

D-Link®



Smart Wi-Fi **Smart Life**



Enjoy robust 360° spherical coverage courtesy of a sophisticated antenna design and advanced AI technology, ensuring fast and consistent Wi-Fi in every corner of your home.

Pack of 3

Uninterrupted Wi-Fi Everywhere



Eco-friendly Design

Made with Post-Consumer Recycled case and packed in recyclable packaging.



Rapid Connectivity

Revel in speeds up to 3 Gbps with an extra antenna on the faster 5 GHz band, assuring seamless video streaming, video conferencing, and smooth gaming.



Gigabit Wired Connection

1× Gigabit WAN port + 4 × Gigabit LAN ports allow you to make fast and reliable connections to wired devices like smart TVs, gaming PCs and more.



Mesh Technology

Scale-as-you-need Mesh Create a robust mesh network with other AQUILA PRO AI routers and extenders.

AQUILAPRO AI Mesh Router M30

One Connection, Infinite Possibilities

CONTENTS

Securaty









- 6 Security news roundup from the region and beyond
- Ram Narayanan, Country Manager Middle East at Check Point, discusses the company's cutting-edge security solutions and how they provide companies with a 360-degree view of their security posture.
- Rahil Ghaffar, VP EMEA , WhiteSwan Security explains how it's crucial for organizations to prioritize identity security because compromised credentials can lead to breaches that are difficult to detect and can cause extensive damage.
- Serkan Yusuf, Director of Services at OTIFYD, discusses OTIFYD's cutting-edge cybersecurity services and solutions that leverage strategy to drive people, process, information and technology advancement.

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT sets new standard in cybersecurity with first-ever

100%

rating in SE Labs CDR (content disarm & reconstruction) test.



Talk to one of our experts today or book a demo

opswat.com/get-started

Read the full SE Labs report

selabs.uk/reports





EDITOR'S NOTE



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

Anita Joseph Editor

EVENTS





RESHAPING THE DEFENCE LANDSCAPE

n the ever-evolving landscape of cybersecurity, 2024 presents a daunting array of threats that challenge the very fabric of our digital existence. From sophisticated ransomware attacks crippling essential services to the proliferation of deepfake technology threatening the integrity of information, the need for innovative solutions has never been more urgent. Fortunately, as adversaries continue to sharpen their tools, so does the arsenal of defense, with **A SECURE FUTURE** artificial intelligence (AI) emerging as a formidable ally in the battle

against cyber threats.

Al, with its capacity for rapid analysis and pattern recognition, stands at the forefront of cybersecurity defense in 2024. Its ability to sift through vast amounts of data in realtime enables the detection of anomalies and potential threats with unprecedented speed and accuracy. Through machine learning algorithms, AI systems continuously adapt and evolve, staying one step ahead of malicious actors who seek to exploit vulnerabilities in our digital infrastructure.

One of the most pressing challenges in cybersecurity today is the rise of sophisticated social engineering attacks, where adversaries

leverage psychological manipulation to deceive users and gain unauthorized access to sensitive information. Al-driven solutions are revolutionizing defense strategies by detecting subtle cues indicative of fraudulent activity, thus thwarting such attacks before they cause harm.

Moreover, as the internet of things (IoT) expands, so does the attack surface for cybercriminals. With Al-powered threat

> detection mechanisms integrated into IoT devices. vulnerabilities can be

identified and mitigated in real-time, safeguarding critical infrastructure and personal privacy.

However, as AI becomes increasingly autonomous, there are concerns regarding unintended consequences and the potential for algorithmic bias. Therefore, it is imperative that stringent regulations and ethical guidelines govern the development and implementation of AI in cybersecurity to ensure transparency, accountability, and fairness.

By strategically harnessing the power of artificial intelligence, we can fortify our digital defenses and pave the way for a safer and more secure cyber environment in 2024 and beyond.

FOUNDER, CPI Dominic De Sousa (1959-2015)

Published by



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

anita.joseph@cpimediagroup.com Online Editor

Daniel Shepherd daniel.shepherd@cpimediagroup.com PRODUCTION AND DESIGN Designer Ulysses Galgo ulygalgo@gmail.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 natasha.pendleton@cpimediagroup.com

EDITORIAL

Editor

Anita Joseph

Sales Directo Sabita Miranda sabita.miranda@cpimediagroup.com

SENTINELONE UNVEILS FUTURE OF AUTONOMOUS SECURITY

SentinelOne, a global leader in Al-powered

security, has announced new capabilities within its Singularity Platform designed to democratize advanced cybersecurity operations. The company unveiled the capabilities, which make top-tier Security Operations Centers (SOC) a reality for companies of all sizes, at RSA 2024.

"Imagine a future where security solutions not only help enterprises respond to threats, but anticipate and mitigate them before they lead to a security incident. This is the future we are creating at SentinelOne," said Tomer Weingarten, CEO of SentinelOne. "Our solutions are designed to

transform how security teams manage the complexity of their environments and defend threats. With our latest innovations, customers can move from the reactive operating paradigm of today and enable a predictive and autonomous future."

SentinelOne is democratizing cybersecurity through AI and automation, enabling every enterprise to operate at the same scale, speed and sophistication, regardless of budgets and resources. When combined with the visibility of the Singularity Platform and the breadth and scale of the Singularity Data Lake, Purple AI provides an always-on, expert analyst



to augment the skills of any security team and supercharge their capabilities.

"It's no secret that security teams are overwhelmed with data, alerts and labor-intensive triage," said Ric Smith, Chief Product and Technology Officer, SentinelOne. "Purple Al doesn't just do what you ask it to, it does what you need it to."

VEEAM LAUNCHES KASTEN V7.0, ENABLING CYBER RESILIENCE AND ENTERPRISE-FOCUSED INNOVATION

Veeam Software, the #1 leader by

market share in Data Protection and Ransomware Recovery, has announced the release of new Veeam Kasten for Kubernetes V7.0 during Red Hat Summit 2024. With more than 30 new features and enhancements, this milestone version from Veeam, the leading provider of Kubernetes data protection solutions, delivers rigorous, standardcompliant security measures including Federal Information Protection Standard (FIPS) for federal sector environments. This brings enhanced ransomware protection, including integrations with Microsoft Sentinel, and broadens enterprise integration opportunities for large-scale Kubernetes application platforms, including Red Hat OpenShift.

Container usage continues to rise, with 59% of enterprises running containers in production and another 37% either rolling them out or planning to do so. Addressing the market need



for robust container security alongside expanded Kubernetes deployments, Veeam Kasten V7.0 delivers cyber resilience and enterprise-focused innovation to help customers efficiently protect and secure their applications and data. These capabilities are critical to enabling organizations' application modernizations and migrations away from traditional on-premises virtual machines (VMs), particularly through Red Hat OpenShift Virtualization,

even if they aren't ready to fully refactor their applications now. This release notably strengthens Veeam's collaborations with Red Hat and Microsoft further broadening the solution's capabilities.

"Veeam continues to set the standard in Kubernetes data protection and is trusted by the world's largest organizations," said Gaurav Rishi, vice president of Product Management at Veeam. "Veeam Kasten delivers purpose-built and secure Kubernetes native data protection and application mobility at scale across a wide range of distributions and platforms. Proven to recover entire applications quickly and reliably and coupled with its core tenet of simplicity, Veeam Kasten gives operations and application teams confidence in their cyber resilience and the ability to protect and scale their cloud-native applications more efficiently."

PROOFPOINT SETS NEW INDUSTRY STANDARDS IN EMAIL SECURITY

Proofpoint, a leading cybersecurity and

compliance company, has unveiled two industry-first innovations that redefine email security with the most comprehensive and effective end-to-end email protection across the entire email delivery chain. Uniquely combining new pre-delivery, click-time, and post-delivery detections, Proofpoint's enhanced core email security packages now include:

The industry's first and only predelivery defense against both social engineering threats and malicious links and; New adaptive email security capabilities, offering a fully integrated layer of behavioral AI-based defense post-delivery to stop targeted threats such as lateral internal phishing and advanced email fraud for the most at-risk employees—all while offering seamless API integration with Microsoft 365

Every month, Proofpoint blocks over 66 million attempted BEC attacks targeting its customers. As attackers have also become more reliant on URLs, threat volume has surged; Proofpoint detects over 4.5 million unique malicious URLs daily, an increase of 119% in the last three years.



