ISSUE 83 | APRIL 2024

WWW.TAHAWULTECH.COM

ADVISOR

MIDDLE EAST

RESILGERE

Secur2

FADY RICHMANY, REGIONAL VICE PRESIDENT, EMERGING MARKETS, COMMVAULT, TELLS ANITA JOSEPH IN A CANDID CHAT, ALL ABOUT CYBER RESILIENCE AND HOW THE COMPANY IS FOCUSED ON ENHANCING THE CYBER RESILIENCE OF COMPANIES BY PROVIDING THEM WITH OPTIONS THAT SUIT THEIR SPECIFIC BUSINESS MODEL.





OPSWAT.

Protecting the Pulse of Industry 4.0

Discover how OPSWAT is driving CIP (critical infrastructure protection) cybersecurity forward at GISEC. Dive into a world of innovation and learn how OPSWAT is protecting IT, OT, and everything in between to help create a better, more secure, and safely interconnected future.



Join us at Hall 7 – Stand C38 to experience the OPSWAT MetaDefender Platform.



Can't make it to the booth? No problem.

Contact us: Sales-inquiry@opswat.com Scan the QR code and learn more about our solutions to get started today.

CONTENTS







BUILDING CYBER RESILIENCE

News from the world of security and beyond.

6

22 Ned Baltagi, Managing Director – Middle East, Turkey and Africa at SANS Institute on the palpable enthusiasm for embracing Al in cybersecurity and the need for comprehensive, continuous professional education, to implement it effectively. **38** Finesse spokespersons-Eljo J P, Chief Business Officer & Director and Yogendar Kumar, Head of Information Security, on the company's comprehensive approach to IT & OT security.

40 Rick Vanover - Senior Director Product Strategy at Veeam, on how IT teams need to be more technically agile and make the most of reorganizing their cloud environments.



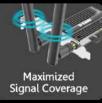
LIGHTNING-SPEED CONNECTIVITY

Desktop Use | Intel Chip | Bluetooth 5.2

The D-Link DWA-X586E is a PCIe network card for desktops, compatible with Wi-Fi6E. It offers speeds up to 574Mbps (2.4GHz), 2400Mbps (5GHz), and 6GHz. With Bluetooth 5.2 support, it ensures stable connections for gaming, streaming, and VoIP. Equipped with dual high-gain antennas for extended range.













Bluetooth 5.2 Compatible







EDITOR'S NOTE



Talk to us: E-mail: anita.ioseph@ cpimediagroup.com

> Anita Joseph Editor

EVENTS



GISEC 2024-SETTING **NEW STANDARDS**

FOSTERING INNOVATION AND

THOUGHT LEADERSHIP.

et against the backdrop of escalating cyber threats and evolving technological landscapes, GISEC 2024 stands as a beacon for collaboration innovation, and fortification in the face of unprecedented challenges.

For security companies in the region. participation in GISEC is not merely about showcasing products and services; it's about contributing to a collective endeavor to elevate security standards. With cyber threats becoming increasingly sophisticated and pervasive, the need for proactive

been more urgent. GISEC serves as a platform for stakeholders to converge,

measures has never

exchange insights, and forge alliances that are instrumental in fortifying our digital ecosystems.

From refining cutting-edge technologies to unveiling groundbreaking solutions, each participant is primed to demonstrate their commitment to safeguarding digital infrastructures. Whether it's advancements in Al-driven threat detection, robust encryption protocols, or comprehensive cybersecurity frameworks, GISEC 2024 will be a testament to the industry's resilience and ingenuity.

leadership. Through keynote speeches, panel discussions, and interactive workshops. attendees will gain invaluable insights into emerging threats, evolving regulatory landscapes, and best practices for mitigating risks. By harnessing collective expertise and harnessing the power of collaboration, GISEC 2024 promises to chart the course for a more secure digital future.

Moreover, the event serves as a crucible

for fostering innovation and thought

Beyond the technological showcase, GISEC 2024 embodies a spirit of inclusivity

> and diversity. It provides a platform for startups, SMEs, and industry veterans alike

to converge, network, and chart the path forward. By nurturing a culture of inclusivity, GISEC fosters an environment where ideas flourish, partnerships thrive, and innovation knows no bounds.

As security companies gear up to showcase their prowess, they reaffirm their commitment to safeguarding our digital frontiers. By leveraging the collective wisdom and ingenuity of stakeholders, GISEC 2024 is poised to set new benchmarks for excellence in security innovation and resilience.

Published by

FOUNDER, CPI ominic De Sousa (1959-2015)

ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com

EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.com

Online Editor

Daniel Shepherd

PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@cpimediagroup.com

Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAF

Tel: +971 4 5682993

© Copyright 2024 CPI All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

Publishing Director

Natasha Pendleton daniel.shepherd@cpimediagroup.com natasha.pendleton@cpimediagroup.com

Sales Directo Sabita Miranda sabita.miranda@cpimediagroup.com

CLOUDFLARE ENTERS OBSERVABILITY MARKET WITH ACQUISITION TO ENHANCE SERVERLESS PERFORMANCE

Cloudflare, Inc, the leading connectivity

cloud company, announced an entrance into the observability market with the acquisition of Baselime, the cloud-native observability platform. By integrating Baselime's technology with Cloudflare's developer platform, Cloudflare will be uniquely positioned to bring deep knowledge of serverless platforms and developer experience together to solve the challenges of observability for serverless apps.

Today, entire applications are built on serverless architectures, from compute to databases, storage, queues, and more. Still, observability is often regarded as one of the weaknesses of serverless architectures — trading off visibility into the application's behavior for scalable infrastructure that doesn't need to be managed. Building and debugging production applications requires the ability to understand trends and patterns, identify performance bottlenecks, and isolate errors to ensure ongoing reliability, scalability, and security. Having access to this level of visibility, preferably all within one platform, is a critical factor developers consider when choosing a platform on which to build.

"Two million developers building on Cloudflare trust us to help scale their apps globally, but can still struggle to understand the behavior of their cloud



applications," said Matthew Prince, cofounder and CEO, Cloudflare. "We believe that to be the leading developer platform, having the best observability tools built in is going to be table-stakes. Baselime has raised the standard for serverless observability and we can further unlock those insights for every developer building on our platform."

POSITIVE TECHNOLOGIES DETECTS A SERIES OF CYBERATTACKS AGAINST GOVERNMENT ORGANIZATIONS IN RUSSIA AND THE CIS

Positive Technologies Expert Security

Center (PT ESC) discovered a new cybergroup called Lazy Koala. Experts confirm that the criminals use simple but effective attack techniques. Victims of the group include organizations from Russia and six CIS countries, with approximately 867 employee accounts compromised to date.

As part of the threat research, PT ESC specialists discovered a series of attacks aimed at organizations in Russia, Belarus, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, and Armenia. Government and financial organizations, as well as medical and educational institutions, were the main targets. Positive Technologies specialists notified affected organizations that they were compromised.

Research shows that the attackers' main goal was to steal accounts to



various services from government organization employee computers. The next step was likely use this information in further attacks on the internal structures of the organizations. Stolen data can also be sold on the dark web cyber services market.

Behind the attacks is a previously

unknown group that experts have dubbed Lazy Koala because of its basic techniques and the username. Koala of the person managing the Telegram bots with stolen data. Researchers were unable to establish connections with already known groups using the same techniques.

GOOGLE CLOUD APPOINTS NOOR AL-SULAITI TO LEAD CYBERSECURITY BUSINESS DEVELOPMENT AND GOVERNMENT RELATIONS FOR MIDDLE EAST, TURKEY, AND AFRICA

Google Cloud has announced the

appointment of Noor Al-Sulaiti as Head of Security Business Development and Government Relations for the Middle East, Turkey, and Africa region (META). Noor, an industry veteran known for her innovative leadership, brings a wealth of experience in the telecommunications and technology sectors to her new role.

Noor's appointment is yet another testament to the company's commitment to the region and safeguarding governments' digital assets. In this position, Noor will be responsible for Google's security expansion in the Middle East, Turkey and Africa underscoring the growing importance of cybersecurity for the company. She will foster strategic partnerships with the public sector to leverage Google Cloud's cutting-edge cybersecurity solutions, including Cybershield, a powerful cybersecurity solution tailored specifically for



governments and inspired by the concept that organizations inside a nation and around the world need to "lock shields" and stand united in their defense against shared attackers.

Noor's distinguished career includes her role as CEO of Ooredoo Oman. There, she established herself as the youngest and first female CEO in the company's history, spearheading a transformation into a digitally led, data-powered, and customer-centric organization. Prior to joining Ooredoo Oman, Noor was the CEO of Starlink, a retail chain and IT service provider in Qatar. She was also the general manager of Phono and FASTtelco in Kuwait. She has been recognized as one of the most powerful businesswomen by Forbes Middle East and as a notable business leader by other prominent publications.

