# [+] (IN)SECUREMagazine

03 | 2020

ISSUE 65.5

## #RSAC 2020

(ISC)²

# Commit to CERTIFICATION in 2020

## *Here's Everything You Need to Succeed – Without Excuses*

Prepping for (ISC)² certification is a BIG commitment. We know you're dedicated, and this is the year to take it to the next level. We need talented, skilled people working to ensure a safe and secure cyber world for all. The movement has started. It's time for you to elevate yourself even higher! Leave excuses behind, set your goal and commit now.

**Get your no-excuses guide to success.**

(ISC)² Exam Action Plan ▶

CISSP. SSCP. CCSP. CAP. CSSLP. HCISPP.

**RSA Conference** concluded its 29th annual event in San Francisco on Friday, February 28. More than 36,000 attendees, 704 speakers and 658 exhibitors gathered at the Moscone Center to explore the Human Element in cybersecurity through hundreds of keynote presentations, track sessions, tutorials, seminars and special events.

Some of the most pressing topics included privacy, machine learning and artificial intelligence, policy and government, applied crypto and blockchain, and, new for RSA Conference 2020, open source tools, product security and anti-fraud.

“Our mission is to connect cybersecurity professionals with diverse perspectives and backgrounds to inspire new ways of thinking and push the industry forward,” said Linda Gray Martin, Senior Director and General Manager, RSA Conference. “This week proved the importance and impact of the human element in cybersecurity, and we thank all of our attendees for bringing their passion, commitment and ideas to RSA Conference for another amazing year.”

RSA Conference 2020 highlights:

- 29 keynote presentations on two stages.
- SECURITI.ai was named RSA Conference 2020’s “Most Innovative Startup” during the fifteenth annual RSAC Innovation Sandbox Contest.
- Three early stage cybersecurity startups, Dasera, Inc., Soluble and Zero Networks, pitched their ideas to a panel of VCs in the RSAC Launch Pad.
- Professor Joan Daemen and Professor Vincent Rijmen, two world-renowned cryptographers, received the annual RSAC Excellence in the Field of Mathematics Award.
- Over 130 CISOs participated in the CISO Boot Camp, a one-and-a-half day program designed to spark open and frank conversations between top cybersecurity leaders.
- RSAC College Day welcomed 650 college students, recent grads and faculty to network with leading companies, explore career opportunities, attend dedicated education events and experience RSA Conference sessions and the expo floor.

**PAGE 20** CyberArk

**PAGE 11** Cymatic

**PAGE 16** DigiCert

**PAGE 22** Infoblox

**PAGE 04** ProcessUnity

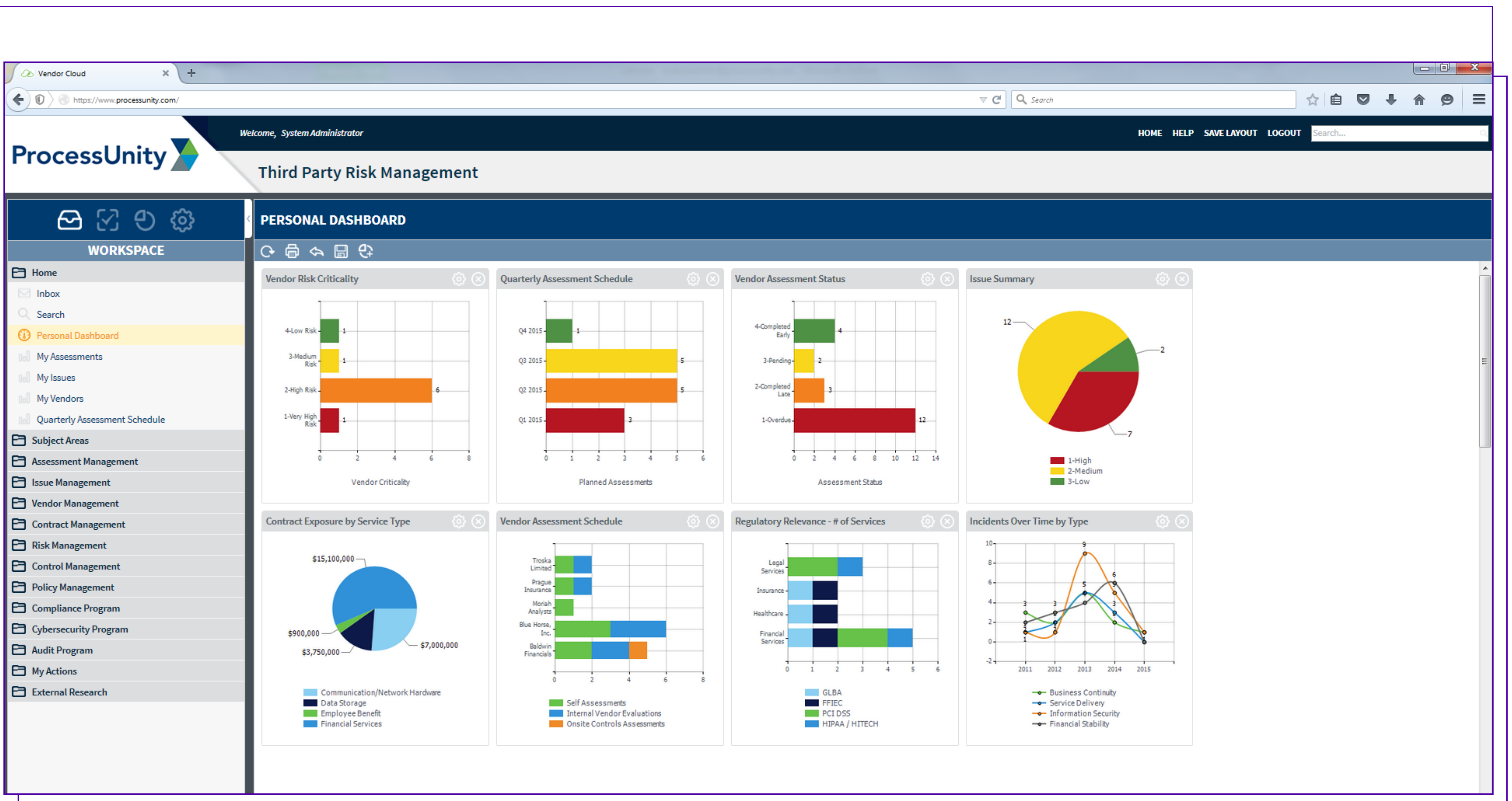
Visit the magazine website and subscribe at www.insecuremag.com

**Mirko Zorz**
Editor in Chief
mzorz@helpnetsecurity.com

**Zeljka Zorz**
Managing Editor
zzorz@helpnetsecurity.com

**Berislav Kucan**
Director of Operations
bkucan@helpnetsecurity.com

Photography by RSA Conference and (IN)SECURE Magazine.



# ProcessUnity Vendor Risk Management expanded to include new Best Practices Configuration

ProcessUnity, a leading provider of cloud-based applications for risk and compliance management, announced a new pre-built configuration of its award-winning Vendor Risk Management solution.

Best Practices Configuration for ProcessUnity Vendor Risk Management (VRM) is a pre-configured Third-Party Risk Management program with turn-key workflows, assessments, calculations, risk analysis and reporting, allowing small to midsize organizations to successfully launch and maintain a third-party risk program from day one.

Developed by Third-Party Risk Management subject matter experts leveraging knowledge from hundreds of successful customer implementations, ProcessUnity's Best Practices Configuration delivers a complete program with high-quality, repeatable vendor assessment processes.

The low-touch, low-cost implementation gets customer programs up and running in a few short weeks, and includes the following:

**Complete data model:** Best Practice Configuration includes a sophisticated data model with pre-built relationships and workflows between data elements and system users. Key elements of the data model include Third Parties, Third-Party Requests, Third-Party Services, Service Reviews, Agreements, Assessments, Questionnaires and Third-Party Issues.

**Prescriptive workflows:** Pre-configured workflows establish the repeatable processes necessary for effectively managing third-party risk – from initial service identification and onboarding, through contracts, ongoing vendor monitoring and termination. Key workflows capture new service requests, automatically calculate inherent risk, perform due diligence and manage issues and agreements.

**Industry-standard questionnaires:** Automated questionnaires featuring SIG Core and SIG Lite from Shared Assessments put an end to inefficient paper surveys and spreadsheets and simplify the assessment process for both organizations and their third parties.

**Built-in calculations & scoring:** Best Practices Configuration provides built-in calculations, rating tiers, scoring and other logic critical to an automated Third-Party Risk Program, including Inherent Risk, Automated Scoping, Assessment Review Ratings, Residual Risk, Issue Remediation and Automated Response Analysis. These calculations save time and remove subjectivity, identifying which vendors need further evaluation while automatically recommending assessment scope based on risk levels.

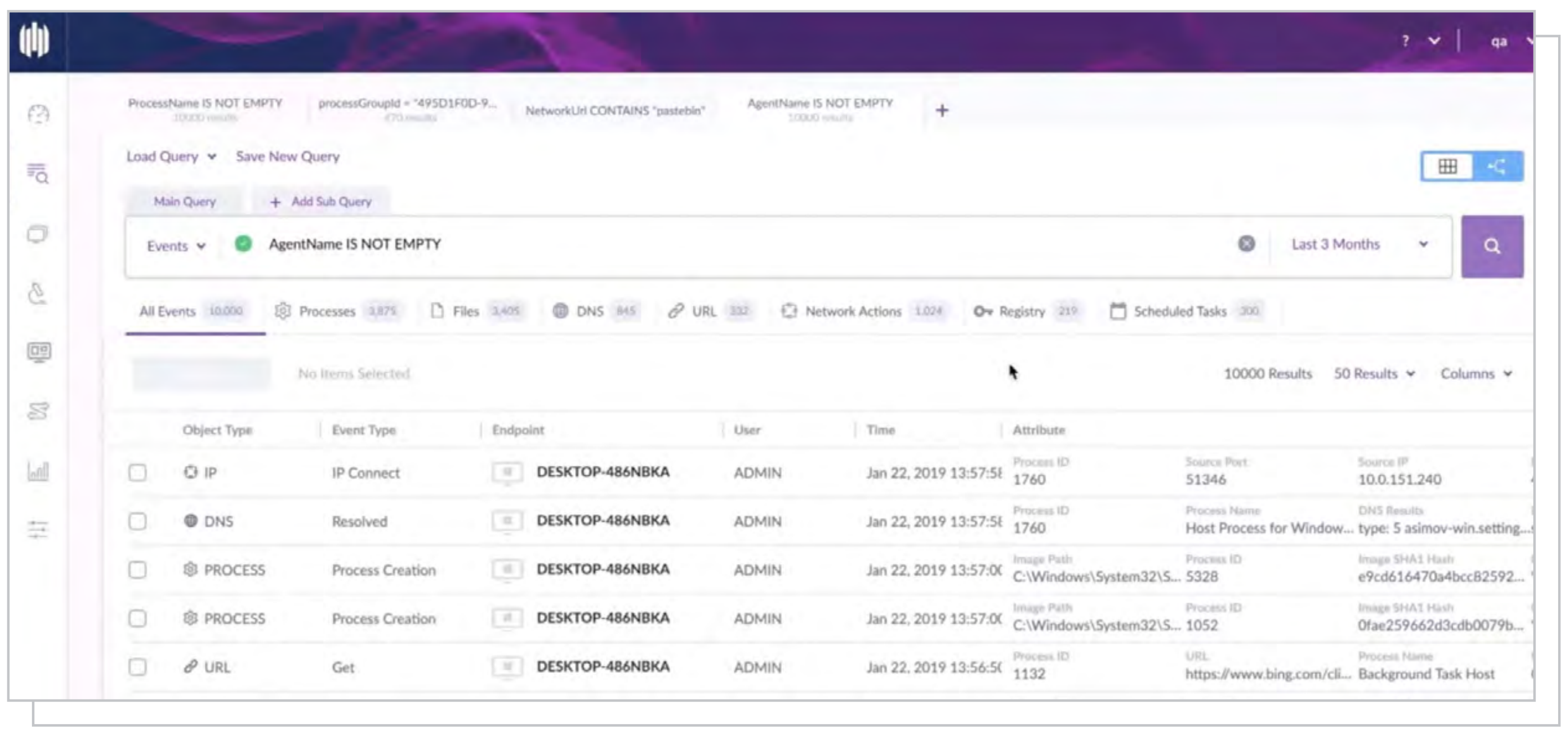
**Comprehensive vendor portal:** ProcessUnity's Vendor Portal provides third parties with a secure, online environment to complete questionnaires, provide responses and comments, and attach supporting documentation. The easy-to-use interface, instructions and guidance improves vendor response time and response quality.

**Interactive, dashboards & reports:** Extensive built-in reports provide real-time visibility into the state of third-party risk and demonstrate to regulators the existence of a consistent, reliable and repeatable program. Interactive dashboards give visibility into ongoing risk assessment progress, the status of remediation activity and vendor ratings. Drill-down capabilities also allow risk managers to quickly find the details in areas of concern.

## SentinelOne Singularity: AI-Powered XDR platform transforms enterprise security

SentinelOne unveiled its Singularity Platform, an industry first data lake that fuses together the data, access, control, and integration planes of its endpoint protection (EPP), endpoint detection and response (EDR), IoT security, and cloud workload protection (CWPP) into a centralized platform.

With Singularity, organizations gain access to back-end data across the organization through a single solution, providing a cohesive view of their network and assets by adding a real-time autonomous security layer across all enterprise assets.



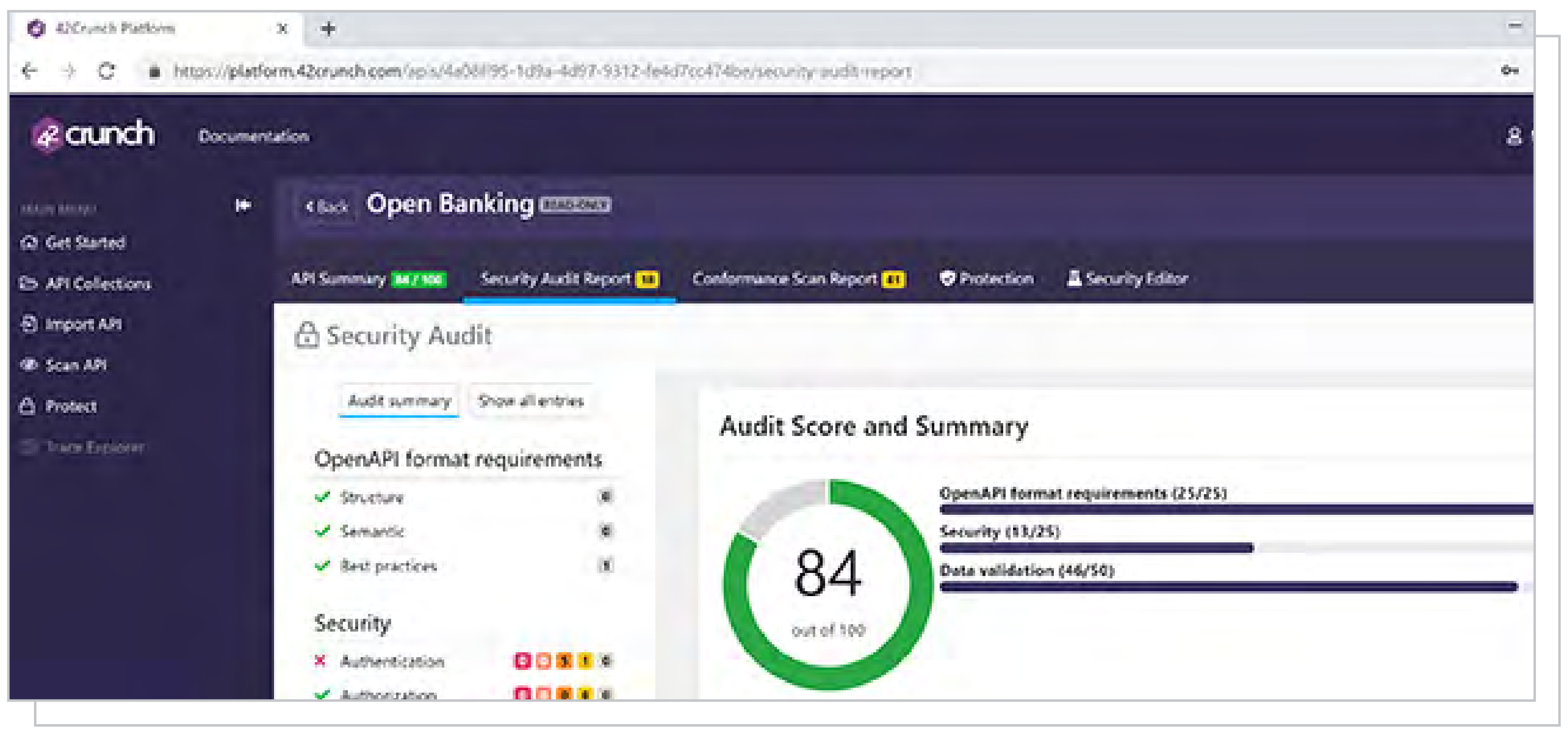
AgentName IS NOT EMPTY

| Object Type | Event Type | Endpoint | User | Time | Attribute | | |
|---|---|---|---|---|---|---|---|
| IP | IP Connect | DESKTOP-486NBKA | ADMIN | Jan 22, 2019 13:57:5 | Process ID<br>1760 | Source Port<br>51346 | Source IP<br>10.0.151.240 |
| DNS | Resolved | DESKTOP-486NBKA | ADMIN | Jan 22, 2019 13:57:5 | Process ID<br>1760 | Process Name<br>Host Process for Window... | DNS Results<br>type: 5 asimov-win.setting... |
| PROCESS | Process Creation | DESKTOP-486NBKA | ADMIN | Jan 22, 2019 13:57:0 | Image Path<br>C:\Windows\System32\S... | Process ID<br>5328 | Image SHA1 Hash<br>e9cd616470a4bcc82592... |
| PROCESS | Process Creation | DESKTOP-486NBKA | ADMIN | Jan 22, 2019 13:57:0 | Image Path<br>C:\Windows\System32\S... | Process ID<br>1052 | Image SHA1 Hash<br>0fae259662d3cdb0079b... |
| URL | Get | DESKTOP-486NBKA | ADMIN | Jan 22, 2019 13:56:5 | Process ID<br>1132 | URL<br>https://www.bing.com/cli... | Process Name<br>Background Task Host |

## 42Crunch launches new self-registration feature for its API Security Platform

42Crunch announced the launch of its new self-registration feature for its API Security Platform. Development, security and operations teams now have instant access to a comprehensive set of API security tools that easily integrate into existing workflows and enable an agile DevSecOps process.