With both threats, speed kills; Proofpoint's data set, spanning trillions of daily messages, shows that one in seven clicks on malicious URLs occurred within 60 seconds of the message hitting the inbox, underscoring the criticality of both pre and post-delivery protection capabilities.

DELL TECHNOLOGIES INTRODUCES MULTICLOUD DATA PROTECTION AND AI ADVANCES TO COUNTER INCREASING CYBERATTACKS

Dell Technologies is expanding its data

protection portfolio of appliances, software and as-a-Service offerings to help customers strengthen cyber resiliency in the face of increasing cyberattacks.

With advances across the Dell Data Protection portfolio, Dell is helping customers build a modern and resilient foundation to protect data on-premises, in public clouds and at the edge. These innovations help address concerns raised in the 2024 Dell Global Data Protection Index (GDPI) survey, which revealed that 75% of organizations believe their existing data protection measures are unable to cope with ransomware threats. Nearly 70% lacked confidence that they could reliably recover from a cyberattack.

"With the exponential growth of data, generative AI (GenAI) presents organizations with opportunities to streamline processes, improve decision-making and drive innovation, but it also extends the attack surface for cyberattacks – especially with trained



models, which are quickly becoming one of the most valuable assets for enterprises," said Arthur Lewis, president, Infrastructure Solutions Group, Dell Technologies. "With this expanding digital landscape that exposes more vulnerability gaps, companies are increasing their reliance on Dell to help protect their data wherever it resides with trusted data protection and Al offerings."

"With increasing cyber threats putting organizations on constant high alert, the demand for trusted high performance

data protection systems has never been greater," said Phil Goodwin, research vice president, IDC. "Dell's portfolio of data protection solutions support numerous data protection best practices to help organizations modernize their data protection environment. With major performance enhancements in backup and restore, we expect the latest PowerProtect Data Domain appliances to remain a key element of critical data protection and cyber recovery infrastructure."

www.tahawultech.com MAY 2024

SOLARWINDS LAUNCHES CONSULTATIVE SALES MODEL TO HELP CUSTOMERS MAXIMIZE VALUE OF ITSM SOLUTIONS

SolarWinds has unveiled a

groundbreaking new consultative approach to maximize the value of IT service management (ITSM) solutions for enterprises without the burdensome costs and staffing requirements typically associated with high-level IT consultancy. With the launch of a free online evaluation and assessment tool, SolarWinds now offers enterprises a deeper understanding of their current ITSM practices and provides a tailored, actionable roadmap toward operational excellence, cost reduction, and superior service delivery.

While most enterprises today leverage

ITSM solutions to simplify day-to-day IT operations, standardize processes, and streamline workflows, ongoing challenges prevent them from realizing ITSM's full potential. The SolarWinds ITSM Maturity Model provides an unparalleled way for IT professionals to understand, evaluate, and advance their technical and strategic readiness to deal with complexities and resolve issues amid escalating IT complexities.

"Today, IT services are the backbone of every modern enterprise, yet many don't realize the full, strategic potential of ITSM," said Cullen Childress, Senior VP of Product at SolarWinds. "SolarWinds



is proud to offer the best of both worlds: the ease and simplicity of our solutions, complemented by the kind of expert, consultative support typically associated with much higher price tags. Our goal is to demystify the complexities of IT service management, making the journey towards maturity as seamless and straightforward as possible."

GLOBAL BLOCKCHAIN INTELLIGENCE LEADER, CHAINALYSIS, ESTABLISHES REGIONAL HQ IN DUBAI

Chainalysis, the blockchain intelligence

platform, has inaugurated its headquarters for Southern Europe, Middle East, Central Asia, and Africa in Dubai. This move follows three years of exponential growth in the region for the company, as it has established itself as the leading provider of crypto investigation, Web3 growth, and crypto risk solutions to government and private sector entities.

Chainalysis provides data, software, services, and research to government agencies, virtual asset service providers, financial institutions, and insurance and cybersecurity companies in over 70 countries. The company's data has helped solve some of the world's most high-profile criminal cases involving North Korean hacking, ransomware, darknet market activity, and more, resulting in seizures of more than US\$10B by law enforcement agencies.



In support of the UAE's push to be a global crypto hub, Chainalysis has been actively engaging with key government stakeholders to offer guidance and best practices for the development of the regulations and frameworks necessary to foster a thriving crypto ecosystem. This includes partnering with the UAE's Ministry of Artificial Intelligence, Digital Economy and Remote Work Applications to set up a Centre of Excellence that helps government

employees upskill on blockchain technologies. Most recently, Chainalysis signed an MoU with Emirates NBD to support the banking leader's Digital Asset Lab program.

"The UAE government has spearheaded the crypto revolution with forward-focused regulations, and business-friendly policies. At Chainalysis, we have been actively driving the maturity of the region's crypto ecosystem in line with the latest developments across the globe," said Michael Gronager, CEO at Chainalysis. "The true potential and value of cryptocurrencies lies in their ability to transfer value, and we're seeing an upward trend of overall transfer activity. Utilisation is the underlying success story of the industry, and the UAE is strongly positioned to lead innovation with novel use cases that deliver tangible value to consumers and businesses."

KASPERSKY RELEASES ESG REPORT FOR H2 2022-2023

In its new Sustainability report for H2

2022 and 2023, Kaspersky reveals the key results of the company's sustainable development initiatives and projects in the respective period. The report encompasses five strategic areas identified as the company's ESG priorities: namely safer cyberworld, future tech, safer planet, people empowerment, and ethics and transparency.

Pursuing its mission to build a safer world for more than 25 years, Kaspersky has been an active contributor to the creation of a more sustainable world not only by creating protection technologies, but also by investing in numerous ESG projects. In 2023, Kaspersky presented the company's first Sustainability report, which was drafted in accordance with international GRI and SASB standards.

Kaspersky plays a pivotal role in shaping a cyber resilient future by

combating threats with its world-class security solutions and services. Operating in more than 200 countries and territories, Kaspersky gathers real-time intelligence from across the globe, dealing with an extensive array of security challenges in threat landscape. These efforts result in the detection of 411,000 new malicious files every day. Overall, Kaspersky prevented more than 437 million cyberattacks during the reporting period.

kaspersky

One of the most serious threats to businesses of all sizes is ransomware. To protect organizations from this urgent threat, Kaspersky experts discovered 43 new ransomware families and more than 23,000

of its modifications throughout H2 2022 and 2023. In 2023 alone, cybercriminals attempted attacking thousands of users, including 53,000 corporate ones and about 6,000 users associated with small and mediumsized businesses.

Kaspersky researchers have also noted a steady increase in the number of stalkerware attacks – programs used to covertly monitor victims through their personal devices. In particular, Kaspersky security solutions detected more than 31,000 attacks on users worldwide. The victims of such attacks are most frequently women in abusive relationships. Kaspersky is working to address the issue of cyberstalking by partnering with non-profit organizations, industry experts, research companies, and government agencies around the world.

ESET INCLUDED AMONG NOTABLE VENDORS IN MOBILE THREAT DEFENSE SOLUTIONS LANDSCAPE REPORT

ESET Research has released its

deep-dive investigation into one of the most advanced server-side malware campaigns, which is still growing and has seen hundreds of thousands of compromised servers in its at least 15-year-long operation. Among the activities of the infamous Ebury group and botnet over the years has been the spread of spam, web traffic redirections, and credential stealing. In recent years it has diversified to credit card and cryptocurrency theft. Additionally, Ebury has been deployed as a backdoor to compromise almost 400,000 Linux, FreeBSD, and OpenBSD servers; more than 100,000 were still compromised as of late 2023. In many cases, Ebury operators were able to gain full access



to large servers of ISPs and well-known hosting providers.

Ten years ago, ESET published a white paper about Operation Windigo, which uses multiple malware families working in combination, with the Ebury malware family at its core. In late 2021, the Dutch National High Tech Crime Unit (NHTCU), part of the Netherlands national police, reached out to ESET regarding servers in the Netherlands suspected of being

compromised with Ebury malware. Those suspicions turned out to be well-founded and with NHTCU's assistance, ESET Research has gained considerable visibility into operations run by the Ebury threat actors.

