting data centers and blinking lights, to focus on high-risk, high-opportunity data that gives

the user a richer, higher-level experience. Partnership because a more open culture with vendors cooperating to develop technologies that meet the challenge can compensate for widespread duplication of effort across organizations," Dr. Johnson explains.

Getting the board on board

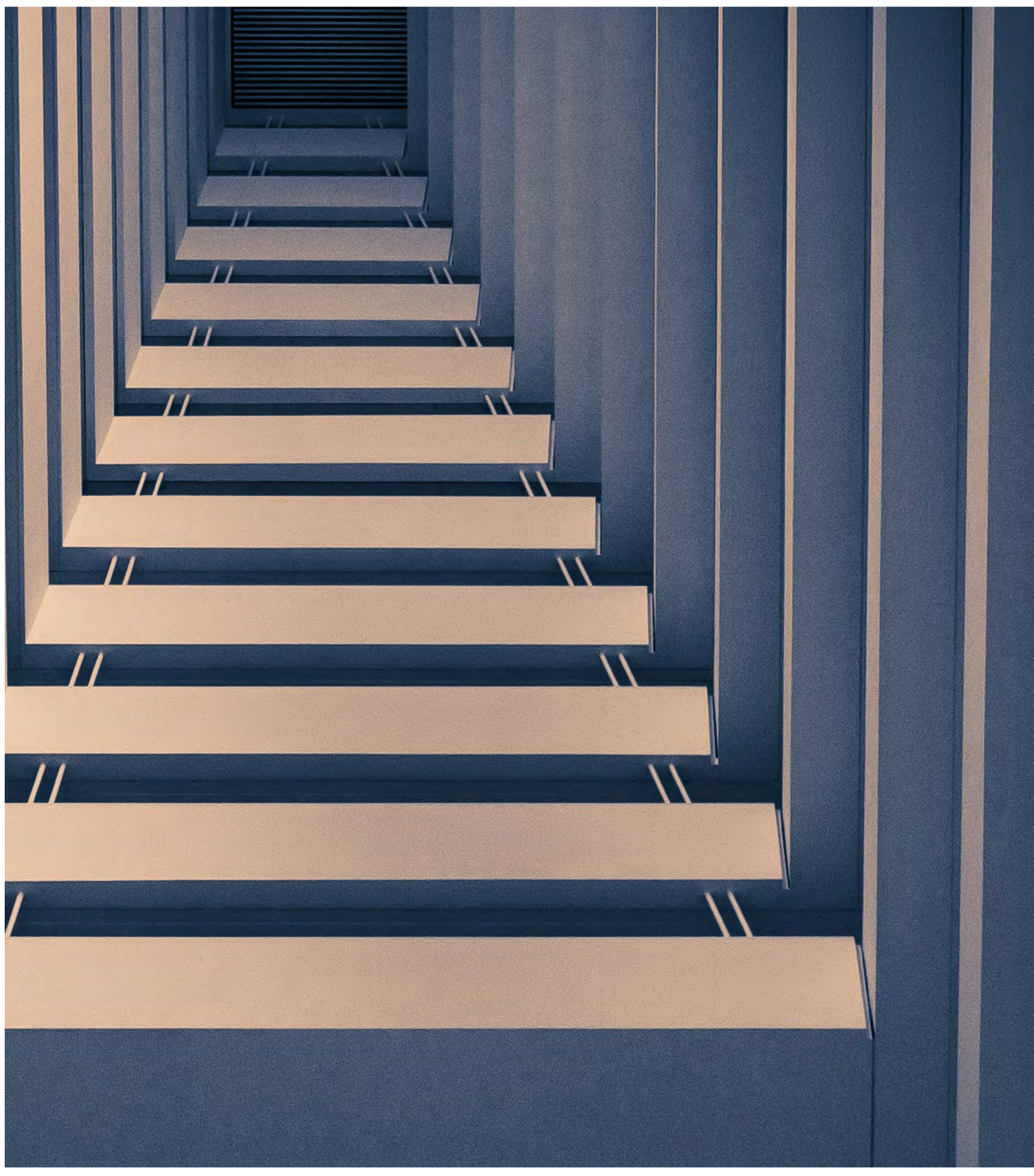
But for an effective defense, it's crucial to get the company's board and the C-level executives on board and to work well with them. The key to doing this is good communication, solid strategic plans and strong execution backed by measureable results.

