ISSUE 82 | MARCH 2024

WWW.TAHAWULTECH.COM

Security ADVISOR MIDDLE EAST

A STEP AHEAD

MO MOBASSERI, CEO OF emt Distribution, DISCUSSES THE COMPANY'S FUTURE-FORWARD GROWTH TRAJECTORY AND INNOVATION-FIRST APPROACH.

cnme computer news middle east SUPPLEMENT

D-Link®
FOR BUSINESS

nuclias
cloud

Delivers Powerful
Wi-Fi, Even In
Extreme Temperatures

DBA-3620P & DBA-3621P

These are the best-in-class outdoor access points designed specifically for enterprise environments.

- Centralized cloud-based management
- 2 x 2 MU-MIMO Antenna with two spatial streams
- The latest 128-bit Personal and 192-bit Enterprise encryption
- Secure guest network with social login
- Supports Power over Ethernet
- With Zero Touch Deployment

Download on the App Store
GET IT ON Google Play

CONTENTS

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

Cybersecurity, everywhere you need it

www.fortinet.com

FORTINET®

EDITOR'S NOTE

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

Anita Joseph
Editor

CONVERGENCE OF AI & SECURITY

In the rapidly evolving landscape of digital technology, the intersection of cybersecurity and artificial intelligence (AI) has emerged as a focal point for both innovation and concern. As we navigate the complexities of an increasingly interconnected world, it becomes imperative to scrutinise the symbiotic relationship between these two domains.

Artificial intelligence has undoubtedly revolutionized cybersecurity, offering a potent arsenal of tools to combat ever-evolving threats. Machine learning algorithms can analyse vast amounts of data with unparalleled speed and accuracy, detecting anomalies and patterns that might elude human analysts. From identifying malware and phishing attempts to predicting potential breaches, AI-driven solutions empower organisations to fortify their defenses and respond swiftly to emerging risks.

However, this transformative power also raises significant ethical and security considerations. The same AI algorithms designed to safeguard against cyber threats can potentially be exploited by malicious actors to orchestrate sophisticated attacks. Adversarial machine learning techniques, where attackers manipulate AI systems by feeding them deceptive data, pose a formidable challenge to cybersecurity practitioners.

Moreover, the reliance on AI in cybersecurity introduces concerns regarding accountability and transparency. As AI systems autonomously make decisions based on complex algorithms, understanding the rationale behind their actions becomes increasingly opaque. This opacity not only complicates efforts to assess the reliability and bias of AI-driven security measures but also raises questions about legal and ethical responsibility in the event of system failures or unintended consequences.

RESPONSIBLE SECURITY

In this issue, we invite our readers to explore the intricate interplay between cybersecurity and artificial intelligence, recognising both the transformative potential and the inherent challenges it presents. By engaging in rigorous dialogue and collaborative problem-solving, we can navigate this complex terrain and shape a future where technology serves as a force for security, resilience, and progress.

EVENTS

tahawultech.com FUTURE SECURITY AWARDS

tahawultech.com CISO50 AWARDS & FORUM

FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by CPI

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

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

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, UAE

Tel: +971 4 5682993

KYNDRYL AND CLOUDFLARE ANNOUNCE GLOBAL STRATEGIC ALLIANCE TO DRIVE ENTERPRISE NETWORK TRANSFORMATION AND ZERO TRUST SECURITY


Paul Savil


Matt Harrel

Kyndryl, the world's largest IT infrastructure services provider, and Cloudflare, Inc. a leading connectivity cloud company, have announced a Global Strategic Alliance, an expansion of their partnership, to enable enterprises to migrate and manage networks for multi-cloud connectivity and comprehensive network security. The partnership combines Kyndryl's end-to-end consulting services and expertise across enterprise networking, security, and resiliency, with Cloudflare's robust connectivity cloud that offers security, performance, and cloud flexibility all-in-one.

Kyndryl and Cloudflare first partnered in May 2023 to modernize enterprise infrastructure with end-to-end services, bringing managed WAN-as-a-Service and Cloudflare Zero Trust to the entire corporate network. Now, the two companies are focused on further innovation across all technology stacks to design, build, manage, and modernize customers' vital systems. Cloudflare's capabilities will now be activated across Kyndrly's practice areas including Network & Edge and Security & Resilience.