"Following the release of the Windigo paper in early 2014, one of the perpetrators was arrested at the Finland-Russia border in 2015, and later extradited to the United States. While initially claiming innocence, he eventually pleaded guilty to the charges in 2017, a few weeks before his trial at the U.S. District Court in Minneapolis was set to proceed, and where ESET researchers were scheduled to testify," said Marc-Etienne M. Léveillé, the ESET researcher who investigated Ebury for more than a decade.

www.tahawultech.com MAY 2024



A HOLISITIC APPROACH TO SECURITY

RAM NARAYANAN, COUNTRY MANAGER MIDDLE EAST AT CHECK POINT, DISCUSSES THE COMPANY'S CUTTING-EDGE SECURITY SOLUTIONS AND HOW THEY PROVIDE COMPANIES WITH A 360-DEGREE VIEW OF THEIR SECURITY POSTURE.

hat did it mean for Check Point to participate in GISEC this year?

We were super excited to be part of the GISEC platform. It was three exciting days for us to network with our partners and showcase our unique technology that addresses their challenges. We were thrilled to be part of this event.

What products or solutions did you showcase at GISEC this year?

We showcased several solutions to address the current cybersecurity landscape. With AI and cloud becoming more prevalent, we highlighted the Check Point Infinity platform, which consolidates cybersecurity technologies into one unified, AIdriven, cloud-delivered platform. Specifically, we introduced Infinity Al Co-Pilot, which automates security operations to simplify daily tasks, and AI Playblocks, which enhances prevention capabilities. These technologies, part of our Infinity architecture, aim to address the evolving needs of our customers.

Additionally, we focused on three key pillars of the Infinity platform: Quantum for network security, CloudGuard for cloud security, and Harmony for user and access security. These solutions collectively form a comprehensive security framework.

How is Check Point integrating emerging technologies, especially AI, into its solutions portfolio?

We integrate AI in two main ways: The first is by enhancing our solutions and addressing the AI adoption challenges our customers face. Our AI-driven tools, like Infinity AI Co-Pilot and AI Playblocks, automate security operations and prevent threats, streamlining processes and improving response times.

Moreover, we deploy agents to rapidly identify threats in a fast-paced cybersecurity landscape. As AI and large language models introduce new threat vectors, our collaborations with Microsoft and NVIDIA enhance our AI capabilities to address these emerging challenges. Our goal is to ensure AI can be utilized securely within enterprises.

What are the biggest challenges businesses in the region face when implementing new technologies?

Businesses face several challenges, including a skills gap due to the evolving technology landscape, difficulties in integrating new technologies with

THE CHECK POINT
UAE INFINITY PORTAL
ADDRESSES THE NEED
FOR A UNIFIED SECURITY
PLATFORM.

existing systems, and the need for efficient operations. To address these, we provide knowledge transfer and support to elevate their architectural implementations. Our Check Point Infinity platform simplifies integration by offering a consolidated architecture that enhances visibility and efficiency across networks, clouds, and user systems.

Tell us about Check Point UAE Infinity Portal and how it helps businesses in the region enhance their security posture.

The Check Point UAE Infinity Portal addresses the need for a unified security platform. While many vendors offer point solutions, enterprises often struggle with managing multiple technologies. Our platform provides a 360-degree view of their security posture, addressing external threats and ensuring comprehensive protection.

Recognizing UAE's data regulations, we have invested in local data centers to host our services, ensuring data residency and compliance. The Infinity Portal offers a single platform for network security, end-user protection, email security, and cloud security, all managed locally. This unified approach simplifies security management for enterprises and enhances their overall security posture.

11

www.tahawultech.com MAY 2024



PUBLIC SECTOR IT INVESTMENT FOCUSED ON AI, RANSOMWARE PROTECTION.

AND OPERATIONAL EFFICIENCY: NUTANIX

utanix, a leader in hybrid multicloud computing, has announced the findings of its sixth annual global Public Sector Enterprise
Cloud Index (ECI) survey and research report, which measures enterprise progress with cloud adoption in the industry. The research showed that Public Sector IT leaders expect substantial nearterm adoption of multiple IT operating models (87%), yet current usage (57%) is slightly behind the average compared to other industries (60%).

This year's Public Sector ECI report

revealed that the use of hybrid multicloud models in the industry is forecasted to quadruple over the next one to three years as IT decision-makers at public sector organizations look to modernize data centers into private clouds and preserve choice in public cloud deployments.

Primary drivers for IT infrastructure investments in the next year include ransomware prevention, IT modernization, and AI strategy support to gain flexibility and access new capabilities to improve operations and enable mission success.

Public sector survey respondents were asked about their current cloud

challenges, how they're running business and mission critical applications today, and where they plan to run them in the future. Key findings from this year's report include:

- Hybrid multicloud deployments lag behind other industries. The vast majority of both public sector organizations (85%) and all sectors (90%) agreed that their organizations now embrace cloud-smart IT deployment strategies. However, just 8% of global public sector organizations reported using a hybrid multicloud approach.
- When public sector organizations are investing in IT infrastructure, protection from ransomware is the primary driver. Respondents in the public sector most often chose the infrastructure's ability to protect against ransomware and other malware as their single top priority (17%). This factor was followed by the infrastructure's performance/response time potential (15%) and its ability to allow IT to flexibly move workloads across private and public cloud platforms (14%).
- Security and compliance are the biggest drivers of application relocation and the top priority for CIO/CTOs, as public sector organizations recover from high rates of ransomware attacks. The vast majority of ECI respondents—92% in the public sector group and 95% globally—said they had moved one or more applications to a different IT environment in the past 12 months.
- Al use is ramping up, though issues concerning data privacy and best practices persist. Though Al support ranked fairly low on public sector infrastructure purchasing criteria, respondents expressed high levels of interest in the technology elsewhere. 80% of the public sector said they expect to increase their investments in Al technology in the next year. About a third (32%) said that those investment increases would be "significant."

 ■

DRIVING DIGITAL PROGRESS

JOJI SAMUEL HAS BEEN APPOINTED THE NEW CEO OF GEEKS. AN INTEGRAL PART OF THE GEEKS FAMILY SINCE 2018, HE IS KNOWN FOR HIS EXTENSIVE UNDERSTANDING OF THE IT LANDSCAPE AND CUSTOMER CHALLENGES. HE SPEAKS TO ANITA JOSEPH ABOUT HIS ROLE AND RESPONSIBILITIES AND HOW GEEKS IS REDEFINING THE IT INDUSTRY BY BEING A TRUSTED IT PARTNER FOR BUSINESSES IN THE REGION.



The CEO Role

As CEO of Geeks, my appointment brings added responsibilities.

- Oversee strategic direction, operational excellence, and technology innovation.
- Maximize value from our service offerings, to foster strong client relationships.
- Drive market share expansion, service expansion and regional expansion.
- Solidify Geeks' position as a trusted partner in digital transformation for SMBs.

Career Background

With a career deeply rooted in customer service, sales, account management, operations, and leadership, I bring a wealth of experience in understanding all aspects of the business. This diverse background has proven invaluable in driving our mission of "Simplifying Technology Experiences for All," my passion lies in empathizing with customers, walking in their shoes, and crafting simple yet highly effective technology solutions that are easy to understand, quick to deploy, highly impactful and costeffective. Prior to assuming the role of CEO at Geeks, I've successfully navigated multiple roles within the business, leveraging my ground knowledge to innovate and streamline technology solutions across industries.

www.tahawultech.com MAY 2024 1



Geeks Reinvention of IT

Geeks is revolutionizing the world of IT by ensuring that technology serves as an enabler, not a barrier, for businesses. Our mission is to make technology accessible, reliable, and user-friendly for everyone, allowing SMBs to focus on their growth while we navigate the complexity of technology. In short, make enterprise grade IT support available for small and medium businesses.

Our aim is to redefine the traditional IT support model with a streamlined managed service approach, delivering value at a predictable cost and guaranteeing maximum ROI. This is achieved through:

- i) Swift Support
- ii) Personalized Service
- iii) Strategic Guidance Comparable to CIO-level Advice
- iv) Technology Stack for Success, Security and Compliance.
- v) Comprehensive IT Lifecycle Management.

Leading IT-related causes of business downtime

Here are top IT related causes for downtime in my opinion

• Cybersecurity Incidents:

Threats exposing sensitive data, leading to financial loss and reputational harm.

- Unplanned Hardware Failures:
 Unexpected crashes or malfunctions causing system downtime and data loss.
- Data Loss and Corruption:
 Accidental deletion or corruption resulting in critical data loss.
- Inefficient IT Infrastructure: Subpar infrastructure causing network outages and slow performance.
- Human Error: Employee
 mistakes like accidental data
 deletion or misconfigured
 systems disrupting operations.