Noor Al-Sulaiti said: "I am honored to join Google Cloud, a company that has inspired me throughout my career. Google Cloud is continuously helping governments around the world enhance their security capabilities and respond holistically at the national level to keep their citizens and critical assets safe, and I'm ready to lead the charge to bring these capabilities to the Middle East, Turkey and Africa."

PROOFPOINT UNLEASHES THE POWER OF BEHAVIORAL AI TO THWART DATA LOSS OVER EMAIL

Proofpoint, Inc., a leading cybersecurity

and compliance company, has announced the general availability of Adaptive Email Data Loss Prevention (DLP) to automatically detect and prevent accidental and intentional data loss over email before it becomes a costly mistake for organizations. Combining Proofpoint's industry-leading threat and data loss protection technology and intelligence with Tessian's AI-powered behavioral and dynamic detection provides organizations with the most comprehensive defense available against human layer risks.

Data loss over email is a widespread yet preventable problem; 75% of IT professionals in the UAE attribute the main cause of data loss at their organization to careless employees, attaching the wrong files in an email, emailing sensitive data to a personal account, or sending emails to the wrong recipient. In fact, misdirected email is one of the simplest and most significant sources of data loss – about one-third of employees send emails to the wrong recipient each year. A misdirected email containing employee or customer data can potentially trigger a significant fine under privacy frameworks like CCPA and GDPR.

"Data doesn't lose itself – people lose it, careless employees mishandle it, malicious users walk out the door with it, and compromised accounts are hijacked



to steal it," said Ryan Kalember, chief strategy officer at Proofpoint. "Rulesbased DLP systems are a critical part of every company's security program, but they can only catch pre-defined risks, making them blind to many data loss incidents. Adaptive Email DLP takes a behavioral AI-based approach to catch what rules-based DLP systems miss and help organizations reduce human risk."

SOPHOS PARTNERS WITH TENABLE TO LAUNCH NEW SOPHOS MANAGED RISK SERVICE

Sophos, a global leader of innovative

security solutions that defeat cyberattacks, has announced a strategic partnership with Tenable®, the Exposure Management company, to provide Sophos Managed Risk, a worldwide vulnerability and attack surface management service. The new service features a dedicated Sophos team that leverages Tenable's exposure management technology and collaborates with the security operations experts from Sophos Managed Detection and Response (MDR) to provide attack surface visibility, continuous risk monitoring, vulnerability prioritization, investigation, and proactive notification designed to prevent cyberattacks.

The modern attack surface has expanded beyond traditional on-premises IT boundaries, with organizations operating frequently unknown numbers of external and internet-facing assets that are unpatched or under protected, leaving them vulnerable to cyberattackers. This is evident in the newest Sophos Active Adversary Report, which identifies three tasks that organizations must prioritize to minimize the risk of brazen intrusions that lead to ransomware or other types of attacks. These include closing exposed Remote Desktop Protocol (RDP) access, enabling multi-factor authorization and patching vulnerable servers, all of which were top entry points in breaches handled by Sophos Incident Response in 2023. The Sophos Managed Risk service can assess an organization's external attack surface, prioritize the riskiest exposures, such as open RDP, and provide tailored remediation guidance to help eliminate blind spots and stay ahead of potentially devastating attacks.

"Sophos and Tenable are two industry security leaders coming together to address urgent, pervasive security challenges that organizations continuously struggle to control. We can now help organizations identify and prioritize the remediation of vulnerabilities in external assets, devices and software that are often overlooked. It is critical that organizations



manage these exposure risks, because unattended, they only lead to more costly and time-consuming issues and are often the root causes of significant breaches," said Rob Harrison, senior vice president for endpoint and security operations product management at Sophos. "We know from Sophos' worldwide survey data that 32% of ransomware attacks start with an unpatched vulnerability and that these attacks are the most expensive to remediate. The ideal security layers to prevent these issues include an active approach to improving security postures by minimizing the chances of a breach with Sophos Managed Risk, Sophos Endpoint, and 24x7 Sophos MDR coverage."

CONFLUENT ANNOUNCES GENERAL AVAILABILITY OF CONFLUENT CLOUD FOR APACHE FLINK, SIMPLIFYING STREAM PROCESSING TO POWER NEXT-GEN APPS

Confluent, Inc, the data streaming

pioneer, announced the general availability of Confluent Cloud for Apache Flink®, a fully managed service for Apache Flink® that enables customers to process data in real time and create high-quality, reusable data streams. Confluent Cloud for Apache Flink® is available across Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. Backed by Confluent's 99.99% uptime SLA, Confluent's cloudnative service for Flink enables reliable, serverless stream processing.

As the de facto stream processing standard, Flink is relied upon by innovative



companies like Airbnb, Uber, Netflix, and Stripe to support mission-critical streaming workloads. As a leading cloudnative, serverless Flink offering, Confluent Cloud for Apache Flink® enables customers to easily build high-quality, reusable data streams to power all of their real-time applications and analytics needs.

"Stream processing allows organizations to transform raw streams of data into powerful insights," said Shaun Clowes, chief product officer at Confluent. "Flink's high performance, low latency, and strong community make it the best choice for developers to use for stream processing. With Kafka and Flink fully integrated in a unified platform, Confluent removes the technical barriers and provides the necessary tools so organizations can focus on innovating instead of infrastructure management."



23-25 APR 2024 DUBAI WORLD TRADE CENTRE

THE SUPER CONNECTOR EVENT FOR

9,156 5 6 34

367137 71,73524

CYBERSECURITY COMMUNITY

EMPOWER THE CYBER-SECURED FUTURE

8143670502 7949370 48850259 57950876

#45824702**884**703692

Enquire about Exhibiting, Sponsorship, **Speaking Opportunities & more!**

gisec@dwtc.com | tel: +971 4 308 6469



SCAN HERE

#gisecglobal | gisec.ae

HOSTED BY

TUTTUT





مركز كالخث للأمز لألكتروني

LECTRONIC SECURITY O

















LinkShadow is positioned as a Representative Vendor in the 2024 Gartner[®] Market Guide for Network Detection and Response(NDR)

Gartner

LINKSHADOW POSITIONED AS A REPRESENTATIVE VENDOR IN THE 2024 GARTNER MARKET GUIDE FOR NDR

inkShadow, a global leader in intelligent Network Detection and Response (NDR) has been recognized in the Gartner 2024 Market Guide for NDR solution. This insightful Gartner Report elaborates on how NDR can amplify infrastructure security by seamlessly integrating with various technologies such as SOAR, SIEM, EDR, MDR and numerous others.

As per Gartner, "The network detection and response market continues to grow

and expand to hybrid network scenarios with IaaS deployment. Security and risk management leaders should reprioritize NDR as a key provider of AI analytics in the context of more automated security operations assistants."

Gartner also recommends that "Enterprises should strongly consider NDR solutions to complement signaturebased network security tools and network sandboxes. Many Gartner clients have reported that NDR tools have detected suspicious network traffic that other perimeter security tools had missed."

Commenting on this Fadi Sharaf, Regional Sales Director, LinkShadow said "We believe this Gartner recognition strengthens LinkShadow's positioning in the NDR domain. Our aim is to extend the robust LinkShadow NDR capability to enterprises and empower them to stay ahead of the threat curve, taking a proactive approach to safeguard their sensitive assets."

According to Gartner "Despite strong competition from other platforms, NDR



global market revenue continues to grow double digit, registering an increase of 19% for the period 1Q23 through 3Q23, year over year. When the NDR market was nascent, it was composed of a mix of pure-play startups and network monitoring companies expanding to security use cases. As the market grows, it is attracting more and more large platform providers."

Gartner Key Findings:

 Network detection and response (NDR) is commonly used as a complementary detection and response technology as part of a broader arsenal of security operations center (SOC) tools.

- The emergence of "AI-augmented" analytics overlays, in the form of SOC assistants, will benefit the NDR market as a useful source of insights for aggregated and summarized views.
- A handful of NDR vendors capture most of the attention in the market. Higher maturity organizations, often with more specialized detection use cases, often mix these well-known vendors with emerging local players in their shortlists.
- Most organizations value the response capabilities during their NDR provide evaluations, but only

ENTERPRISES SHOULD STRONGLY CONSIDER NDR SOLUTIONS TO COMPLEMENT SIGNATURE-BASED → NETWORK SECURITY TOOLS AND NETWORK SANDBOXES.

deploy very narrowly automated responses past the pilot phase.

