[+] (IN)SECUREMagazine

06 | 2022

ISSUE 71.5

#RSAC 2022

Acronis

www.acronis.com

All-in-One Cyber Protection

With solutions for service providers, businesses, and home users, Acronis Cyber Protection Solutions help lower risk by protecting all data, applications, and systems – wherever they are.

- ✓ Automate your backup and recovery processes
- ✓ Prevent cyberattacks with advanced anti-malware, ransomware protection, virus scanning, vulnerability assessments, patch management, and more
- ✓ Streamline your endpoint protection management

Learn More

Trusted cybersecurity and the best backup for complete cyber protection

AV-TEST The Independent IT-Security Institute Magdeburg Germany

VirusTotal

vb 100 VIRUS virus BULLETIN

MRG Effitas EFFICACY ASSESSMENT & ASSURANCE

ICSA labs

NioGuard Security Lab

RSA Conference concluded its 31st annual event at the Moscone Center in San Francisco on Friday, June 10. Several of the most pressing topics discussed during this year's Conference included issues surrounding privacy and surveillance, the positive and negative impacts of machine learning and artificial intelligence, the nuances of risk and policy, and cybersecurity-focused innovations across crypto and blockchain.

"RSA Conference plays a critical role in bringing the cybersecurity industry together. As cyberattacks grow in frequency and sophistication, it's imperative that practitioners and experts across the public and private sector convene to hear unique perspectives to help address today's biggest challenges," said Linda Gray Martin, Vice President, RSA Conference.

"RSA Conference is where the world talks security, and this week has been an amazing example of the importance of this event to our community," said Dr. Hugh Thompson, Program Committee Chair at RSA Conference and Managing Partner of Crosspoint Capital Partners.

FEATURED NEWS

SPONSORS

GOLD: Acronis, cynet

SILVER: CONCENTRIC, DARKTRACE, VOTIRO

BRONZE: MEND, PIXM

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

Zeljka Zorz
Editor-In-Chief
press@helpnetsecurity.com

Mirko Zorz
Director of Content
press@helpnetsecurity.com

Berislav Kucan
Director of Operations
bkucan@helpnetsecurity.com

Photography by (IN)SECURE Magazine.

Acronis introduces unique, turn-key DLP solution

Acronis debuted a new Advanced Data Loss Prevention (DLP) pack for Acronis Cyber Protect Cloud, a game-changing solution that shields MSPs and businesses of all sizes from data leakage. Notably, the solution does not require months for deployment, and highly skilled teams to maintain it.

Drawing from decades-long experience enabling MSPs in data protection, this expansion resolves the main obstacles hindering the broader adoption of DLP solutions: grueling roll-out and cumbersome ongoing administrative execution.

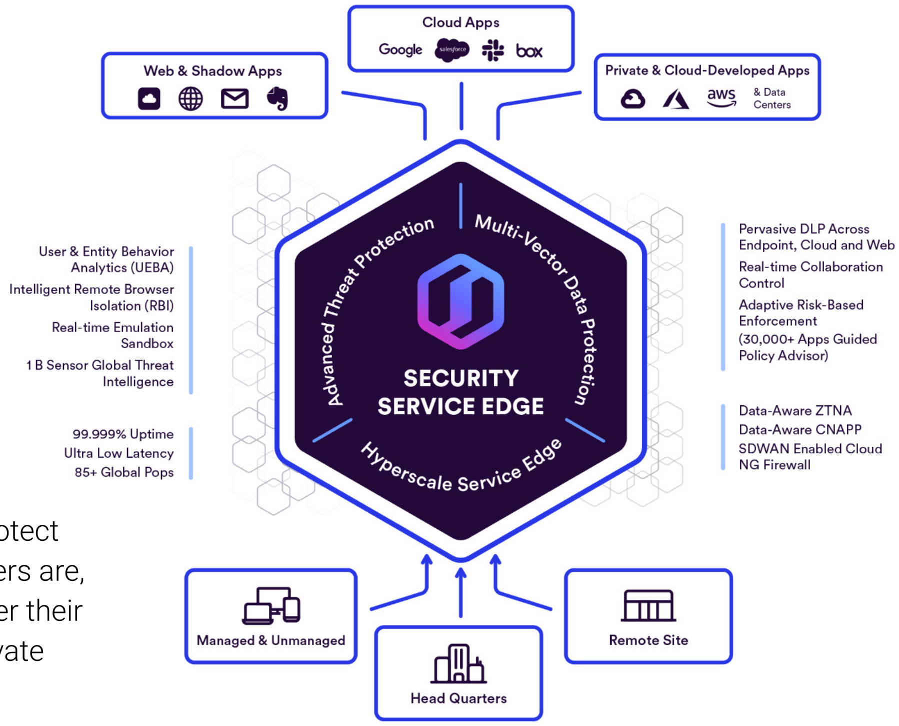
For years, organizations have struggled to protect sensitive data from unauthorized access via external attacks or insider risks such as IT misconfigurations and human error. Only a handful of large enterprises had the resources to manage the overall complexity, high deployment costs, and more significant obstacles that come with DLP adoption. This is why the global DLP market size is set to exceed US$6 billion by 2026, according to Global Industry Analysts Inc.

The integration of behavioral-based DLP capabilities into the Acronis Cyber Protect Cloud platform is what extends its ability to deliver unified data protection, cybersecurity and management across systems, data and workloads regardless of their location. It offers an unparalleled range of cyber protection capabilities that span the NIST cybersecurity framework from Identification to Recovery to ensure business continuity in the face of cybercriminals, insider risk threats or technology failure.

The Early Access version of Acronis Advanced DLP:

- Protects sensitive data transferred via a wide array of user and system connections including for example, instant messaging and peripheral devices.
- Uses the same, unified Acronis Cyber Protect Cloud console and agent for data visibility and classification.
- Offers out-of-box data classification templates for common regulatory frameworks including GDPR, HIPAA and PCI DSS.
- Provides continuous monitoring for DLP incidents with multiple policy enforcement options, enabling ongoing automated policy adjustment to business-specifics.
- Includes robust audit and logging capabilities, giving administrators the ability to respond effectively to DLP events and conduct post-breach forensic investigations.

Skyhigh Security SSE platform enhancements protect data regardless of where it lies


Cloud Apps
Google
salesforce
box
Web & Shadow Apps
Private & Cloud-Developed Apps
aws
& Data Centers
User & Entity Behavior Analytics (UEBA)
Intelligent Remote Browser Isolation (RBI)
Real-time Emulation Sandbox
1 B Sensor Global Threat Intelligence
99.999% Uptime
Ultra Low Latency
85+ Global Pops
Advanced Threat Protection
Multi-Vector Data Protection
SECURITY SERVICE EDGE
Hyperscale Service Edge
Pervasive DLP Across Endpoint, Cloud and Web
Real-time Collaboration Control
Adaptive Risk-Based Enforcement
(30,000+ Apps Guided Policy Advisor)
Data-Aware ZTNA
Data-Aware CNAPP
SDWAN Enabled Cloud NG Firewall
Managed & Unmanaged
Head Quarters
Remote Site

With Skyhigh SSE, organizations can protect sensitive data no matter where their users are, what device they are using, and wherever their data resides: on the web, cloud, and private applications.

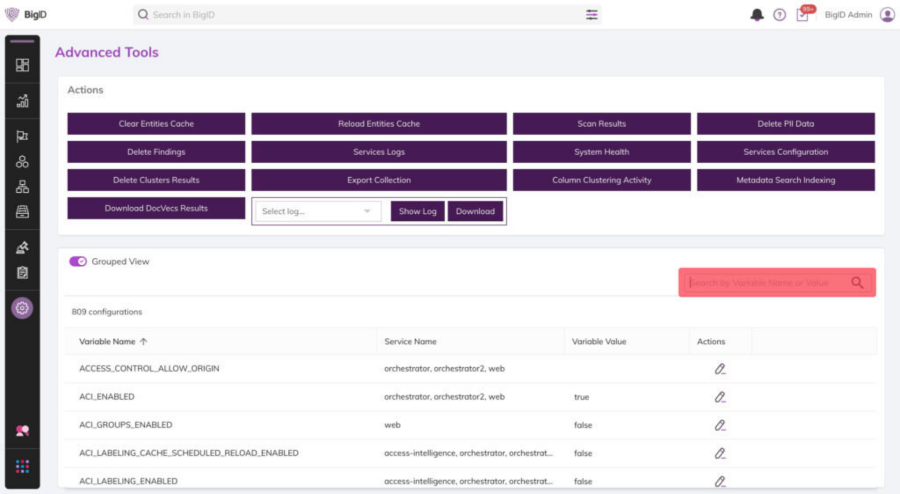
According to anonymized internal data, Skyhigh Security processes approximately 8.6 billion events tied to systems, devices, software, applications, and services that are without explicit IT department approval (shadow IT) and 1.6 billion events that are approved (sanctioned) daily, demonstrating the rapid adoption of cloud services. With remote and hybrid workforces becoming the norm, organizations need long-term solutions in place to secure data that is no longer necessarily routed through their corporate network or managed devices. Skyhigh Security's latest advancements solve this challenge while reducing cost, simplifying data protection, and enabling this new work environment.