Additionally here are factors that amplify the downtime and its impact:

- Siloed IT Approach:
 Disconnected systems impairing collaboration and efficiency.
- Lack of IT Strategy: Absence of a clear IT roadmap causing inefficiencies.
- Insufficient IT Support: Lack of

- technical expertise leading to issue resolution delays.
- Absence of Backup and Disaster Recovery Plan: No safeguard against data loss or system downtime.

Understanding these factors is crucial for SMBs to mitigate risks and ensure uninterrupted operations.

How important is the Middle East region for Geeks? What are the opportunities and challenges?

The Middle East's demand for managed services is booming due to its drive for digital progress, better technology, stronger cybersecurity, wider cloud use, and a focus on sustainability. Geeks sees this market as crucial, aiming to offer tailored solutions that meet the region's evolving needs and help businesses thrive.

- Opportunities
 - o Rapidly expanding SMB sector
 - Significant demand for cybersecurity services
 - o Increasing emphasis on digital transformation
- Challenges
 - o Talent Shortage
 - o Integration and Regulatory
 Issues
 - o Commoditization Of Services and Competition 1

OUR MISSION IS TO MAKE TECHNOLOGY
ACCESSIBLE, RELIABLE, AND USER-FRIENDLY
→ FOR EVERYONE, ALLOWING SMBS TO FOCUS ON THEIR GROWTH.



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

Cybersecurity, everywhere you need it

www.fortinet.com







www.tahawultech.com MAY 2024

AI IS BEING DEPLOYED ACROSS VARIOUS CYBERSECURITY APPLICATIONS, FROM THREAT DETECTION TO INCIDENT RESPONSE.

monitor and analyze endpoint activity to detect malicious behavior. Similarly, Al-powered security information and event management (SIEM) systems can correlate data from multiple sources, identifying threats that might be missed by traditional methods.

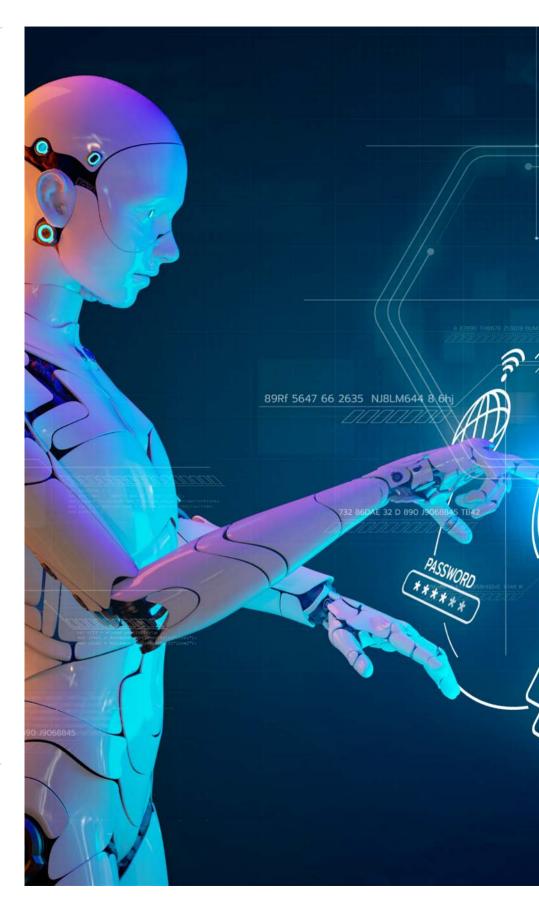
In the realm of network security, Al is enhancing intrusion detection systems (IDS) and intrusion prevention systems (IPS). These systems leverage Al to detect unusual network traffic patterns, quickly identifying and mitigating potential threats. Additionally, Al is playing a pivotal role in automated threat hunting, where it scans for indicators of compromise (IoCs) and potential vulnerabilities, reducing the workload on cybersecurity teams.

Challenges and Ethical Considerations

While AI offers significant benefits, its integration into cybersecurity also presents challenges. One major concern is the potential for AI systems to be fooled by adversarial attacks, where attackers manipulate data inputs to deceive the AI. This highlights the need for robust AI training and validation processes to ensure resilience against such attacks.

Ethical considerations are also paramount. The deployment of AI in

INDUSTRY LEADERS
AND EXPERTS ARE
OPTIMISTIC ABOUT
THE FUTURE OF AI IN
CYBERSECURITY.





cybersecurity raises questions about privacy, data security, and the potential for misuse. Organizations must navigate these issues carefully, implementing AI solutions that are transparent, explainable, and compliant with relevant regulations.

Expert Opinions and Predictions

Industry leaders and experts are optimistic about the future of AI in cybersecurity. According to Dr. John Smith, a cybersecurity researcher, "AI has the potential to transform our

THE DEPLOYMENT OF
AI IN CYBERSECURITY
RAISES QUESTIONS

→ ABOUT PRIVACY,
DATA SECURITY, AND
THE POTENTIAL FOR
MISUSE

approach to cybersecurity, offering unprecedented capabilities in threat detection and response." However, he also cautions that "we must remain vigilant about the ethical implications and ensure that AI systems are secure and trustworthy."

Predictions for the future include the development of more sophisticated AI-driven security platforms that can autonomously manage and respond to threats. Experts also foresee increased collaboration between AI systems and human analysts, leveraging the strengths of both to create a more effective cybersecurity defense.

Practical Implementation: Steps for Businesses

For businesses looking to adopt AI-driven cybersecurity solutions, there are several key steps to ensure successful implementation. First, organizations should conduct a thorough assessment of their current security posture and identify areas where AI can add value. Next, selecting the right AI tools and

AI IS POISED TO PLAY A
TRANSFORMATIVE ROLE
IN CYBERSECURITY,

OFFERING NEW
CAPABILITIES IN
THREAT DETECTION,
PREVENTION, AND
RESPONSE.



platforms is crucial, considering factors such as scalability, integration capabilities, and vendor support.

Training and education are also essential. Cybersecurity teams need to understand how to work with AI systems and interpret their outputs effectively. Finally, businesses should establish robust monitoring and evaluation processes to continuously assess the performance and effectiveness of AI-driven solutions.

The Future of AI in Cybersecurity

Al is poised to play a transformative role in cybersecurity, offering new capabilities in threat detection, prevention, and response. While challenges and ethical considerations remain, the potential benefits of Aldriven security solutions are immense. As Al continues to evolve, it will become an integral part of the cybersecurity landscape, helping organizations stay ahead of ever-evolving cyber threats.

www.tahawultech.com MAY 2024

CYBERCRIMINALS EXPLOITING NEW INDUSTRY VULNERABILITIES 43% FASTER THAN 1H 2023: FORTINET



ortinet, the global cybersecurity leader driving the convergence of networking and security, has announced the release of the FortiGuard Labs 2H 2023 Global Threat Landscape Report. The latest semiannual report is a snapshot of the active threat landscape and highlights trends from July to December of 2023, including analysis on the speed with which cyber attackers are capitalizing on newly identified exploits from across the cybersecurity industry and the rise of targeted ransomware and wiper activity against the industrial and OT sector.

Derek Manky, Chief Security Strategist and Global VP Threat Intelligence,

FortiGuard Labs said, "The 2H 2023 Global Threat Landscape Report from FortiGuard Labs continues to shine a light on how quickly threat actors are taking advantage of newly disclosed vulnerabilities. In this climate, both vendors and customers have a role to play. Vendors must introduce robust security scrutiny at all stages of the product development life cycle and dedicate themselves to responsible radical transparency in their vulnerability disclosures. With over 26,447 vulnerabilities across more than 2,000 vendors in 2023 as cited by NIST, it is also critical that customers maintain a strict patching regimen to reduce the risk of exploitation."