"APIs are becoming one of the primary attack vectors, yet, API security remains confusing and most solutions out there are incomplete expensive platforms requiring talking to an enterprise salesperson to get started" says Jacques Declas, CEO and Founder of 42Crunch.

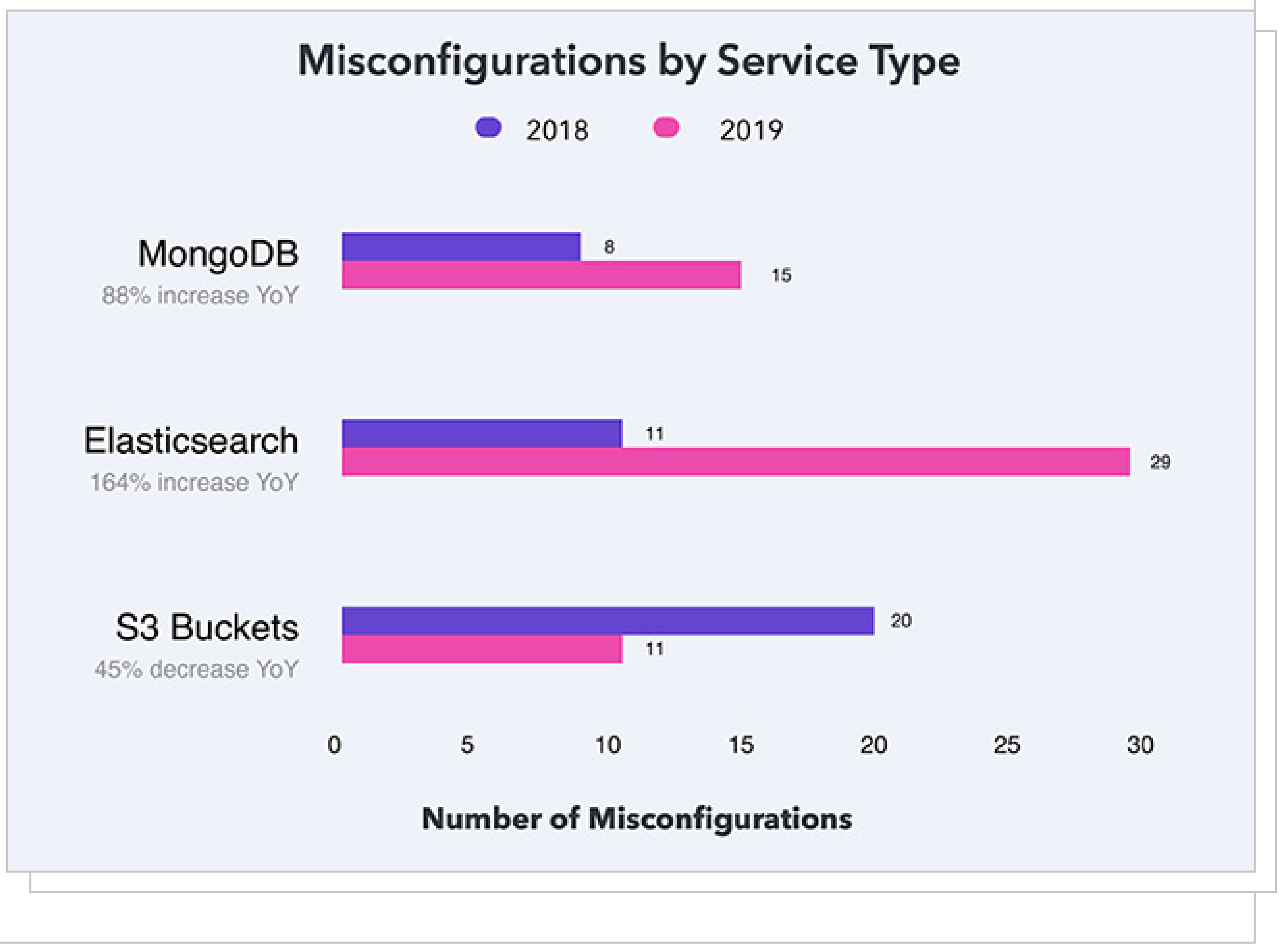


## Cloud misconfigurations surge, organizations need continuous controls

Nearly 33.4 billion records were exposed in breaches due to cloud misconfigurations in 2018 and 2019, amounting to nearly $5 trillion in costs to enterprises globally, according to DivvyCloud research.

Year over year from 2018 to 2019, the number of records exposed by cloud misconfigurations rose by 80%, as did the total cost to companies associated with those lost records. Unfortunately, experts expect this upward trend to persist, as companies continue to adopt cloud services rapidly but fail to implement proper cloud security measures.

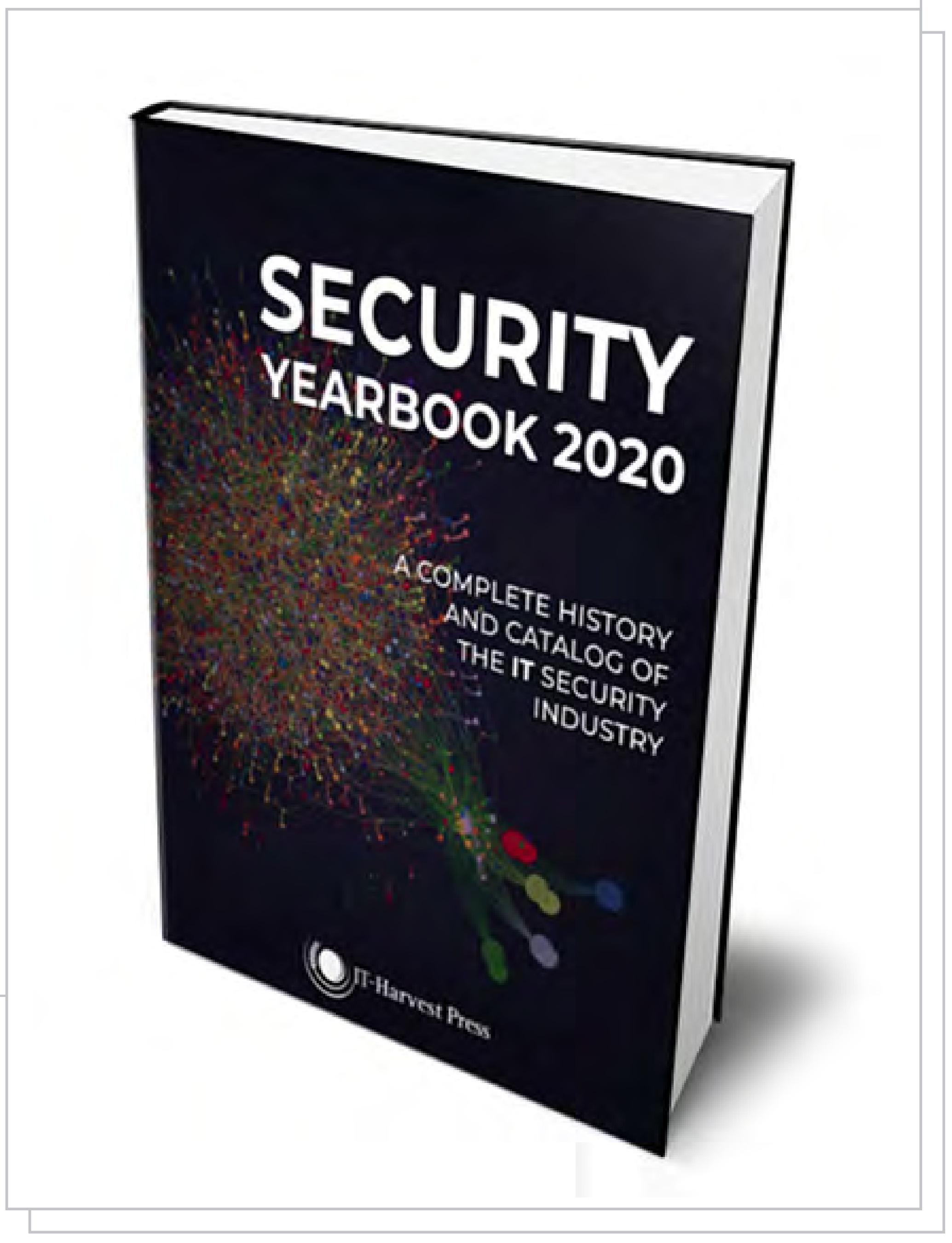
"The rush to adopt cloud services has created new opportunities for attackers – and attackers are evolving faster than companies can protect themselves. The fact that we have seen a 42% increase from 2018 to 2019 in cloud-related breaches attributed to misconfiguration issues proves that attackers are leveraging the opportunity to exploit cloud environments that are not sufficiently hardened. This trend is expected to continue as more organizations move to the cloud," Charles "C.J." Spallitta, Chief Product Officer at eSentire, told (IN)SECURE Magazine.



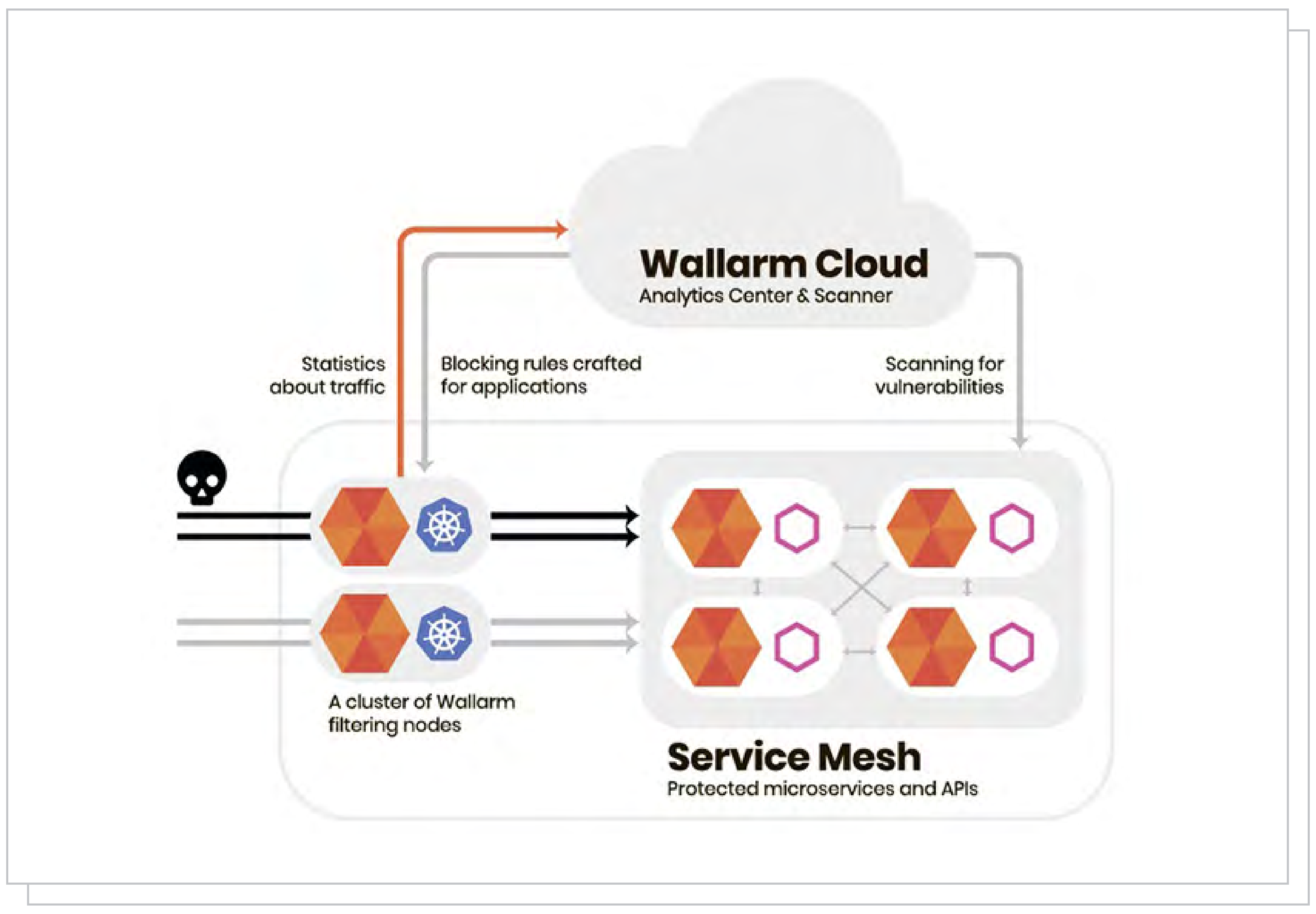
## Richard Stiennon publishes Security Yearbook 2020

Richard Stiennon - author, industry analyst, and founder of IT-Harvest - announced the release of "Security Yearbook 2020: A History and Directory of the IT Security Industry."

Security Yearbook 2020 is not a review of technologies; this is a book filled with rich histories of the vendors and the people behind the companies – the misfits and pioneers – that have together built the $300+ billion cybersecurity industry of today.



# Wallarm advances API security with native gRPC and GraphQL support


Wallarm Cloud
Analytics Center & Scanner
Statistics about traffic
Blocking rules crafted for applications
Scanning for vulnerabilities
A cluster of Wallarm filtering nodes
Service Mesh
Protected microservices and APIs

Wallarm released an expanded set of parsers, detection of API-specific vulnerabilities and API schema analysis for gRPC and GraphQL. With Wallarm context-specific protection is delivered both for externally-facing APIs and for service-to-service internal APIs for a true zero trust use case.

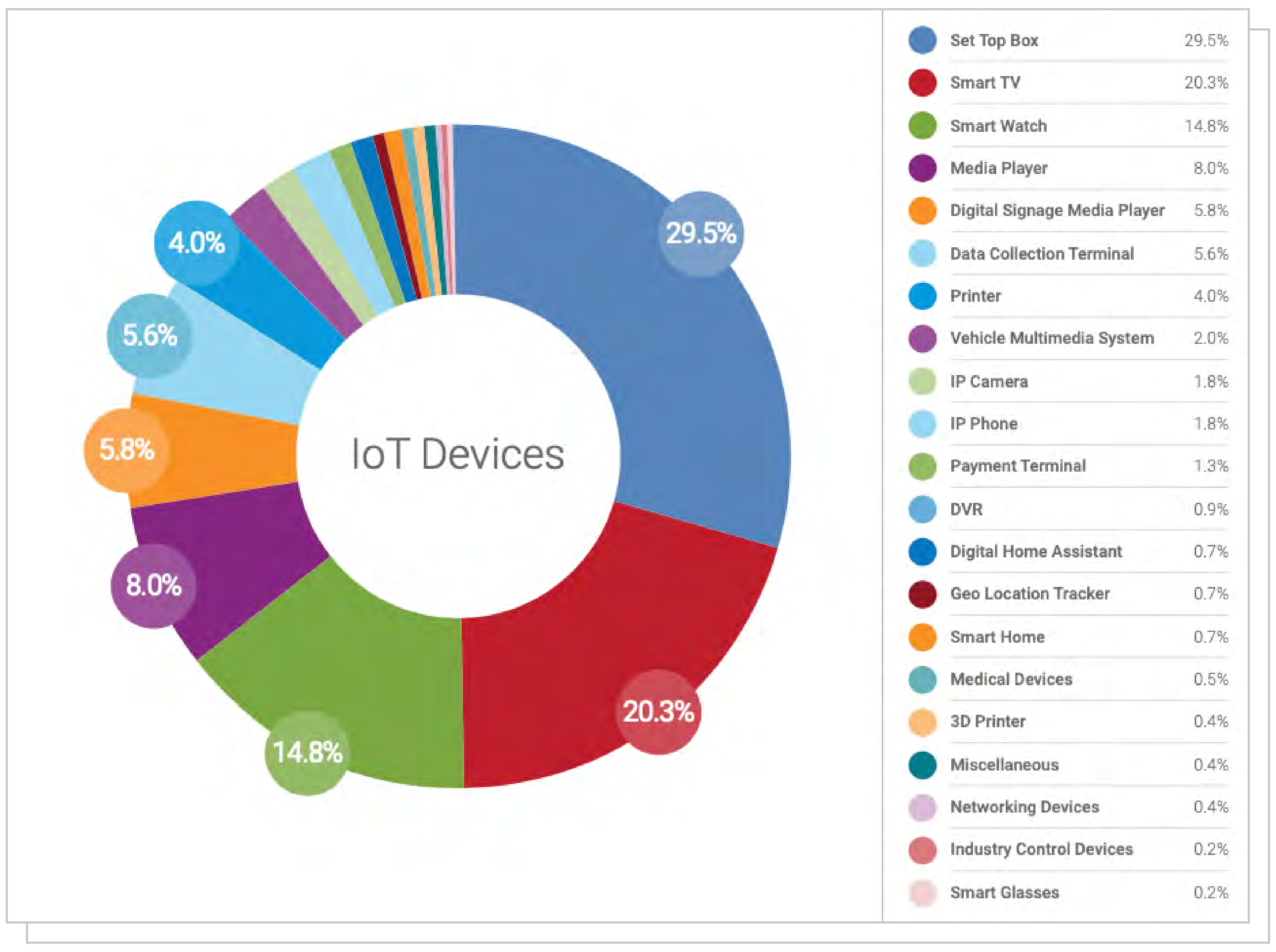
“More than half of our customers are actively moving to the cloud-native stack. For them support for gRPC and GraphQL is not just a ‘nice-to-have’, but a strong requirement for all the security solutions, including WAF and DAST. Wallarm is stepping up to provide just that. We consistently follow all the modern application stacks, from serverless and WebSockets to Kubernetes-native, Envoy proxy, and now, gRPC and GraphQL as well”, said Ivan Novikov, CEO of Wallarm.