Gartner Recommendations:

- Start small. Implement NDR to detect abnormal behaviors and provide investigation capabilities for post breach activity, extending incrementally across different types of networks.
- Identify how NDR's behaviorbased detections, once tuned, might augment your SOCability to respond to incidents faster and more accurately.
- Compare NDR vendors by defining rationalized metrics and evaluating how these NDR tools positively impact threat detection and incident response.
- Roll out automated response progressively, based on your existing incident response SLA for the type of incident and on the false positive rate of the detection engines.

WHILE AI OFFERS GREAT POSSIBILITIES FOR SECURITY, IT'S IMPORTANT TO UNDERSTAND THAT IT WON'T REPLACE HUMAN OVERSIGHT AND DECISION-MAKING ENTIRELY.

BALANCING TECHNOLOGY AND ETHICS

DR. ROB ROWE, VP, DATA SCIENCE, HID, TELLS SECURITY ADVISOR MIDDLE EAST ABOUT THE IMPORTANCE OF BEING METICULOUS ABOUT DATA SOURCING, ENSURING CLEAR AND DEFINED PURPOSES FOR DATA COLLECTION AND MAINTAINING TRANSPARENCY WITH DATA SUBJECTS.

ow has the rise of artificial intelligence impacted traditional security measures ? There are many

advantages and challenges with AI, but the analytic capabilities of AI should be seen as the low-hanging fruit to enhance identity management. Identity analytics has the potential to utilize AI to pore over data from a wide range of sources to rapidly bring to light trends and patterns as well as anomalies not visible to the human eye.

Promising use cases include embedding advanced AI machinelearning capabilities into products and offerings or applying AI analytics to identify gaps in internal business processes—whether it's to optimize performance in applications such as customer service, technical support, etc., or to help detect issues before they become costly problems.

How can AI be utilized to enhance cybersecurity defenses against evolving threats?

Perhaps the most visible application of AI is biometrics, which uses machine learning to identify individuals through facial recognition, fingerprint analysis, and spoof detection. Sophisticated algorithms are crucial for these tasks.

A more sophisticated biometrics approach is in behavioral modeling, which leverages machine learning to identify and analyze behavioral and transaction patterns, enabling proactive detection of anomalies and potential threats. So, machine learning plays a crucial role in this, allowing the security system to learn and adapt to individual baselines.

How can organizations ensure the transparency and accountability of AI algorithms used for security purposes?

Al relies on vast amounts of data, and data presents a significant challenge: bias. When data inherits biases, specific conclusions and outcomes in security systems can be skewed, opening the doors for malicious actors to exploit these biases and bypass security measures. In that sense, Al outputs should be used a guide, not a definitive result.

Beyond addressing data bias, robust and ethical data governance practices are essential. This means being meticulous about data sourcing, ensuring clear and defined purposes for data collection, and maintaining transparency with data subjects.

In what ways can AI contribute to proactive threat detection and prevention strategies?

For example, embedding AI and machine learning directly on edge devices (devices that are located closer to where the data is collected such as a security camera with facial recognition capabilities at airport gates) facilitates real-time anomaly detection and a more efficient response to threats. This shift from reactive to proactive security represents a significant advancement in the field. Many in the security arena already are heading this way, according a recent survey HID conducted with 2,600 end users and industry partners (installers, integrators, and original equipment manufacturers) from across the globe: in addition to analytics, 11% said they are using AI-enabled RFID devices, 15% are using AI-enabled biometrics, and 18% have AI supporting their physical security solutions.

What are the implications of Aldriven autonomous security systems for human oversight and decisionmaking?

While AI offers great possibilities for security, it's important to understand that it won't replace human oversight and decision-making entirely. Security is a complex field, and responsible deployment of AI in this context requires a pragmatic approach. This means AI won't eliminate people and jobs. Instead, it will act as a powerful tool to help people be more productive, reduce errors and help them identify risks before they occur. So, for tasks requiring human judgment, interaction, or a higher ROI, traditional security practices will remain in place. 1

BUILDING CYBER RESILIENCE

FADY RICHMANY, REGIONAL VICE PRESIDENT, EMERGING MARKETS, COMMVAULT, TELLS ANITA JOSEPH IN A CANDID CHAT, ALL ABOUT CYBER RESILIENCE AND HOW THE COMPANY IS FOCUSED ON ENHANCING THE CYBER RESILIENCE OF COMPANIES BY PROVIDING THEM WITH OPTIONS THAT SUIT THEIR SPECIFIC BUSINESS MODEL.

hy is cyber resilience important today? A robust cyber resilience strategy is imperative for ensuring business continuity. Its significance transcends merely fortifying an enterprise's security framework and mitigating risks to its critical infrastructure. Indeed, cyber resilience serves as a defensive wall against financial losses and reputational damage.

Cyber resilience is crucial for safeguarding a company's continuity, financial stability, and reputation. Recent studies, like the one by IDC commissioned by Commvault, reveal that 61% of organizations see data loss due to cyber threats as increasingly likely within a year. Cyber resilience is about preparedness—not if, but when attacks occur, and how often.

Furthermore, the adoption of a well-crafted cyber resilience strategy by businesses fosters heightened trust among clients and customers in their day-to-day operations. This, in turn, bolsters an organisations' competitive edge by facilitating streamlined and effective performance, ensuring that operations run smoothly even under threat.

How and why has Commvault shifted its focus to cyber resilience this year?

For over 30 years, Commvault has led with innovative solutions for safeguarding and recovering customer data. Now, recognizing the evolving cyber threats, we've deepened our focus on cyber resilience. As such, Commvault simplifies data protection, cyber recovery and cyber resilience – in one cloud platform – while striving to make the world a better place for everyone. Throughout our long rich history, we have developed more than 1,400 patents, which help more than 100,000 companies and organizations with their data security & recovery.

Over the past year specifically, Commvault has focused on enhancing the cyber resilience of companies by providing them with options that suit their business models, such as Commvault Cloud, powered by Metallic® AI, a cyber-resilience platform built for the hybrid enterprise. This solution delivers the protection that any company needs in a single platform to eliminate security





gaps. The platform uses Metallic AI to power early warning, threat detection, incident readiness, rapid response and cyber recovery – offering the speed, insight and confidence to deal with cyber-attacks across any workload in any environment.

With products such as the aforementioned, we're enhancing companies' abilities to detect threats and recover quickly, ensuring they stay resilient against any cyber challenge.

As well as this, we have recently announced the acquisition of cloud cyber resilience company, Appranix. We have made this acquisition to help enterprises get up and running even faster after an outage or cyberattack. As we already know, Commvault is helping organisations reduce downtime by recovering data rapidly – but fast data recovery is only part of the equation.

There are necessities vitally needed to rebuild critical cloud applications and the cloud infrastructure that runs it all. These include networking, DNS configuration, application load balancing, security group access, and much more that enable cloud applications to operate at optimal efficiency. Appranix automates all of this and can reduce the time it takes to rebuild from days or weeks to, in some cases, hours or minutes.

We are marrying our extensive risk, readiness, and recovery capabilities with Appranix's next-generation cloudnative rebuild capabilities. Acquiring Appranix was the next logical step for our company, in order to achieve true cyber resilience-at-speed, and enabling our customers' goals of complete cyber resilience to become a reality.



What are the potential integration methods for AI within organizations' data protection and cyber resilience strategies?

Organizations of all shapes and sizes face unprecedented volumes of cyber threats that can disrupt business operations and tarnish brand reputations. It's chaotic to say the least. As this threat landscape continues to evolve, it's crucial for businesses to stay ahead of the bad actors and escalate their cyber defenses .

Al integration is transforming how organizations manage cyber risks. By partnering with a wide ecosystem of the top AI and cybersecurity firms, Commvault integrates AI to provide advanced threat detection and proactive security measures and help to address the chaos. Our Commvault Cloud platform leverages AI for real-time data insights and enhanced security, ensuring organizations can quickly respond to and mitigate potential threats.

COMMVAULT CLOUD IS THE INDUSTRY'S FIRST PLATFORM FOR → TRUE, CLOUD CYBER RESILIENCE AND IS A TRAILBLAZER IN THIS AREA.

These strategic integrations alongside our own platform allow us to leverage AI for real-time data insights and enhanced security, ensuring organizations can quickly respond to and mitigate potential threats.

In what ways does Commvault Cloud cater to customers seeking to fortify their cyber resilience and bolster their enterprise cloud strategy?