Appgate SDP 6.0 accelerates zero trust implementations for enterprises

Appgate SDP 6.0's new risk model capability will enable customers to assign high/medium/low sensitivity levels to specific workloads and resources. It will provide a simple, flexible way to measure user/device risk at sign-on—via security tools they already have in place—against the sensitivity of the resource they are trying to access. The risk model will then dynamically adjust access rights based on the risk score.

"While Zero Trust is becoming more widely adopted, many organizations have very complex IT environments, including a wide range of already-deployed security tools, and it can be difficult to know where to begin," said Jawahar Sivasankaran, President and Chief Operating Officer, Appgate. *"The user-friendly risk model in the latest version of Appgate SDP will help organizations get the most out of the cybersecurity investments they've already made, while bringing these tools forward into a Zero Trust security model. We're focused on continually innovating our solutions to help our customers simplify their cybersecurity journeys, accelerate progress and scale as their IT infrastructures evolve."*

BigID unveils SmallID to help customers improve security posture across the cloud



809 configurations

Variable Name ↑	Service Name	Variable Value	Actions
ACCESS_CONTROL_ALLOW_ORIGIN	orchestrator, orchestrator2, web		✎
ACI_ENABLED	orchestrator, orchestrator2, web	true	✎
ACI_GROUPS_ENABLED	web	false	✎
ACI_LABELING_CACHE_SCHEDULED_RELOAD_ENABLED	access-intelligence, orchestrator, orchestrat...	false	✎
ACI_LABELING_ENABLED	access-intelligence, orchestrator, orchestrat...	false	✎

SmallID brings cloud-native data privacy and protection to organizations of all sizes, making it easy to find and mitigate risk across their entire cloud environment. Customers can easily reduce their attack surface, identify high-risk data, and automatically discover dark data across the cloud – without impacting business.

"Cloud-native organizations leave themselves vulnerable to bad actors and a host of other complex issues when they don't have insight into what kind of data they are collecting," said Tyler Young, Chief Information Security Officer at BigID. *"SmallID is a huge step forward for organizations of all sizes to have on-demand cloud protection that reduces the attack surfaces through allowing teams to identify and mitigate risk across their entire cloud environment."*

FortiRecon gives enterprises adversary's perspective of their attack surface

Fortinet announced FortiRecon, a complete Digital Risk Protection Service (DRPS) offering that uses a combination of machine learning, automation capabilities, and FortiGuard Labs cybersecurity experts to manage a company's risk posture and advise meaningful action to protect their brand reputation, enterprise assets, and data.

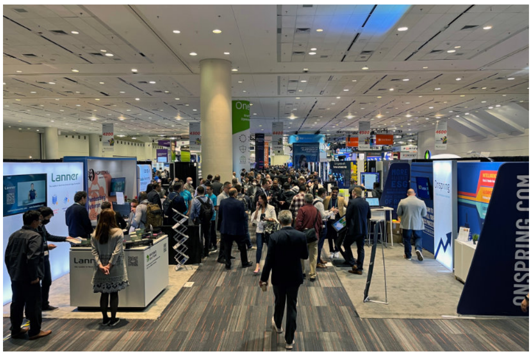
FortiRecon delivers a triple offering of outside-in coverage across External Attack Surface Management (EASM), Brand Protection (BP), and Adversary-Centric Intelligence (ACI) to counter attacks at the reconnaissance phase – the first stage of a cyberattack – to significantly reduce the risk, time, and cost of later stage threat mitigation.

Optiv CRS protects mission-critical assets and enhances recovery

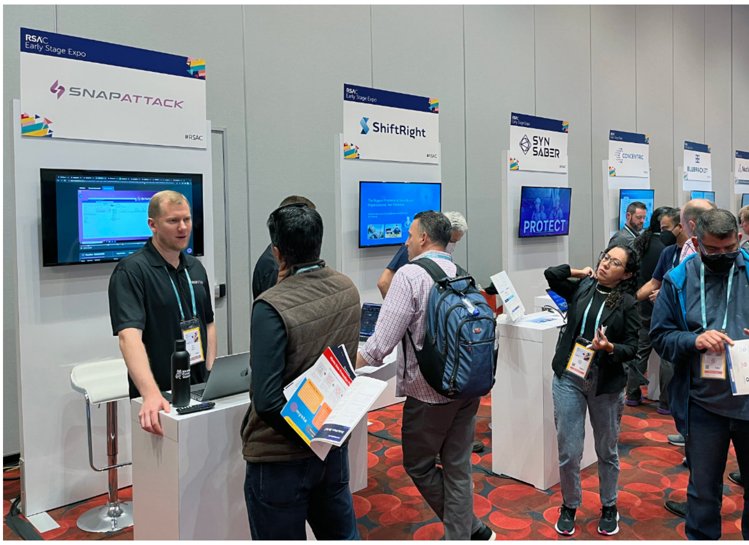
Optiv's CRS helps organizations get back to business faster by providing strategic and tactical advisory and technology solutions for cyber readiness while enabling rapid recovery to a secure state. CRS identifies and prioritizes the protection of critical assets through automated workflows that backup business-essential data, systems, and applications and supports the implementation of a vaulted, data-isolated, air-gapped backup solution that reduces the risk of data loss.

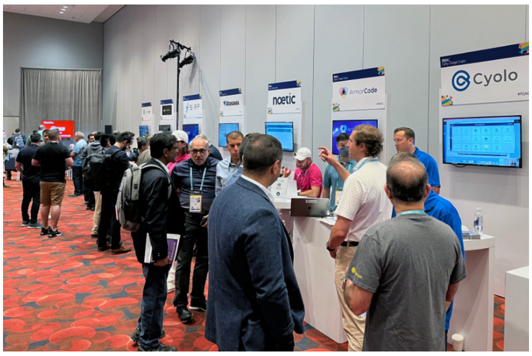
#RSAC 2022 GALLERY

Acronis #CyberFit
Streamline with complete cyber protection
One Platform, One License
Detect
Acronis
Behavioral DLP & EDR
www.acronis.com



#RSAC 2022
EARLY STAGE EXPO





Top three most critical areas of web security

Akamai Technologies revealed three research reports at the RSA Conference 2022, focusing on three of the most critical areas of web security: ransomware, web applications and APIs, and DNS traffic.

Analyzing trillions of data points across its multiple platforms, the research team uncovered new findings on threat actor behavior via popular attack traffic and techniques. The three reports link the most prominent security trends and paint an accurate map of the modern attack landscape. An up-to-date analysis of ransomware attack trends highlight the risks and suggest mitigation, while an analysis of Web app and API attack trends offers a fresh look at the infection vectors used by ransomware operators and others. An analysis of DNS complements the reports with a view of overall attacks analyzed via one of the internet's most foundational technologies. The analysis centers on attack trends and techniques as well as solutions to solve today's most pressing cybersecurity issues.

Highlights from each report

Ransomware threat

With the rise of Ransomware-as-a-Service (RaaS) attacks, including from the Conti ransomware gang, Akamai analyzed and discovered the most recent and effective components of ransomware attackers' methodologies, tools and techniques. Key findings include:

- Sixty percent of successful Conti attacks were conducted on United States companies, while 30% occurred in the European Union.
- An analysis of the industries attacked highlights the risk of supply chain disruption, critical infrastructure impact, and supply chain cyberattacks.
- Most successful Conti attacks target businesses with $10-250 million in revenue, indicating a "goldilocks" range of successful attack targets among medium and small businesses.
- The gang's tactics, techniques, and procedures (TTPs) are well-known, but highly effective – a sobering reminder of the arsenal that is at the disposal of other hackers. But also that these attacks can be prevented with the right mitigation.
- Conti's emphasis in their documentation on hacking and hands-on propagation, rather than encryption, should drive network defenders to focus on those parts of the kill chain as well, instead of focusing on the encryption phase.

Web application & API threat

Through the first half of 2022, significant increases were observed in web application and API attacks across the globe, with more than nine billion attack attempts to date. Details for each of the company's key observations are as follows:

- Web application attack attempts against customers grew by more than 300% year over year in H1, the largest increase ever observed.
- LFI attacks now surpass SQLi attacks as the most predominant WAAP attack vector, increasing by nearly 400% year over year.
- Commerce is the most impacted vertical, accounting for 38% of recent attack activity, while technology has seen the most growth so far in 2022.