Since partnering, enterprises have turned to Cloudflare and Kyndryl for complete network modernization, protections, and performance solutions — across sectors worldwide — from supply chain distribution in the US, a leading financial institution in Spain, to Ashok Leyland, a leading commercial vehicle manufacturer in India.

"As one of the premier automotive manufacturers worldwide, it is imperative that we are equipped with robust and secure networks to ensure our global IT infrastructure runs seamlessly. From dealer management to vehicle tracking, we need to run our 50+ Internet applications with zero or minimal disruption and enhanced security," said Vinod Gopinathan, CIO at Ashok Leyland. "Kyndryl's managed services with Cloudflare's DDoS protection and mitigation solution enables Ashok Leyland to focus on our pursuit to technology innovation, advanced engineering, and enhanced connectivity."

VERITAS BACKUP EXEC STRENGTHENS RESILIENCE AGAINST RANSOMWARE FOR SMBS

Veritas Technologies, the leader in secure multi-cloud data management, has announced enhancements to Veritas Backup Exec, the unified backup and recovery solution trusted by more than 45,000 small and midsize businesses (SMBs) worldwide. The latest updates include malware detection capabilities, role-based access control and additional optimisations for fast backup and recovery of business-critical data.

With ransomware attacks on the rise, data security is a growing concern for all businesses. Veritas research found that over the last two years, 65% of businesses had fallen victim to a ransomware attack in which bad actors infiltrated their systems. A majority also said data security risks are increasing. Small businesses can be especially vulnerable to ransomware attacks, without the in-house expertise to manage the complexities of data security. Many also forgo cyber insurance with a mistaken assumption that by virtue of their smaller size, they are more likely to fly under the radar of cybercriminals.

Simon Jelley, general manager for Backup Exec at Veritas, said: "Make no mistake, SMBs face the same danger as large enterprises. Hackers target smaller companies just as frequently and with more devastating consequences. Only one thing can guarantee recovery if attackers get in – having a reliable backup system. Veritas Backup Exec provides a simple-to-use, all-in-one solution for protecting SMBs' critical data wherever it lives – in SaaS or specialised applications and workloads, on premises or in the cloud."

SOPHOS IS A LEADER IN THE IDC MARKETSCAPE REPORT FOR WORLDWIDE MODERN ENDPOINT SECURITY FOR SMALL BUSINESSES 2024 VENDOR ASSESSMENT

Sophos, a global leader in innovating and delivering cybersecurity as a service, has announced it is a Leader in the IDC MarketScape: Worldwide Modern Endpoint Security for Small Businesses 2024 Vendor Assessment,* which evaluates the product offerings and business strategies of 18 modern endpoint security (MES) vendors. This news closely follows Sophos being named a Leader in the IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment.**

We believe Sophos being named a Leader in both reports validates its commitment to understanding and meeting the needs of small and midsize businesses (SMBs) with an expansive portfolio of world-class products and managed security services that are compatible with virtually any environment or tech stack.

The IDC MarketScape for Modern Endpoint Security for Small Businesses notes, Sophos is a "strong consideration for small businesses, particularly those with large business security requirements that have little to no in-house security expertise." In addition, the IDC MarketScape recognizes Sophos' constant innovation to stay ahead of the evolving threat landscape: "Even with the most diligent efforts to deflect attackers, there are no guarantees that all manner of attacks can be thwarted. Addressing this potential, Sophos recently added several new capabilities: adaptive attack protection, critical attack warning, and data protection and recovery."

Sophos Endpoint defends more than 300,000 organizations worldwide against advanced attacks with anti-ransomware, anti-exploitation, behavioral analysis, and other innovative technologies. With an extensive range of integrated capabilities, Sophos Endpoint seamlessly integrates with other Sophos products and managed security services, including Sophos Managed Detection and Response (MDR), the most widely adopted MDR offering. The IDC MarketScape noted, "Sophos MDR, already in use by over 20,000 Sophos customers, is a time-tested MDR service combined with Sophos' engagements with cyberinsurance providers delivers the confidence small businesses need to attain their endpoint security objectives without being security experts."

TENABLE EXPANDS GENERATIVE AI CAPABILITIES FOR FASTER ATTACK PATH ANALYSIS AND MITIGATION GUIDANCE

Tenable, the Exposure Management company, has announced innovative enhancements to ExposureAI, the generative AI capabilities and services within its Tenable One Exposure Management Platform. The new features enable customers to quickly summarise relevant attack paths, ask questions of an AI assistant and receive specific mitigation guidance to act on intelligence and reduce risk. The platform's generative AI-powered search and chat applications are fueled by Google Cloud – including Gemini models in Vertex AI.