"C-level executives need to understand your situation, to know how real the threats are, and to know how damaging and how costly breaches can be. Fear can be a great motivator, and in this case, the fears are very real," she explains.

"Once you get their attention, you need to lead them with a strategic plan that addresses your situation. Our plans emphasize leveraging our expertise and that of partners, and automating wherever possible, to make the most of the resources we have. These are concepts that we apply successfully in other parts of the business, so our executives are quick to grasp where we're going."

> With top executives on board, they've gotten consensus to make cybersecurity a critical focus area in their research labs as well as a critical customer requirement, so security is "baked in" during product development.

The final requirement – measureable results – is achieved by measuring their performance in a number of ways, including tracking attempts to breach their infrastructure and their success rate in keeping would-be intruders out.



Bridging the priority gap between IT and security in DevOps

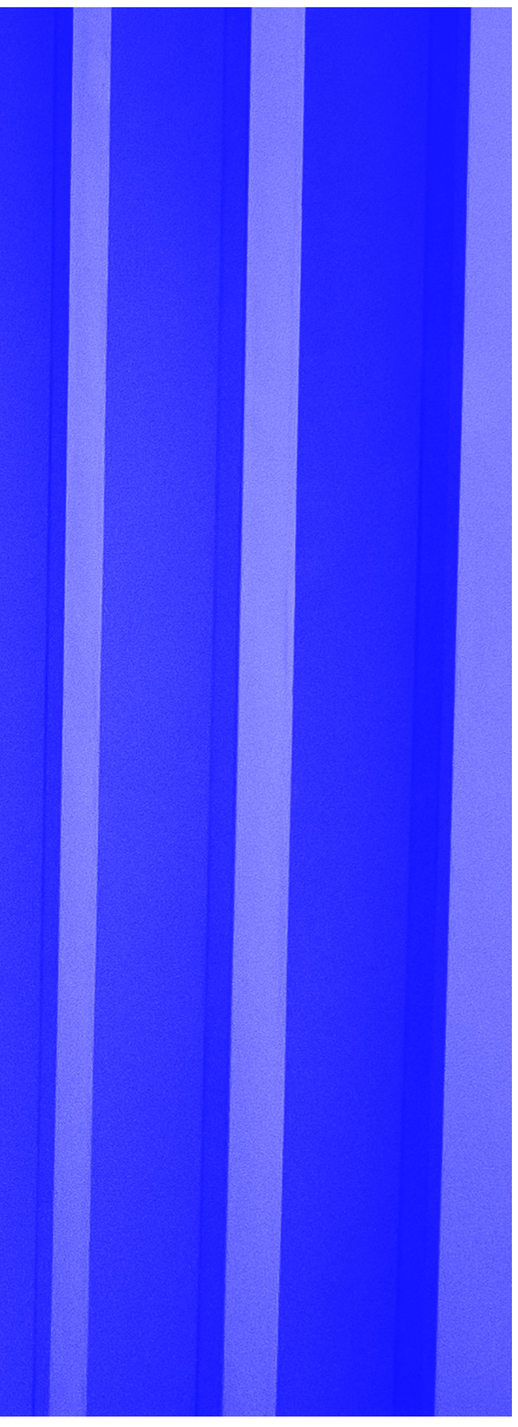
AUTHOR_ Edward Amoroso, CEO,
TAG Cyber

Let’s start with a test: Suppose that you manage a corporate network gateway across which a critical programmed transaction is scheduled to occur in exactly one hour. Suppose that the firewall protecting this gateway is functionally misbehaving and will almost certainly block any programmed activity with your transaction partner. This is a serious concern because your boss has made clear to you (several times!) the importance of this planned transaction.

Your team continues to work the technical problem, but it is now 15 minutes before the transaction is scheduled, and it is still not working - and your boss is unreachable. Your team explains that the firewall rules management function has failed, and that by disabling the entire firewall, the transaction can be made to proceed. You are told that such action, however brief, will leave the corporation open to inbound attacks, a blatant violation of security policy.

So, what do you do? If you decide that disabling the firewall, an action which you rationalize as really nothing more than just a brief administrative change, is clearly the lesser of two evils, then your tendency matches that of many IT professionals. If, however, you decide that exposing the corporation to inbound attacks could produce negative results far worse than missing some scheduled transaction, then your tendency is more in line with that of security professionals.