DNS traffic insights threat

Analyzing more than 7 trillion DNS queries per day and proactively identifying and blocking threats, including malware, ransomware phishing, and botnet, researchers found:

- More than 1 of 10 monitored devices communicated at least once to domains associated with malware, ransomware, phishing or command and control (C2).
- Phishing traffic showed that most victims were targeted by scams that abused and mimicked technology and financial brands, which affected 31% and 32% of the victims, respectively.
- According to research that analyzed more than 10,000 malicious JavaScript samples — representing threats like malware droppers, phishing pages, scammers and cryptominers' malware — at least 25% of the examined samples used JavaScript obfuscation techniques to evade detection.

Tenable closes acquisition of Bit Discovery and announces new solution to reduce cyber risk

Tenable announced it has closed its acquisition of Bit Discovery, a provider of external attack surface management (EASM).

Tenable will launch Tenable.asm, a new solution that will provide the full capabilities of Bit Discovery's technology and enable customers to gain a more complete 360-degree view of their full attack surface so they can better understand how attackers could gain access via the internet and help prioritize remediation steps.

Code42 adds watchlists functionality to its Incydr product to help teams manage insider risk events

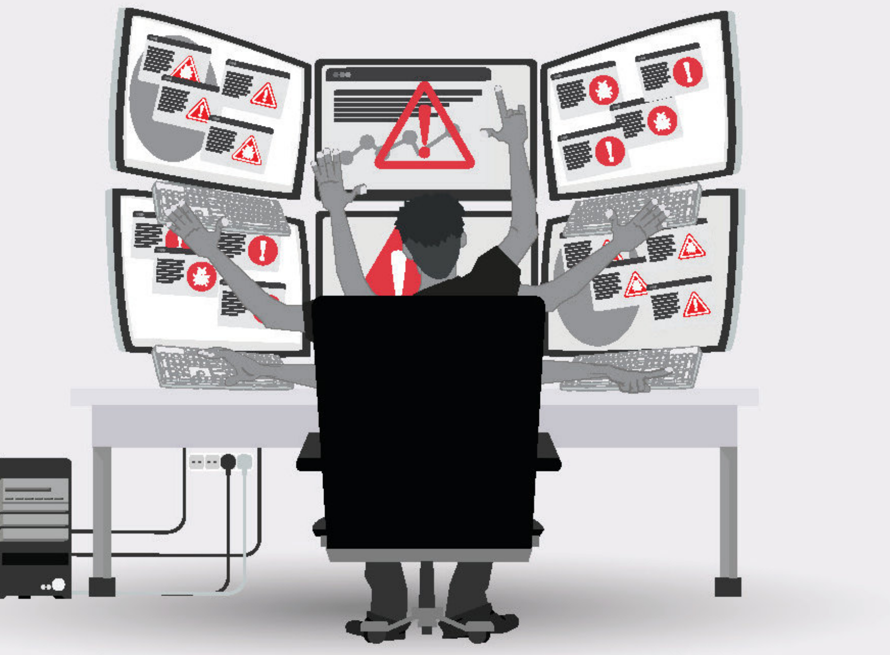
Code42 announced it expanded the data risk detection capabilities in the Code42 Incydr product to give security teams visibility and context to situational Insider Risk events.

Through its watchlist functionality, Incydr simplifies security teams' ability to focus on data risk tied to distinct user groups that are most likely to put data at risk, such as departing employees, contractors, privileged users and new hires. Teams can also create custom watch lists for specific projects or departments or for users with common attributes.

"Since the launch of Incydr, we've been giving security teams visibility to insider risk events tied to departing employees, which continues to be a primary trigger for data exfiltration. We've learned that other clusters of employees, such as new hires, employees that have repeatedly neglected security protocols, or teams working on confidential projects, exhibit similar patterns of risky data movement – whether unintentional or malicious. Security teams can now closely monitor the data movement and exposure of these groups to apply tailored responses that will reduce data risk," said Dave Capuano, senior vice president of product management at Code42. *"The context provided through watchlists helps security teams respond more quickly and accurately to insider risk events and drive targeted training to improve collaboration habits that decrease future data risk."*

cynet

Old way



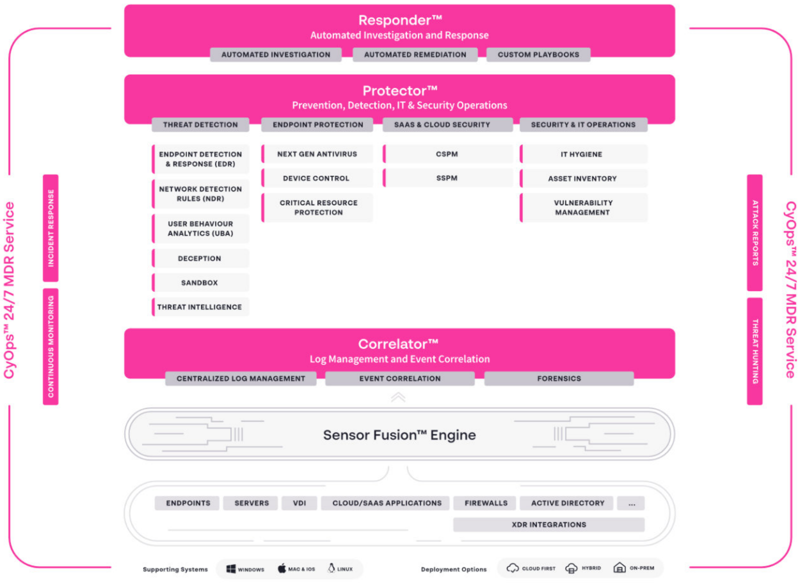
New way

Cynet 360 AutoXDR™

is a single solution that makes cybersecurity easy for small teams. You can stop trying to grow extra arms just to manage your security operations.

www.cynet.com

Cynet Automated Response Playbooks empowers security teams to reduce their alert investigation



Cynet launched Cynet Automated Response Playbooks. These playbooks automatically investigate and remediate security alerts as part of Cynet's 360 AutoXDR platform at no additional cost.

This is the industry's first XDR platform to include these capabilities without a hefty premium. This cost-effective approach is designed to help organizations maintain superior levels of security and relieve the pressure on overwhelmed security teams that must investigate an ongoing torrent of alerts, and then remediate discovered threats.

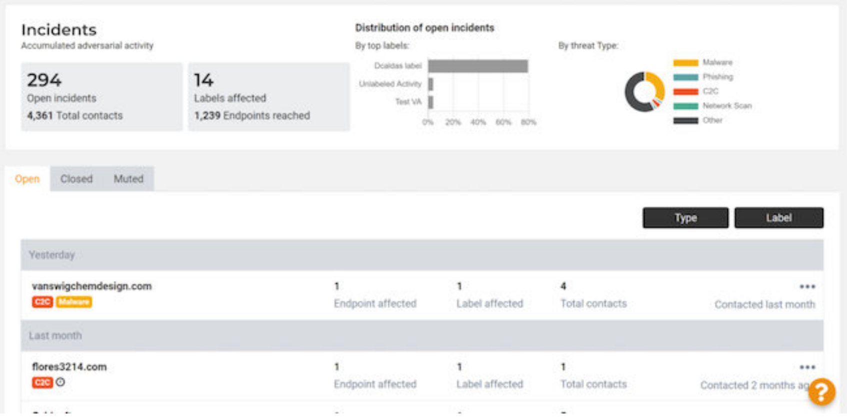
Cynet's Automated Response Playbooks automate manual tasks and workflows, empowering security teams to reduce their alert investigation and response times by 90%. In addition to freeing up valuable time for security teams, the playbooks provide a defined, consistent response process for more accurate security decisions and ensure that all alerts are properly addressed. Security teams can also take advantage of an intuitive drag-and-drop playbook builder to quickly and easily build custom playbooks for their organization.

"Most companies, especially those with smaller security teams, are overwhelmed with security alerts. Even though every significant alert should be fully investigated, the reality is that many security analysts don't have the time or skills to do this. The unfortunate result is that these burned-out analysts tend to ignore some alerts," said Eyal Gruner, CEO, Cynet.

Pindrop platform enhancements monitor fraudulent attempts to pass voice verification

Expanding the limits of voice technology, Pindrop has increased the level of intelligence derived from voice analysis to include demographic insights. Pindrop's contact center customers can now receive API-driven information like predicted age range and spoken language, to better route callers and improve authentication performance. These predictions can also allow for deeper intelligence on possible security threats from account takeover when used in combination with other tools and Pindrop's anti-fraud solution.