Organisations face a high volume of exposures and more complicated threat actor tactics, techniques and procedures (TTP's) across the modern attack surface today. They are also facing a global cyber workforce shortage of 5.5 million trained professionals, according to the most recent data from ISC2. Even the most seasoned security experts struggle to sort through, understand and prioritise complex attack paths.

As a result, 44% of IT and cyber leaders say they are either very confident or extremely confident that they can leverage generative AI to improve their organisation's cybersecurity strategy. Tenable Attack Path Analysis, part of the Tenable One platform, leverages generative AI-based capabilities to help organisations enhance their preventive security. This includes explainability functionality that provides specific mitigation guidance with clear visibility and succinct analysis of complex attack paths, specific assets or security findings.

These new AI capabilities enable virtually anyone in the security team to digest and take action on the most complex attack paths across various exposures to stay steps ahead of attackers.

OPSWAT SETS NEW STANDARD IN CYBERSECURITY WITH FIRST-EVER 100% RATING IN SE LABS CONTENT DISARM & RECONSTRUCTION TEST

OPSWAT, a global leader in perimeter defense cybersecurity and pioneer of Deep CDR technology, has achieved a 100% Protection and Accuracy Score from SE Labs, an independently-owned and run testing company that assesses security products and services. OPSWAT is the first company to achieve this rating in CDR testing.

Cybercriminals frequently exploit vulnerabilities using file-based threats to compromise system security and execute malicious activities on a user's device or network. OPSWAT's Deep CDR employs a prevention-based approach and treats every file as a potential threat. By dissecting files into discrete components, eliminating potentially harmful or out-of-policy objects, and reconstructing usable files while preserving functionality, OPSWAT ensures comprehensive protection without compromising file integrity.

SE Labs tested using Office documents, archive files, and others such as images, web pages, and LNK link files, and with a malware component that would give the testers remote access to the victim if they opened the file. SE Labs then scored two aspects of OPSWAT's Deep CDR: Protection Accuracy to score the ability to eliminate threats, and Legitimate Accuracy to score the preservation of useful components. OPSWAT Deep CDR achieved 100% in both categories, demonstrating its capability to ensure both security and file integrity. Its unique approach of discarding non-compliant parts while maintaining the usability of compliant components contributed to its perfect score.

"SE Labs runs the most advanced and challenging security tests publicly available. We commend OPSWAT for submitting its CDR solution to this extremely tough assessment and for performing so well," said Simon Edwards, CEO and founder of SE Labs. "We rigorously evaluated Deep CDR's capabilities, focusing on its ability to pre-empt disruptions to productivity, safeguard data integrity and comprehensively eradicate malware threats."

NETAPP EMPOWERS CUSTOMERS TO SECURELY "TALK TO THEIR DATA" IN COLLABORATION WITH NVIDIA

NetApp has announced it is collaborating with NVIDIA to advance retrieval-augmented generation (RAG) for generative AI applications.

The new collaboration directly connects the just-announced NVIDIA NeMo Retriever microservices coming to the NVIDIA AI Enterprise software platform for development and deployment of production-grade AI applications, including generative AI—to exabytes of data on NetApp's intelligent data infrastructure. Every NetApp ONTAP customer will now be able to seamlessly "talk to their data" to access proprietary business insights without having to compromise the security or privacy of their data.

NetApp customers can now query their data, whether spreadsheets, documents,

presentations, technical drawings, images, meeting recordings, or even data from their ERP or CRM systems through simple prompts – all while maintaining the access control they've already established when storing the data.

"As the leader in unstructured data management, NetApp makes data infrastructure intelligent to securely turbocharge AI innovation. Together with NVIDIA, we have helped accelerate over 500 data-driven businesses to become AI-ready," said George Kurian, CEO at NetApp. "Through our joint work, NetApp's installed base can seamlessly and securely use NVIDIA's tools with their unstructured data. AI is defining a new data-driven era and NetApp and NVIDIA are at the forefront of ensuring success for customers as they adopt and deploy AI."