Setting aside any justifiable quibbles you might have with stereotyping individuals working in IT and security, most observers would agree that some priority gaps do exist in the motivation, emphasis, and objectives associated with each of these important roles in an organization. Executives who do not acknowledge these priority differences should expect occasional, perhaps even frequent, operational challenges in projects involving both IT and security.



One area where priority collisions emerge between the two groups is DevOps, which is the preferred modern lifecycle model for developing software in most environments. IT and development teams will typically view DevOps in terms of its advertised benefits: faster cycle times for new features, higher satisfaction rates for programmers, greater levels of agility for ever-changing user requirements, and so on. These are truly positive benefits.

Security professionals, however, will often raise reasonable protection concerns regarding the DevOps process. The core of their common argument is that going faster in any lifecycle can lead to errors, which might then lead to exploitable vulnerabilities.

+ Security pros will tend to remind DevOps teams that despite the need to introduce software features in a more agile manner, attention to basic security controls still cannot be ignored during the process.

This challenging priority gap between IT and security in the DevOps lifecycle might be addressed in different ways. For example, it can be arbitrated or even adjudicated by managers who keep an ear to the ground in all compliance and governance disputes, and who try to maintain order amongst teams regarding risks. While such efforts are always advised, larger DevOps environments will require more methodical controls than just diligent management.

Instead, IT and security teams are beginning to recognize an important area where the DevOps process can advance the goals and agenda for both groups. This area is automation. The various options for introducing automated support, especially for cyber risk and compliance, have grown in recent years to include many attractive vendor offerings that are rooted in practical, empirical experience.

For DevOps teams to address this priority gap, the best strategy involves optimizing automated solutions to support the governance, risk, and compliance activities that are now considered essential to any modern software process. Such automated approaches are consistent with industry models such as the Gartner Application Security Risk Threat Management (ASTRM) model.

The good news is that DevOps teams have excellent commercial options at their disposal to address this growing security risk.

+ The result of DevOps enhancement via cyber risk and compliance automation is many-fold.

Firstly, it introduces important GRC controls to reduce risk and improve compliance support for DevOps. Secondly, it helps security controls keep up with the agile pace of modern software processes. And thirdly (and perhaps most importantly) it effectively supports the goal of reducing the priority gap that exists between IT and security teams working DevOps.

The meteoric rise of cyber threats in the last few years has shown that organizations must continuously stay ahead of adversaries to protect their data, intellectual property, finances, and people.

Over the years, I've designed incident response teams from the ground up as well as led and developed such teams in mature organizations. They all had one thing in common: the incident response (IR) plan.

Some people still believe that they can do a quick search online, find a template that they can fill out, and voila', a plan! Unfortunately, this couldn't be further from the truth.

When the time comes to actually implement such a cookie-cutter plan, organizations may find that they are woefully unprepared, so it's absolutely imperative that businesses create plans that come from critically thinking through their specific needs.

Are you ready? A good incident response plan can protect your organization

AUTHOR_ Sean Mason, Director of Threat Management and Incident Response, Cisco

Organizations must have conversations that lead to the generation of a custom-fit IR plan. This not only includes what to do in the event of an incident, but also how to address incidents before they occur.

Let's look at four key components that make up a solid incident response plan:

Be proactive: Assess and then plan for today's and tomorrow's attacks

Incident response has continued to evolve over the years to the point where I struggle in calling it "incident response."

The industry has learned that proactive planning well-ahead of an incident must become the new norm. It's important to draw up the incident response plan before a cybersecurity crisis and to update it as time passes.

Additionally, an IR plan is usually best paired with an Incident Response Readiness Assessment (IRRA). An IRRA can help uncover organizational vulnerabilities or other gaps in preparedness. Businesses that dash off a plan without this step may miss key components that are not immediately apparent.

+ If you don't have the resources or expertise to conduct this assessment in-house, bring in an expert team.

In fact, it's often better to outsource this step as a third-party organization can take a more objective look at your organization's needs. Just as critical, involve your senior leadership and other cross-functional team members in the planning from the outset. They have a vested interest in the business and gaining their support and buy-in can ensure that you are all on the same page.