Lumu Incident View empowers security teams to prioritize incidents based on the progression of attacks


Incidents
Accumulated adversarial activity

294
Open incidents
4,361 Total contacts

14
Labels affected
1,239 Endpoints reached

Distribution of open incidents

Yesterday

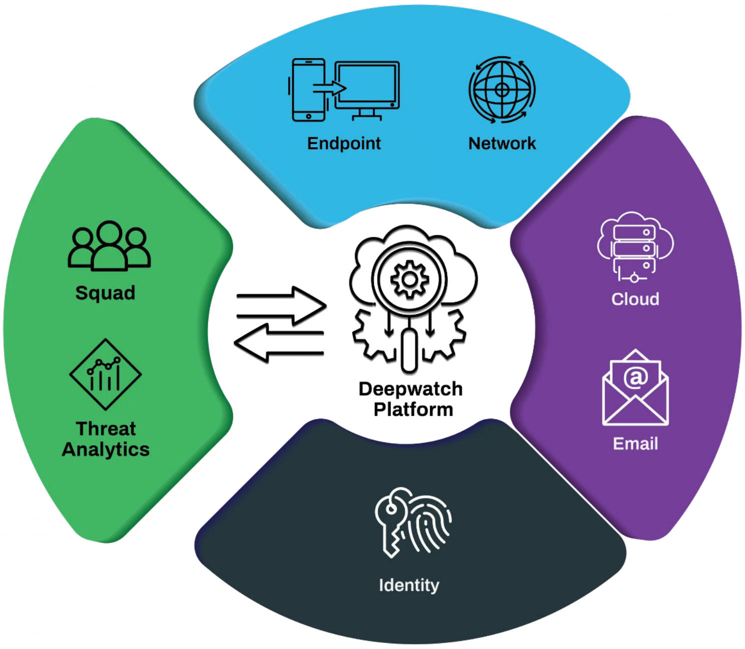
vanswigchemdesign.com C2C Malware — 1 Endpoint affected — 1 Label affected — 4 Total contacts — Contacted last month

Last month

flores3214.com C2C — 1 Endpoint affected — 1 Label affected — 1 Total contacts — Contacted 2 months ag

When it comes to early incident detection and response, operators receive alerts without much context, a problem that Lumu has been working to solve. Lumu's Incident View shows operators everything they need to know in one place for swift and precise response. Teams receive actionable information about who was impacted, when the incident took place and how best to respond before it escalates to a bigger problem. The Incidents View capability contains details about which actions were taken by other elements of a company's cybersecurity stack for better incident management.

Deepwatch launches MXDR service to improve threat detection for enterprises



Deepwatch MXDR significantly reduces the risk of business impacting security incidents by responding at machine speed, allowing analysts to do the rest in human time. Leveraging the Deepwatch SecOps platform to collect, process, and analyze security telemetry from data sources, Deepwatch produces the most comprehensive high-fidelity alerts.

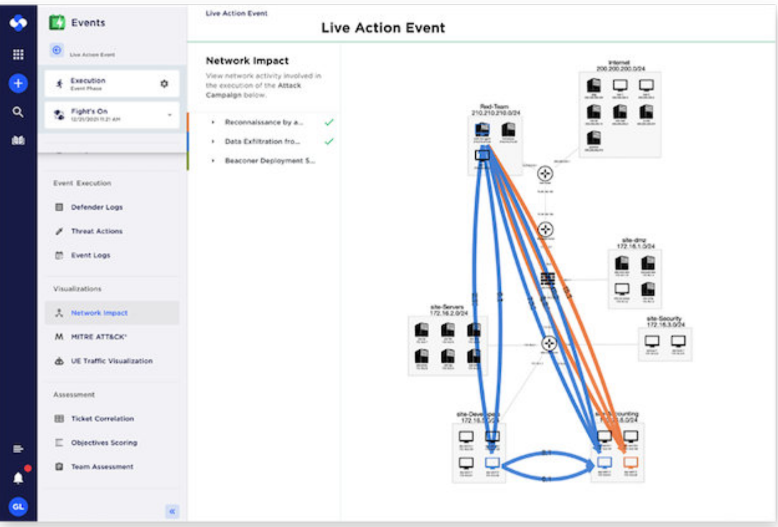
Deepwatch improves threat detection and reduces alert overload by correlating related threat activity for a single entity and escalating only the alerts that exceed the customer-defined risk threshold. Informed by Deepwatch's advanced detection capabilities, Deepwatch MXDR drives automated response actions that eliminate the lag time and dependence on security staff and cross-departmental resources.

IBM acquires Randori to strengthen its portfolio of AI-powered cybersecurity products and services

Randori helps clients continuously identify external facing assets, both on-premise or in the cloud, that are visible to attackers – and prioritize exposures which pose the greatest risk. This news further advances IBM's Hybrid Cloud strategy and strengthens its portfolio of AI-powered cybersecurity products and services.

Randori is IBM's fourth acquisition in 2022 as the company continues to bolster its hybrid cloud and AI skills and capabilities, including in cybersecurity. IBM has acquired more than 20 companies since Arvind Krishna became CEO in April 2020.

SimSpace platform enhancements help security teams validate their incident response operations



View network activity involved in the execution of the Attack Campaign below.

The new enhancements allow customers to deploy fully-customizable high-fidelity ranges with increased coverage for cloud services, critical infrastructure, and OT and IoT devices. SimSpace has further expanded its capabilities with a full battery of automated attacks, enhanced training content and emerging threat intelligence from SimSpace and leading partners, including Mandiant, Cymulate and others.

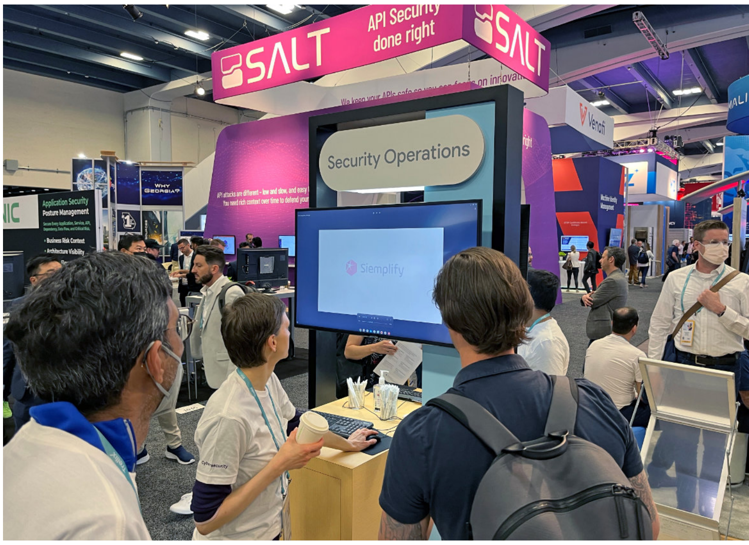
"CISOs are under increasing pressure to improve their security posture, reduce risk and optimize their security investments – all while facing the most challenging cyber staffing environment in modern history," said William Hutchison, CEO, SimSpace. *"It's essential for CISOs to build the confidence that their teams are prepared and well-trained to face cyber attacks. That's why we're proud to deliver an open platform that provides the live-fire exercises, team training and the necessary hands-on experience to validate their incident response playbooks against a variety of attack vectors: insider threats, known APTs and nation-state threat actors."*

#RSAC 2022 GALLERY

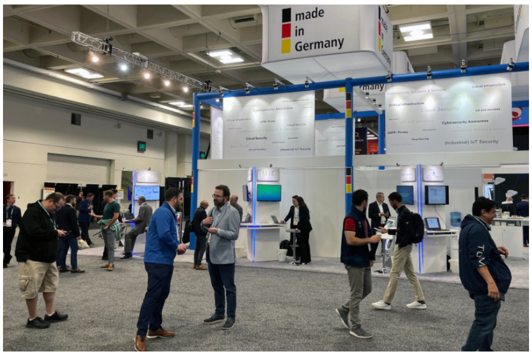
RSAC Sandbox
TRANSFORM
Spreading Application Security Ownership and Responsibility Across the Entire Organization

Acronis
Behavioral DLP & EDR
Joe Staley
treamline with complete yber protection
Security, Data Protection and Management
acronis.com

#RSAC 2022 GALLERY



GEORGE KURTZ & MIKE SENTONAS
THURS, JUNE 9
9:40 AM
A unified platform approach to stopping breaches



Intruder dwell time jumps 36%

Sophos released the Active Adversary Playbook 2022, detailing attacker behaviors that Sophos' Rapid Response team saw in the wild in 2021. The findings show a 36% increase in dwell time, with a median intruder dwell time of 15 days in 2021 versus 11 days in 2020.