# Shadow IoT: A growing threat to enterprise security

Zscaler released their second annual IoT report, compiled after analyzing their customers' IoT transactions in the Zscaler cloud for two weeks. The company found 553 different IoT devices across 21 categories from 212 manufacturers.

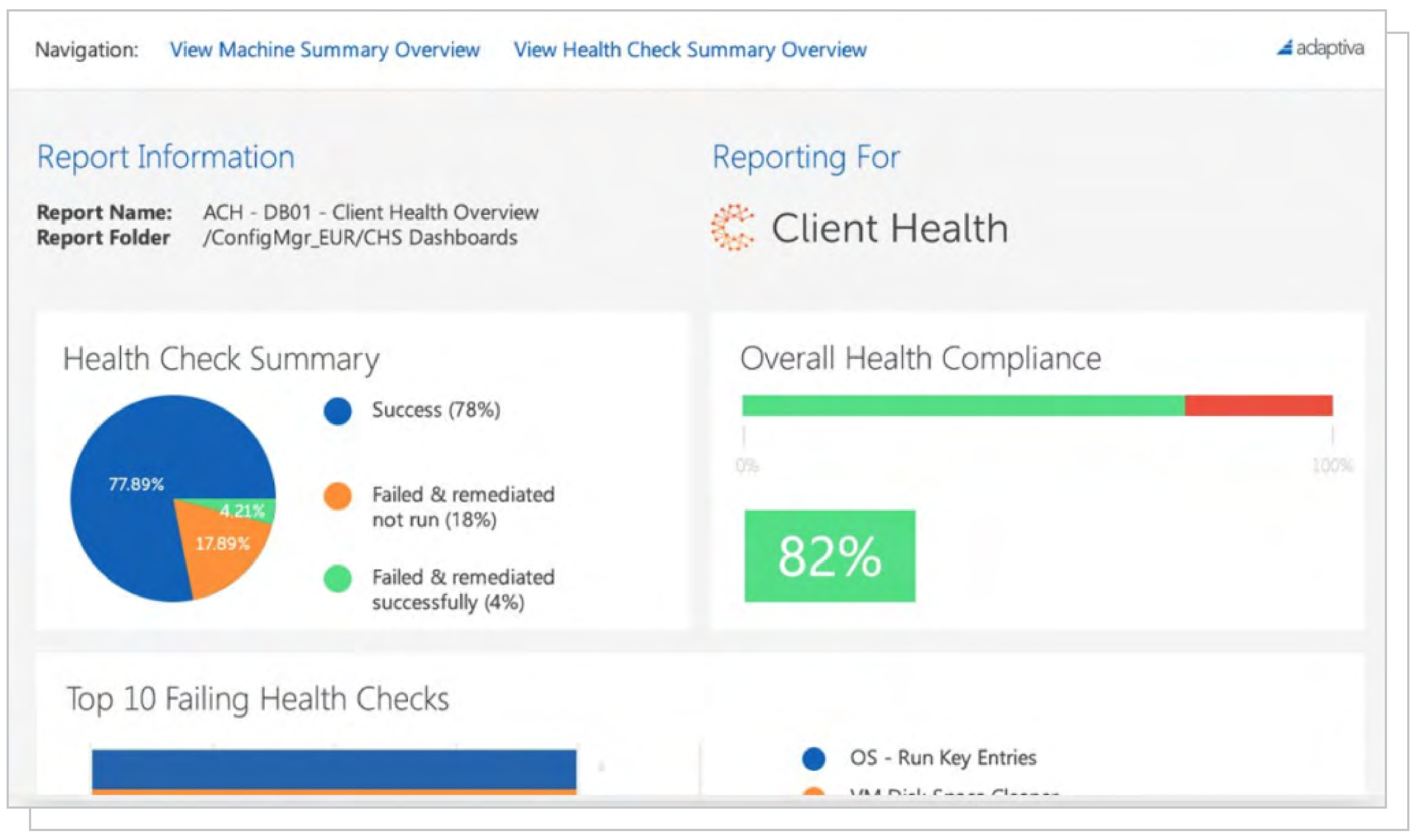
Organizations around the world are observing this Shadow IoT phenomenon, where employees are bringing unauthorized devices into the enterprise. With this onslaught of unknown and unauthorized devices, IT and security teams often won't know these devices are on the corporate network nor how they impact an organization's overall security posture.

The company also identified a number of unique and interesting IoT devices connecting to the Zscaler cloud, such as smart refrigerators, music furniture (a combination table lamp and smart media player device named Symfonisk), Tesla and Honda automobile media players, and Wi-Fi memory cards.



"We have entered a new age of IoT device usage within the enterprise. Employees are exposing enterprises to a large swath of threats by using personal devices, accessing home devices, and monitoring personal entities through corporate networks," said Deepen Desai, Vice President of Security Research, Zscaler.

"As an industry, we need to implement security strategies that safeguard enterprise networks by removing shadow IoT devices from the attack surface while continuously improving detection and prevention of attacks that target these devices."


Navigation: View Machine Summary Overview View Health Check Summary Overview
adaptiva

Report Information

**Report Name:** ACH - DB01 - Client Health Overview
**Report Folder** /ConfigMgr_EUR/CHS Dashboards

Reporting For

Client Health

Health Check Summary
77.89%
4.21%
17.89%
Success (78%)
Failed & remediated not run (18%)
Failed & remediated successfully (4%)
Overall Health Compliance
0%
100%
82%
Top 10 Failing Health Checks
OS - Run Key Entries

## Adaptiva launches Endpoint Health, its automated endpoint health and remediation solution

Endpoint Health runs 111 health checks enterprise-wide within minutes. This includes several new health checks devoted to patching, security and Windows 10 maintenance. These latest checks were created based on customer requests for an even wider range of specific, automated activities that can maximize service availability while reducing the inflow of support tickets.

IDVision®
with iovation®

# The future is trust.

## Discover the power of data identity.

- **Establish identity**
- **Authenticate consumers**
- **Prevent fraud**

TransUnion®

# Checkmarx simplifies AST automation for modern development and DevOps environments

Checkmarx "Flow" (CxFlow) is an orchestration module for the Checkmarx Software Security Platform that tightly integrates with application release orchestration and agile planning tools. This results in improved operational "flow" of secure software development and the delivery of more actionable vulnerability findings.

CxFlow also drives faster adoption by reducing friction between development, DevOps, and DevSecOps, and enabling automated scanning earlier in the code management process by integrating directly into source control management systems or CI/CD tools.

## GreatHorn unveils biometric solution with keystroke analysis to match typing patterns

GreatHorn unveiled the first and only biometric solution that effectively identifies compromised accounts and blocks takeover attempts by validating users with their unique typing patterns. By leveraging passwordless authentication to further enhance its capabilities, GreatHorn ensures that organizations can now benefit from first-factor authentication without adding friction to end-user email workflows.

# SECURITI.ai named Most Innovative Startup at RSA Conference 2020

SECURITI.ai was selected winner of the fifteenth-annual RSA Conference Innovation Sandbox Contest and named "Most Innovative Startup" by a panel of leading venture capitalists, entrepreneurs and industry veterans.

SECURITI.ai is a leader in AI-powered PrivacyOps. Its PRIVACI.ai solution automates privacy compliance with patent-pending People Data Graphs and robotic automation. It enables enterprises to give rights to people on their data, comply with global privacy regulations and build trust with customers.

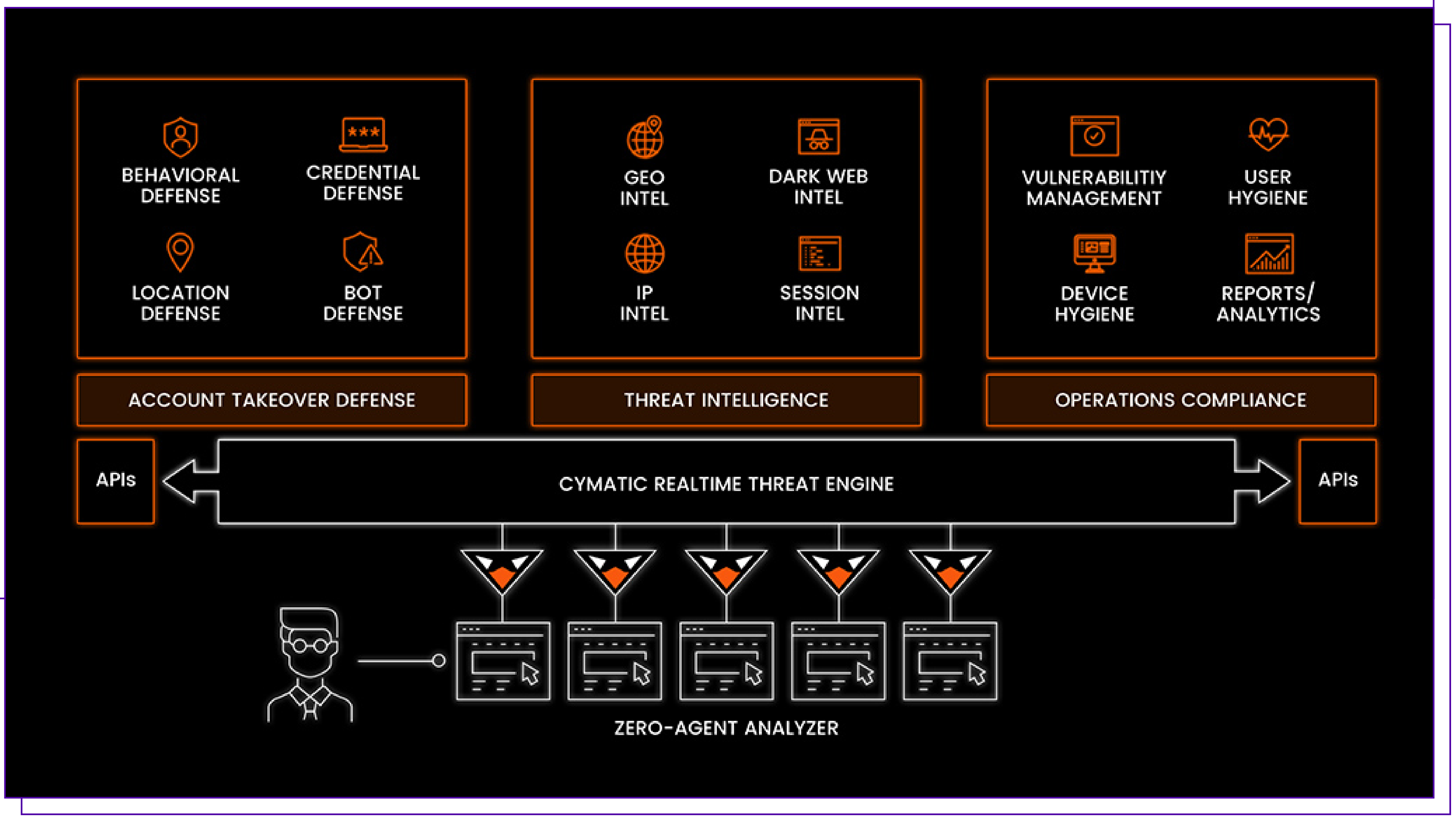
"We are honored to join such an impressive roster of past recipients," said Rehan Jalil, CEO of SECURITI.ai. "Privacy is a basic human right and companies want to honor individual rights of privacy and data protection. Privacy compliance and operations are only getting more complex for businesses around the world, and we're humbled that the judges recognized our vision for AI-powered PrivacyOps and data protection."

# Cymatic presents all-in-one web application defense platform

At RSA Conference 2020, Cymatic demonstrated the success of the only unified web defense that deploys at the client through a simple line of JavaScript without agents or proxies to deliver first-look, first-strike capability that is earliest in the kill chain.

Cymatic's next-generation all-in-one web application defense platform provides universal in-session visibility and control to reduce risk across web applications, networks, and users while decreasing network traffic loads and eliminating user friction.

The Cymatic platform provides universal in-session visibility and control to reduce risk by protecting against user-derived and device-based threats such as poor credential hygiene, dark web vulnerabilities, and potentially risky devices.