Taking the time to assess how prepared your organization is before you get into an incident gives you the opportunity to both plan for remediating those areas and to understand where you need to improve your defenses.

Keep it simple

Don't overthink it. While many security teams will attempt to come up with a plan for every possibility, there is no one-size-fits-all plan or playbook. The key is to establish a robust framework and process within which your organization can operate. And, if you find that there are issues that must be addressed immediately, don't wait for the plan to be fully developed - take care of them now to avoid problems later.

You must also be able to quickly reach out to the right players and experts inside and outside your business to fill in any missing elements at a moment's notice. And those individuals must be clued into – and buy into – the plan to expedite execution. They are likely to be able to help enhance the plan beyond your team's expertise.

As your organization continues to evolve, you will need to dynamically make changes to the plan and processes. You are likely to end up capturing different data that can help you both track and measure in what direction your organization is heading.

Keep it flexible

+ An IR plan must be easily modified without countless reviews and executive approvals.

By keeping the plan simple, you allow your organization to operate within a framework and workflow that should be able to adapt more quickly.

Over time, the evolution and maturity of the program can result in adding new plan sections that do not require a full overhaul or revisiting the entire scope. This can save valuable time that is better spent elsewhere when minutes count.

Measuring up: How do you know if your plan works?

Measuring your IR capabilities is critical to the success of any organization. This can help the leadership make decisions based on facts and data. By ensuring there are metrics that are captured along the way and reported on frequently, you can demonstrate the maturity of the organization. You also can pinpoint areas for process improvement in either prevention, detection, or operational response.

Some of our preferred metrics to track over the years include containment time, dwell time, collection and analysis time, and detection success by tool or technique. Another metric that is getting a solid look is time to reporting. For example, with GDPR and the 72-hour requirement to report an incident, organizations must ensure they are monitoring their capabilities and removing any inefficiencies that may arise. This will help ensure your organization is in compliance with guidelines and can avoid costly penalties.

The most important takeaways in the development and execution of a well-constructed and efficient incident plan include:

- Many templates and guides can explain what elements need to be part of an IR plan. But they typically miss what's specific to your organization. These requirements can be identified in a needs assessment.
- IR plans need to be built proactively and in a simple, flexible, and measurable way.
- An IR plan should be robust enough to provide a great framework to operate within, but flexible to handle multiple threat scenarios.
- Keep it flexible to facilitate updates. Review and update the document regularly as the organization's needs or market dynamics change.
- Understand how you will measure your plan's effectiveness. This is critical when it comes to developing the team infrastructure as the organization matures. It also will tell you when the plan is working as designed or when it needs to be adjusted.

Events

RSA Conference 2019

March 4 – 8, 2019
Moscone Center, San Francisco
https://www.rsaconference.com/helpnet-us19

Looking for cybersecurity intel? Your search starts and stops here, at RSA Conference 2019, March 4 – 8 in San Francisco. A hub for innovation, industry experts and up-and-coming talent alike, RSAC 2019 is where the world talks security. And security talks back.

From expert-informed keynotes, enlightening seminars, and interactive exhibitions, the agenda is filled with critical discussions on today's trends, challenges and forward motion. AI, machine learning, geopolitics—it's all on the table. All you have to do is join in.

In fact, why not join in right now? Register by February 1 to save $900 on your Full Conference Pass - https://www.rsaconference.com/helpnet-us19

Gulf Information Security Exhibition and Conference 2019 (GISEC)

April 2 – 4, 2019
Dubai World Trade Centre
https://www.gisec.ae

The Gulf Information Security Expo & Conference (GISEC) brings together over 8,000 top Infosec and tech sector professionals to discover cutting-edge solutions, share insights with industry experts and equip themselves with the right tools to protect their businesses from rapidly-evolving cyber attackers.