The report also reveals the impact of ProxyShell vulnerabilities in Microsoft Exchange, which Sophos believes some Initial Access Brokers (IABs) leveraged to breach networks and then sell that access to other attackers.

"The world of cybercrime has become incredibly diverse and specialized. IABs have developed a cottage cybercrime industry by breaching a target, doing exploratory reconnaissance or installing a backdoor, and then selling the turn-key access to ransomware gangs for their own attacks," said John Shier, senior security advisor at Sophos.

"In this increasingly dynamic, specialty-based cyberthreat landscape, it can be hard for organizations to keep up with the ever-changing tools and approaches attackers use. It is vital that defenders understand what to look for at every stage of the attack chain, so they can detect and neutralize attacks as fast as possible."

The research also shows that intruder dwell time was longer in smaller organizations' environments. Attackers lingered for approximately 51 days in organizations with up to 250 employees, while they typically spent 20 days in organizations with 3,000 to 5,000 employees.

"Attackers consider larger organizations to be more valuable, so they are more motivated to get in, get what they want and get out. Smaller organizations have less perceived 'value,' so attackers can afford to lurk around the network in the background for a longer period. It's also possible these attackers were less experienced and needed more time to figure out what to do once they were inside the network. Lastly, smaller organizations typically have less visibility along the attack chain to detect and eject attackers, prolonging their presence," said Shier.

"With opportunities from unpatched ProxyLogon and ProxyShell vulnerabilities and the uprise of IABs, we're seeing more evidence of multiple attackers in a single target. If it's crowded within a network, attackers will want to move fast to beat out their competition."

Additional key findings:

The median attacker dwell time before detection was longer for "stealth" intrusions that had not unfolded into a major attack such as ransomware, and for smaller organizations and industry sectors with fewer IT security resources. The median dwell time for organizations hit by ransomware was 11 days. For those that had been breached, but not yet affected by a major attack, such as ransomware (23% of all the incidents investigated), the median dwell time was 34 days. Organizations in the education sector or with fewer than 500 employees also had longer dwell times.

Longer dwell times and open entry points leave organizations vulnerable to multiple attackers. Forensic evidence uncovered instances where multiple adversaries, including IABs, ransomware gangs, cryptominers, and occasionally even multiple ransomware operators, were targeting the same organization simultaneously.

Despite a drop in using Remote Desktop Protocol (RDP) for external access, attackers increased their use of the tool for internal lateral movement. In 2020, attackers used RDP for external activity in 32% of the cases analyzed, but this decreased to 13% in 2021. While this shift is a welcome change and suggests organizations have improved their management of external attack surfaces, attackers are still abusing RDP for internal lateral movement. Sophos found that attackers used RDP for internal lateral movement in 82% of cases in 2021, up from 69% in 2020.

Common tool combinations used in attacks provide a powerful warning signal of intruder activity. For example, the incident investigations found that in 2021 PowerShell and malicious non-PowerShell scripts were seen together in 64% of cases; PowerShell and Cobalt Strike combined in 56% of cases; and PowerShell and PsExec were found in 51% of cases. The detection of such correlations can serve as an early warning of an impending attack or confirm the presence of an active attack.

Fifty percent of ransomware incidents involved confirmed data exfiltration – and with the available data, the mean gap between data theft and the deployment of ransomware was 4.28 days. Seventy-three percent of incidents Sophos responded to in 2021 involved ransomware. Of these ransomware incidents, 50% also involved data exfiltration. Data exfiltration is often the last stage of the attack before the release of the ransomware, and the incident investigations revealed the mean gap between them was 4.28 days and the median was 1.84 days.

Conti was the most prolific ransomware group seen in 2021, accounting for 18% of incidents overall. REvil ransomware accounted for one in 10 incidents, while other prevalent ransomware families included DarkSide, the RaaS behind the notorious attack on Colonial Pipeline in the U.S. and Black KingDom, one of the "new" ransomware families to appear in March 2021 in the wake of the ProxyLogon vulnerability. There were 41 different ransomware adversaries identified across the 144 incidents included in the analysis. Of these, around 28 were new groups first reported during 2021. Eighteen ransomware groups seen in incidents in 2020 had disappeared from the list in 2021.

"The red flags that defenders should look out for include the detection of a legitimate tool, combination of tools, or activity in an unexpected place or at an uncommon time," said Shier.

"It is worth noting that there may also be times of little or no activity, but that doesn't mean an organization hasn't been breached. There are, for instance, likely to be many more ProxyLogon or ProxyShell breaches that are currently unknown, where web shells and backdoors have been implanted in targets for persistent access and are now sitting silently until that access is used or sold."

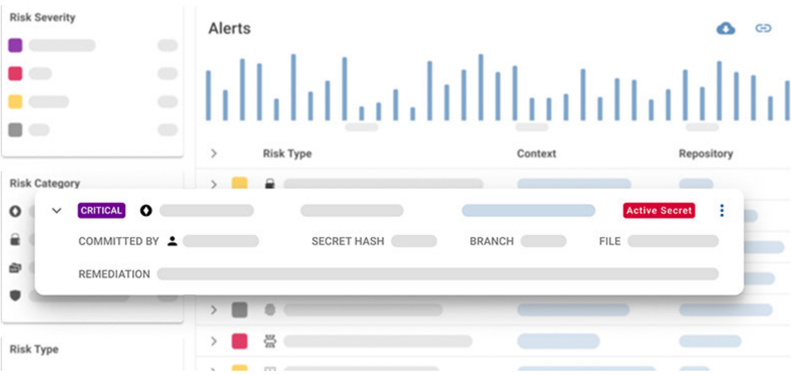
"Defenders need to be on the alert for any suspicious signals and investigate immediately. They need to patch critical bugs, especially those in widely used software, and, as a priority, harden the security of remote access services. Until exposed entry points are closed and everything that the attackers have done to establish and retain access is completely eradicated, just about anyone can walk in after them, and probably will."

Votiro collaborates with National Wildlife Federation to help remove pollution from the Great Lakes

Votiro announced a partnership with the National Wildlife Federation (NWF) during the 2022 RSA Conference.

"At Votiro, we understand the importance of protecting our digital and physical environments from harmful pollution. And, while we can provide a digital solution to the malware pollution of enterprises' data lakes, we know that more can be done to stop the pollution of our freshwater systems and restore the Great Lakes. That's why we're partnering with the National Wildlife Federation with the goal of raising funding and awareness for their protection efforts," said Ravi Srinivasan, CEO at Votiro.

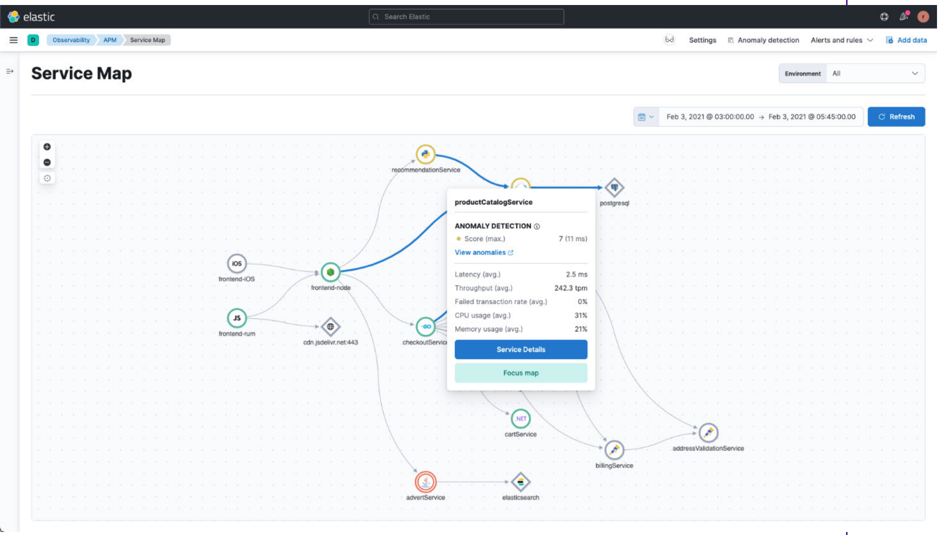
BluBracket enhances its code security solution to help enterprises protect software supply chains



BluBracket does what SAST, DAST, and dependency analysis cannot – it finds the secrets and PII that hackers are using to accelerate their attacks. Many of the existing application security solutions are unable to address certain risks that BluBracket can. Experts are referring to code developed internally, which most often resides in git repositories, as the internal software supply chain and calling this the new attack surface.