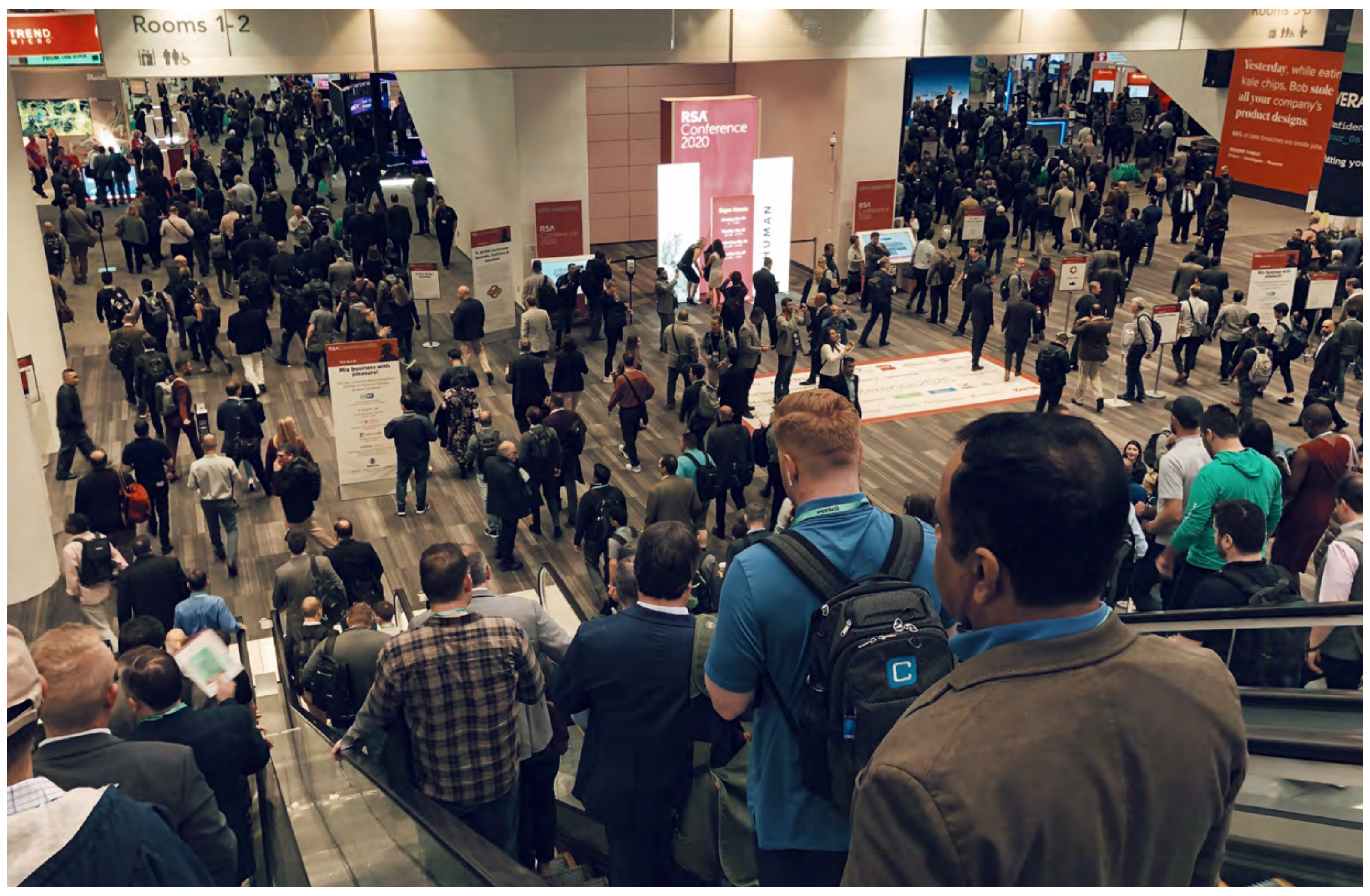


# Entrust Datacard eliminates employee passwords and accelerates secure customer onboarding

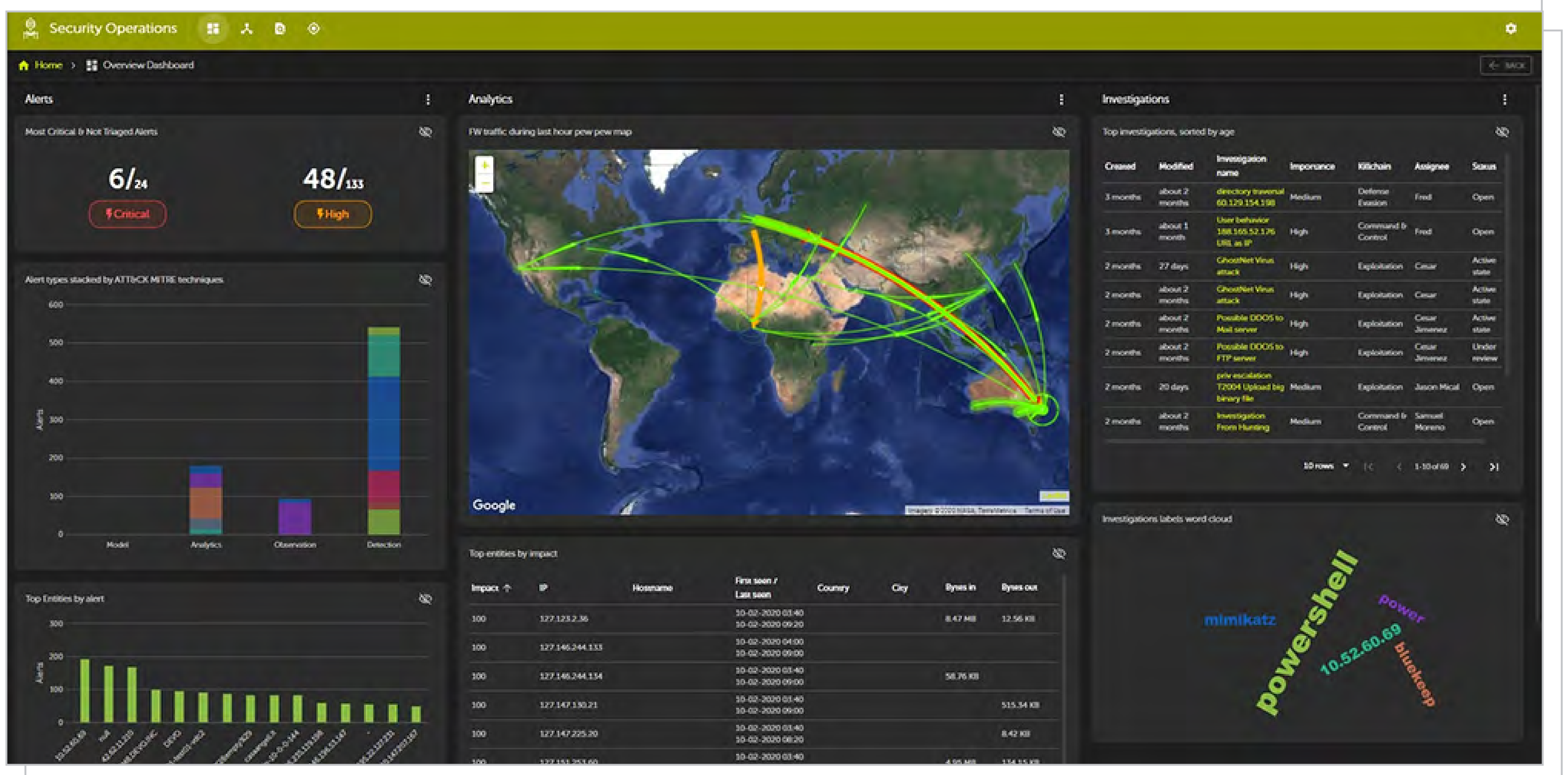
Entrust Datacard's Passwordless SSO Authentication solution turns employee smartphones into biometrics-protected virtual smart cards that allow instant proximity-based login to both workstations and applications. The solution creates a frictionless authentication experience, eliminating passwords and putting an end to the risk of bad actors stealing user credentials and compromising critical information.

Entrust Datacard's new Identity Proofing solution lets banks, hospitals, government agencies and other customer and citizen-facing organizations offer customers a simple, seamless onboarding experience, either inside or outside physical locations. With Identity Proofing, customers use their smartphones or a kiosk to capture their images and scan government-issued identity documents – such as a driver's license, passport or national ID card – for fast, AI-based authentication and verification.

# #RSAC 2020 gallery



# Devo Security Operations: Transforming the SOC and scaling security analyst effectiveness



Top investigations, sorted by age

| Created | Modified | Investigation name | Imporance | Killchain | Assignee | Status |
|---|---|---|---|---|---|---|
| 3 months | about 2 months | directory traversal 60.129.154.198 | Medium | Defense Evasion | Fred | Open |
| 3 months | about 1 month | User behavior 188.165.52.176 URL as IP | High | Command & Control | Fred | Open |
| 2 months | 27 days | GhostNet Virus attack | High | Exploitation | Cesar | Active state |
| 2 months | about 2 months | GhostNet Virus attack | High | Exploitation | Cesar | Active state |
| 2 months | about 2 months | Possible DDOS to Mail server | High | Exploitation | Cesar Jimenez | Active state |
| 2 months | about 2 months | Possible DDOS to FTP server | High | Exploitation | Cesar Jimenez | Under review |
| 2 months | 20 days | priv escalation T2004 Upload big binary file | Medium | Exploitation | Jason Mcal | Open |
| 2 months | about 2 months | Investigation From Hunting | Medium | Command & Control | Samuel Moreno | Open |

10 rows 1-10 of 69

Top entities by impact

| Impact | IP | Hostname | First seen / Last seen | Country | City | Bytes in | Bytes out |
|---|---|---|---|---|---|---|---|
| 100 | 127.123.2.36 | | 10-02-2020 03:40<br>10-02-2020 09:20 | | | 8.47 MB | 12.56 KB |
| 100 | 127.146.244.133 | | 10-02-2020 04:00<br>10-02-2020 09:00 | | | | |
| 100 | 127.146.244.134 | | 10-02-2020 03:40<br>10-02-2020 09:00 | | | 58.76 KB | |
| 100 | 127.147.130.21 | | 10-02-2020 03:40<br>10-02-2020 09:00 | | | | 515.34 KB |
| 100 | 127.147.225.20 | | 10-02-2020 03:40<br>10-02-2020 08:20 | | | | 8.42 KB |
| 100 | [illegible] | | 10-02-2020 03:40 | | | [illegible] | [illegible] |

Devo Technology announced Devo Security Operations, the first security operations solution to combine critical security capabilities together with auto enrichment, threat intelligence community collaboration, a central evidence locker, and a streamlined analyst workflow.

This powerful combination transforms the SOC and scales security analyst effectiveness. Analysts no longer must rely on multiple tools to manually assemble the data, context, and intelligence required to identify and investigate the threats that matter most to their business.

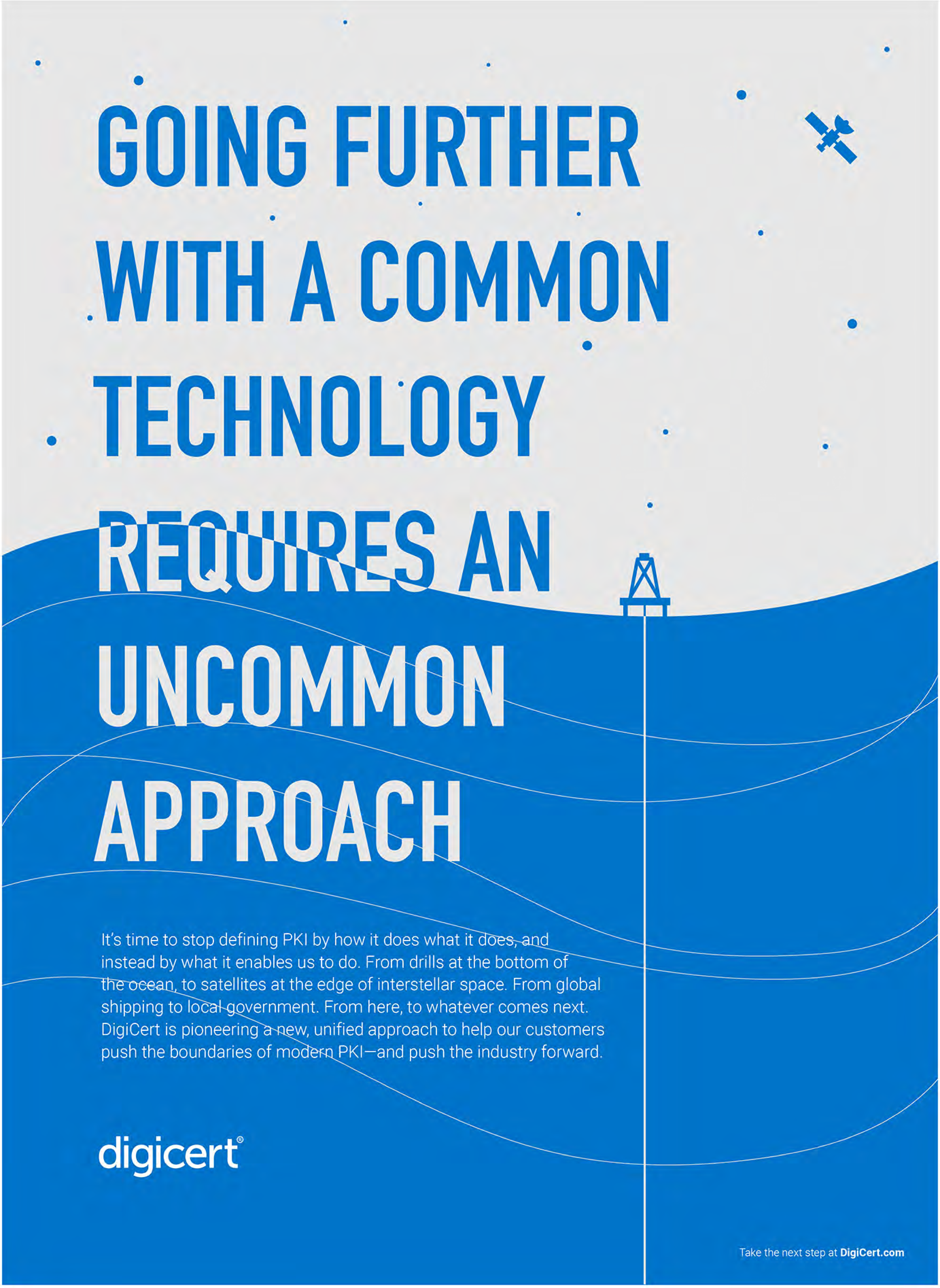
## Trustifi's OCR tool enhances email security by auto-encrypting sensitive images

Trustifi has incorporated a new AI-enabled feature into its industry-leading email encryption and DLP (data loss prevention) solution that also works via Optical Character Recognition technology (OCR). This integrated OCR tool scans email attachments such as images and PDF files. The tool recognizes elements such as a scan of a credit card or a screenshot of a financial statement and categorizes those attachments as sensitive.

# VMware advances intrinsic security for the world's digital infrastructure

VMware announced new innovations to advance the company's strategy to make security intrinsic to the digital enterprise. Intrinsic security makes protecting critical applications and data more automated, proactive and pervasive across the entire distributed enterprise. The announcements include:

- New VMware Advanced Security for Cloud Foundation, which will enable customers to replace legacy security solutions and deliver unified protection across private and public clouds
- Advancements to the VMware Carbon Black Cloud, which including automated correlation with the MITRE ATT&CK framework and upcoming prevention coverage for Linux machines
- New VMware Secure State auto-remediation capabilities to automate actions across cloud environments and proactively reduce risk



# #RSAC 2020 gallery

digicert
CYBERBIT | RANGE
Hyper-Realistic Cyber Training Platform
PKI
IoT
TLS
digicert
UNMATCHED FLEXIBILITY
See Lateral Movement in Real-Time

# DigiCert introduces upgraded TLS certificate, business manager for channel partners

DigiCert, the world's leading provider of TLS/SSL, IoT and PKI solutions, is upgrading channel partners to DigiCert CertCentral Partner, a comprehensive TLS certificate management solution for cloud and hosted environments.

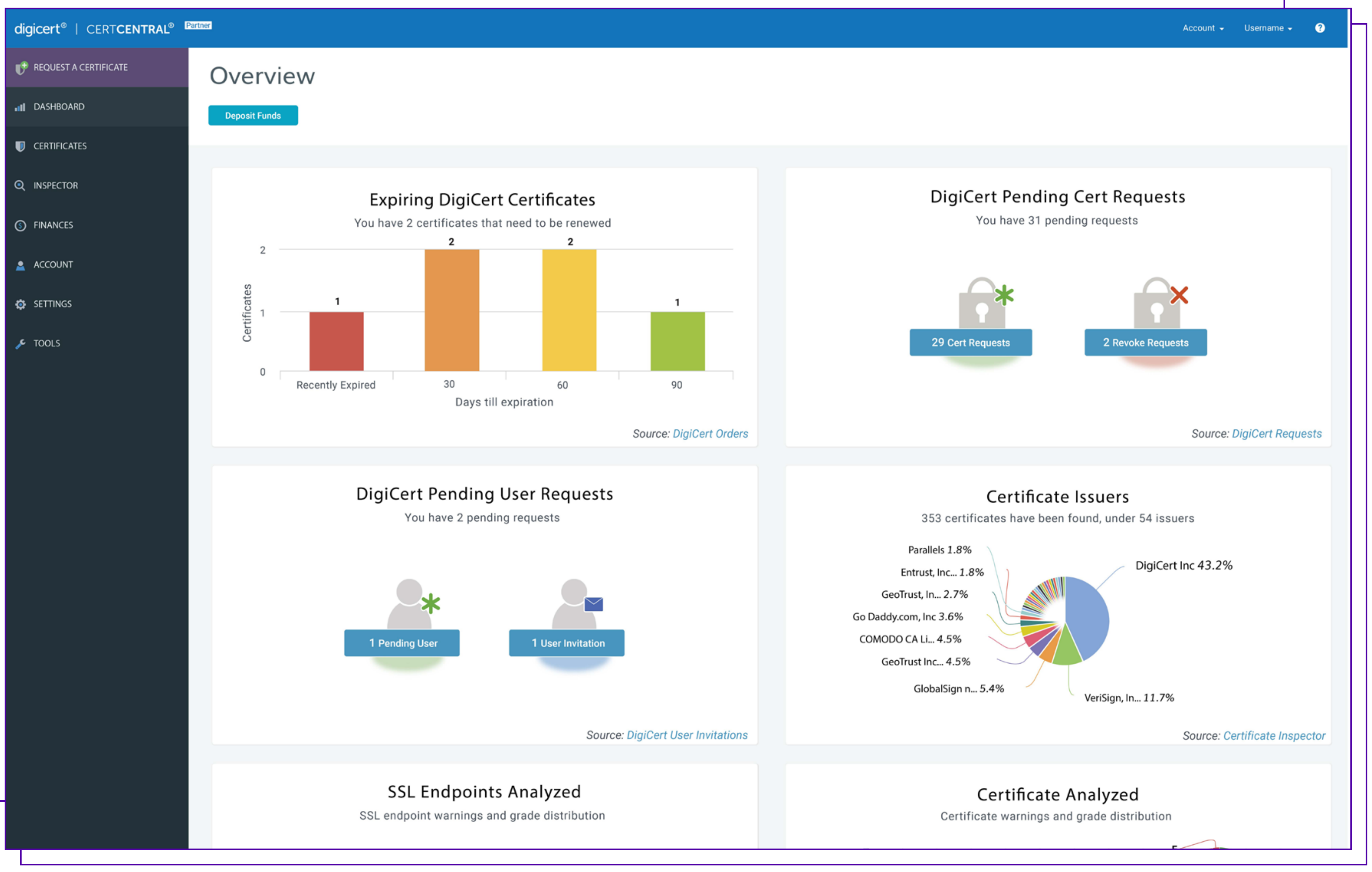
CertCentral Partner offers an updated API that lets partners easily integrate key features into their own offerings for their customers. Pre-validation capabilities, as well as support for change orders during order processing, help improve business agility. Using CertCentral, partners can support multiple sub-accounts under a main account, simplifying management of customer accounts, ordering, payments and other processes.

"DigiCert CertCentral Partner is part of our comprehensive strategy to support our partners with world-class technology and services to help them succeed," says Philip Antoniadis, executive vice president of worldwide sales at DigiCert. "Many of our partners are already experiencing compelling business outcomes, including new growth and organizational efficiencies."

"Partners have distinct requirements for managing customers' digital certificates, and DigiCert CertCentral Partner helps them better address each customer's specific needs," says Tobias Zatti, product manager at DigiCert. "CertCentral Partner helps partners simplify and expedite their selling processes while delivering a superior experience to end customers to set the stage for growth, new revenue and upsell opportunities."