The next generation of cybersecurity is powered by machine learning

Arm your business with future-ready technology

We use machine learning and big data to help our clients protect home user

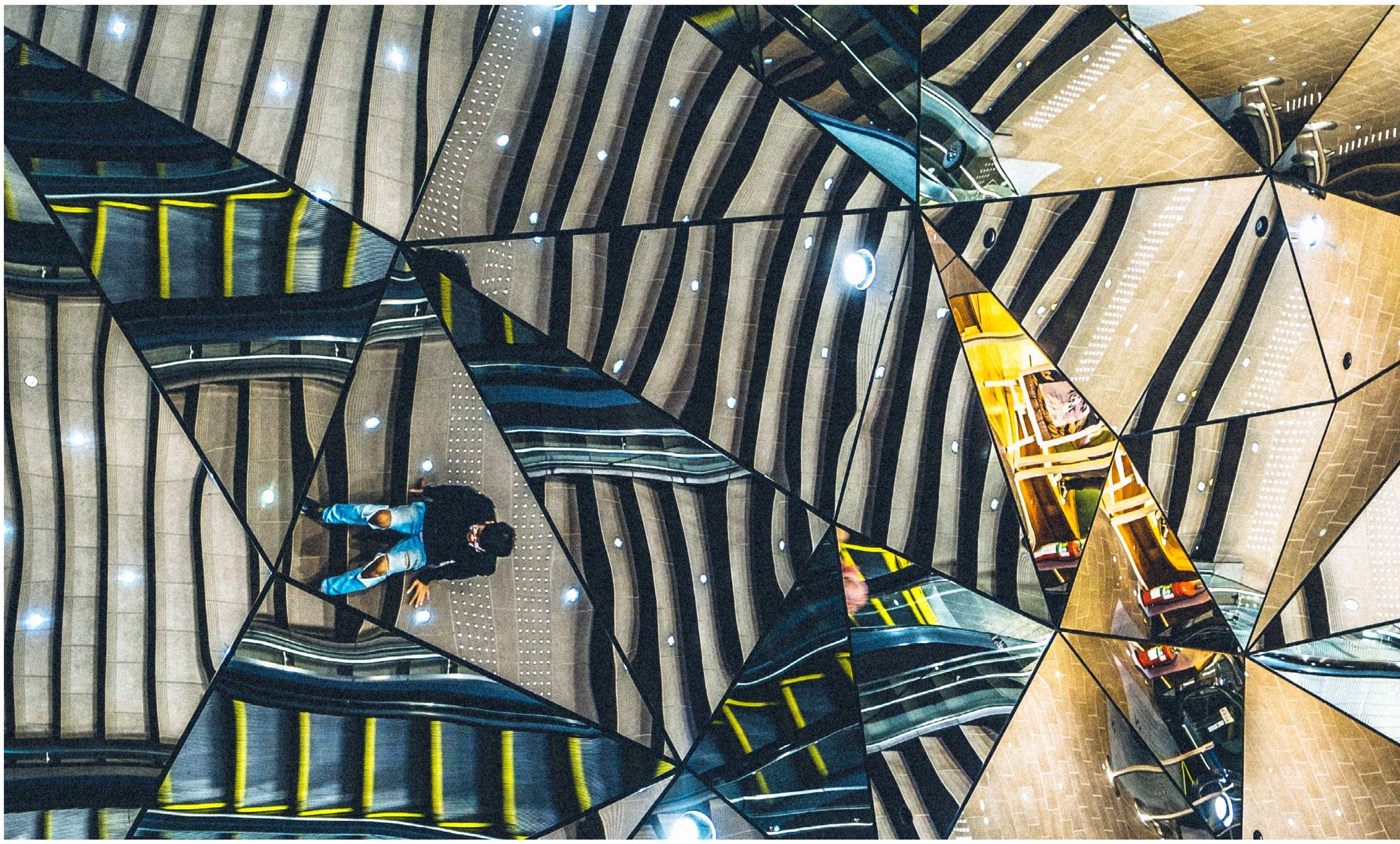
Personalize UX
Precisely identify all devices on the network and customize protection

Secure all devices
Block all known and new threats on all devices, including IoT

Offer full control
Manage devices, set limits, block content, unwanted devices and threats

CUJOAI

Find out more: cujo.com



Privacy laws do not understand human error: Securing unstructured data in the age of data privacy regulations

AUTHOR_Mark Bower, CRO, Egress Software

In a world of increasingly punitive regulations like the GDPR, the combination of unstructured data and human error represents one of the greatest risks an organization faces. Understanding the differences between unstructured and structured data – and the different approaches needed to secure it – is critical to achieve compliance with the many data privacy regulations that businesses in the U.S. now face.

Structured data is comprised of individual elements of information organized to be accessible, repeatable, predictable, and governed and secured by machines in a highly automated manner. A database containing identity information — name, address, Social Security number — is an example of structured data.