Cyber resilience can be the gateway to drive hybrid cloud adoption. But what you need is a partner with true cloud cyber resilience. One that supports cloud maturity by enabling data security and rapid cyber recovery across workloads, wherever they live on their cloud journey. According to the industry reports in 2023, 98% of global tech executives report their business has been impacted by

THE STATE OF DIGITAL TRANSFORMATION WITHIN THE MIDDLE EAST IS AT AN ADVANCED LEVEL COMPARED TO → OTHER REGIONS, SO THE NEED FOR CYBER RESILIENCE IS, IN TURN, AT A FAR GREATER LEVEL. increasing complexity of data across the cloud, and 82% of breaches these days involve data stored in the cloud - public, private, or multiple environments.

Commvault Cloud is the industry's first platform for true, cloud cyber resilience and is a trailblazer in this area, delivering the highest security, most intelligence, and fastest recovery. It differs from others by avoiding complex setups and offering a straightforward, comprehensive cloud solution that secures data across all cloud environments. Our platform ensures that your data is always protected, accessible, and recoverable, no matter where it resides.

Only Commvault Cloud enables true data security and recovery in the cloud. Companies can now back up, monitor, report, manage, and recover their data, wherever it lives, from one, central cloudbased solution.

How can organizations effectively tackle and advance their digital transformation amidst mounting cyber threats and other challenges?

Digital transformation presents

numerous advantages for businesses, including heightened efficiency, improved customer experience, diversified revenue streams, data-informed decisionmaking, and increased agility. However, it also brings its own challenges, such as resistance to change, cybersecurity vulnerabilities, financial investments, skills shortages, and technology integration complexities.

In the contemporary business arena, data assumes unparalleled value as firms pursue advancement. The necessity for digital transformation has become evident, particularly when you consider substantial shifts in both operational

OVER THE PAST FOUR YEARS, COMMVAULT HAS DILIGENTLY > ENHANCED ITS PLATFORM TO EFFECTIVELY MERGE IT AND SECURITY FUNCTIONS. practices and IT frameworks, notably with the proliferation of remote work setups.

Effectively harnessing data for customer satisfaction and innovation presents hurdles when dispersed across disparate platforms such as silos, clouds, and on-premises storage, managed through diverse backup and recovery systems. A modernized data protection strategy is indispensable, one that fosters agility and adaptability across the entirety of the infrastructure, rather than in isolated segments. This demands a solution that harmonizes diverse workloads, streamlining the environment and facilitating seamless digital transformation endeavours.

One of the many ways Commvault addresses these is by integrating early warning systems and cyber deception into our data security and cyber recovery services, allowing us to detect threats faster than industry norms. Our comprehensive approach helps businesses manage data across platforms, ensuring swift recovery and continued innovation without disruption.

Over the past four years, Commvault has diligently enhanced its platform



to effectively merge IT and security functions. This empowers our customers to proactively combat threats by integrating threat defense, backup, and recovery like never before. With Commvault's comprehensive workload coverage and dependable recovery capabilities, enterprises can swiftly recover from attacks or outages, minimizing downtime and ensuring seamless business continuity.

What are the prominent industry trends anticipated to reshape the approaches organizations adopt in safeguarding their data in 2024?

According to a recent IBM report, the global average cost of a data breach in 2023 was USD 4.45 million, representing a 15% increase over the previous three years. Furthermore, 51% of organizations are planning to boost security investments in the aftermath of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools. Organizations that heavily employ security AI and automation save an average of USD 1.76 million compared to those that do not.

In 2024 so far and for the remainder of the year, we expect to see more focus on enhancing cloud security frameworks, encryption mechanisms, and identity and access management solutions to safeguard data stored in cloud environments.

We can expect to see a growing focus on IoT security, as organizations strive

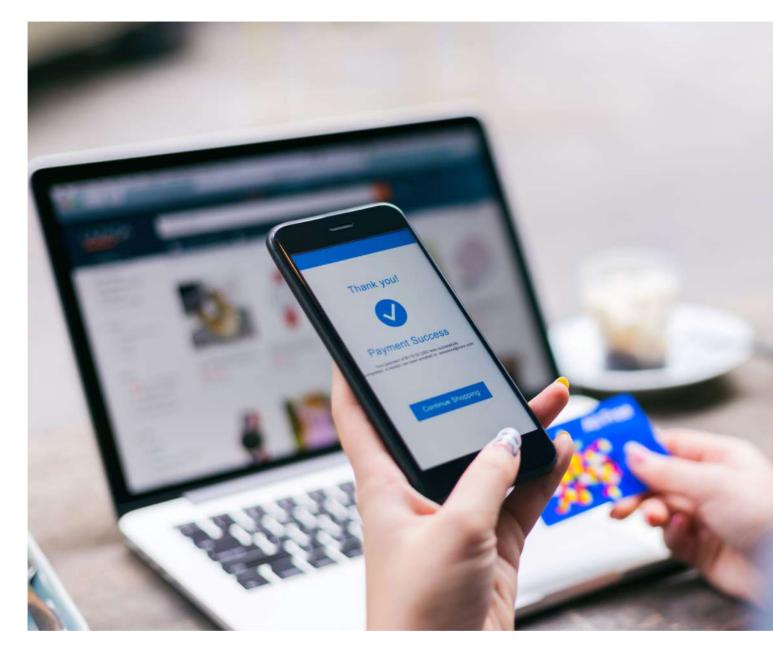
AS THE THREAT LANDSCAPE CONTINUES TO EVOLVE, IT'S CRUCIAL FOR BUSINESSES TO STAY AHEAD OF THE BAD ACTORS AND ESCALATE THEIR CYBER DEFENSES.



to protect their devices and data from cyberattacks. This will include developing new security standards and protocols for IoT devices, as well as raising awareness of the risks associated with them . In addition to increased focus on AI and Machine Learning (ML), enhanced focus on Mobile Security, improving the Cybersecurity skills and culture among the employees.

As well as this, we are seeing that organisations of all sizes across the region are becoming more aware of the importance of a sound cyber resilience strategy. Previously, it would be left to the IT teams to develop and integrate solutions to protect their data in order to enable efficient digital transformation. However, it has now become a C-level and board-level priority. The state of digital transformation within the Middle East is at an advanced level compared to other regions, so the need for cyber resilience is, in turn, at a far greater level. If you're serious about your data protection and backup capabilities, then you are serious about cyber resilience.

To summarise, looking ahead for the remainder of 2024, key trends to keep an eye on include enhanced cloud security frameworks and encryption, heightened IoT security, and a focus on AI and ML for improved cybersecurity. Commvault is at the forefront, incorporating these innovations to ensure our customers can navigate the complex landscape of data protection and thrive in an increasingly digital world.



GENETEC HIGHLIGHTS TOP DATA PRIVACY PRACTICES FOR PHYSICAL SECURITY LEADERS



enetec Inc. ("Genetec"), a leading technology provider of unified security, public safety, operations, and business intelligence solutions, has shared a comprehensive set of data protection best practices to help physical security leaders protect privacy, safeguard data, and enable trust without compromising security.

This initiative comes as a response to the escalating importance of data security in an increasingly interconnected digital landscape. By prioritizing privacy, organizations can effectively contribute to a safer digital and physical landscape for all.

"Organizations should never have to choose between data privacy and security. By equipping physical security professionals with these essential strategies, Genetec is spearheading a paradigm shift towards a more resilient and trustworthy security ecosystem. It is an ongoing process, and organizations should regularly update protocols, stay informed and continuously educate their teams on best practices", said Firas Jadalla, Regional Director – Middle East, Turkey and Africa (META) Genetec.

Genetec recommends organizations ensure their security systems respect data privacy by:

1. Collecting and Storing Only What You Need:

A fundamental rule of data security is to collect and store only essential information. The potential impact of a security breach can be reduced by minimizing stored data. It's important to regularly review and audit data and dispose of unnecessary information responsibly.

2. Limiting Access to Sensitive Data:

Enhancing data security involves restricting access to sensitive information. Genetec recommends implementing data-sharing best practices, such as removing personally identifiable information to safeguard individual privacy. Techniques for anonymizing personal information while retaining its utility include:

- Randomization (adding noise to numerical values such as an individual's age or income),
- pseudonymization (such as replacing names with unique identifiers), tokenization (such as replacing credit card numbers with tokens that have no direct correlation to the original numbers),

- generalization (such as converting exact birthdates to age ranges),
- and data masking (showing only the first few digits of a phone number).

3. Ensuring Privacy without Compromising Evidence:

By making use of technologies such as KiwiVision™ Privacy Protector, organizations can automatically anonymize images of people, so they can continue to survey surveillance footage while respecting privacy. This technology also offers an additional layer of security that ensures only authorized users can "unlock" and view unmasked footage while maintaining an audit trail.