Key findings from the second half of 2023 include:

- Attacks started on average 4.76 days after new exploits were publicly disclosed: Like the 1H 2023 Global Threat Landscape Report, FortiGuard Labs sought to determine how long it takes for a vulnerability to move from initial release to exploitation, whether vulnerabilities with a high Exploit Prediction Scoring System (EPSS) score get exploited faster. and whether it could predict the average time-to-exploitation using EPSS data. Based on this analysis, the second half of 2023 saw attackers increase the speed with which they capitalized on newly publicized vulnerabilities (43% faster than 1H 2023).
- Some N-Day vulnerabilities remain unpatched for 15+ years: It's not just newly identified vulnerabilities that CISOs and security teams must worry about. Fortinet telemetry found that 41% of organizations detected exploits from signatures less than one month old and nearly every organization (98%) detected N-Day vulnerabilities that have existed for at least five years.
- Less than 9% of all known endpoint vulnerabilities were targeted by attacks: In 2022,



FortiGuard Labs introduced the concept of the "red zone." which helps readers better understand how likely it is that threat actors will exploit specific vulnerabilities. To illustrate this point, the last three Global Threat Landscape Reports have looked at the total number of vulnerabilities targeting endpoints. In 2H 2023, research found that 0.7% of all CVEs observed on endpoints are actually under attack, revealing a much smaller active attack surface for security teams to focus on and prioritize remediation efforts.

 44% of all ransomware and wiper samples targeted the industrial sectors: Across all of Fortinet's sensors, ransomware detections dropped by 70% compared to the first half of 2023. The observed slowdown in ransomware over the last year can best be attributed to attackers shifting away from the traditional "spray and pray" strategy to more of a targeted approach, aimed largely at the energy, healthcare, manufacturing, transportation and logistics, and automotive industries.

 Botnets showed incredible resiliency, taking on average 85 days for command and control (C2) communications to cease after first detection: While bot

VENDORS MUST INTRODUCE ROBUST SECURITY
SCRUTINY AT ALL STAGES OF THE PRODUCT

→ DEVELOPMENT LIFE CYCLE AND DEDICATE THEMSELVES
TO RESPONSIBLE RADICAL TRANSPARENCY IN THEIR
VULNERABILITY DISCLOSURES.

traffic remained steady relative to the first half of 2023, FortiGuard Labs continued to see the more prominent botnets of the last few years, such as Gh0st, Mirai, and ZeroAccess, but three new botnets emerged in the second half of 2023, including: AndroxGh0st, Prometei, and DarkGate.

38 of the 143 advanced persistent threat (APT) groups listed by MITRE were observed to be active during 2H 2023: FortiRecon, Fortinet's digital risk protection service, intelligence indicates that 38 of the 143 Groups that MITRE tracks were active in the 2H 2023. Of those, Lazarus Group, Kimusky, APT28, APT29, Andariel, and OilRig were the most active groups. Given the targeted nature and relatively short-lived campaigns of APT and nation-state cyber groups compared to the long life and drawn-out campaigns of cybercriminals, the evolution and volume of activity in this area is something FortiGuard Labs will be tracking on an ongoing basis.

Turning the Tide Against Cybercrime

With the attack surface constantly expanding and an industrywide cybersecurity skills shortage, it's more challenging than ever for businesses to properly manage complex infrastructure composed of disparate solutions, let alone keep pace with the volume of alerts from point products and the diverse tactics, techniques, and procedures threat actors leverage to compromise their victims.

It's through constant technology innovation and collaboration across industries and working groups, such as Cyber Threat Alliance, Network Resilience Coalition, Interpol, the World Economic Forum (WEF) Partnership Against Cybercrime, and WEF Cybercrime Atlas, that will collectively improve protections and aid in the fight against cybercrime globally.

www.tahawultech.com MAY 2024 **2**

MOST ORGANIZATIONS HIT BY RANSOMWARE WORKED WITH LAW ENFORCEMENT: SOPHOS



ophos, a global leader of innovative security solutions that defeat cyberattacks, released additional findings from its annual "State of Ransomware 2024"

survey. According to the report, among organizations surveyed, 97% of those hit by ransomware over the past year engaged with law enforcement and/or official government bodies for help with the attack.

In addition, more than half (59%) of those organizations that did engage with law enforcement found the process easy or somewhat easy. Only 10% of those surveyed said the process was very difficult.

Based on the survey, impacted organizations reached out to law enforcement and/or official government bodies for a range of assistance with ransomware attacks. Sixty-one percent reported they had received advice on dealing with ransomware, while 60% received help investigating the attack. Fifty-eight percent of those that had their data encrypted received help from law enforcement to recover their data from the ransomware attack.

"Companies have traditionally shied away from engaging with law enforcement for fear of their attack becoming public. If they are known to have been victimized it could impact their business reputation and make a bad situation worse. Victim shaming has long been a consequence of an attack, but we've made progress on that front, both within the security community and at the government level. New regulations on cyber incident reporting, for example, appear to have normalized engaging with law enforcement, and this survey data shows organizations are taking steps in the right direction," said Chester Wisniewski, director, Field CTO, Sophos. "If the public and the private sectors can continue to galvanize as a group effort to help businesses, we can continue to improve our ability to recover quickly and gather intelligence to protect others or even potentially hold those conducting these attacks responsible."

Recent in-the-field findings from Sophos X-Ops' Active Adversary report highlighted the continued threat of ransomware to small-and-medium sized businesses. Data from more than 150 incident response (IR) cases in 2023 found that ransomware was, for the fourth year running, the most frequently encountered attack type, occurring in 70% of IR cases Sophos X-Ops investigated.



"While improving cooperation and working with law enforcement after an attack are all good developments, we need to move from simply treating the symptoms of ransomware to preventing those attacks in the first place. Our most recent Active Adversary report showed that many organizations are still failing to implement key security measures that can demonstrably reduce their overall risk profile; this includes patching their devices in a timely manner and enabling multi-factor authentication. From the law enforcement side, while they have had some recent successes with takedowns and arrests from LockBit to Qakbot, these successes have proven to be more akin to temporary disruptions than longer term or permanent wins.

"Criminals are successful in part due to the scale and efficiency with which they operate. To beat them back, we need to match them in both these areas. That means that, going forward, we need even

greater collaboration, both within the private and public sector—and we need it at a global level," said Wisniewski.

"Today's threat environment is constantly evolving—and it's more severe and more complex than ever before. The bad guys aren't constrained by international borders, so we shouldn't be, either.

"At the Bureau, we've been doubling down in particular on our work with the private sector, in their capacity as victims of cyberattacks, of course, because the mission of the FBI always has been—and always will be—victim-centric—but also as integral partners, who can share valuable information about threats and trends, and, increasingly, join in our operations themselves," said Christopher Wray, FBI director.

Data for the State of Ransomware 2024 report comes from a vendor-agnostic survey of 5,000 cybersecurity/IT leaders conducted between January and February 2024. Respondents were based in 14 countries across the Americas, EMEA and Asia Pacific. Organizations surveyed had between 100 and 5,000 employees, and revenue ranged from less than \$10 million to more than \$5 billion. \$2

GOING FORWARD, WE NEED EVEN GREATER
COLLABORATION, BOTH WITHIN THE PRIVATE AND
PUBLIC SECTOR—AND WE NEED IT AT A GLOBAL LEVEL.

www.tahawultech.com MAY 2024 **2**



FUTURE OF IDENTITY SECURITY

RAHIL GHAFFAR, VP – EMEA, WHITESWAN SECURITY TELLS ANITA JOSEPH HOW IT'S CRUCIAL FOR ORGANIZATIONS TO PRIORITIZE IDENTITY SECURITY BECAUSE COMPROMISED CREDENTIALS CAN LEAD TO BREACHES THAT ARE DIFFICULT TO DETECT AND CAN CAUSE EXTENSIVE DAMAGE.

hat are some common examples of identity-centric attacks in today's digital landscape, and how do they exploit vulnerabilities in authentication systems?

In today's digital landscape, common identity-centric attacks include Phishing, Credential stuffing, Man in the Middle Attacks, SIM Swapping etc.

These attacks exploit vulnerabilities such as weak passwords, lack of multifactor authentication (MFA), or unsecured network connections, to gain unauthorized access to user accounts and sensitive data.

The global trend is also reflected in the Middle East and Africa region (MEA), with the use of valid local accounts and valid cloud accounts, making up the primary cause of cyberattacks against organizations in the region.

Exploiting valid accounts has become the path of least resistance for cybercriminals, with billions of compromised credentials accessible on the Dark Web today.

Could you explain how multifactor authentication (MFA) can mitigate the risks associated with identity-centric attacks, and what best practices organizations should follow when implementing MFA?