Unstructured data is free-range data living outside of the confines of a database. This is represented by the day-to-day business communications,

operational files, spreadsheets, videos, PDFs, Word docs, emails and the hundreds of other applications present on our laptops, phones and other devices.

Gartner now estimates that close to 80 percent of all data in the enterprise is unstructured. In a world where more and more stringent data privacy regulations are being enacted, it is critical that organizations minimize this potential for risk to prevent data breaches that now come with hefty financial and reputational costs.

The human challenges of unstructured data

Unstructured data poses a greater risk primarily because this information is handled by humans (as opposed to purely machine-based processes).

Adding humans to the equation creates a host of potential risks due to the way we share, hoard, store and propagate information. Additionally, structured data can often be easily exported by users and IT administrators and end up in an unstructured format.

This is why new and innovative approaches are needed to effectively handle the risks of unstructured data. Too often, enterprises rely on strategies that are transmuted from structured data security protocols and either forget to deal with the risk of human error or don't actually know how to in the first place.

Typically, the tools applied in this method are clunky, cumbersome and difficult to use for a non-technical user. If the user is not empowered with simple ways to secure their data, they are more likely to expose information to potential risks without being aware they're doing so.

Another challenge is posed by workarounds people might use in business operations. For example: employees using a cloud file sharing system might accomplish the tasks they need to do as part of their job, while at the same time exposing the business to untold risks and compromise because they don't understand the security protocols of the applications they use.

These system risks are compounded by the challenge posed by human error. For example: common automation tools built into email applications such as Outlook and Gmail help people communicate freely and easily. However, the autocomplete function that enters addresses as you type can also lead to embarrassing mistakes and, too often, errors that lead to data compromises and breaches.

These are common problems that every organization faces and struggles with, but there are best practices and new technologies that can help minimize the risk.

Start with data detection

Knowing where sensitive data is stored and how it's used is crucial to complying with regulations and securing data, particularly when the organization stores and processes data that is subject to multiple regulations.

New technologies can automate the detection and classification process of unstructured data by sifting through the vast quantities of emails, files and folders that users create to map where sensitive data lives.

This classification process should drive policies that define who in the organization can access and share this information.

Organizations can also add metadata tags to documents to "fingerprint" sensitive information

and follow it wherever it goes. This provides an understanding of the magnitude of the risk an organization faces as data travels from user to user and directs the policies that instruct how the data should be secured to comply with all required regulations.

Encrypt everything

As part of the discovery and classification process, organizations can enforce automated encryption on any information that is deemed sensitive. If the data is not secure, then every other step to achieving security and compliance is at risk.

Encryption has been around for a long time, but typically falls in the “hard to use” category of technologies that non-technical users avoid. Enforcing the use of encryption starts with ensuring that it’s embedded within the user workflow and doesn’t represent another step, application or process they need to add on. It needs to seamlessly integrate with the way employees currently work and share information.

Encrypting data ensures that a lost device or accidental email won’t put your organization at financial risk.

Predicting and stopping human error

Accidentally uploading the wrong file, sharing permissions with people who are not approved to review information, or simply sending an email to the wrong person can happen to anyone. Stopping unforced errors is one of the hardest parts of security.

One area we’re seeing great advancement in is the application of AI to predict user error before it happens. For example, much like Outlook predicts and auto-inserts email addresses, AI can understand the email patterns and behaviors users exhibit to prevent the wrong email address from being inserted, or the user sharing information with someone they typically don’t communicate with.

It can identify anomalous downloads and access, and combined with rights management, can stop employees from sharing sensitive files with cloud applications, eliminate the “copy and paste” practice for sensitive data, and other ways that we accidentally leak our own data.

Conclusion

> Whether they realize it or not, organizations are at a tipping point. The volume of unstructured data is only going to increase and so will the risk of accidental loss.

New laws like the NYDFS cybersecurity regulation, the new California citizen privacy regulation AB 375, and the EU General Data Protection Regulation (GDPR) have changed the game for compliance, and organizations need to start protecting unstructured data by default rather than as an after-thought.

The right way to do this is to look at the users creating, storing and interacting with this data, understanding the different levels of sensitivity, and making sure the right level of security and control is applied.