4. Being Transparent and Get User Consent:

Building trust through transparency and user consent is essential. It's important to clearly communicate with users about the data collection process, promoting informed decisions. Organizations should also gain explicit consent before collecting and processing data.

5. Choosing a Reliable Data Storage Provider:

Organizations should select a data storage provider carefully, ensuring a clear understanding of data storage, handling, and sharing practices. If using third-party services, organizations should demand strong security measures and reliable data handling practices. Establish who "owns" any data stored in the cloud, and any rights/privileges associated with the use or disclosure of any information.

6. Establishing Strong Policies:

To ensure long-term data safety, Genetec recommends putting in place robust policies across the organization. Enforcing a transparent chain of custody through technology, such as a Digital Evidence Management System (DEMS), ensures accountability and traceability at every stage of the data lifecycle.

SANS INSTITUTE IS AT THE FOREFRONT OF PREPARING TOMORROW'S SECURITY PROFESSIONALS FOR THE CHALLENGES AND OPPORTUNITIES PRESENTED BY AI AND EMERGING TECHNOLOGIES.

REDEFINING EXCELLENCE IN CYBERSECURITY

NED BALTAGI, MANAGING DIRECTOR – MIDDLE EAST, TURKEY AND AFRICA AT SANS INSTITUTE, TELLS SECURITY ADVISOR MIDDLE EAST THAT WHILE THERE IS PALPABLE ENTHUSIASM FOR EMBRACING AI IN CYBERSECURITY, ITS IMPLEMENTATION'S EFFICACY IS CONTINGENT UPON COMPREHENSIVE, CONTINUOUS PROFESSIONAL EDUCATION.

ell us about the highlights of your participation at GISEC 2024. What is SANS Institute showcasing at the event?

At this year's GISEC, we're putting the spotlight on AI security, particularly the vital role of cybersecurity in AI development. We are keen to engage with visitors and professionals around our entire portfolio of training courses, as well as our initiatives supporting national government entities in bridging the talent gap in the META region.

Highlighting our agenda is the inaugural CISO Networking Sessions on April 23, a platform where thought leaders like James Lyne, our Chief Technology and Innovation Officer, and Kevin Ripa, a distinguished Senior Instructor, will lead in-depth discussions with CISOs. The session aims to navigate through the complexities of GenAl, the indispensability of zero trust architectures, the strategic importance of cloud security, and much more, setting a new precedent for cybersecurity excellence.

Why is an event like GISEC important for SANS Institute?

Participating in an event like GISEC is pivotal for SANS Institute, as it provides an unparalleled platform for visibility and engagement within the global cybersecurity ecosystem. It allows us to forge meaningful connections with a wide array of stakeholders, including government leaders from various regions, industry partners, and dedicated cybersecurity practitioners, all convened in a singular, dynamic setting. This convergence facilitates a rich exchange of ideas and strategies to tackle pressing cybersecurity challenges. More importantly, GISEC enables us to underscore the critical need for continuous, comprehensive training in both technical and strategic dimensions of cybersecurity, aiming to substantially mitigate the prevalent talent gap in the field.

This year's GISEC theme is AI-driven Cyber Resilience. How well-equipped are cybersecurity professionals in the region, to implement AI-driven cybersecurity?

The theme of AI-driven Cyber Resilience at this year's GISEC spotlights a pivotal shift towards more advanced, intelligent cybersecurity strategies. However, the readiness of cybersecurity professionals in the region to

SPECIAL INTERVIEW / SANS INSTITUTE



implement these AI-driven solutions varies widely. The spectrum ranges from early adopters, who are already integrating AI to enhance threat detection and response capabilities, to those still navigating the foundational challenges of adopting such technologies.

At SANS Institute, we've observed a growing awareness among professionals in leveraging AI for cybersecurity, yet there's a significant need for upskilling and strategic training. This is precisely where targeted educational initiatives, like our AIS247 course, come into play. They are designed to not only impart the technical know-how required to deploy AI-driven security measures effectively but also to foster an understanding of the ethical and operational nuances that accompany the adoption of these technologies.

In essence, while there is palpable enthusiasm for embracing AI in cybersecurity, its implementation's efficacy is contingent upon comprehensive, continuous professional education and the cultivation of a robust, AI-savvy cybersecurity workforce in the region.

How is SANS Institute equipping security professionals of the future to deal with AI & emerging technologies?

SANS Institute is at the forefront of preparing tomorrow's security professionals for the challenges and opportunities presented by AI and emerging technologies. Our latest offering, AIS247: AI Security Essentials for Business Leaders, is a prime example of this commitment. This 90-minute online course is crafted for managers and senior leaders, focusing on the integration of Generative AI (GenAI) tools in the business sphere and emphasizing cybersecurity's essential role in AI development.

AIS247 is designed to demystify the complexities surrounding AI, equipping leaders with the necessary knowledge and tools to navigate the AI landscape in their organizations effectively. A key component of the course is risk management, which teaches professionals not only to identify AI-related threats but also to develop and implement robust strategies for mitigating these risks. Beyond risk management, the course delves into AI policy development, guiding participants on how to establish and enforce effective Al strategies that align with their organization's goals.

SANS Institute is laying the groundwork for a new generation of security leaders, adept in leveraging AI for enhanced security and operational efficiency. Recognizing that AI's influence permeates all areas of cybersecurity, we are committed to continuously updating our curriculum to reflect the latest advancements in AI technology. This includes not only the introduction of courses like AIS247 but also the comprehensive integration of AI-related content across our existing courses. By spotlighting Al's role in various cybersecurity domains, we aim to provide our participants with a holistic understanding of how AI technologies impact security practices, threat detection, risk management, and policy development. Through this evolving curriculum, SANS Institute ensures that cybersecurity professionals are wellequipped to navigate the rapidly changing landscape and harness the power of AI to secure the future. 1



Complexity Impacts Effective Security Eliminate Complexity through Convergence and Consolidation Enabled by the Fortinet Security Fabric

Cybersecurity, everywhere you need it





Copyright ©2023 Fortinet, Inc. All Rights Reserved.

www.fortinet.com

FORTINET RELEASES 2023 SUSTAINABILITY REPORT



ortinet, the global cybersecurity leader driving the convergence of networking and security, released its 2023

Sustainability Report. This annual report outlines the company's approach, commitments, and progress on the sustainability issues that matter most to Fortinet and its stakeholders, including employees, investors, suppliers, partners, and customers.

Ken Xie, Founder, Chairman of the Board, and CEO at Fortinet, said, "Our commitment to sustainability is critical to help address today's societal challenges while supporting the long-term success and resilience of our business. As part of this commitment, our work in building a safer digital world has become missioncritical and essential to our society and economy. While we are proud of the progress in this year's sustainability report, we are mindful that advancing our sustainability goals and efforts is a continuous journey of improvement."

As detailed in the report, Fortinet's sustainability approach has four pillars: addressing cyber risks to society, diversifying cybersecurity talent, respecting the environment, and promoting responsible business across its value chain. In support of the company's commitment to sustainability and the Sustainable Development Goals (SDGs), Fortinet joined the UN Global Compact in 2023 and adheres to its human rights, labor, environment, and anti-corruption principles. Additionally, Fortinet was recognized in the 2023 Dow Jones Sustainability Indices (DJSI) World and North America indices for the second year as a testament to the company's ongoing sustainability efforts and dedication to building a more sustainable future for all.

Highlights from the Fortinet 2023 Sustainability Report include:

Progress toward net-zero
greenhouse gas emission targets:
The company continues investing
in green energy sources, including
its new garage space in Sunnyvale,
where solar panels will cover
the power needs of Fortinet's
headquarters and nearby owned
sites. In 2024, Fortinet will submit its
decarbonization plan to the ScienceBased Targets initiative (SBTi) for
validation.

Improving product energy efficiency: Fortinet continues to improve the power efficiency of its FortiGate appliances—its 2023 models consume, on average, 62% less power than the previous generation of equivalent models.

- Sustainable packaging: Fortinet continues to explore and introduce packaging made from biodegradable materials, applying it to more than 60 models across its product lines. The eco-friendly packaging manufactured in 2023 helped Fortinet avoid an estimated 455 tons of CO2 emissions.
- Progress toward training 1 million people in cybersecurity by 2026: As of December 31, 2023, Fortinet stands at 43% of its five-year goal. Last year, the company expanded its efforts to close the cyber skills gap by providing free access to various curricula, fostering online safety awareness and nurturing future cybersecurity professionals among students.
- Diversity, Equity, and Inclusion (DEI): In 2023, Fortinet strengthened its internal leadership development program to further drive a focus on inclusion. As a result, over 340 Fortinet leaders were trained to foster inclusion.
- Partnerships to disrupt cybercrime: Fortinet continues expanding its collaboration efforts to combat cybercrime. In 2023, the company joined the Joint Cyber Defense Collaborative (JCDC) and through the INTERPOL Gateway program contributed to the arrest of 15 cybercriminal groups and the prevention of \$40 million in financial losses.
- Commitment to ethical business

OF IMPROVEMENT.