Traditional IAM solutions only are at the perimeter and therefore once the login completes there is no MFA activity or prompts. For example after login no one is prompted for an rdp to a server he has not accessed before. For Traditional PAMs it is hard to extend identity centric defences to the lowest granularity. For MFA to be effective there should be

- Layered Defense: MFA requires at least two forms of evidence to verify a user's identity, making unauthorized access considerably more difficult for attackers even if they obtain one credential, like a password.
- 2. **Diverse Factors:** Organizations should use a combination of something the user knows (password), something they have (security token or TPM chip of Laptop), and something they are (biometrics).
- 3. Adaptive Authentication:
 Implement adaptive MFA
 that adjusts authentication
 requirements in response to user
 behavior and risk assessment.
- Education and Training: Educate
 users on the importance of MFA
 and guide them through setup and
 usage to ensure compliance and
 proper use.

How do identity-centric attacks differ from traditional cybersecurity threats, and why is it crucial for organizations to prioritize identity security in their defense strategies?

Identity-centric attacks specifically target the credentials and identity attributes of individuals to gain unauthorized access, differing from traditional threats that often focus on penetrating network defenses or exploiting software vulnerabilities. These attacks are more personalized and can bypass conventional security measures if identity security is weak. Remember Humans are the weakest link here. Ensuring that MFA is used and access privileges of users and admins are managed is extremely essential.

It's crucial for organizations to prioritize identity security because compromised credentials can lead to breaches that are difficult to detect and can cause extensive damage. Identity security ensures that the right individuals access the right resources at the right times for the right reasons, aligning with the principle of least privilege and reducing the attack surface.

What role does user education play in preventing identity-centric attacks, and what are some effective methods for raising awareness about the importance of secure authentication practices?

User education is pivotal in preventing identity-centric attacks, as these often exploit user behavior. Effective awareness programs can significantly reduce such risks. Methods include:

Regular Training Sessions:

IT'S CRUCIAL FOR ORGANIZATIONS TO PRIORITIZE IDENTITY SECURITY BECAUSE COMPROMISED

CREDENTIALS CAN LEAD TO BREACHES THAT ARE DIFFICULT TO DETECT AND CAN CAUSE EXTENSIVE DAMAGE.

- Conduct workshops to educate users on the latest threats and safe practices.
- **Simulated Attacks:** Run simulated phishing exercises to teach users how to recognize and respond to attacks.
- Engaging Content: Use multimedia content like videos and infographics to make learning about cybersecurity engaging.
- Updates and Reminders: Send out regular updates and reminders about secure authentication practices.
- Clear Guidelines: Provide clear, concise guidelines on creating strong passwords and protecting credentials.

Can you discuss emerging technologies or trends that are shaping the future of identity-centric security, and how organizations can adapt their security measures to address these advancements?

Emerging technologies are indeed redefining identity-centric security. Many Enterprises and Govt entities are now beginning to use Identity Centric Zero Trust Network Access (ZTNA). shifting focus from traditional models to prioritize user identity and context. This evolution from password dependency to a model that continuously verifies user identities and device health, adopting least-privilege access, and tailoring adaptive policies, enhances security, reduces attack surfaces, and aligns with the dynamic nature of threats, offering a more resilient and user-friendly approach to safeguarding against unauthorized access in various environments, from cloud to IoT. It's important to add here that a simple ZTNA solution doesn't cut it for users and admins – third party access to internal infra is a nightmare and managing user cloud entitlements and their access to cloud infra is a big issue. Managing these diverse use cases while ensuring connectivity needs a different approach.

www.tahawultech.com MAY 2024 27

PROOFPOINT SETS NEW STANDARDS IN EMAIL SECURITY

roofpoint, Inc., a leading cybersecurity and compliance company, has unveiled two industryfirst innovations that redefine email security with the most comprehensive and effective end-to-end email protection across the entire email delivery chain. Uniquely combining new pre-delivery, click-time, and post-delivery detections, Proofpoint's enhanced core email security packages now include:

- The industry's first and only pre-delivery defense against both social engineering threats and malicious links and:
- New adaptive email security capabilities, offering a fully integrated layer of behavioral Al-based defense post-delivery to stop targeted threats such as lateral internal phishing and advanced email fraud for the most at-risk employees—all while offering seamless API integration with Microsoft 365

Proofpoint's new semantic, Albased detection innovations provide comprehensive protection before they can reach Microsoft 365 and Google Workplace inboxes and do harm. Leveraging NexusAl, Proofpoint's proprietary AI engine built on trillions of data points, pre-delivery LLMbased detection enables organizations to stop payloadless social engineering threats such as advanced email fraud and malicious links.



Now part of Proofpoint's detection ensemble across all its email security products, pre-delivery semantic analysis interprets a threat actor's message intent regardless of word variation or language used. This optimizes Proofpoint's NexusAI-based detection models by 10X, with close to nil additional processing time. Paired with Proofpoint's recent release of the industry's first pre-delivery suspicious URL hold and sandboxing capability, these enhancements create

the most formidable set of defense-in-depth measures available for organizations to prevent attacks from reaching their targets.

Adaptive Email Security:

Proofpoint Adaptive Email Security is an Integrated Cloud Email Security (ICES) solution that delivers an additional layer of behavioral AI-based detection of advanced threats, including BEC, social engineering, and lateral phishing messages, offering seamless API integration with Microsoft 365. Adaptive Email Security can be applied to the riskiest users identified by Proofpoint's Targeted Attack Protection, or other potential high value targets, as informed by Proofpoint's unique human risk scoring.

Once deployed, Adaptive Email Security enriches all detections with easy-to-understand explanations about behavioral

anomalies observed. It automatically quarantines high confidence threats, while delivering real-time coaching using contextual warning banners to alert users to the risks in social engineering and BEC-type emails that don't contain an obvious malicious payload.

Adaptive Email Security is available on a rolling basis for select customers as part of Proofpoint's standard email security packages for an organization's most at-risk employees. 1





presents

INFOSEC & **CYBERSECURITY**

CONGRESS 2024

ABU DHABI

24th June 2024

👤 VOGO Abu Dhabi Golf Resort & Spa

DUBAI

25th June 2024

Habtoor Grand Resort, Autograph Collection, JBR Dubai

In today's era of digital business transformation, where 'digital' permeates every aspect of enterprise operations, security and risk management leaders are called upon to become catalysts for secure digital evolution. Also, security organizations must evolve into proactive collaborators, anticipating and mitigating cyber threats while also ensuring robust governance and regulatory compliance frameworks to drive overall enterprise excellence.

Then again, as cyber threats grow increasingly sophisticated, businesses must also contend with complex regulatory requirements aimed at safeguarding data privacy and security.

The Infosec & Cybersecurity Congress 2024, hosted by ISACA UAE & Tahawultech serves as a vital platform for addressing these challenges head-on. Throughout the event, attendees will engage in discussions and presentations exploring innovative approaches to cybersecurity governance, risk management, and compliance in the digital age. Join us as we pave the way for a secure and compliant digital future.

GOLD SPONSOR



SILVER SPONSOR



OFFICIAL PUBLICATIONS

HOSTED BY





Securaty

🗱 tahawultech.com



AN INTELLIGENT APPROACH TO SECURITY

SERKAN YUSUF, DIRECTOR OF SERVICES AT OTIFYD, TELLS TAHAWULTECH ABOUT OTIFYD'S CUTTING-EDGE CYBERSECURITY SERVICES AND SOLUTIONS THAT LEVERAGE STRATEGY TO DRIVE PEOPLE, PROCESS, INFORMATION AND TECHNOLOGY ADVANCEMENT.

ould you tell us about the products or solutions you're showcasing here at the event?

OTIFYD is a dedicated

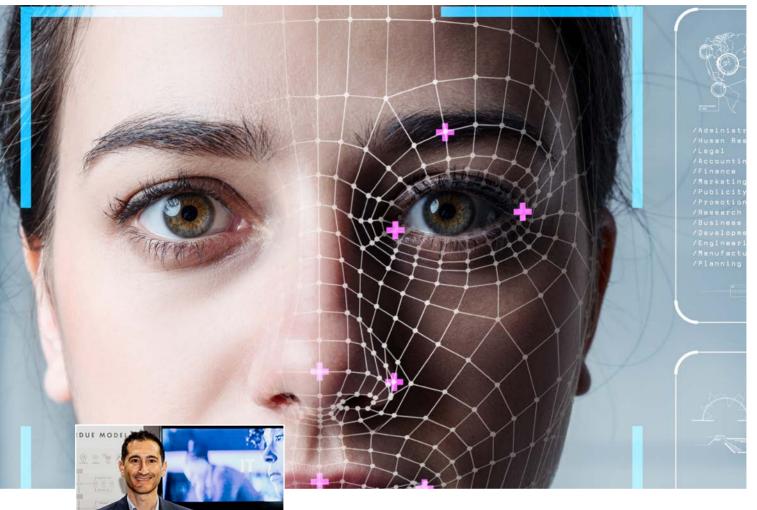
oTIFYD is a dedicated cybersecurity consultancy firm specializing in providing professional services, solutions, and training to

industrial clients and organizations.
From a services standpoint, we
offer a comprehensive range, from
consultancy and risk assessments
to more technical offerings like
penetration testing and Incident
Response Management. Our solutions
portfolio involves partnering with

Best-In-Breed providers to deliver end-to-end consultancy, from design to deployment.