The BluBracket Code Security Platform is the first solution that consolidates and acts on security risks from both the internal and external software supply chain. BluBracket scans code to protect software supply chains by preventing, finding, and fixing risks in source code, developer environments, and pipelines. The BluBracket code security solution addresses top risks in code that include secrets in code, exposed PII, access risks, and code leaks.

Elastic Security for Cloud expands visibility and protection of cloud-native environments



productCatalogService

ANOMALY DETECTION

Score (max.) 7 (11 ms)

View anomalies

Latency (avg.)	2.5 ms
Throughput (avg.)	242.3 tpm
Failed transaction rate (avg.)	0%
CPU usage (avg.)	31%
Memory usage (avg.)	21%

Elastic Security for Cloud expands the capabilities of Elastic Security by bringing together the ability to enforce security posture for cloud-native and hybrid environments with infrastructure detection and response (IDR) to give customers deep visibility into cloud workloads and perform expert prevention, detection and response. Customers can monitor for deployment time risks and run-time threats in the unified Elastic Search Platform.

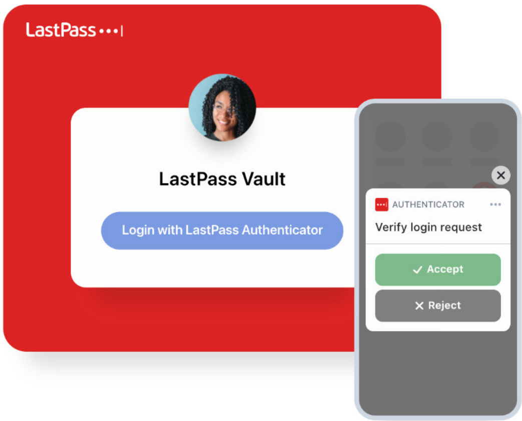
Elastic Security also delivers out-of-the-box rules and machine learning models to identify known and unknown threats with insights derived from Elastic Security Labs, the company's threat research, malware analysis, and detection engineering team.

LastPass allows customers to access their vault with a passwordless login

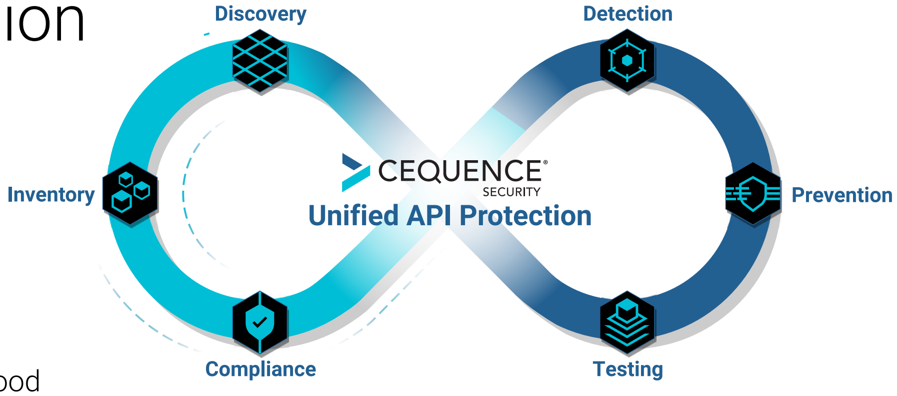
LastPass customers can now access their vault, and all sites stored in it, with a secure passwordless login using the LastPass Authenticator.

"On the heels of tech giants and identity providers unveiling their plans to enable passwordless across their operating systems, web browsers, devices and applications, LastPass is excited to be the first solution and only password manager to allow users to securely and effortlessly login, manage their account credentials and get instant access to the accounts used every day – without ever having to enter a password," said Chris Hoff, Chief Secure Technology Officer at LastPass.

"While broad implementation and adoption of passwordless is the industry's ultimate goal, it will likely take years before people experience an end-to-end passwordless login across all applications, but LastPass helps get you there sooner."



Cequence Security Unified API Protection enables security teams to protect their APIs



By stopping attacks without disrupting good traffic, security teams deploying the Cequence Unified API Protection solution enable their organizations to increase revenues, lower service delivery costs, and improve user experience across all their API-enabled applications. And they relieve the anxiety and costs of unknown risk because they eliminate previously unprotected and unmitigated API security and compliance exposures.

The Cequence Unified API Protection solution improves visibility and protection while reducing cost, minimizing fraud, business abuse, data losses, and non-compliance while creating attack futility, failure, and fatigue for even the most relentless of attackers.

Malwarebytes DNS Filtering helps IT and security teams block access to malicious websites

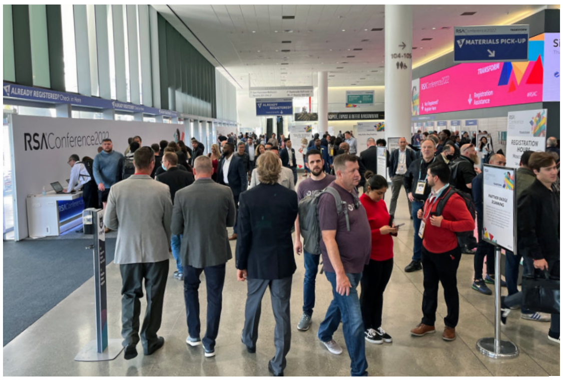
Malwarebytes DNS Filtering is powered by Cloudflare's zero trust platform to deliver a flexible and comprehensive zero trust solution for Nebula users. Malwarebytes DNS Filtering module for Nebula helps block access to malicious websites and limit threats introduced by suspicious content.

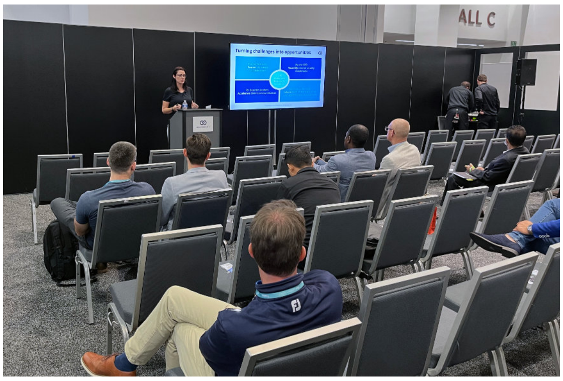
"It's challenging for organizations today to manage access to malicious sites and keep their end users safe and productive," said Mark Strassman, Chief Product Officer, Malwarebytes.

"Malwarebytes' DNS Filtering module extends our cloud-based security platform to web protection. After evaluating other Zero Trust providers it was clear to us that Cloudflare could offer the comprehensive solution IT and security teams need while providing lightning fast performance at the same time. Now, IT and security teams can block whole categories of sites, take advantage of an extensive database of pre-defined scores on known, suspicious web domains, protect core web-based applications and manage specific site restrictions, removing the headache from overseeing site access."

In addition to preventing access to sites that are known threats, the module provides IT and security teams with tools to manage exceptions and also encrypts domain name requests. The DNS Filtering module is powered by real-time protection capabilities, enabling the isolation and remediation of suspicious content once downloaded to prevent exposure.

#RSAC 2022 GALLERY

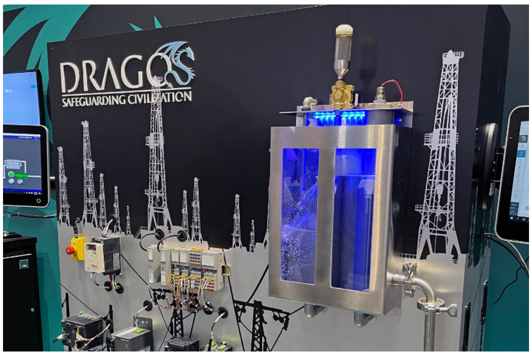




Checkmarx
Security Information and Event Management
VOTIRO
What's Polluting Your Data Lake?
Prevent inbound threats in your cloud...and beyond.
Visit us
votiro.com
Votiro Cloud API for...Anywhere
VOTIRO

#RSAC 2022 GALLERY

RSAConference2022
Moscone South
Registration • RSAC Early Stage Expo • RSAC Sandbox • Sessions • South Expo • South Expo Keynotes



How effective are public-private partnerships?

Ninety-three percent of cyber decision-makers say public-private partnerships are vital to national defense, but only 34 percent believe they are very effective, according to a study from MeriTalk and RSA Conference.

When asked to grade current efforts, cyber decision-makers give public-private partnerships "C's" for coordinating incident response, protecting critical infrastructure, and identifying systemic risk – one of the biggest threats they see to national and economic security.

The study – which surveyed 100 Federal and 100 private sector cybersecurity decision-makers – found that data privacy concerns and trust issues hold public-private partnerships back. Ninety-two percent of organizations are actively sharing information with partners, yet 43 percent of organizations feel it is more common for the private sector to share threat information with the government than the other way around. The study found 69 percent of cybersecurity decision-makers say there is reticence in their organization around cybersecurity information sharing.