CertCentral Partner provides an advanced set of account management tools for better TLS certificate deployment to end customers. Leading features allow partners to:

- Access all certificate types from one place, through an advanced API, to better address end customer requirements and easily build new solutions that help drive growth
- Take advantage of flexible ordering processes, including order changes, for improved efficiency, enhanced agility and an improved experience for end customers
- Gain 360-degree visibility through an easy-to-use UI that provides fast access to everything they require in just a few clicks
- View and use a comprehensive library of documentation with API details, technical support and more



Expiring DigiCert Certificates

You have 2 certificates that need to be renewed

Source: DigiCert Orders

DigiCert Pending Cert Requests

You have 31 pending requests

Source: DigiCert Requests

DigiCert Pending User Requests

You have 2 pending requests

Source: DigiCert User Invitations

Certificate Issuers

353 certificates have been found, under 54 issuers

Source: Certificate Inspector

SSL Endpoints Analyzed

SSL endpoint warnings and grade distribution

Certificate Analyzed

Certificate warnings and grade distribution

## Employees aware of privacy risks, but unsure of how they affect the workplace

62 percent of employees are unsure if their organization has to comply with the recently enacted CCPA, which gives California residents enhanced consumer data privacy rights, according to a survey of more than 1,000 employees conducted by Osterman Research.

The findings reveal progress in cybersecurity awareness. However, many respondents continue to hold false impressions about malware, phishing, and cloud file-sharing, putting their personal and employers' data at risk.

"The benefits and rewards of digital technology are many, but so are the risks. As states race to address cybersecurity and data privacy risks with new compliance measures, businesses are under more pressure than ever to educate their employees, or prepare to face increasingly negative outcomes," MediaPRO Chief Strategist Lisa Plaggemier said.

"To adequately protect consumer data, companies must quickly transform employees from bystanders into security advocates, and that begins with awareness programs that engage employees and reinforce behaviors that align with security and compliance goals."

The survey assessed employee engagement with and understanding of good cybersecurity and privacy practices (or lack thereof) across multiple risk areas. Overall results show more than 50 percent of respondents fall within the "vulnerable" side of the spectrum regarding their reported practices and attitudes.

"The survey revealed a number of key issues that decision makers should address right away," said Michael Osterman, Principal Analyst of Osterman Research. "Among them is the need for more and better security awareness training and improving employees' perception of their role as a key line of defense for both security and privacy compliance."

## BigID unveils discovery and security features for managing sensitive data

BigID's new data security capabilities address critical cybersecurity use cases: empowering customers to protect crown jewel data, discover dark data, automate labelling and policy enforcement, leverage access insight to highlight security vulnerabilities and overexposed data and remediate risk on their most sensitive data.

## ElectionShield protects political campaigns from online threats

ElectionShield utilizes BrandShield's technology to protect political campaigns and candidates from a growing range of online threats. These include social impersonation; fraudulent fundraising schemes; domain squatting; sale of unauthorized merchandise; fake social media content; phishing, social phishing and fake news.

### Gurucul Risk Analytics platform automates threat detection and response for MITRE ATT&CK Framework

Gurucul announced the Gurucul Risk Analytics platform has added and aligned machine learning models to detect and enable automated responses to adversarial tactics and techniques defined by the MITRE ATT&CK Framework.

Gurucul's ML models span users and entities across hybrid/ borderless environments combined with advanced threat chaining provides 83 percent coverage for MITRE ATT&CK indicators of compromise and unprecedented visibility for organizations to understand and improve their security posture.

### CrowdStrike Endpoint Recovery Services: Accelerating business incident recovery

By leveraging the power of the cloud-native CrowdStrike Falcon Platform and Threat Intelligence at the hands of CrowdStrike's highly experienced Services team, Endpoint Recovery Services helps customers actively remediate ongoing security threats and rapidly recover from a potential incident while minimizing business interruptions.

Endpoint Recovery Services accelerates the standard lifecycle of incident recovery, saving businesses from expensive downtime in their efforts to quickly detect, prevent and recover from known security incidents.

# #RSAC 2020 gallery

# CyberArk Endpoint Privilege Manager enhanced with new deception feature

CyberArk released the industry's first privilege-based deception capabilities designed to defend against credential theft on workstations and servers.

Local administrator rights are often left on endpoints, making them attractive targets for attackers who can use these credentials to elevate privileges and launch into other parts of the network.

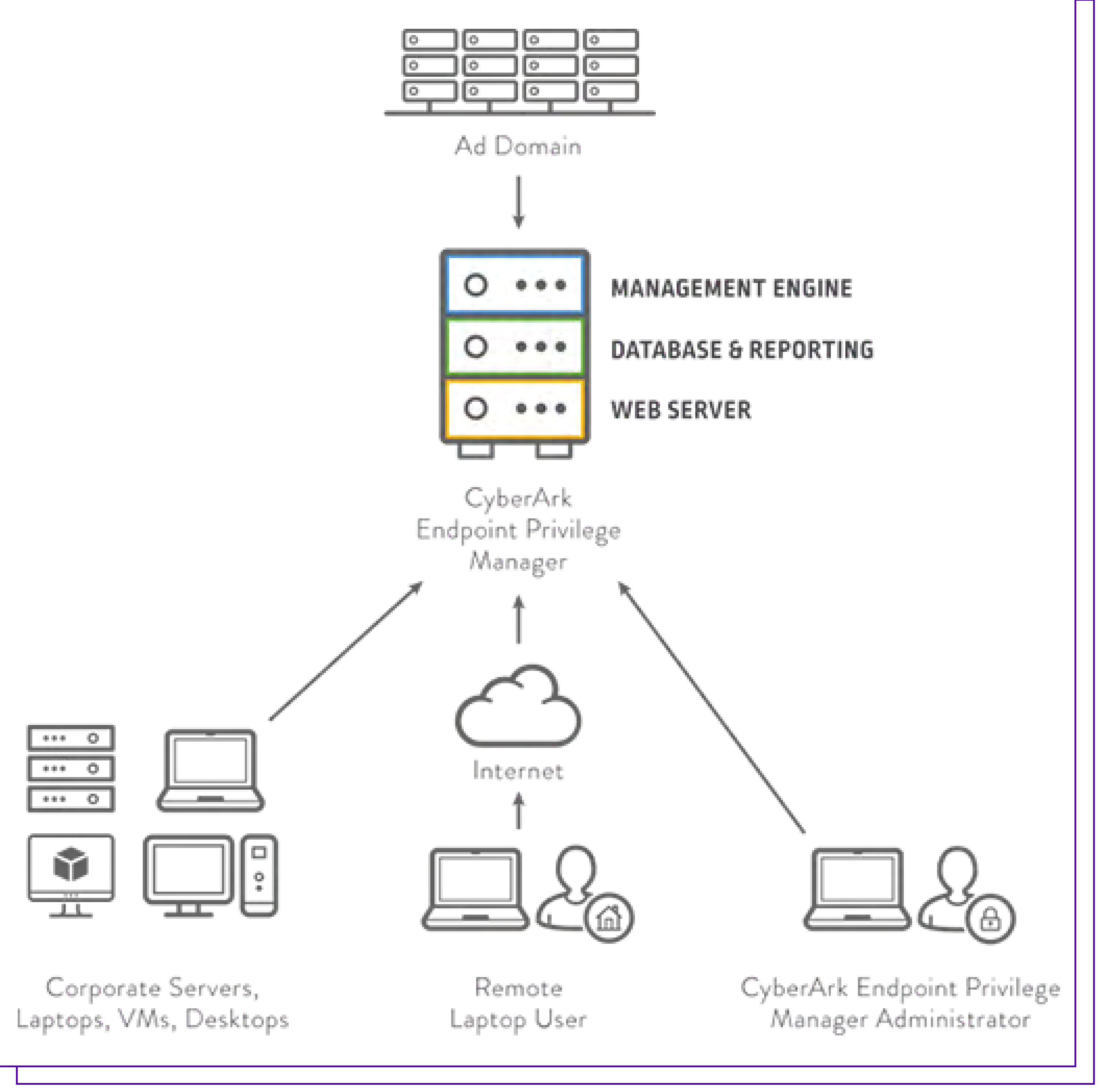
An enhancement to CyberArk Endpoint Privilege Manager, the new deception feature enables defenders to quickly detect and proactively shut down in-progress attacks. CyberArk helps break the attack chain at the initial point of entry by providing a deliberate and controlled way to track and mislead potential attackers, mitigate the exploitation of privileged credentials, and reduce dwell time.

Part of the CyberArk Privileged Access Security Solution, Endpoint Privilege Manager is a SaaS-based solution that allows organizations to reduce the risk of unmanaged administrative access on Windows and Mac endpoints. Additional capabilities include:

**Just-in-time elevation and access:** Just-in-time capabilities enable organizations to mitigate risk and reduce operational friction by allowing admin-level access on-demand for a specific period of time with a full audit log and the ability to revoke access as necessary.

**Enforcement of least privilege:** Implementing least privilege strategies, organizations reduce the attack surface by eliminating unnecessary local administrator privileges and allowing only enough access to perform the required job, no more no less.

**Credential theft blocking:** Advanced protection against credential theft enables an organization to detect and block attempted theft of endpoint credentials and those stored by the operating system, IT applications, remote access applications and popular web browsers.


Ad Domain
MANAGEMENT ENGINE
DATABASE & REPORTING
WEB SERVER
CyberArk Endpoint Privilege Manager
Internet
Corporate Servers, Laptops, VMs, Desktops
Remote Laptop User
CyberArk Endpoint Privilege Manager Administrator

# Hacking has become a viable career, according to HackerOne

HackerOne announced findings from the 2020 Hacker Report, which reveals that the concept of hacking as a viable career has become a reality, with 18% describing themselves as full-time hackers, searching for vulnerabilities and making the internet safer for everyone. Not only are more hackers spending a higher percentage of their time hacking, they're also earning a living doing it.

The annual report is a study of the bug bounty and vulnerability disclosure ecosystem, detailing the efforts and motivations of 3,150 hackers from over 120 countries who successfully reported one or more valid security vulnerabilities on HackerOne.

"Hackers are a global force for good, working together to secure our interconnected society," said Luke Tucker, Senior Director of the Global Hacker Community. "The community welcomes all who enjoy the intellectual challenge to creatively overcome limitations. Their reasons for hacking may vary, but the results are consistently impressing the growing ranks of organizations embracing hackers through crowdsourced security — leaving us all a lot safer than before."

Key findings include:

- Global growth of bug bounty programs is being followed by the globalization of the hacker community. Hackers from Switzerland and Austria earned over 950% more than in the previous year, and hackers from Singapore, China, and other countries in APAC earned over 250% more than in 2018.
- The hacker community continues to grow at a robust pace, nearly doubling in the past year to more than 600,000 registered.
- Hundreds of hackers are registering to join the ranks every day — nearly 850 on average — working to secure the technologies of more than 1,700 global customer programs.
- Hacking also provides valuable professional experience, with 78% of hackers using their hacking experience to help them find or better compete for a career opportunity.
- Hacking is becoming a popular income supplement or career choice. Nearly 40% of hackers devote 20 hours or more per week to their search for vulnerabilities. And 18% of our survey respondents describe themselves as full-time hackers.
- Most of the polled hackers are are self-taught, underscoring the importance of community and online resources.
- Hackers earned approximately $40 million in bounties in 2019 alone, which is nearly equal to the bounty totals for all preceding years combined. At the end of this past year, hackers had cumulatively earned more than $82 million for valid vulnerability reports.
- In addition to the seven hackers who have passed the $1 million earnings milestone, thirteen more hit $500,000 in lifetime earnings.
- Hackers in the U.S. earned 19% of all bounties last year, with India (10%), Russia (8%), China (7%), Germany (5%), and Canada (4%) rounding out the top 6 highest-earning countries.
- Most of the polled hackers prefer to hack websites (71%), the rest go for APIs, iOS and Android mobile apps, and other software.
- The polled hackers found the Burp Suite to be the most useful tool when hacking (89%), followed by tools they built (39%), fuzzers (32%), and web proxies/scanners (25%).

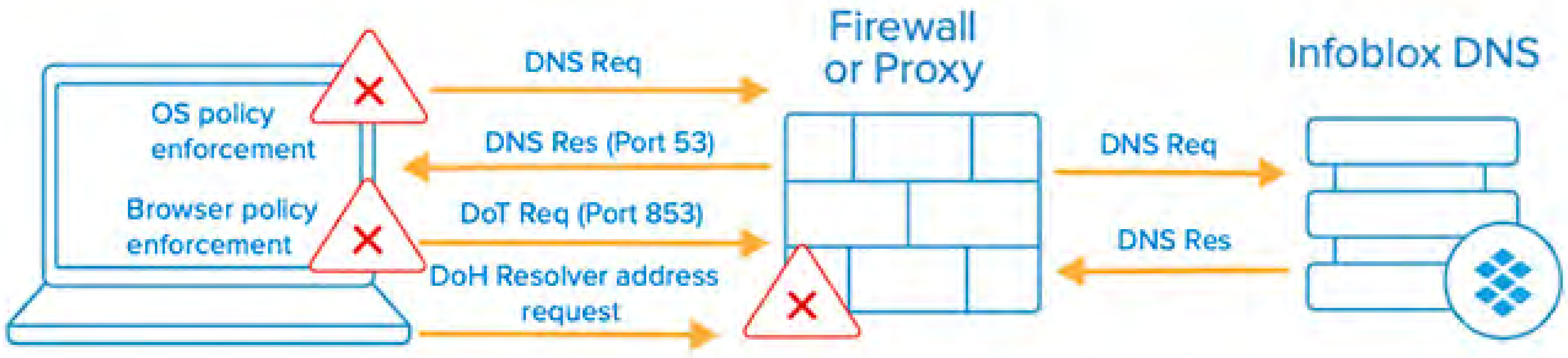
# Infoblox announces enterprise best practices for DoT/DoH

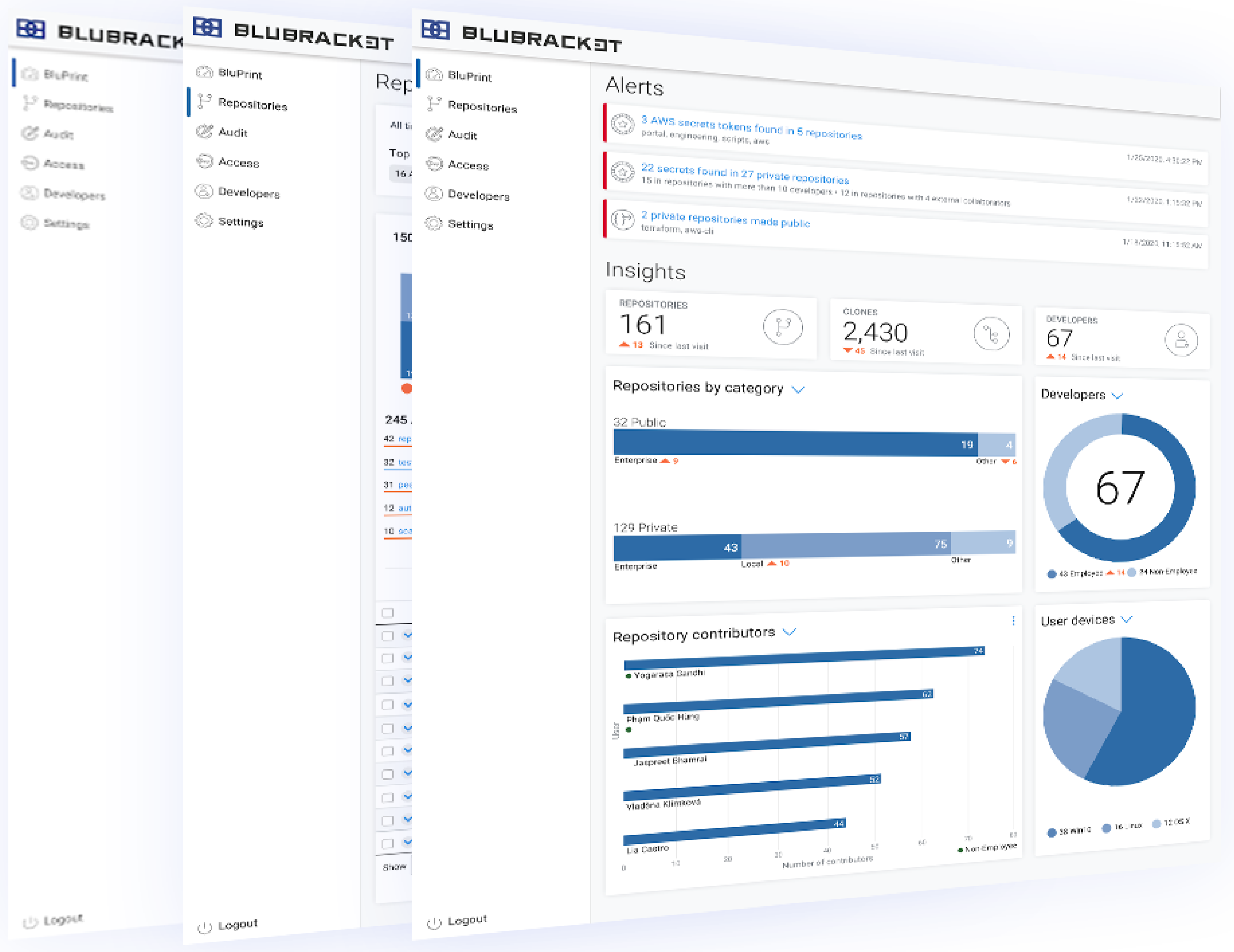
Infoblox, the leader in Secure Cloud-Managed Network Services, announced Enterprise best practices on DNS over TLS (also known as DoT) and DNS over HTTPS (DoH). These DoT/DoH guidelines are based on Infoblox's longtime commitment to providing customers with DDI services that enable them to easily and effectively secure their own DNS communications.