WHILE WE ARE PROUD OF THE PROGRESS IN

THIS YEAR'S SUSTAINABILITY REPORT, WE ARE

MINDFUL THAT ADVANCING OUR SUSTAINABILITY

GOALS AND EFFORTS IS A CONTINUOUS JOURNEY



practices and legal compliance:

In 2023, 100% of the company's distributors and key contract manufacturers completed Fortinet's business ethics and compliance training, acknowledging their alignment with Fortinet's values and principles.

Information security and privacy: Fortinet launched its Trust Resource Center to offer customers visibility on certifications, compliance, and security information. Fortinet also renewed information security certifications and examinations and completed new ones, including expanding the products and services covered by ISO 27001, SOC 2, and HIPAA.

Fortinet's 2023 Sustainability Report references the Task Force on Climaterelated Financial Disclosures (TCFD). the Global Reporting Initiative (GRI) Standards, Sustainability Accountability Standards Board (SASB) Standards, and the United Nations Sustainable Development Goals (UN SDGs). The report details Fortinet's progress and metrics across eight priority issues: innovating for a safe internet, information security and privacy; product environmental impacts; environmental management and climate change impacts; diversity, equity, and inclusion; cybersecurity skills gap; business ethics; and responsible product use. 🚦

APRIL 2024 27

oogle Cloud has announced the appointment of Noor Al-Sulaiti as Head of Security Business Development and Government Relations for the Middle East, Turkey, and Africa region (META). Noor, an industry veteran known for her innovative leadership, brings a wealth of experience in the telecommunications and technology sectors to her new role.

Noor's appointment is yet another testament to the company's commitment to the region and safeguarding governments' digital assets. In this position, Noor will be responsible for Google's security expansion in the Middle East, Turkey and Africa underscoring the growing importance of cybersecurity for the company. She will foster strategic partnerships with the public sector to leverage Google Cloud's cutting-edge cybersecurity solutions, including Cybershield, a powerful cybersecurity solution tailored specifically for governments and inspired by the concept that organizations inside a nation and around the world need to "lock shields" and stand united in their defense against shared attackers.

Noor's distinguished career includes her role as CEO of Ooredoo Oman. There, she established herself as the youngest and first female CEO in the company's history, spearheading a transformation into a digitally led, data-powered, and customer-centric organization. Prior to joining Ooredoo Oman, Noor was the CEO of Starlink, a retail chain



GOOGLE CLOUD APPOINTS NOOR AL-SULAITI TO LEAD CYBERSECURITY BUSINESS DEVELOPMENT & GOVERNMENT RELATIONS FOR META and IT service provider in Qatar. She was also the general manager of Phono and FASTtelco in Kuwait. She has been recognized as one of the most powerful businesswomen by Forbes Middle East and as a notable business leader by other prominent publications.

Noor Al-Sulaiti said: "I am honored to join Google Cloud, a company that has inspired me throughout my career. Google Cloud is continuously helping governments around the world enhance their security capabilities and respond holistically at the national level to keep their citizens and critical assets safe, and I'm ready to lead the charge to bring these capabilities to the Middle East, Turkey and Africa."



ACCELERATE YOUR DIGITAL TRANSFORMATION TO UNLOCK BUSINESS VALUE

YOU CAN COUNT ON US

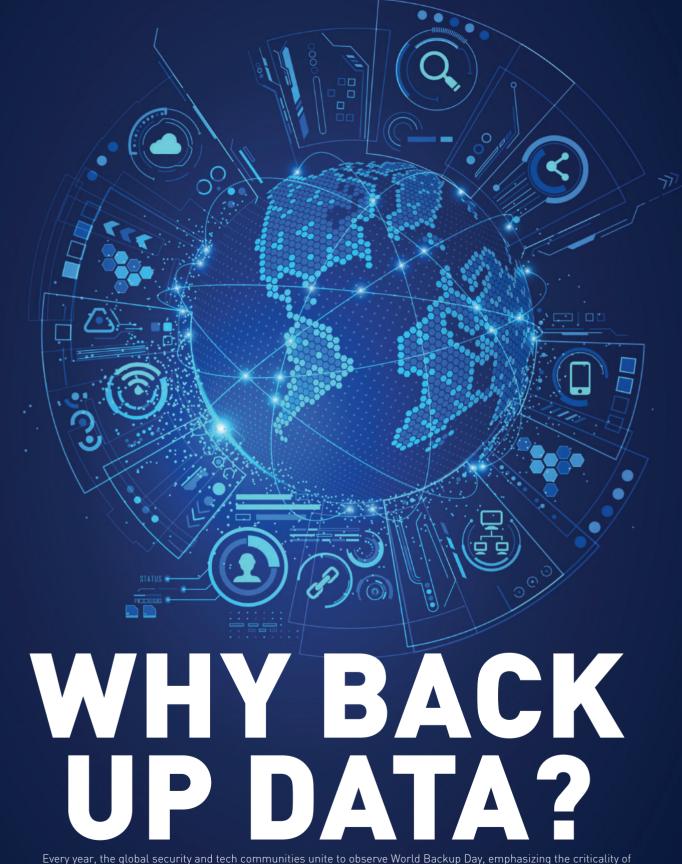
Rapid advancements in technologies are reshaping industries, fostering new business models, and challenging traditional practices. To thrive in the coming decade, organizations must embrace change, reinvent themselves, accelerate digitization and deliver great customer experience.

At BCT, for over 24 years, we've assisted clients worldwide in unlocking business value from their digital transformation initiatives. Our winning formula comes from our unique combination of innovative IP products, customer-centric IT services, and strategic technology partnerships.



www.bahwancybertek.com

FEATURE / WORLD BACKUP DAY



safeguarding data and fortifying system and computer security measures. Security Middle East takes a look at why backing up data is important today and how businesses can navigate the maze of modern-day back up strategies to choose what matters.

Bernard Montel EMEA Technical Director and Security Strategist, Tenable

hile it might seem that there is a day for everything, what each looks to do is raise awareness of a particular issue - be it health related, community spirited, or in the case of World Backup Day an initiative to drive change.

"When it comes to backing up our data, there are a number of driving factors - perhaps the most obvious is to recover quickly when something goes wrong - be it equipment failure, human error or third party manipulation such as ransomware. However, not all backups are equal and it's not just a tick box exercise. This World Backup Day spend a few moments thinking about why you're backing up your data and how you are doing this.

"In the case of ransomware gangs,

they have evolved their tactics to also compromise backed up data. By encrypting backups, you can limit ransomware's impact on it, although it could still be stolen by threat actors. Therefore consideration should also be given to how you manage encryption keys, with third party offerings an effective option. Spread the risk by storing backups on a different operating system to your backup servers. All of this will help limit the impact should ransomware strike. However, the best offence really is a strong defence. While thinking through your backup strategy, also take a moment to understand your organisation's unique risk profile, discover where vulnerabilities exist and prioritise remediation efforts to root out those that could be the most harmful first



Ezzeldin Hussein Regional Senior Director Solution Engineering –META, SentinelOne

t is important to highlight the significance of data backup strategies in safeguarding against potential loss or theft. Data loss incidents can occur unexpectedly due to various factors such as accidents, device failures, or cyberattacks.

Shockingly, a significant percentage of individuals have never made a backup, leaving themselves vulnerable to potential disasters. As everything turns digital, it is essential to implement solutions that ensure the safety and accessibility of important files. Whether through online backup



services, external storage solutions, or device-specific backups, taking proactive measures to secure data can prevent irreparable loss and provide peace of mind.

As advocates for data security, we encourage individuals to take the World Backup Day pledge and commit to backing up their important documents and memories as regularly as possible. By spreading awareness and adopting proactive backup practices, we can collectively minimize the impact of data loss incidents and better protect our digital assets."

John Shier Field CTO Threat Intelligence, Sophos



ackups are integral to an organization's resilience. Therefore, it's not surprising that attackers proactively attempt to compromise them. Early detection and a swift response to anomalous activity on a network can prevent attackers from reaching backups in the first place.

"Without complete, reliable backups, ransomware attack victims could be forced to make choices they might otherwise avoid, such as paying a 'basic' ransom or paying an even higher than normal ransom because there's no other recourse to get that data back. Ransomware attacks can have serious impacts on business operations; without dependable options for recovery, they can be devastating.