Technologies need to be adopted that empower users to work securely, enabling privacy as a natural part of business that builds customer trust and is seen as a critical to the way work is carried out. Otherwise, organizations will leave themselves and their customers exposed to the ever-increasing risk of a data breach, which now comes with an even higher price tag attached.

The future of OT security in critical infrastructure

AUTHORS_Edward Amoroso, CEO, TAG Cyber
_Andrew Ginter, Vice President of Industrial Security, Waterfall Security

Both the likelihood and consequences of cyberattacks to OT/ICS components continue to grow for modern industrial operations. While current advances in OT/ICS cyber security are impressive, new approaches are needed to gain defensive advantage over already-capable cyber adversaries, to keep up with new OT/ICS technologies, and to serve business risk management needs in increasingly-demanding, competitive environments.

In all these cases, progress only comes when both IT and OT stakeholders can (1) correctly assess current and emerging risks to industrial operations, (2) correctly assess the strength and benefits of candidate threat mitigation measures, and (3) convince business decision-makers of the correctness of these assessments to commit funds to business process and security modernization initiatives. All three of these cases are essential, but also have their corresponding pitfalls to avoid.
In practice, IT stakeholders often underestimate cyber threats to industrial operations, and overestimate the effectiveness of software-based security measures. OT stakeholders are often less predictable, sometimes underestimating threats and resisting investment in improved security posture, while other times overestimating threats and raising safety concerns that impair modernization efforts. In all cases, communicating threats, defensive postures, and the need for change to business decision-makers can be difficult.

To address these challenges, we discuss below three specific areas in the context of both improved enterprise operational effectiveness, and enhanced security for industrial control systems:

Industrial Internet of Things (IIoT) – Internet-based cloud services for industrial automation promise significant benefits to industrial enterprises, while dramatically increasing industrial attack surfaces.

Universal Security Monitoring – Modern enterprises rely on Security Operations Centers (SOCs) and Security Information and Event Management Systems (SIEMs) with limited visibility into their industrial operations.

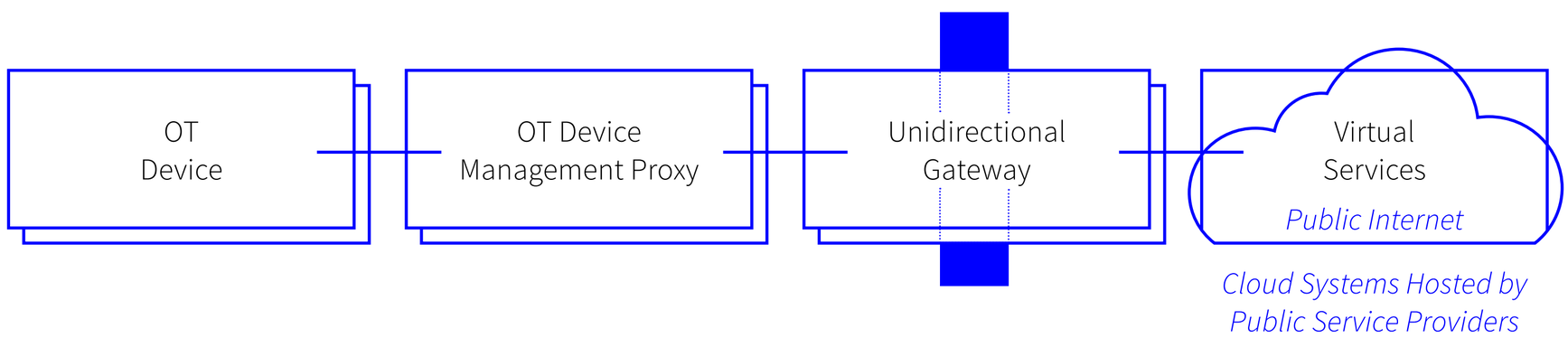
Tamper-Proof Forensics – Since no defensive posture can ever be perfect, strong support for incident response and recovery is a high priority, especially for industrial networks that may be targeted by sophisticated threat actors.

These three cases highlight the types of considerations that many OT/ICS security engineers are working on today. Each is discussed in more depth below.