Most agree a government-led partnership is the way forward, but there is little consensus on the best approach. The ideal ways for public and private organizations to work together to reduce cyber risk are – a government-led committee of private and public cybersecurity leaders (29 percent), government-issued directives for both public and private organizations (21 percent), a private organization-led committee of public and private cybersecurity leaders (20 percent), and both sectors working individually, only sharing information that is believed relevant (23 percent). Private sector decision-makers significantly prefer a government-led committee (35 percent to 22 percent), while public sector decision-makers significantly prefer for both sectors to work individually (30 percent to 15 percent).

"Improving communication and trust between the public and private sectors is key to reducing cybersecurity risks," said Nicole Burdette, principal, MeriTalk. *"From MeriTalk's perspective at the heart of government IT, it's gratifying to see cyber decision-makers say President Biden's Cybersecurity Executive Orderprompted their organization to review internal processes and rethink the way they collaborate with public and private sector partners."*

"It's encouraging that the data illustrates a general appreciation and respect for public-private partnerships and the role they play in reducing cyber risk. Given the increase in cyberattacks worldwide, it's critically important for public and private sectors to find common ground, create a sustainable blueprint, execute on sharing information across the ecosystem, and make these partnerships work," said Linda Gray Martin, VP, RSA Conference.

"With this research, RSA Conference 2022 next month, and ongoing conversations with information sharing groups, RSA Conference will continue to serve as a place for the exchange of ideas and sharing of information across both sectors."

Going forward, 95 percent say improved information sharing will provide critical insight in an interconnected world and 97 percent feel successful public-private partnerships are key to their organization's cyber resilience. The report recommends public and private sector cyber decision-makers mend the gap by:

- **Clarifying leadership and responsibilities** – starting with a unified strategy that bridges both sectors
- **Making information sharing a two-way street** – restructuring reporting procedures and appointing a single point of contact to streamline communication
- **Building trust** – solidifying data privacy expectations and considering mutual trust agreements to combat hesitancy
- **Thinking holistically** – modernizing legacy systems, adopting identity strategies, and implementing zero trust architectures to strengthen joint resilience

Cisco announces innovations for end-to-end security across hybrid multi-cloud environments

Cisco unveiled its plan for a global, cloud-delivered, integrated platform that secures and connects organizations. The company is designing the Cisco Security Cloud to be the industry's most open platform, protecting the integrity of the entire IT ecosystem – without public cloud lock-in.

"With the complexity of hybrid work, continued acceleration of cloud adoption, and the ever-advancing threat landscape, organizations are looking for a trusted partner to help them achieve security resilience. We believe Cisco is uniquely positioned due to its scale, breadth of solutions and cloud-neutral business model to meet their needs," said Jeetu Patel, Executive Vice President and General Manager of Security and Collaboration at Cisco. *"Cisco is already delivering upon key tenets of our cloud platform vision. We're excited to increase our innovation velocity to truly deliver on the vision of the Cisco Security Cloud."*

RedSeal Stratus allows organizations to monitor and secure their multi cloud environments

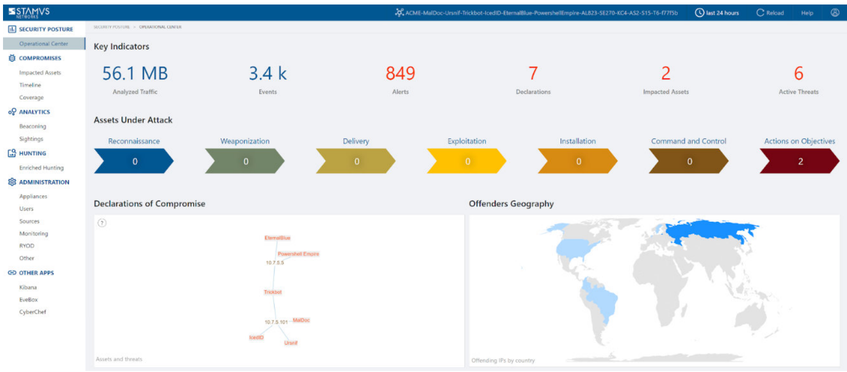
RedSeal Stratus, a Cloud Native Application Protection Platform (CNAPP) solution, gives security professionals a 'blueprint map' of their enterprise cloud to allow them to accurately identify where and how their business-critical resources are exposed to the Internet.

Stratus provides a singular view of an organizations cloud infrastructure, either Amazon AWS or Microsoft Azure or both, by creating a comprehensive visualization of connectivity within and between clouds using an agent-less API driven approach.

Stratus evaluates policies in cloud gateways, 3rd party firewalls, subnets (NACL policies) and instances (security group policies) with full attack path analysis to calculate unintended exposure and quickly begin remediation steps to prevent ransomware attacks and data breaches.

Bryan Barney, CEO at RedSeal, commented: *"Public cloud models do not have clear perimeters making it a very different reality compared to on-premise security. It has become a large and highly desirable attack surface for online criminals who will quickly exploit poorly secured cloud ports."*

Stamus Networks U38 provides earlier detection of cyber threats



Stamus Networks announced its latest software release, Update 38 (U38). The new release represents a significant enhancement to the company's flagship Stamus Security Platform (SSP), aimed at giving defenders earlier detection of cyber threats and clearly presenting the comprehensive evidence required to quickly resolve an incident.

"This new SSP release was inspired by our recent experiences in the last two NATO live-fire cyber exercises conducted by the Cooperative Cyber Defence Centre of Excellence (CCDCOE) and requests from our growing customer base," said Ken Gramley, CEO of Stamus Networks.

Onapsis' product updates strengthen business application security

Building on the momentum from the Assess Baseline launch, Onapsis is extending the reach of Onapsis Research Labs to the network layer to make it easier for cybersecurity teams to protect what matters most with a new Network Detection Rule Pack for Onapsis Defend and further enhancing support for SAP SuccessFactors, a cloud-based human capital management (HCM) solution, and the Onapsis SaaS platform.

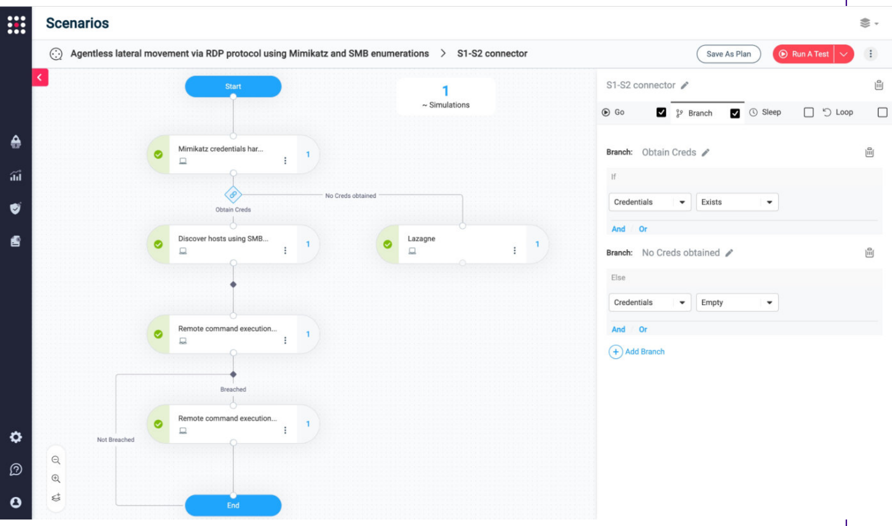
Onapsis' new product updates will deliver valuable, business-critical threat intelligence capabilities to an organization's existing network security solutions; increase support for cloud-based SAP SuccessFactors to better track user privileges, permissions, and suspicious behavior; and enhance its SaaS for Assess offering.

Forcepoint unveils new solutions to simplify connectivity and network security for enterprises

Forcepoint's 'Symphony' offers at-a-glance, interactive insights that help C-level and security professionals better leverage security investments to move the business forward. It enables users to quickly visualize and quantify financial value of security efficacy delivered by Forcepoint's products across key performance indicators such as adoption, data and threat protection, policy violations, performance, and risk.

The new Forcepoint FlexEdge Secure SD-WAN series integrates application-centric SD-WAN with the company's proven network security and threat protection technologies to simplify connectivity and network security for branch offices and remote sites of all sizes.