Michael Cade Field CTO Cloud Native Product Strategy and Global Technologist, Veeam

hile the rise of ransomware and legislation like NIS2 has certainly meant more companies are back up of their data seriously, the fundamentals – having multiple, protected, reliable copies of data – remain the same. "What has changed in regards to back up are the environments businesses now need to protect. Workloads aren't all under one roof anymore, there are multiple platforms to protect and backup. Physical, virtual, cloud-native and SaaS environments, which all interlock and integrate, must be reliably backed up and recovered. It's no surprise that according to our recent research, the two most important attributes sought in an 'enterprise backup' solution are reliability and the protection of cloud-hosted workloads (IaaS & SaaS).

"As businesses broaden their tech horizons and embrace the cloud, virtualisation, containers or whatever environment helps them optimise performance and lower costs, when it comes to backing these up - you need the right tool for the job. Naturally, the tech comes first, but backup can't be an afterthought. Make it part of the thinking from day one and you'll see a radical shift in your organisation's resilience.



Mohammad Meraj Hoda Vice President Emerging Markets, Ring

orld Backup Day reminds us of the importance of securing what truly matters. We stand committed to providing our users with peace of mind and reliable protection every step of the way. With Ring Protect subscriptions, available on the Ring app in two tiers, Basic and Plus, users can unlock features such as Person Alerts and Package Alerts to ensure they get the alerts that matter the most. Customers can scroll through their timeline at their convenience to view the moments they missed throughout the day and choose those they would like to download to save or share with family, friends, or neighbors.



Ramzi Itani Regional Director of Emerging Region Veritas Technologies

ere are three key considerations when evaluating your data protection strategy this World Backup Day:

Uniting data protection with data security and data governance improves cyber resilience. Malware attacks affect the entirety of IT. Multiple teams typically manage the response using disparate tools. Hackers love patchwork defenses because the interaction points can become potential vulnerabilities. An integrated ecosystem of data security, data protection and data governance is the only way to achieve gap-free cyber resilience.

The cloud is not inherently safer. In the cloud-native era, organizations often incorrectly assume they're buying an outcome, when they're really buying infrastructure. There's a shared responsibility model between cloud service providers (CSPs) and their customers around data protection that far too many fail to understand. CSPs are responsible for the resilience of the cloud, but customers are responsible for the resilience in the cloud. You're still responsible for protecting your data.

Today's complex, heterogeneous, multi-cloud environments require autonomous data management. The proliferation of applications and data from edge to core to cloud is unprecedented and real-time manual protection is no longer possible. Reducing operational complexity through data management that responsibly harnesses AI and hyper-automation to continually self-provision and self-optimise should be your goal.

Ranjith Kaippada Managing Director, Cloud Box Technologies

ata backup is no longer just about preserving data but companies have understood how integral data is to keep their businesses in operation. Modern data backup strategies take advantage of the latest technology advancements to ensure resilience against cyberattacks or data losses due to disasters or incidents.

Data is a lifeblood for businesses meaning losing the data or getting attacked can cause businesses financial and/or reputational damage. Data backup strategies now employ the latest technologies such as AI-driven analytics, automation, and cloud storage. Here, AI can help predict instances of cyberattacks and fortify defence against such attacks.

Automation in data backup strategies cuts back reliance on humans to manually intervene and ensures data is protected with scheduled backups. There's also a real-time monitoring feature that flags any abnormalities in the systems. Al algorithms can be leveraged to identify trends and patterns as well as find potential weaknesses as well as optimize the strategies required to make systems resilient."



Rob T. Lee Chief Curriculum Director and Faculty Lead SANS Institute



he adoption of multi-cloud strategies and edge computing will necessitate more flexible and decentralized backup solutions. Future backup systems will need to efficiently manage data across diverse cloud environments, ensuring data availability and integrity while minimizing latency. Edge computing, where data processing occurs closer to the data source, will require new approaches to data backup that can accommodate the distributed nature of data generation and storage. Technologies such as blockchain could potentially offer immutable and verifiable data backups, enhancing security and trust in backup processes.

Moreover, automation and AI can significantly enhance cloud-compatible backup strategies by optimizing backup schedules based on data usage patterns, predicting potential data loss events, and automatically adjusting resources to meet backup demands. AI algorithms can improve data deduplication and compression techniques, reducing storage costs and improving backup efficiency. Furthermore, AI-driven security can help identify and mitigate threats in real time, ensuring the integrity of backup data. Automation simplifies the management of complex, multi-cloud environments, allowing for more consistent and reliable backup processes."



o

0

0

8222228

رقمیات Raqmiyat

Secure Your Digital Future Simple. Secure. Resilient.



www.raqmiyat.com UAE | KSA | INDIA

D

A HOLISTIC A HOLISTIC

ANITA JOSEPH CAUGHT UP WITH FINESSE SPOKESPERSONS-ELJO J P, CHIEF BUSINESS OFFICER & DIRECTOR AND YOGENDAR KUMAR, HEAD OF INFORMATION SECURITY-TO FIND OUT MORE ABOUT THE COMPANY'S COMPREHENSIVE APPROACH TO IT & OT SECURITY.

an you elaborate on how Finesse integrates IT (Information Technology) and OT (Operational Technology) security to address the convergence of these domains effectively?

Finesse takes a comprehensive approach to integrating IT and OT security, leveraging the expertise of dedicated teams in both domains. Cyberhub is powered by Finesse's partnership with Claroty to deliver purpose-built cybersecurity controls that identify, protect, monitor, and optimize all OT, IoT, and BMS assets, systems, and processes in an industrial environment. Finesse's Cyberhub provides a comprehensive solution to address the convergence of IT (Information Technology) and OT (Operational Technology) security in the context of the Extended Internet of Things (XIoT).

- Unified Visibility: Cyberhub offers a centralized platform that provides complete visibility across the entire XIoT environment, spanning IT, OT, and IoT assets. This holistic view enables security teams to identify and monitor all connected devices, regardless of their domain.
- Asset Inventory and Vulnerability Management: The platform maintains a detailed asset inventory, including information about each device's type, vendor, firmware version, and known vulnerabilities. This allows for effective vulnerability assessment

and remediation across the converged IT-OT landscape.

- Network Segmentation and Access Control: Cyberhub supports the implementation of strong network segmentation and access control policies, ensuring that communication between IT and OT domains is strictly monitored and regulated. This helps mitigate the risk of lateral movement and cross-domain attacks.
- Threat Detection and Response: The solution leverages advanced analytics and machine learning to detect anomalies and potential threats across the IT-OT convergence. It provides actionable insights and automated response







capabilities to enable swift mitigation of security incidents.

- Compliance and Reporting: Cyberhub helps organizations maintain compliance with industry-specific regulations and standards, such as IEC 62443 and NIST, by providing comprehensive reporting and audit trails for the entire XIoT environment.
- Seamless Integration: The platform integrates with existing IT and OT security tools, allowing organizations to leverage their existing investments and streamline security operations across the converged domains.

In what specific ways does Finesse prioritize the protection of critical infrastructure and industrial control systems against cyber threats? Finesse prioritizes the protection of

critical infrastructure and industrial control systems (ICS) by employing specialized OT security experts. These experts have in-depth knowledge of ICS protocols, SCADA systems, and industrial automation processes. Finesse implements segmentation strategies, deploys purpose-built security solutions for OT environments, and enforces strong access controls and authentication mechanisms to secure these critical systems against cyber threats. Additionally, Finesse makes sure only the right people can access these critical systems by setting strict access control rules and monitoring who's trying to access the resources, which helps reduce the risk of cyber-attacks.

Could you explain the role of Cognitive SOC (Security Operations Center) in Finesse's cybersecurity framework and how it enhances threat detection and response capabilities?

Finesse cognitive SOC uses advanced analytics, machine learning, and artificial intelligence to detect sophisticated and ever evolving cyber threats. It can identify patterns and anomalies in network traffic, system logs, and user behaviour that may indicate a potential security breach. Finesse leverages automated incident response mechanisms to isolate affected systems, gather forensic evidence, and initiate remediation procedures.

Through the analysis of historical data, threat intelligence feeds and contemporary trends, our Cognitive SOC can detect potential future threats and vulnerabilities. This detection capability empowers the Finesse team to proactively implement preventive security measures and maintain a proactive strategy against emerging cyber threats.

How does Finesse leverage advanced analytics and artificial intelligence within its Cognitive SOC to proactively identify and mitigate potential security risks before they escalate?