BloxOne Threat Defense, a hybrid foundational security solution from Infoblox that uses DNS as the first line of defense, blocks resolution to DoH domains and facilitates a graceful fallback to existing internal DNS. This helps prevent DoH misuse and mitigates risk.

BloxOne Threat Defense includes the following features to help manage DoH:

- Policy threat intelligence feeds for DoH, which provide the ability to control the DNS access method used to detect and mitigate threats by disabling DoH-based security policies. A threat intelligence feed containing canary domains is available to achieve this. Browsers will gracefully fallback to the organization's managed DNS without interrupting user activity.
- DoH-Policy feed for known DoH IPs and DoH domains added to Threat Intelligence Data Exchange, Infoblox's threat intelligence aggregation and distribution platform, which can then be used by other security tools like NGFWs to block DoH traffic to external servers.
- Ability to review DoH-related domains and IPs within Dossier, Infoblox's threat investigation tool.





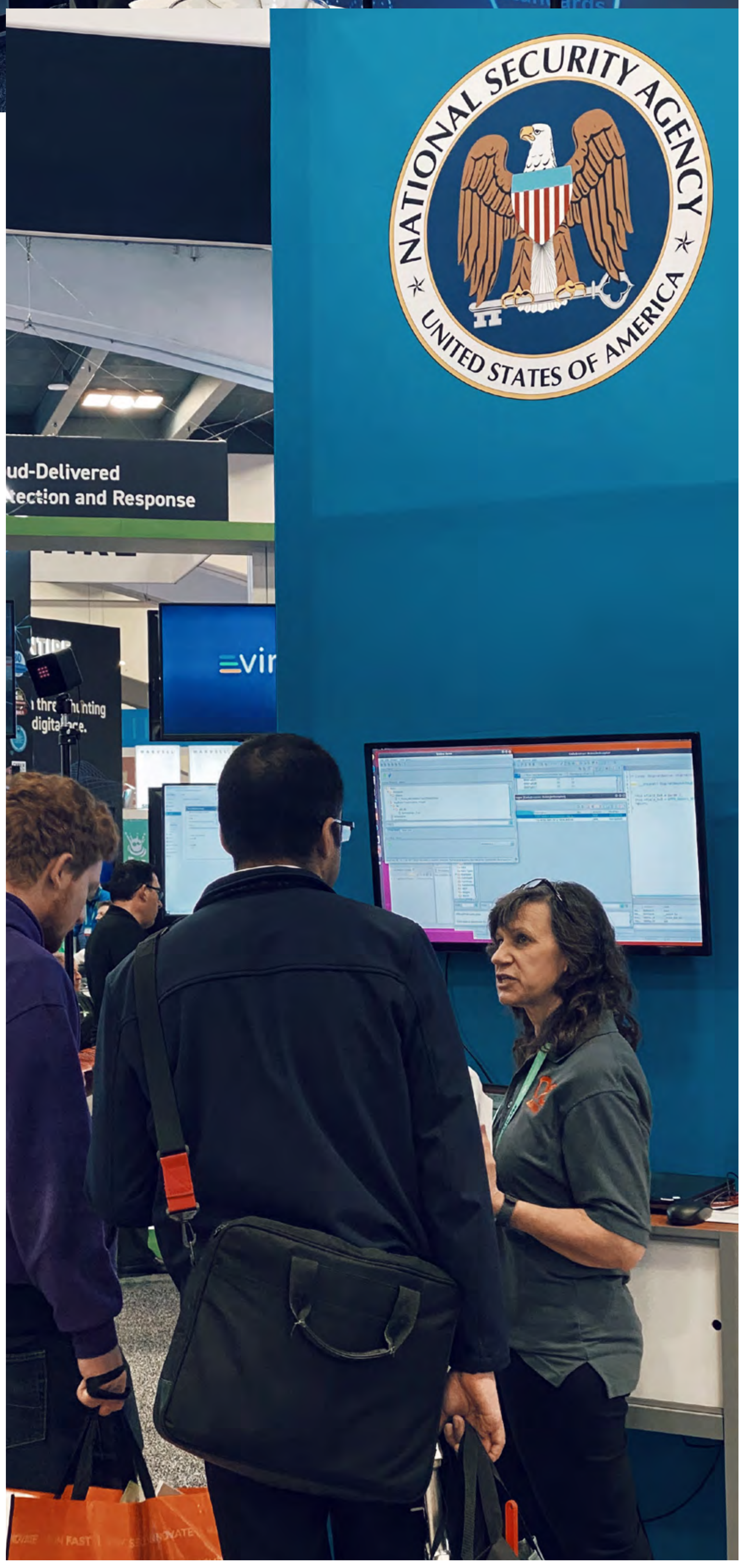
## BluBracket unveils security solution that makes code safe

BluBracket introduced its product suite, representing the industry's first comprehensive security solution for code in the enterprise. BluBracket combines deep expertise in enterprise security with innovative and developer-friendly technology. Its BluBracket:CodeInsights and BluBracket:CodeSecure products give companies the key to unlock software innovation while protecting their enterprise infrastructure and valuable intellectual property.

# #RSAC 2020 gallery

THE FIRST "FULLY CLOUD-BASED" CYBERSECURITY COMPANY EVER
Recorded Future
CenturyLink
Cyber Everywhere
ISRAEL
Combat Threats Multi-Cloud Analytics-Driven Cloud SIEM

SKYSYNC
ACT TO THE FUTURE
ACCESS CLASSIFY TAKE ACTION
ENTERPRISE CONTENT ORCHESTRATION
Holland IT Security House
DeLorean



## Zero Networks Access Orchestrator: Autonomous, airtight network access security at scale

Zero Networks Access Orchestrator is a network security platform that automatically defines, enforces and adapts user- and machine-level network access policies to create a continuous airtight zero trust network model, at scale.

Assuming users and machines inside the network can be completely trusted leaves the door open for malicious insiders and hackers to do almost anything they want. Zero Networks minimizes these risks, with the click of a button, constraining access in the network to only what users and machines should be doing.

## Increased monetization means more ransomware attacks

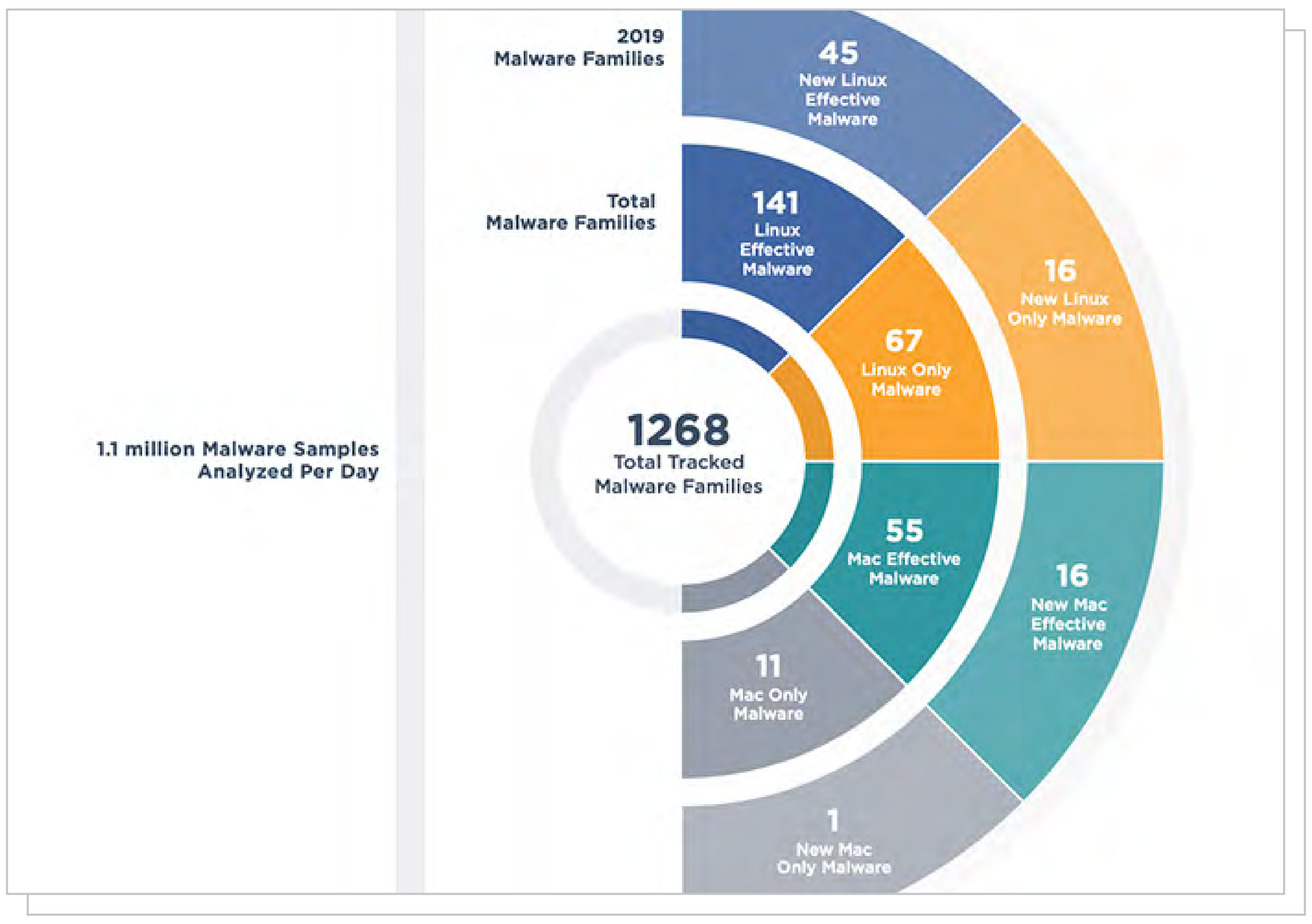
Organizations are detecting and containing attacks faster as the global median dwell time (defined as the duration between the start of a cyber intrusion and it being identified) was 56 days. This is 28% lower than the 78-day median observed in the previous year, according to FireEye.

Consultants attribute this trend to organizations improving their detection programs, as well as changes in attacker behaviors such as the continued rise in disruptive attacks (e.g., ransomware and cryptocurrency miners) which often have shorter dwell times than other attack types.

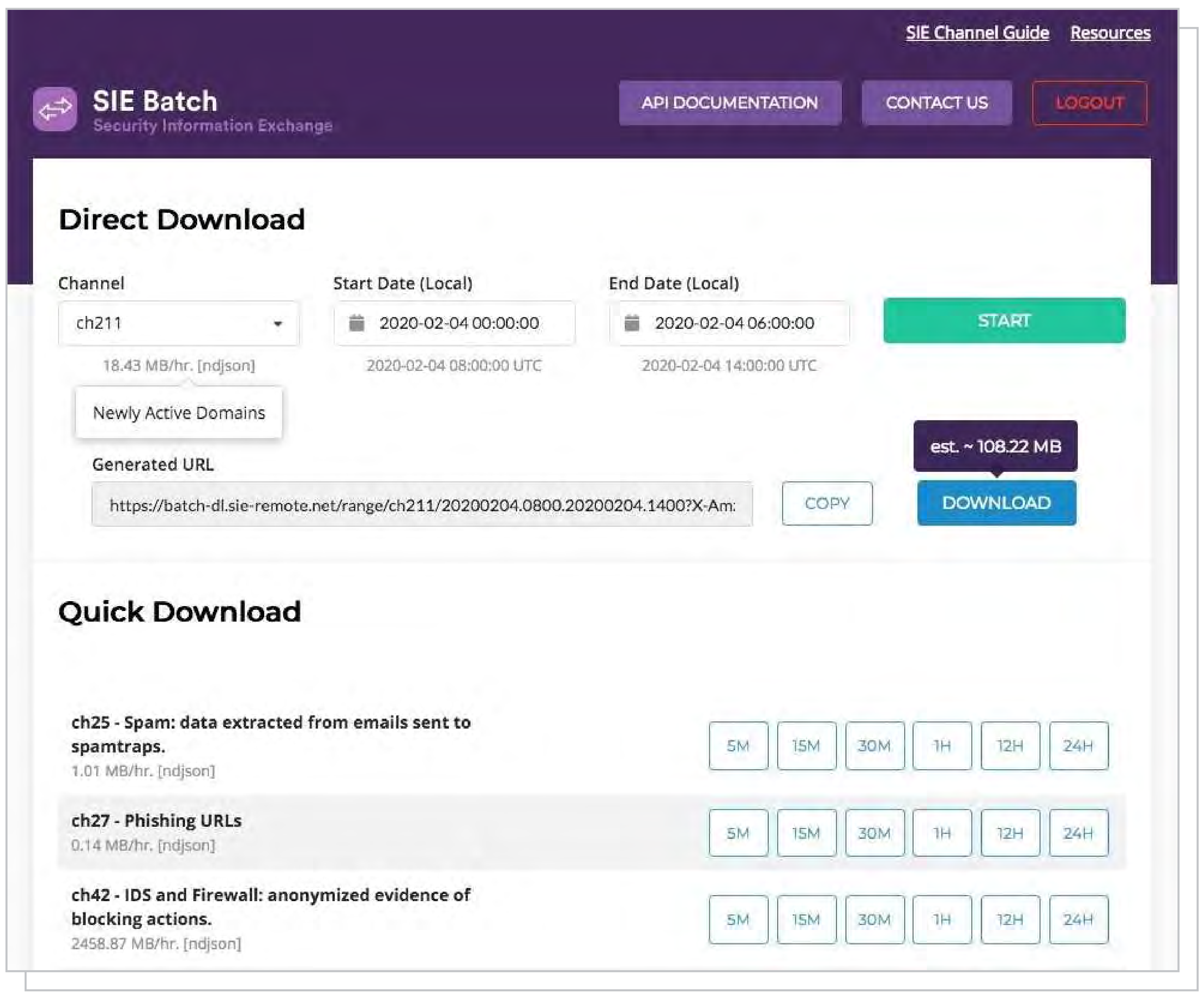
The report details how of all the malware families observed in 2019, 41% had never been seen before. Furthermore, 70% of the samples identified belonged to one of the five most frequently seen families, which are based on open source tools with active development.

These points demonstrate that not only are malware authors innovating, cybercriminals are also outsourcing tasks to monetize operations faster.

Also of note: the majority of new malware families impacted either Windows or multiple platforms. While new malware families solely impacted Linux or Mac, this activity remains in the minority.



## Farsight Security enhances its Security Information Exchange data-sharing platform



Direct Download

Channel: ch211
18.43 MB/hr. [ndjson]
Newly Active Domains

Start Date (Local): 2020-02-04 00:00:00
2020-02-04 08:00:00 UTC

End Date (Local): 2020-02-04 06:00:00
2020-02-04 14:00:00 UTC

Generated URL: https://batch-dl.sie-remote.net/range/ch211/20200204.0800.20200204.1400?X-Am:

est. ~ 108.22 MB

Quick Download

ch25 - Spam: data extracted from emails sent to spamtraps.
1.01 MB/hr. [ndjson]

ch27 - Phishing URLs
0.14 MB/hr. [ndjson]

ch42 - IDS and Firewall: anonymized evidence of blocking actions.
2458.87 MB/hr. [ndjson]

Farsight Security announced enhancements to its flagship, Security Information Exchange (SIE) data-sharing platform to help security professionals measurably improve the prevention, detection and response of the latest cyberattacks.

Newly active domains: The industry's first real-time DNS Intelligence data feed that reports domains as they resume activity on the Internet after a period of inactivity (10 days or more). This data is very useful to detect, block, and investigate domains used by threat actors who acquire and reuse expired domains with previously good reputations or by patiently waiting to establish a harmless reputation for their domain before utilizing it.

SIE batch: A new easy-to-use and easy-to-integrate delivery method to access data from our powerful, proven real-time solutions – available via both API and a Web interface – including Newly Observed Domains, DNS Changes and the newly added, Newly Active Domains, as well as high-value third-party data feeds including Darknet, Spam, Phishing URLS and DDoS Events, all available via the company's flagship Security Information Exchange platform.