Under the High Patronage of His Majesty King Mohammed VI

GITEX AFRICA Morocco

UNDER THE AUTHORITY OF: Kingdom Of Morocco Head Of Government Ministry Of Digital Transition and Administration Reform

HOSTED BY: #ADD Digital Development Agency

ORGANISED BY: KAOUN INTERNATIONAL

CO-LOCATED WITH: WORLD FUTURE HEALTH AFRICA

29 - 31 MAY 2024 MARRAKECH

VISIT THE LARGEST TECH & STARTUP SHOW IN AFRICA

Creating A Bold Future For Africa

- Discover **MORE** tech solutions
- Hear **MORE** ground-breaking opinions
- Meet **MORE** tech brands
- Network with **MORE** tech professionals

... than anywhere else on the entire African continent

- Ai Everything (AI x Cloud x IoT x Data)
- Cybersecurity
- Consumer Tech
- Digital Finance
- Telecoms & Connectivity
- North Star Africa
- Digital Cities
- Digital Health

UNLOCK AFRICA'S DIGITAL FUTURE AT GITEX AFRICA
MAY 29-31, MARRAKECH, MOROCCO

Book to secure your Early Bird Ticket today. Expires **18 April 2024**

gitexafrica.com

FIND YOUR WORLD

GITEX AFRICA Morocco | GITEX GLOBAL — DUBAI — | GITEX EUROPE Berlin

PROVEN CONSULT AND SADQ PARTNERS TO DELIVER CUTTING-EDGE SOLUTIONS

PROVEN Consult (www.Provenconsult.com), the leading intelligent automation solutions provider, announced the signing of an MoU with Sadq (www.sadq.sa), the leading digital signature company in Saudi Arabia. The MoU was signed between Hilel Baroud, CEO of PROVEN Consult, and Dr. Abdulla Allahuo, marking the beginning of a collaborative journey aimed at providing cutting-edge solutions to clients.

Through this partnership, PROVEN Consult and Sadq are committed to enhancing the client experience by offering access to Sadq's seamless e-signature solution. This integration will streamline document signing processes, ultimately boosting efficiency and productivity for clients across various industries.

In addition to the e-signature solution, PROVEN Consult is integrating its powerful Sanad.ai (https://sanad.ai/) Arabic OCR technology into the joint offerings. This tool, renowned for its accuracy and efficiency in text extraction, will further elevate the capabilities of collaborative solutions.

"We are thrilled to partner with Sadq to bring innovative solutions to our clients," said Hilel Baroud, CEO PROVEN Consult. "This collaboration underscores our dedication to providing innovative and comprehensive solutions to address the diverse needs of our clients."

The partnership between PROVEN Consult and Sadq reflects a shared vision of leveraging technology to empower businesses and enhance operational efficiency. Both parties are committed to leveraging their expertise and resources to deliver unparalleled value to clients.

Dr. Abdullah Allahuo, Co-Founder and CEO, Sadq, echoed the sentiment, stating, "The partnership with PROVEN Consult is a testament to our commitment to driving digital transformation and delivering value-added solutions to our clients. Together, we are poised to revolutionise document management and intelligent automation processes."

BAHWAN CYBERTEK

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

www.bahwancybertek.com

SKILL AND KNOWLEDGE ESSENTIAL TO HANDLE ADVANCED CYBERTHREATS

ANITA JOSEPH CAUGHT UP WITH **AMIN HASBINI**, HEAD OF GREAT, META AT KASPERSKY, TO LEARN MORE ABOUT ADVANCED PERSISTENT THREATS AND HOW EMERGING TECHNOLOGIES IMPACT THE THREAT-SECURITY LANDSCAPE.

Can you provide us with an overview of the current Advanced Persistent Threat (APT) landscape? What measures should organisations take to effectively defend against these sophisticated threats?
APTs, or advanced persistent threats, demand specialised attention and measures. While multi-layered defenses are recommended, organisations must go beyond that. Each entity needs to identify its adversaries through modeling studies and subsequently track them using threat intelligence. By understanding the techniques and methods employed by adversaries, organisations can simulate and assess their own readiness. Achieving maturity in handling such threats involves external and internal efforts, market intelligence, government input, and collaboration with security vendors. Skills and knowledge are essential components, as technology alone cannot always thwart these attacks.