Why do you think events like GISEC are important?

Events like GISEC are crucial for us at OTIFYD because they allow us to connect



with potential clients, understand their pain points, and identify prevalent themes and trends in the market. This insight helps us focus our efforts where they're needed most.

How is your firm integrating emerging technologies, particularly AI, into your solutions portfolio?

We leverage AI extensively in our services for tasks like data analysis and asset identification, although we're mindful of confidentiality constraints. Many of our partners are also incorporating AI into threat intelligence and asset discovery solutions to enhance threat detection and risk profiling capabilities.

What do you see as the single most important security trend today?

Al is certainly a prominent theme at JSOC and rightfully so, given its potential to revolutionize cyber defense.

OTIFYD IS A DEDICATED CYBERSECURITY

CONSULTANCY FIRM SPECIALIZING IN PROVIDING

PROFESSIONAL SERVICES, SOLUTIONS, AND TRAINING
TO INDUSTRIAL CLIENTS AND ORGANIZATIONS.

Additionally, regulatory compliance, especially in Operational Technology environments, is garnering increased attention as companies strive to manage risk more effectively.

What's the biggest challenge businesses in the region face when implementing a security framework or technology?

Governance remains a significant challenge, particularly in delineating ownership of OT cybersecurity within organizations. Bridging the gap between IT and engineering disciplines is crucial, and it's a challenge we often encounter. As a company with a background in industrial engineering, we're uniquely positioned to navigate this terrain, facilitating communication and collaboration toward the common goal of securing OT assets and environments.

www.tahawultech.com MAY 2024 **3**

HOW INTEGRATED ITSM SECURITY CAN SUPPORT THE ENGINE OF CHANGE

THESHAN MUDALY, SOLUTIONS ENGINEER - MEA, BEYONDTRUST



s the United Arab Emirates (UAE) has become more and more enmeshed in the cloud and its attendant platforms and services, much has changed. Infrastructure has changed. User experiences and expectations have changed. Costs have changed. And the way IT is delivered has changed. So much now is "aaS", and IT service management (ITSM) reflects this. The helpdesk has changed, as have ticketing systems. Modern ITSM is a slick, automated hum of quick responses and self-service options built around AI and ML, capable of adapting to the changing needs of users inside and outside the enterprise.

Modern ITSM delivers quicker identification of faults, better turnaround times, smoother change management, and lower costs, but also tighter collaboration between teams and shorter release cycles. ITSM in the post-COVID era has given UAE users "Bring Your Own Cloud" (BYOC), multi-cloud environments, and remote work. Modern ITSM can give us more of the things all businesses shoot for — productivity, collaboration, and innovation.

But the UAE did not get to where it is today without due care of the potholes on the road to success. The nation is a prime target for threat actors, intent on exploiting its young, Web-connected population and high average net worth. Modern ITSM must step up and meet

these challenges, securing service delivery by focusing on four main areas.

1. Social engineering

Helpdesk technicians receive more emails than almost anyone else in the organization. As such, they are low-hanging fruit to attackers, who will waste no time in deploying socialengineering tactics such as pretending to be a user in distress looking for a password reset. Helpdesks have recently even become the targets of MFA fatigue attacks — where legitimate users are spammed with second-factor confirmation requests in the hope they will get frustrated and confirm. The best countermeasure against social engineering is a combination of welltrained users and the right technologies. Identity management and privilegedaccess management (PAM) are ideal for this purpose.

2. Vulnerable remote access

To support UAE organizations' mass adoption of remote-work and remote-access tools, technologies such as VPN and RDP have (for the sake of expediency) found their way into use cases where they do not belong. VPNs, for example, lack auditing capabilities or granular control over sessions, so they are inappropriate for BYOD or third-party remote access. In all remote sessions, level and duration of access must be tightly controlled.

3. Poor credential hygiene

Helpdesks need to be quick — resolve the issue in front of you and move on to the next. Often, this requires using admin accounts. Shortcuts like storing credentials in plain text for quick and easy access can lead to disaster. The prevalence of such practices is of great concern to security professionals, as is the frequency with which they are found to be the root cause of an attack. It is also disturbingly common for the same password to be used across many high-privilege accounts.

4. Excess privileges

The cloud environments in which we all now operate have necessitated an authentication explosion that encourages password reuse and over-provisioning of entitlements. To combat this, we must enforce the principle of least privilege. This will not only secure ITSM processes but reduce errors and strengthen regulatory compliance. Each user, from the helpdesk to HR, should receive only those permissions necessary to do their job. No more; no less.

Take your medicine

Modern IT that works to a modern ITSM model, must have modern cybersecurity to match. If it does not, the whole stack will lapse into poor health. Security has to be woven into ITSM. Unfortunately, this often requires the unravelling of current protections to make way for a unified security suite that is free of silos. A tools glut means a lot of running around trying to visualize a problem or validate a red flag. IT admins and security analysts will burn out and may leave the organization, exacerbating the problem.

But with security baked into ITSM, the helpdesk, SOC, and others get security capabilities that apply the right policies automatically and frictionlessly. When procuring a platform that can weave itself neatly into your unique ecosystem, look for broad platform support (Windows, Linux, iOS, Android, and the rest) and

a system that can offer non-disruptive access to endpoints and applications from a single pane. Teams should be able to centralize, manage, and track privileges without end users being required to hop from application to application just to do their job. Any required credentials should be available securely to the service desk from within the ITSM solution while abiding by all best practices.

Just as modern ITSM leaves nobody behind, its integrated security should look after all parties — remote users, employees, and third parties. And they should all be able to gain access through the remote device of their choice while protecting all authorized ITSM approval flows — Incident, Change Request, Problem, and Request. And privileged actions such as configuration or change management should be done directly from a change request, thereby securing sessions but also enforcing change management to adhere to current authorized processes. This interwoven ITSM security provides end-to-end tracking and a documented history of access and workflow approvals. With each record tied to the relevant assets and privileged accounts, organizations will find auditing is much easier.

Engine of change

Just as MLOps and DevOps are now advised to consult the security team early and often, ITSM teams and helpdesks must recognize that their domain needs protecting too. This is especially true since across the Gulf and beyond, ITSM is now seen as the best and most practical way to deliver the IT function. And just as ITSM is a departure from old, siloed thinking, so must its security be integrated to ensure efficiency and adequate collaboration between stakeholders. When done well, an integrated ITSM security solution can reduce risk and be part of the engine of change. 🖡

MODERN IT THAT WORKS TO A MODERN ITSM MODEL, MUST HAVE MODERN CYBERSECURITY TO MATCH.

www.tahawultech.com MAY 2024 33



STAYING AHEAD OF THREATS

BERNARD MONTEL, EMEA TECHNICAL DIRECTOR AND SECURITY STRATEGIST AT TENABLE, TELLS ANITA JOSEPH HOW THE COMPANY LEVERAGES AI TO OFFER BEST-IN-CLASS SECURITY SOLUTIONS TO COMBAT THE LATEST CYBER THREATS.



ow does Tenable incorporate AI into its product offerings while staying ahead of the curve?

The role of AI in cybersecurity is paramount today, particularly with the advent of generative AI. Reflecting on my own experience, it's evident that Al has been a topic of discussion for quite some time. However, with the emergence of generative AI, we've entered a new era. Previously, Al primarily focused on analyzing existing data, but now, the landscape has evolved significantly. At Tenable, we've long recognized the potential of AI and have invested heavily in leveraging our core technologies to assess asset criticality and vulnerability risks. We've integrated data science modules and expanded our analytics capabilities to stay at the forefront of technological advancement.