Industrial Internet of Things

The emerging Industrial Internet of Things (IIoT) consists of edge industrial devices connected directly to cloud systems on the Internet. Significant advantages stem from aggregating and analyzing large amounts of data from many sites and/or clients. Many industrial vendors are investing significant resources in new product offerings in this realm. The security result though, is a significantly expanded attack surface where threats can use known and zero-day vulnerabilities to pivot from one customer, through cloud sites, to sensitive industrial networks at other sites and enterprises. This, and related risks, are impeding the adoption of IIoT technology at many sites.

Waterfall's Unidirectional CloudConnect is a solution that preserves the benefits of cloud-based big data analytics in the IIoT without the increased attack surface for industrial control networks. Unidirectional CloudConnect is an industrial control device having a local unidirectional gateway through which it can gather data from a wide variety of industrial data sources. Translation capabilities are included so that data can be exchanged between the OT and cloud domains. This allows direct connections from sensitive OT networks to the Internet.



This general issue of reducing risk in the IIoT will be one of the most important areas of cyber security in the coming years, especially as more ICS devices are integrated with IT-based or Internet-based cloud services – often for cost reduction. Unless these risks are properly addressed, the consequence implications for OT/ICS infrastructure can be significant.

Universal security monitoring

The Waterfall Security team has observed that while intrusion detection and security monitoring disciplines are mature on IT networks in most enterprises, the discipline tends to stop at the IT/OT gateway in industrial enterprises. In part, this is because few SOCs are equipped to properly gather and interpret telemetry and logs from OT/ICS networks.

An additional issue, however – and this might seem ironic, is that deep monitoring of certain OT/ICS devices is often seen as too sensitive to be installed into a given operational environment. That is, where OT devices are critical to correct and continued operation of important industrial processes, a

management decision might be made to avoid installing intrusion detection probes and security monitoring systems for fear that new security risks might be introduced through connectivity with IT-based or Internet/cloud-based SOCs.

This is an unacceptable situation because security engineers can only secure what they can observe and measure. To address this need, intrusion detection and security monitoring engines are starting to support a much wider variety and depth of industrial systems than was historically the case. To address the security concerns stemming from connectivity with these engines, industrial sites are again deploying Unidirectional CloudConnect or other unidirectional monitoring capabilities.

In a sense, progress here mirrors the problem and progress in the IIoT realm. Both are examples of both risks and benefits stemming from increased connectivity between industrial networks and central IT-based or cloud-based systems. Unlike the emerging field of IIoT big-data analytics though, safe, increased coverage for central security monitoring systems is seen by most industrial sites as a current and urgent problem.

Tamper-proof forensics

With widespread adoption of the NIST Framework by industrial enterprises, many enterprises are seeking to develop robust industrial cyber incident response capabilities. One challenge with industrial incident response is access to reliable forensics. Industrial enterprises increasingly seek to defend their industrial networks against even the most sophisticated attacks. Sophisticated attacks though, frequently involve the intruder modifying, deleting, and erasing evidence of their attacks. This might even include accessing distantly hosted SIEMs and log analyzers if they can be located. Sadly, many of these systems share mutual trust across laterally traversed LANs, which is consistent with most APT methods.

The Waterfall Security team supports this challenge with its BlackBox solution, which includes a unidirectional gateway, and which gathers forensic data from a wide variety of industrial and IT device sources. The collected data is pushed through the one-way hardware into an encrypted and otherwise isolated storage system. The result is a securely stored, protected forensic log that cannot be tampered with by an adversary.

Waterfall Security has also developed a transportable version that response teams can carry to a given site if necessary. The device can be quickly configured to gather reliable forensics, in case the attackers are still active in the compromised network, and might be trying to actively interfere with the investigation. When the team has collected sufficient forensic evidence, analysis can be performed off-line.

Concluding thoughts

There are far fewer industrial control system networks in the world than there are IT networks, and far fewer ICS security practitioners. Historically, this has meant that many well-meaning practitioners take inspiration from IT networks, and apply IT-centric solutions universally to both IT and OT networks.

Fortunately, this is changing. A recent whitepaper by the Gartner Group for example – *Demystify Seven Cybersecurity Myths of Operational Technology and the Industrial Internet of Things* – points out clearly that IT methodologies are not appropriate to calculating risks and assessing threats on OT networks, and that IT cybersecurity designs are not adequate to OT security needs.

Unidirectional Gateways and related products are one of the OT-centric security technologies that Gartner and other experts and authorities are recommending be evaluated for OT security needs, and become part of many OT security solutions.