Finesse's Cognitive SOC utilizes advanced analytics algorithms to establish a baseline of normal network behaviour across both IT and OT environments. Any deviations from this baseline, such as unusual traffic patterns or unauthorized access attempts, trigger alerts as anomalies. Advanced machine learning models continuously analyse historical data, refining anomaly detection accuracy while minimizing false positives.

By inspecting user interactions with systems and data flows, the Cognitive SOC employs User and Entity Behaviour Analytics (UEBA) to detect

CYBERHUB OFFERS A CENTRALIZED PLATFORM THAT PROVIDES COMPLETE VISIBILITY ACROSS \rightarrow THE ENTIRE XIOT ENVIRONMENT, SPANNING IT, OT, AND IOT ASSETS.

anomalies indicative of insider threats, compromised accounts, or unauthorized access attempts. Through diligent analysis of security incident patterns and trends, these models can proactively anticipate potential threats and suggest preventive security measures to mitigate risks before they escalate.

Leveraging the power of AI, Finesse's cognitive SOC incorporates AI-powered automation tools to orchestrate incident response activities and remediation actions seamlessly. When a potential security risk is identified, predefined playbooks are executed automatically, swiftly containing the threat, isolating affected systems, and initiating appropriate response procedures. This automated approach minimizes the time to detect (MTTD) and respond (MTTR) to security incidents, enhancing the overall resilience of the integrated IT-OT environment. **1**

DON'T LET YOUR WORKLOADS GET STUCK IN THE MUD

RICK VANOVER - SENIOR DIRECTOR PRODUCT STRATEGY – VEEAM



s businesses look to optimise their costs to weather economic downturns, ramping up cloud spend can cause

some headaches. While there are lots of different options to help mitigate this, from moving workloads to a more cost-effective environment (or even back to on-premises) or re-architecting to save costs, organisations often lack the technical agility to make the most of them. With modern businesses carrying so much data, some legacy or homegrown applications not allowing for transfer and cloud lock-in all to contend with, it can quickly feel like trying to fit a thousand square pegs through a thousand round holes. All of this is against the backdrop of cyber threats like ransomware - so the right balance between cost and security needs to be found for every workload. To avoid this, IT teams are increasingly designing and adjusting their environments with portability in mind, but there are some questions to ask yourself first.

Why move data at all?

To state the obvious for a second, modern enterprise IT environments are vastly complex. They can be monolithic and highly dispersed, with the growing data gravity of some environments making many companies essentially "digital hoarders." This is problematic as is, as holding on to data you don't need exposes you to unnecessary cybersecurity and



compliance risks. But data bloat in the cloud also brings severe financial consequences and the dreaded "bill shock" when that invoice lands.

So, even though many companies moved to the cloud in the first place to optimise costs, the flexibility that the cloud gives businesses can be something of a double-edged sword. While the attractiveness of the cloud is that you only pay for what you need, the flip side is there is no "spending cap" so costs can easily get out of control. To solve this, better data hygiene can help, but for the data you do need, it's about picking the right platform for the workload. This may involve re-platforming or re-architecting to optimize costs. This is where data governance and hygiene come in before looking to move data or improve processes, you need to know exactly what data you have, and where.

What data can we move?

So, once you've established what data you should think about moving, either to a different environment, server, or storage tier, the next, more difficult question is what data you can move. Unfortunately, this is where many organisations face challenges. Having data portability is crucial to be able to move things around as needed and to simply maintain data hygiene in the long term. But several factors can make it difficult to move or transfer workloads from one location to another. The first is "technical debt" essentially the extra work and maintenance required to update older or scratch-built applications to get them to a point where they are transferable and compatible with other environments. The cause of these issues might be taking shortcuts, making mistakes, or simply not following standard procedures during software development. But leaving it unfixed makes it impossible to optimize environments and can cause additional problems for things like backup and recovery.

IT TEAMS ARE INCREASINGLY DESIGNING AND ADJUSTING THEIR ENVIRONMENTS WITH PORTABILITY IN MIND, BUT THERE ARE SOME QUESTIONS TO ASK YOURSELF FIRST.

The (constant) security question

Finally, it's crucial when building and capitalising on data portability that security is not left behind. Of course, improving security can (and should) be a motive for moving workloads in the first place but if you're migrating workloads to optimise costs this must be balanced against security considerations. Security needs to be part of the data hygiene process, so teams need to ask "What do we have?" "What things do we not need?" and "What are the critical workloads we absolutely cannot afford to lose?" Beyond this, continue to patch servers and when moving data to colder storage etc remove internet access when it's not needed.

As organisations strive to manage their IT environments and avoid financial and cyber security surprises, it's important to constantly assess what data and applications you have, and where they are kept. But to manage this and adjust as needed, businesses must build with portability in mind. By doing this, businesses can create a more agile and cost-effective cloud environment and will find it easier to bounce back and recover from disasters like ransomware.



KASPERSKY WARNS OF DATA STEALERS HUNTING FOR USER CREDENTIALS

s the malware development market continues to flourish with new stealers such as Lumma, for the last three years Redline still remains the dominant data-stealing malware used by cybercriminals. More than half of every device (55%) targeted by password-stealer attacks in 2023 has been infected with the Redline malware, Kaspersky Digital Footprint Intelligence finds.

Infostealers infiltrate devices to illicitly obtain sensitive credentials such as logins and passwords, which are then peddled on the shadow market, posing significant cybersecurity threats to personal and corporate systems.

According to information gleaned from log-files traded or distributed freely on the dark web, Redline was used in 51% of infostealer infections from 2020 to 2023. Other notable malware families included Vidar (17%) and Raccoon (nearly 12%). In total, around 100 distinct infostealer types were identified by Kaspersky Digital Footprint Intelligence between 2020 and

kaspersky

2023 using metadata from log-files.

The underground market for datastealing malware development is expanding, evident from the rising popularity of new stealers. Between 2021 and 2023, the portion of infections caused by new stealers grew from 4% to 28%. Specifically, in 2023, the new "Lumma" stealer alone was responsible for more than 6% of all infections.

"Lumma emerged in 2022 and gained popularity in 2023, through a Malware-asa-Service (MaaS) distribution model. This means any criminal, even those without advanced technical skills, can purchase a subscription for a pre-made malicious solution and use this stealer to carry out cyberattacks. Lumma is primarily designed for stealing credentials and other information from cryptocurrency wallets, commonly spread through email, YouTube, and Discord spam campaigns," - says Sergey Shcherbel, expert at Kaspersky Digital Footprint Intelligence.

To guard against data-stealing malware, individuals are advised to use a comprehensive security solution for any device. This will help prevent infections and alert them to dangers, such as suspicious sites or phishing emails that can be an initial vector for infection. Companies can help their users, employees and partners protect themselves from the threat by proactively monitoring leaks and prompting users to change leaked passwords immediately.

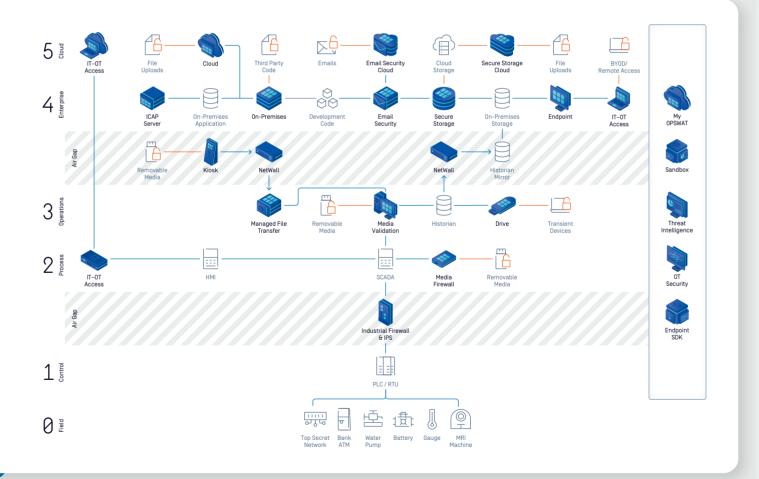
More information about infostealer threat landscape is gathered at Kaspersky Digital Footprint Intelligence website.

OPSWAT.

The Critical Advantage in Cybersecurity

OPSWAT has spent the last 20 years evolving our end-to-end cybersecurity platform to give public- and private-sector organizations the critical advantage needed to protect the most complex environments—from the plant floor to the cloud.

Join us at Hall 7 – Stand C38 to experience the OPSWAT MetaDefender Platform.



Can't make it to the booth? No problem.



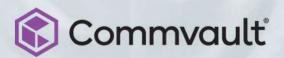




CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD CLEANROOM™ RECOVERY



Visit commvault.com to Learn More