The pivotal question now is how we effectively utilize AI. To this end, we've undertaken initiatives such as publishing reports and developing tools to assist the industry. It's imperative to acknowledge that attackers are already harnessing generative AI to craft sophisticated attacks, emphasizing the need for proactive defense measures. As defenders, our mission is clear: to empower our customers and security practitioners to swiftly understand and mitigate their exposure to emerging threats. We collect a plethora of data, including exposure data from IoT and Identity Cloud, enabling us to delve into intricate aspects like

toxic combinations and attack paths. This becomes particularly crucial in cloud environments, where identity management complexities abound. Our overarching goal is to equip users with intelligent tools that enable quick responses to evolving threats.

Tenable is the only exposure management platform providing complete visibility into IT and OT environments. Can you discuss this further?

Tenable stands out as the sole exposure management platform offering comprehensive visibility into both IT and OT environments. Our approach encompasses a DevOps strategy and a product suite covering various scopes. While our origins lie in IT, we've expanded into OT, becoming the pioneer in merging VM and OT capacities onto a single platform. By aggregating and normalizing data from diverse sources, we provide customers with a holistic, 360-degree view, facilitating governance-driven exposure management.

When it comes to cloud security, what key considerations should organizations keep in mind?

Transitioning to cloud security, organizations must recognize the need for a paradigm shift in their security strategies. Cloud environments introduce a plethora of unique challenges, ranging from serverless computing to containerization. Notably, identity management in the cloud poses significant complexities due

to the multitude of services across different cloud providers. To effectively mitigate exposures, organizations must prioritize visibility and comprehend misconfigurations.

What regional trends in cloud security can you highlight for us?

In terms of regional cloud security trends, a hybrid approach prevails, with not all organizations fully transitioning to the cloud. Consequently, investing in on-prem solutions remains imperative. Tenable is committed to supporting customers in both environments, offering visibility into cloud and on-prem assets alike. We understand the intricacies involved in managing such hybrid environments and provide tailored tools to streamline the process effectively.

Finally, regarding major threats facing the region, several trends warrant attention. Smaller organizations are increasingly targeted due to their associations with larger entities, often lacking adequate cybersecurity measures. Weaknesses in identity management remain a critical area of concern, with attackers exploiting vulnerabilities despite the presence of multi-factor authentication. Furthermore, critical infrastructures, particularly in healthcare, are prime targets for cyberattacks, given the sensitive nature of the data they handle. Organizations must prioritize bolstering their cybersecurity posture, particularly in these sectors, to effectively mitigate emerging threats and safeguard sensitive information.

www.tahawultech.com MAY 2024

Q1 2024 DD0S ATTACK TRENDS – CLOUDFLARE REPORT

loudflare, Inc., the security, performance, and reliability company helping to build a better Internet, has announced its 2024 Q1 DDoS report. This report includes insights and trends about the DDoS threat landscape — as observed across the global Cloudflare network, which is one of the largest in the world.

Starting 2024 with a bang

The first quarter of 2024 is just wrapped up, and, already, Cloudflare's automated defenses have mitigated 4.5 million DDoS attacks - an amount equivalent to 32% of all the DDoS attacks the company mitigated in 2023. Breaking it down to attack types, HTTP DDoS attacks increased by 93% YoY and 51% quarter-over-quarter (QoQ). Networklayer DDoS attacks, also known as L3/4 DDoS attacks, increased by 28% YoY and 5% QoQ.

DNS attacks surge by 80%

DNS-based DDoS attacks have become the most prominent attack vector and its share among all network-layer attacks continues to grow. In the first quarter of 2024, the share of DNS-based DDoS attacks increased by 80% YoY, growing to approximately 54%.

When analyzing the most common attack vectors, Cloudflare also checks for the attack vectors that experienced the largest growth but didn't necessarily make it into the top ten list. Among the top growing attack vectors (emerging



threats), Jenkins Flood experienced the largest growth of over 826% QoQ. Jenkins Flood is a DDoS attack that exploits vulnerabilities in the Jenkins automation server, specifically through UDP multicast/broadcast and DNS multicast services.

Top attacked industries

In the first quarter of 2024, the top attacked industry by HTTP DDoS attacks in North America was Marketing and Advertising. In Africa and Europe, the Information Technology and Internet industry was the most attacked. In the Middle East, the most attacked industry was Computer Software. In Asia, the most attacked industry was Gaming and Gambling. In South America, it was the Banking, Financial Services and Insurance (BFSI) industry. Last but not least, in Oceania, was the Telecommunications industry.

Globally, the Gaming and Gambling industry was the number one most targeted by HTTP DDoS attacks. Just over seven of every 100 DDoS requests that Cloudflare mitigated were aimed at the Gaming and Gambling industry. In second place, the Information Technology and Internet industry, and in third, Marketing and Advertising.

Largest sources of DDoS attacks

When analyzing the sources of HTTP DDoS attacks, Cloudflare looks at the source IP address to determine the origination location of those attacks.

In Q1 2024, the United States was the largest source of HTTP DDoS attack traffic, as a fifth of all DDoS attack requests originated from US IP addresses. China came in second, followed by Germany, Indonesia, Brazil, Russia, Iran, Singapore, India, and Argentina.



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.

1000+	20+	4000+	20+
Customers	Countries	Associates	Partnerships

USA | Singapore | Malaysia | Brunei | Taiwan | India | Oman | UAE | Qatar | Saudi Arabia

NETAPP'S 2024 CLOUD COMPLEXITY REPORT REVEALS

AI DISRUPT OR DIE ERA UNFOLDING GLOBALLY



etApp, the intelligent data infrastructure company, has released its second annual Cloud Complexity Report. The report looks at the experiences of global technology decision makers deploying AI at scale and shows a stark contrast between Al leaders and Al laggards. This year's report provides global insights into progress, readiness, challenges, and momentum since last year's report, what we can learn from both the AI leaders and Al laggards, and the critical role of a unified data infrastructure in achieving Al success.

"Al is only as good as the data that fuels it," said Pravjit Tiwana, General Manager and Senior Vice President of Cloud Storage at NetApp. "Both the Al leaders and Al laggards show us that in the prevailing hybrid IT environment, the more unified and reliable your data, the more likely your Al initiatives are to be successful."

There is a Significant Divide Between Al Leaders and Al Laggards

The report found a clear divide between AI leaders and AI laggards across several areas including:

Regions: 60% of AI-leading countries (India, Singapore, UK, USA) have AI projects up and running or in pilot, in stark contrast to 36% in AI-lagging countries (Spain, Australia/New Zealand, Germany, Japan).

Both AI leaders and AI laggards show a difference in their approach to AI:

- Globally, 67% of companies in Alleading countries report having hybrid IT environments, with India leading (70%) and Japan lagging (24%).
- Al leaders are also more likely to report benefits from Al, including a 50% increase in production rates, 46% in the automation of routine activities, and a 45% improvement in customer experience.

IT Costs and Data Security Emerge as Top Challenges but Won't Impede AI Progress

Rising IT costs and ensuring data security are the two of the biggest challenges in the AI era, but they will not block AI progress. Instead, AI leaders will scale back, cut other IT operations, or reallocate costs from other parts of the business to fund AI initiatives.

- Al leaders will also increase their cloud operations (CloudOps), data security and Al investments throughout 2024, with 40% of large companies saying Al projects have already increased IT costs
- Year over year, "increased cybersecurity risk" jumped 16% as a top concern from 45% to 61%, while all other concerns decreased
- To manage AI project costs, 31% of companies globally are reallocating funds from other business areas, with India (48%), UK (40%), and US (35%) leading this trend.

Security, AI, and CloudOps Drive 2024 Cloud Investments

As global companies, whether AI leaders or AI laggards, increase investments, they are relying on the cloud to support their goals.

- Companies reported that they expect to increase AI-driven cloud deployments by 19% from 2024 to 2030
- 85% of Al leaders plan to enhance their CloudOps automation over the next year.
- Increasing data security investments is a global priority, jumping 25% from 33% in 2023 to 58% in 2024.



Secure Your Digital Future

Simple. Secure. Resilient.



Secure Your Enterprise IT Footprint For A Safer Digital Journey

www.raqmiyat.com UAE | KSA | INDIA



CYBER READINESS BECOMES REALITY

WITH

COMMVAULT® CLOUD CLEANROOM™ RECOVERY





Visit commvault.com to Learn More