# #RSAC 2020 gallery

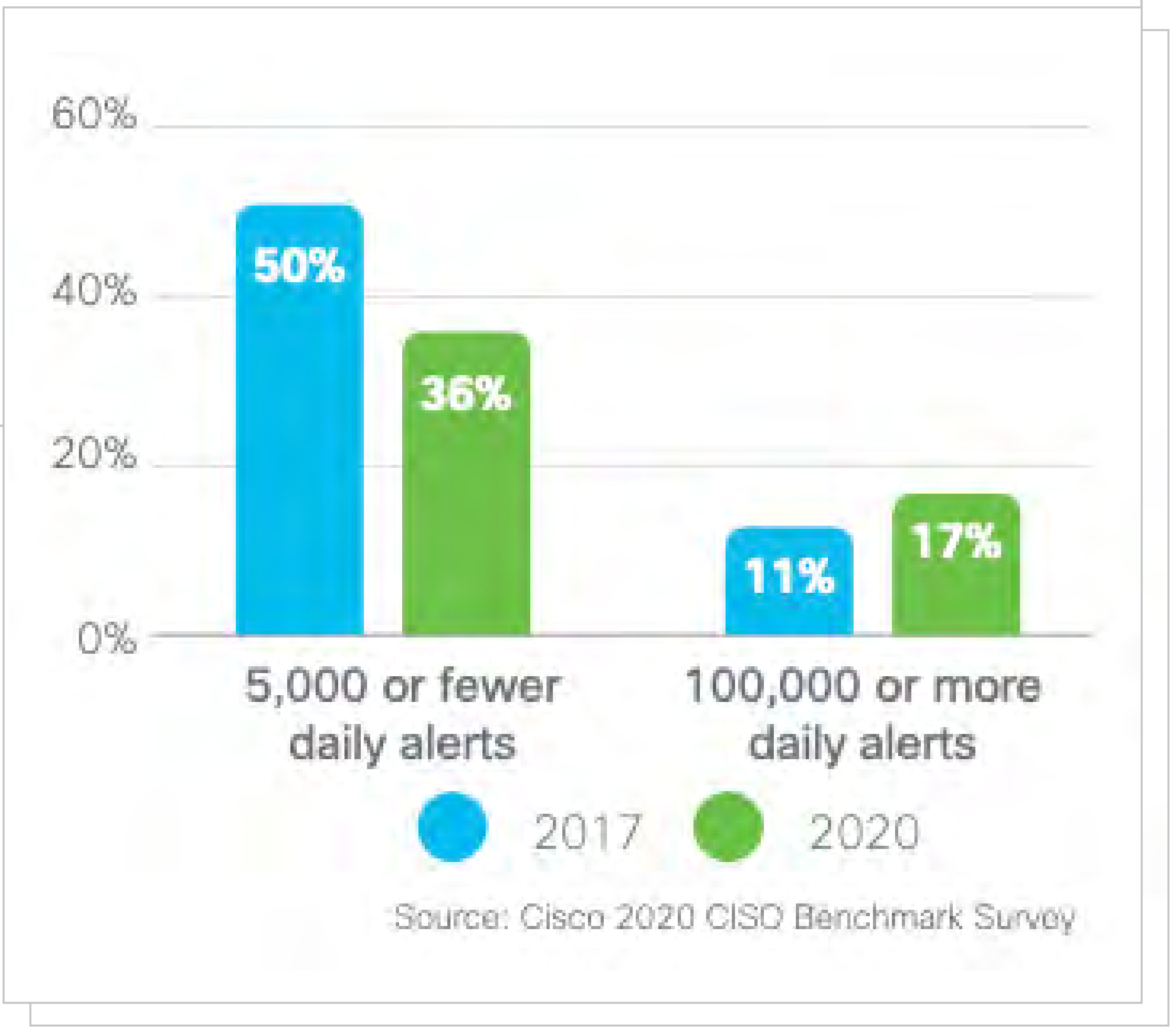
# Combat complexity to prevent cybersecurity fatigue

In today's security landscape, the average company uses more than 20 security technologies. While vendor consolidation is steadily increasing with 86 percent of organizations using between 1 and 20 cybersecurity vendors, more than 20 percent feel that managing a multi-vendor environment is very challenging, which has increased by 8 percent since 2017, according to a Cisco's CISO Benchmark Report for which they surveyed 2,800 security professionals from 13 countries around the globe.

To combat cybersecurity complexity, security professionals are increasing investments in automation to simplify and speed up response times in their security ecosystems; using cloud security to improve visibility into their networks; and sustaining collaboration between networking, endpoint and security teams.

"As organizations increasingly embrace digital transformation, CISOs are placing higher priority in adopting new security technologies to reduce exposure against malicious actors and threats. Often, many of these solutions don't integrate, creating substantial complexity in managing their security environment," said Steve Martino, Senior Vice President and CISO, Cisco.

"To address this issue, security professionals will continue steady movement towards vendor consolidation, while increasing reliance on cloud security and automation to strengthen their security posture and reduce the risk of breaches."



Source: Cisco 2020 CISO Benchmark Survey

## Secureworks launches Cloud Configuration Review

Secureworks' new Cloud Configuration Review pairs its two decades of security operations and consulting experience with the innovative VMware Secure State, a public cloud security and compliance monitoring platform, to give customers an immediate head start against cloud security risks such as misconfiguration. The solution will help customers detect configuration vulnerabilities, understand the business impact of critical risks and address the security and compliance challenges associated with public cloud adoption.

## Exabeam releases Cloud Platform to make every security practitioner more efficient

The Exabeam Cloud Platform helps security leaders mature their security posture; aid architects to secure new use cases by expediting the provisioning and consumption of new applications, tools and content; and make security engineers and analysts more efficient with simplicity of use and deployment. Applications, including the previously announced Exabeam Threat Intelligence Service and the new Exabeam Cloud Archive, will be available on the Cloud Platform through the Exabeam Application Marketplace.

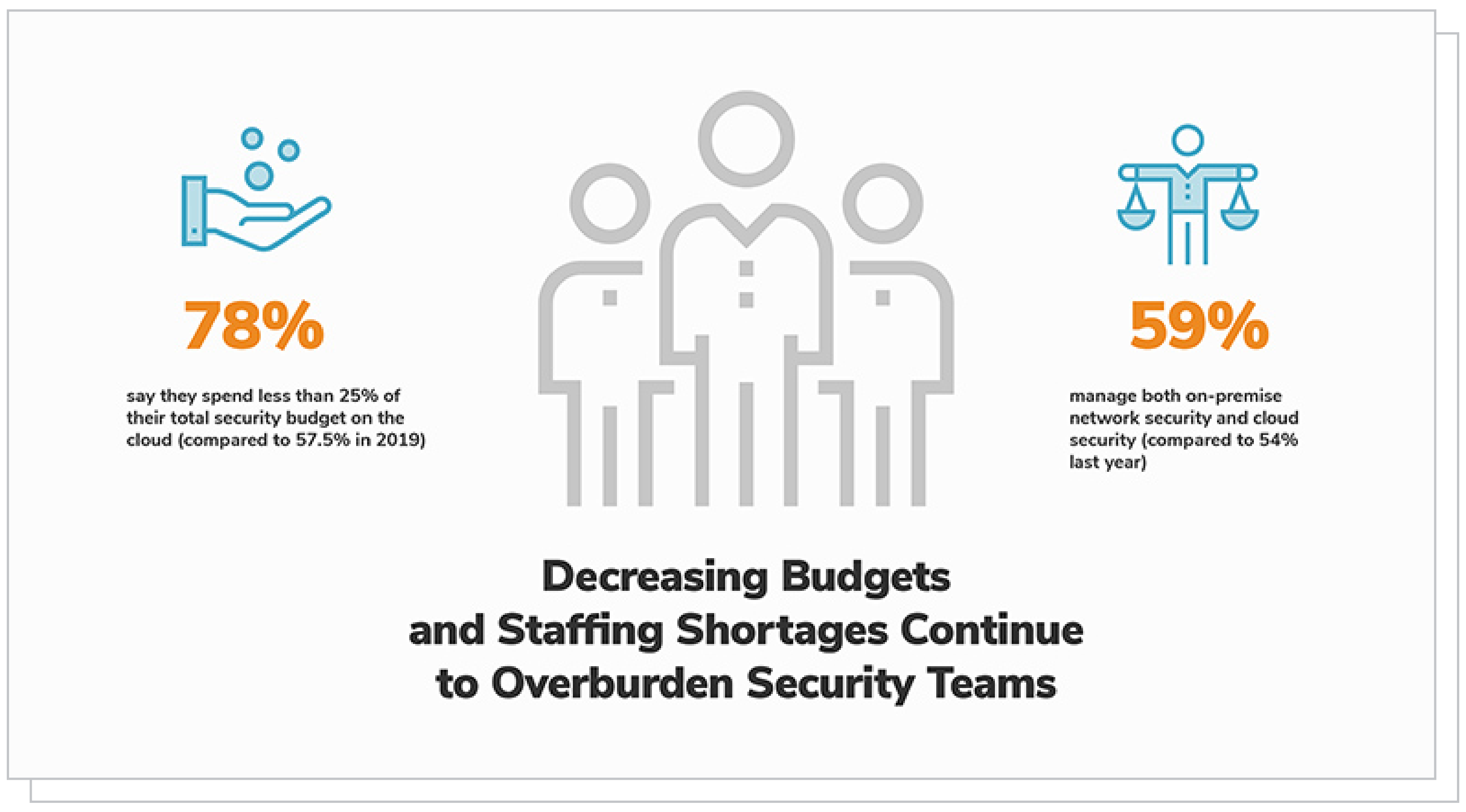
## Exploring the impact that hybrid cloud is having on enterprise security and IT teams

While enterprises rapidly transition to the public cloud, complexity is increasing, but visibility and team sizes are decreasing while security budgets remain flat to pose a significant obstacle to preventing data breaches, according to FireMon's 2020 State of Hybrid Cloud Security Report.

While enterprises increasingly transition to public and hybrid cloud environments, their network complexity continues to grow and create security risks. Meanwhile, they are losing the visibility needed to protect their cloud systems, which was the biggest concern cited by 18 percent of C-suite respondents, who now also require more vendors and enforcement points for effective security.

The 2020 FireMon State of Hybrid Cloud Security Report found that:

- Business acceleration outpaces effective security implementations.
- Nearly 60 percent believed their cloud deployments had surpassed their ability to secure the networks in a timely manner. This number was virtually unchanged from 2019, showing no improvement against a key industry progress indicator.
- The number of vendors and enforcement points needed to secure cloud networks are also increasing; 78.2 percent of respondents are using two or more enforcement points. This number increased substantially from the 59 percent using more than two enforcement points last year. Meanwhile, almost half are using two or more public cloud platforms, which further increases complexity and decreases visibility.


78%
say they spend less than 25% of their total security budget on the cloud (compared to 57.5% in 2019)
59%
manage both on-premise network security and cloud security (compared to 54% last year)
Decreasing Budgets and Staffing Shortages Continue to Overburden Security Teams

## Anitian enhances its Cloud Security Platform with compliance documentation automation

Anitian announced Documentation Automation, an enhancement to its Cloud Security Platform that automates documentation for the most stringent compliance standards. This enhancement further delivers on Anitian's promise to deliver unrivaled time-to-compliance and the fastest possible time-to-market for high-growth SaaS companies.

For the first time, compliance documentation frameworks for FedRAMP, PCI, SOC2, ISO/GDPR, and more can be automated with a single click and collected in a single location. The "enter once, populate everywhere" process slashes the time companies spend creating mandated compliance documents by as much as 80 percent.

## Cyware’s 2.0 suite of cyber fusion products enables orgs to detect, analyze, and act on security threats

Cyware Labs, provider of advanced cyber fusion solutions, announced the release of version 2.0 of the company’s product suite. Available now, enhancements across the matrix of Cyware’s solutions include end-to-end threat intelligence automation, threat response and management capabilities, as well as an improved user interface.

With Cyware, organizations can leverage the best of both the human element and machine-enabled automation to streamline communication and collaboration between all security teams including threat intel, hunting, vulnerability assessment and SecOps.

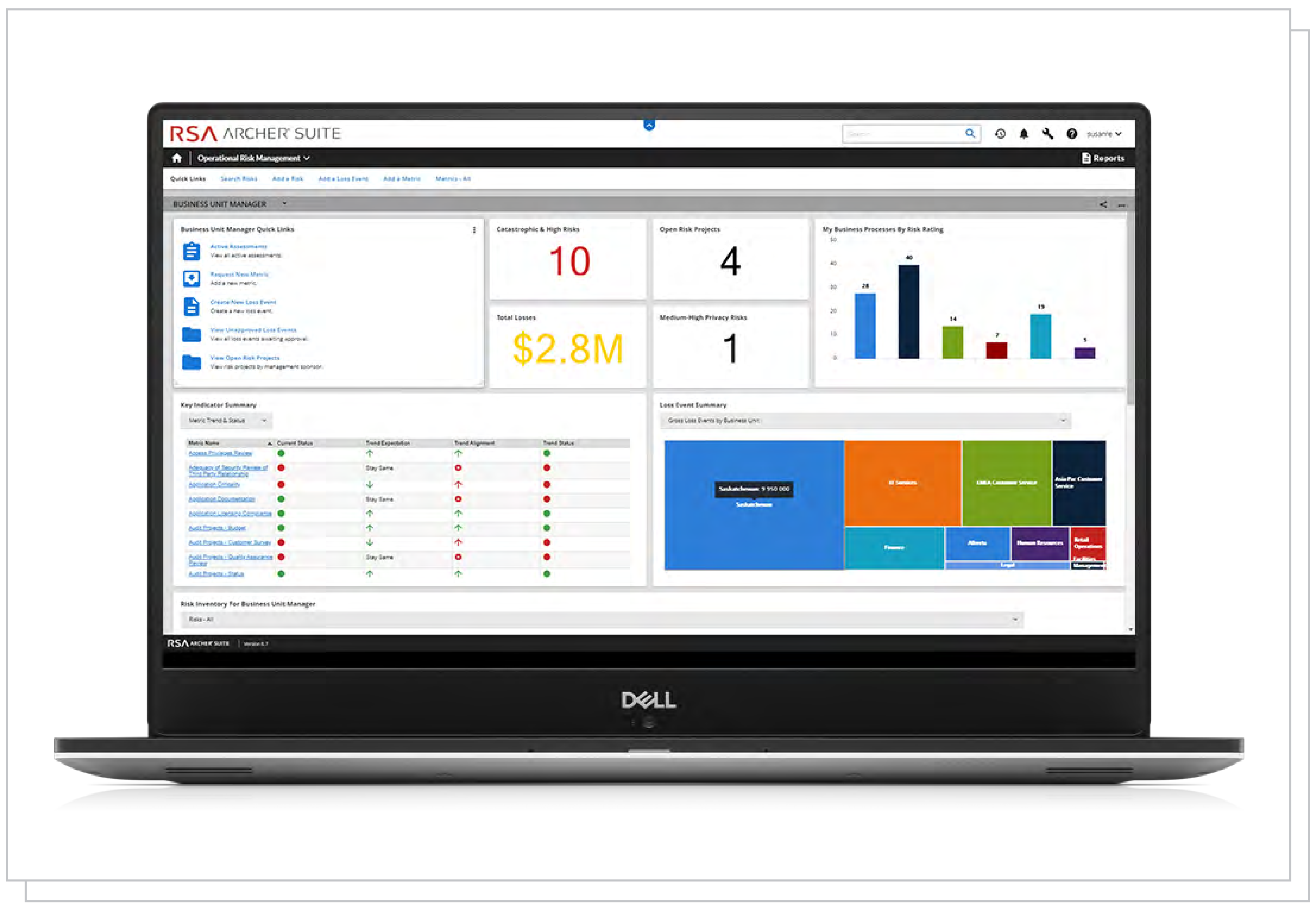
## RSA Archer SaaS: An integrated approach to managing risk

RSA, a global cybersecurity leader delivering Business-Driven Security solutions to help organizations manage digital risk, is now offering RSA Archer SaaS (software as a service) for customers seeking to implement the RSA Archer Suite in the cloud. This offering provides organizations with the speed and agility of an integrated approach to managing risk delivered with flexibility and scalability needed to navigate digital transformation and protect against loss while supporting strategic growth.

“The RSA Archer Suite helps organizations at any stage in their risk management maturity journey to more effectively and efficiently manage risk as they strive to keep up in today’s hyperconnected world,” said David Walter, Vice President, RSA Archer.

Key benefits of RSA Archer SaaS include:

- Quick time to value with the ability to stand up an instance in days/hours
- Flexibility and scalability of the cloud to support organizations’ changing integrated risk management (IRM) and business requirements
- Lower total cost of ownership
- Faster access to the latest RSA Archer features and functionality
- Mission-critical resiliency and committed SLA



## IronKey D300 features advanced security, achieves NATO Restricted Level Certification

After a detailed validation process, the Kingston IronKey D300, IronKey D300S and IronKey D300SM have been listed in the NATO Information Assurance Product Catalogue (NIAPC) for security products that meet NATO’s nations, civil and military bodies’ operational requirements. The IronKey D300 series is now included on this list, which means it is qualified as an encrypted Flash drive that meets the data protection levels established by NATO to protect information against loss or cyber-attacks. Sensitive data-in-transit needs to be protected as any loss or breach can result in harm to NATO’s forces, its members or its mission.

# BlackBerry launches new UES platform for zero trust

BlackBerry announced the BlackBerry Spark platform with a new unified endpoint security (UES) layer which can work with BlackBerry UEM and other unified endpoint management (UEM) solutions to deliver BlackBerry's One Agent, One Console, One Crowd, One Cloud approach to achieve zero trust security.

Leveraging artificial intelligence, machine learning and automation, BlackBerry Spark now offers improved cyberthreat prevention and remediation, and provides visibility across all endpoints, including desktop, mobile, server, and IoT (including automotive).