SafeBreach Studio enables security teams to automate and scale red-team exercises


Scenarios
Start
1
~ Simulations
Mimikatz credentials har...
Obtain Creds
No Creds obtained
Discover hosts using SMB...
Lazagne
Remote command execution...
Breached
Not Breached
Remote command execution...
End

Agentless lateral movement via RDP protocol using Mimikatz and SMB enumerations > S1-S2 connector

Save As Plan | Run A Test

S1-S2 connector

○ Go ☑ | Branch ☑ | Sleep □ | Loop □

Branch: Obtain Creds

If
Credentials | Exists
And Or

Branch: No Creds obtained

Else
Credentials | Empty
And Or

Add Branch

SafeBreach Studio is a no-code red-team automation platform security teams of all skill levels can use to create, customize and execute sophisticated attack scenarios that replicate real-world adversary behavior.

The new offering enables security teams to easily automate and scale red-team exercises across the enterprise without the need for specialized expertise to enhance efficiency and reduce implementation costs.

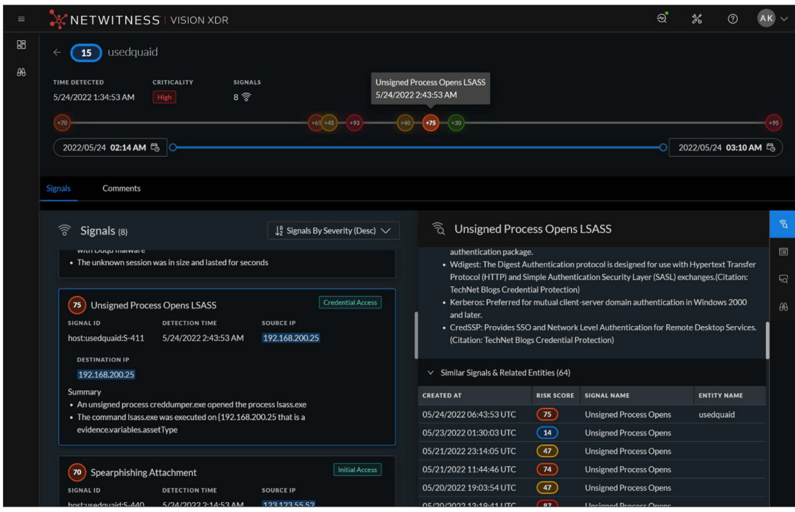
"Red and purple team exercises can be resource intensive, expensive and difficult to operationalize," said SafeBreach CTO and Co-Founder Itzik Kotler. *"With SafeBreach Studio, our customers can consistently design attack workflows that replicate real-world behavior with no additional cost and have the freedom to easily scale attacks and change the exercise scope without any constraints."*

NetWitness XDR helps analysts detect known and unknown attacks

NetWitness announced NetWitness XDR, a family of products and capabilities delivering comprehensive detection and response on premise, in the cloud or as a hybrid of the two. This new offering and product architecture delivers the full range of deployment options enterprises seek today to meet their unique cybersecurity needs and use cases.

NetWitness XDR delivers a robust set of capabilities enabling extended detection and response (XDR) and helping customers stay ahead of the most sophisticated cyber threats.

"NetWitness has enjoyed the trust of some of the world's most security sensitive organizations because of its unique ability to monitor the entire attack surface across the network, endpoint, cloud, IoT, logs and more," said CEO of RSA and NetWitness, Rohit Ghai. *"We have been delivering XDR capability to the market for several years and today we are delighted to announce new innovations in the platform and reintroduce it to the market as NetWitness XDR."*



15 usedquaid

TIME DETECTED 5/24/2022 1:34:53 AM | CRITICALITY High | SIGNALS 8

Unsigned Process Opens LSASS
5/24/2022 2:43:53 AM

2022/05/24 02:14 AM — 2022/05/24 03:10 AM

Signals (8) | Signals By Severity (Desc)

with Duqu malware
- The unknown session was in size and lasted for seconds

75 Unsigned Process Opens LSASS | Credential Access

SIGNAL ID host:usedquaid:S-411 | DETECTION TIME 5/24/2022 2:43:53 AM | SOURCE IP 192.168.200.25

DESTINATION IP 192.168.200.25

Summary
- An unsigned process creddumper.exe opened the process lsass.exe
- The command lsass.exe was executed on {192.168.200.25 that is a evidence.variables.assetType

70 Spearphishing Attachment | Initial Access

SIGNAL ID host:usedquaid:S-440 | DETECTION TIME 5/24/2022 2:14:53 AM | SOURCE IP 123.123.55.52

Unsigned Process Opens LSASS

authentication package.
- Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.(Citation: TechNet Blogs Credential Protection)
- Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
- CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services. (Citation: TechNet Blogs Credential Protection)

Similar Signals & Related Entities (64)

CREATED AT	RISK SCORE	SIGNAL NAME	ENTITY NAME
05/24/2022 06:43:53 UTC	75	Unsigned Process Opens	usedquaid
05/23/2022 01:30:03 UTC	14	Unsigned Process Opens	
05/21/2022 23:14:05 UTC	47	Unsigned Process Opens	
05/21/2022 11:44:46 UTC	74	Unsigned Process Opens	
05/20/2022 19:03:54 UTC	47	Unsigned Process Opens	
05/20/2022 13:19:41 UTC	87	Unsigned Process Opens	

HackerOne OpenASM enables customers to leverage scan data from multiple vendors

HackerOne announced OpenASM, an initiative that combines scan data from customers' attack surface management (ASM) tools with security testing efforts.

Attack surface scans can be used to better set scopes for bug bounties, penetration tests, and vulnerability disclosure programs. In addition, ethical hackers can enrich, risk rank, and prioritize assets, helping organizations reduce risk more effectively.

OpenASM will initially support AssetNote, Darktrace (Cybersprint), Hadrian, Palo Alto Cortex Xpanse, and Project Discovery. OpenASM will also support CSV and JSON import for customers with homegrown attack surface inventory tools. Additionally, HackerOne is working with its partner, SecurityScorecard, on how to deal with the extended supply chain attack surface.

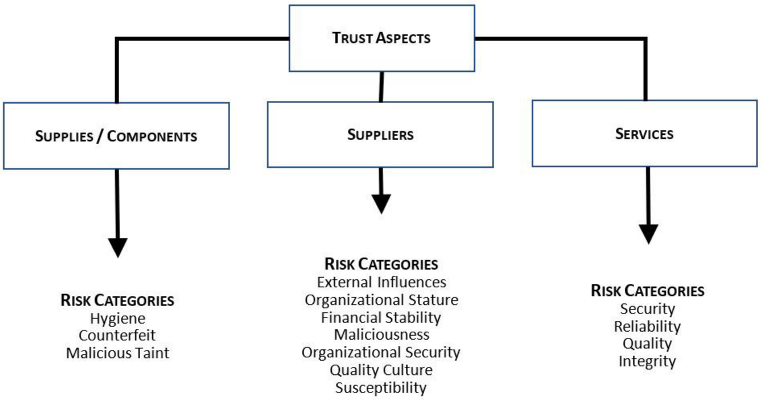
Qrypt collaborates with Vaultree to offer encrypted data processing technology for customers

Qrypt announced a new integration of its Secure Proxy solution with Vaultree's fully encrypted data processing technology.

This partnership incorporates Qrypt's unique key generation with a one-time pad proxy tunnel, to deliver everlasting key and data security in Vaultree's SDK. The partnership makes fast, future secure data processing in a cloud-first world possible.

The Qrypt solution generates identical symmetric keys at multiple endpoints without any distribution of the keys themselves over an insecure channel. Combined with one-time pads and a secure proxy tunnel, the Qrypt and Vaultree integration makes this OTP-protected data everlasting secure – mathematically proven safe against all known attacks, including future quantum computers.

MITRE System of Trust identifies and quantifies supply chain security risks

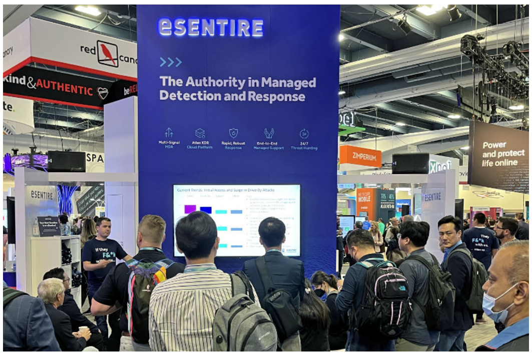


MITRE unveild its new "System of Trust," a framework to provide a comprehensive, community-driven, knowledge base of supply chain security risks and a customizable, security-risk assessment process for use by any organization within the supply chain ecosystem.

For the first time, there's a free and open platform that will help companies identify, discuss, and quantify the risks in major supply chains and with suppliers—including the security concerns posed by software.

#RSAC 2022 GALLERY

CIS Center for Internet Security
Creating Confidence in the Connected World



#RSAC 2022 GALLERY