# Sumo Logic Cloud SIEM Enterprise: Helping SOC personnel to better manage real security events

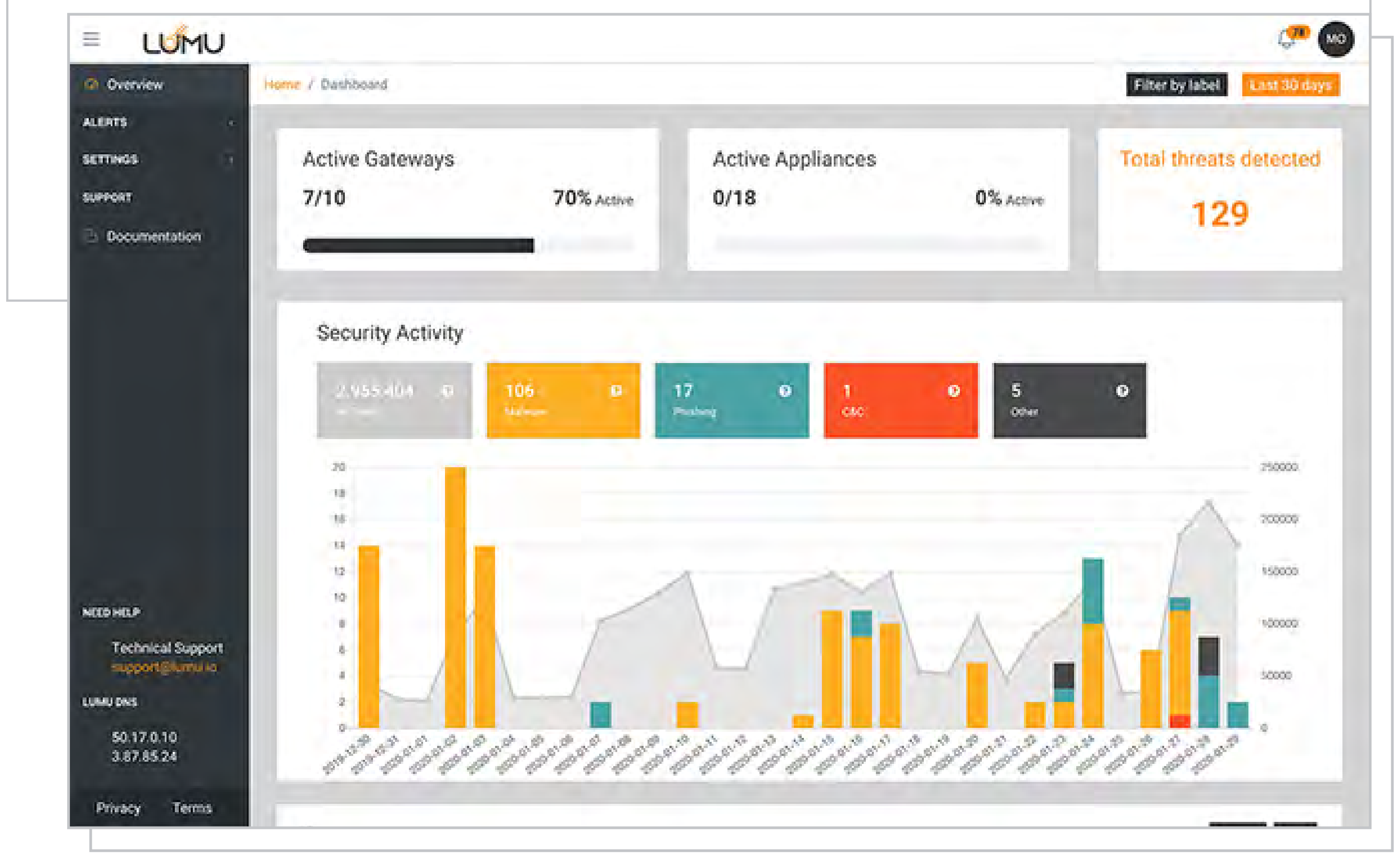
Sumo Logic announced the availability of its new Cloud SIEM Enterprise offering, which includes a rich set of capabilities to ease the burden on security operations center (SOC) personnel.

The new capabilities help identify and prioritize high fidelity threats and automate the analyst workflow, allowing SOC personnel to better manage real security events and effectively enforce security and compliance policies.

# Is your network already compromised? LUMU illuminates network blind spots

LUMU is a cloud-based solution that collects and standardizes metadata from across the network, including DNS queries, Network Flows, access logs from perimeter proxies and/or firewalls, and spam box filters, and then applies AI to correlate threat intelligence from these disparate data sources to isolate confirmed points of compromise.

"While attackers have become adept at covering their tracks once inside the network, they also must themselves use the network to move around, leaving trace remnants behind that become obscured amidst all the network noise. The LUMU solution was purpose-built to sift through massive amounts of network metadata in real-time, detect the telltale signals of compromise, and illuminate those network blind spots with pinpoint accuracy," said Ricardo Villadiego, CEO of LUMU. The LUMU solution can be configured in less than 30 minutes and provides real benefits to enterprise security teams.



Active Gateways
7/10 70% Active

Active Appliances
0/18 0% Active

Total threats detected
129

Security Activity

106 Malware
17 Phishing
1 C&C
5 Other

NEED HELP
Technical Support
support@lumu.io

LUMU DNS
50.17.0.10
3.87.85.24

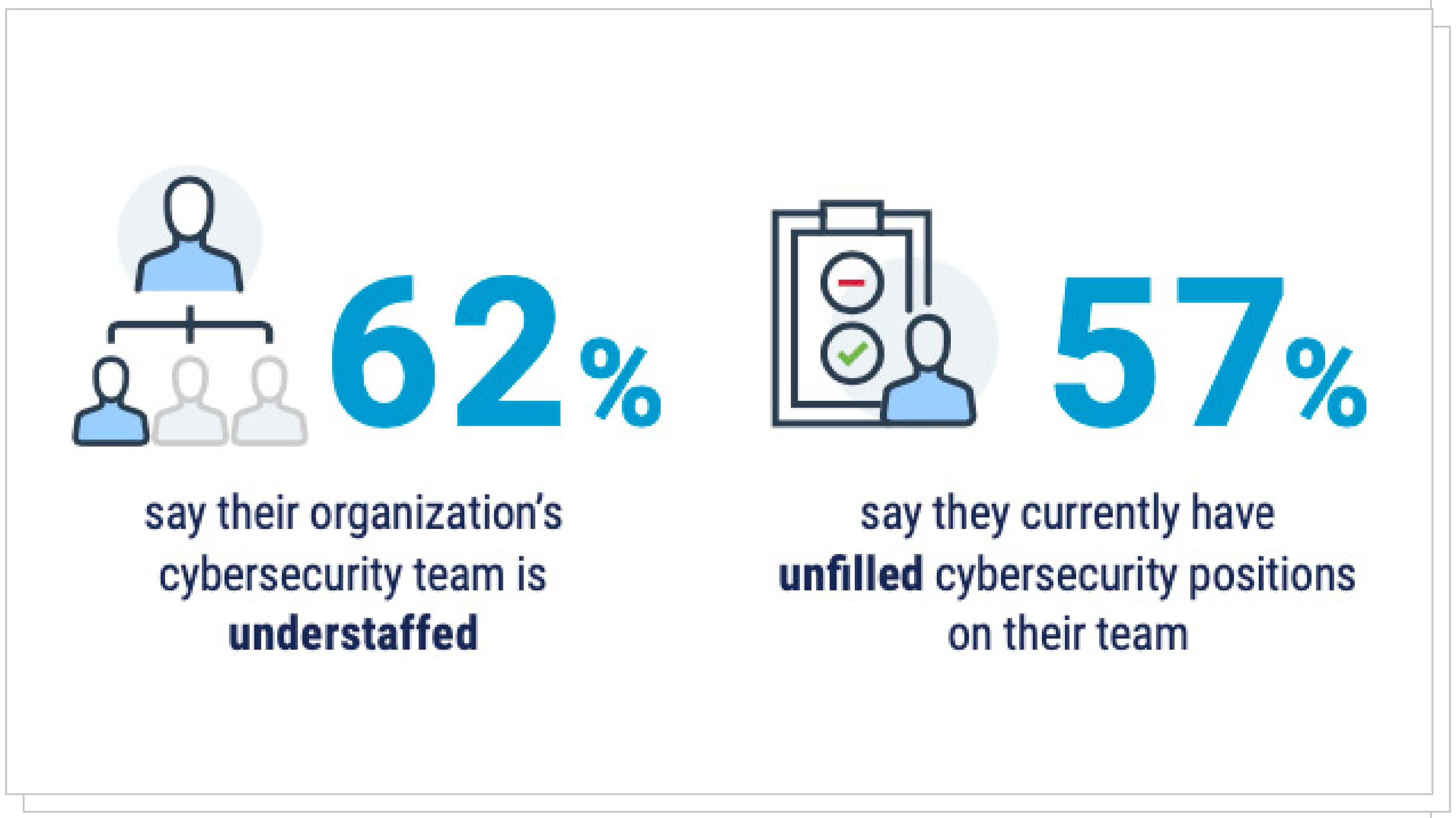
## Cybersecurity hiring challenges and retention issues demand new talent pipelines

Cybersecurity teams continue to struggle with hiring and retention, and very little improvement has been achieved in these areas since last year, according to ISACA.

ISACA's 2020 State of Cybersecurity survey report finds that enterprises are short-staffed, have difficulty identifying enough qualified talent and don't believe their HR teams adequately understand their hiring needs.

Additionally, while slight progress is reported in increasing the number of women in cybersecurity roles and in establishing diversity programs, most cybersecurity teams still indicate they have significantly more men than women, and most report that progress is minimal.

"Cybersecurity jobs are in huge demand but, as many organizations are all too aware, it continues to be a real struggle to find the right candidates with the right skills and experience to meet the demands of these roles," says retired Brigadier General Greg Touhill, ISACA board director, and President of the AppGate Federal Group.



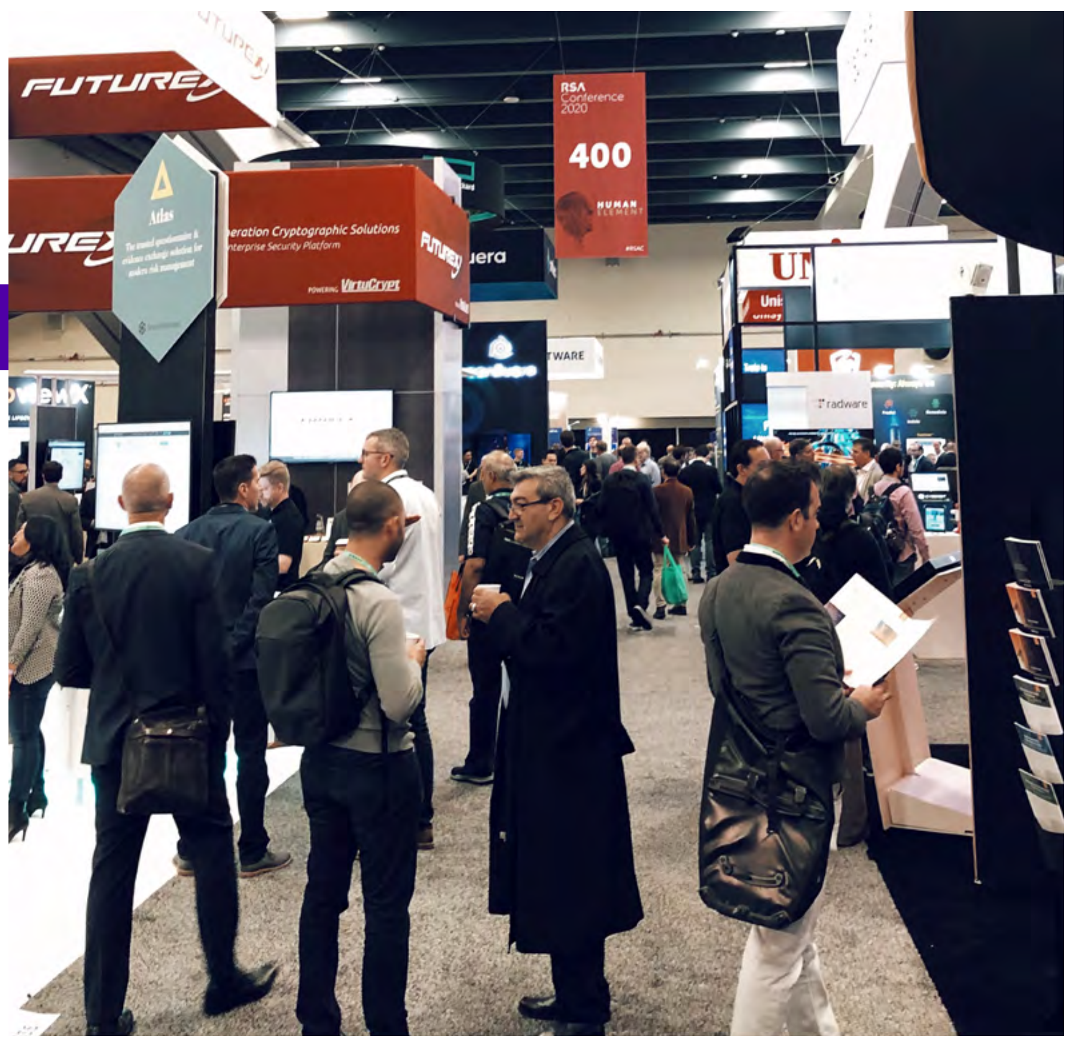
**62%** say their organization's cybersecurity team is **understaffed**

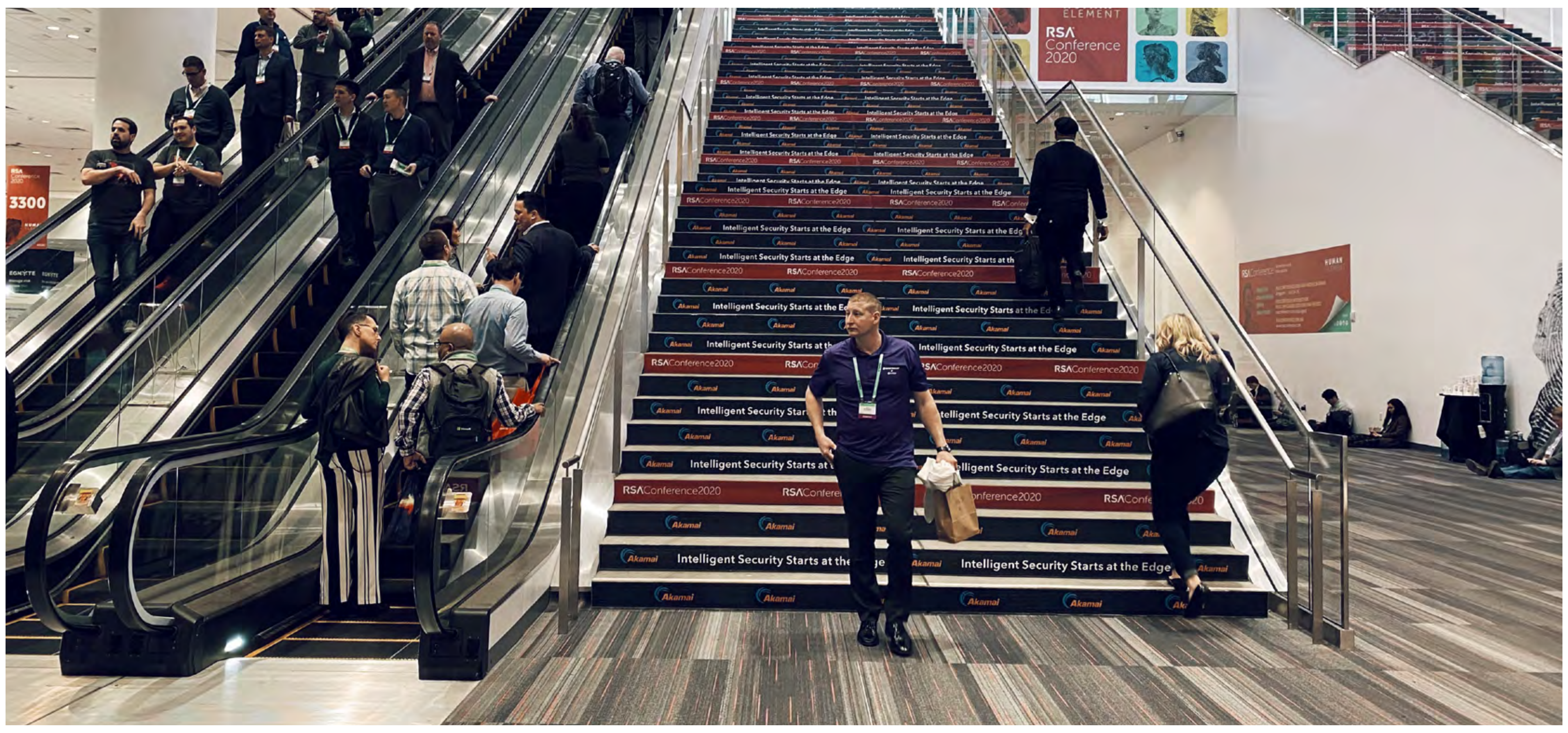
**57%** say they currently have **unfilled** cybersecurity positions on their team

## Cisco SecureX unifies visibility, identifies unknown threats, and automates workflows

Cisco SecureX provides a comprehensive user experience across the breadth of Cisco's integrated security portfolio and customers' existing security infrastructure. It unifies visibility, identifies unknown threats, and automates workflows to strengthen customers' security across network, endpoint, cloud, and applications. Because simplicity is essential to securing today's digital transformation, Cisco SecureX is included with every Cisco Security product.

# #RSAC 2020 gallery





MobileIron Unified Endpoint Management
The Foundation of a Secure Enterprise
Secure passwordless access to the enterprise using any mobile device
9 out of 10 Security leaders believe that mobile devices will be your ID
mobileiron
Ivanti
proven mobile leader
mobileiron