Emerging technologies, like Artificial Intelligence and IoT, raise cybersecurity concerns. How can organisations safely adopt these technologies, balancing innovation and security?
Before engaging with AI or IoT, organisations should conduct an internal study to identify use cases, data access, and potential risks. This allows classification of sensitive data and understanding the impact on the organisation, its business, reputation, and client data. A risk assessment, involving the organisation's risk management department and executives, helps make informed decisions. Executives are then responsible for accepting the associated risks. In case of issues, a predefined plan of action, rules of engagement, and a specialised team are crucial. It all starts with a thorough study of how AI or other technologies will benefit the organisation.

Shifting focus to Smart City technologies, crucial for urban development, they pose security challenges. What potential risks are associated with smart city infrastructure, and how can these dangers be mitigated?
Smart City technologies, especially those connecting critical infrastructure like the power grid, water treatment facilities, and chemical plants, present significant risks. Disruptions to these essential services impact lives directly, underscoring the need for robust strategies, laws, regulations, and technologies. The challenge lies in finding individuals with the right skills, as not every organisation can easily acquire technology or personnel. Addressing these threats requires a comprehensive approach involving legal frameworks, technology deployment, and skill development.

BEFORE ENGAGING WITH AI OR IOT, ORGANISATIONS SHOULD CONDUCT AN INTERNAL STUDY TO IDENTIFY USE CASES, DATA ACCESS, AND POTENTIAL RISKS.

A STEP AHEAD

ANITA JOSEPH CAUGHT UP WITH **MO MOBASSERI**, CEO OF emt Distribution, FOR A CANDID CHAT ON THE COMPANY'S FUTURE-FORWARD GROWTH TRAJECTORY AND ITS INNOVATION-FIRST APPROACH.

emt BOASTS A DEDICATED SERVICE DIVISION, PROVIDING NOT ONLY SUPPORT FOR VENDOR TECHNOLOGIES BUT ALSO VENDOR-NEUTRAL SERVICES.

Mo Mobasseri is CEO of emt Distribution, a specialised Value-Added Technology Distributor (VAD) and service provider with a focus on information security and the most effective cyber threat mitigation strategies. He leads a highly skilled team committed to the company's mission of enhancing information security and implementing highly effective cyber threat mitigation strategies. emt's core mission revolves around delivering innovative solutions and cutting-edge strategies aimed at proactively preventing cybersecurity incidents and safeguarding the digital assets of businesses, education services around emerging technologies and cybersecurity as well as offering best-in-class ITAM Solutions and services. Beyond providing state-of-the-art products, emt also extends support through a comprehensive suite of cybersecurity professional services. These offerings include Privilege Access Maturity Assessments, Essential Eight Maturity Assessment, Cloud Security Assessments, Data Access Governance Implementations and Privilege Access Implementations, among others. By offering cutting-edge products and services, emt strives to empower its partners with the tools and expertise needed to navigate the complex landscape of

cybersecurity threats and ensure a secure digital future for their clients.

Anita Joseph caught up with Mo for a candid discussion on the company's future-forward growth trajectory and its innovative market strategies that have positioned it as the undisputed leader in the fiercely competitive IT distribution market.

DIVERSIFIED, YET FOCUSED

emt Distribution, according to Mo, is laser-focused on strategic expansion initiatives across multiple fronts. Beyond geographical horizons, exemplified by the recent establishment of an office in Saudi Arabia, the company is dedicated to fortifying its presence in this region. This move is not merely about physical expansion; it's about enriching resources to provide unparalleled service to its network of technology partners, resellers, and customers.

The realm of Operational Technology (OT) has been a cornerstone of Emt's operations for some time. However, recognising the pressing challenges facing the OT industry, particularly concerning security management, emt has taken proactive steps to address these issues head-on. With a spotlight on security management within the OT domain, emt is poised to make significant strides in this arena throughout 2024, solidifying its commitment to safeguarding critical infrastructure.

While cybersecurity remains the bedrock of emt's operations, the last 7 years have witnessed a strategic diversification into comprehensive management services and solutions. "This evolution encompasses vital areas such as IT asset management, cost optimisation and the integration of DevOps, FinOps and SecDevOps solutions. The success of this expansion owes much to emt's collaborative approach, leveraging cutting-edge solutions in tandem with its esteemed technology partners. Looking ahead, emt is dedicated to further enriching its service offerings, with an emphasis on customisation and flexibility to meet the unique needs of its clientele," Mo says.

emt Distribution's PROACTIVE APPROACH, COMPREHENSIVE SOLUTIONS, AND COMMITMENT TO EDUCATION POSITION IT AS A LEADER IN THE IT SECTOR.

Setting itself apart from conventional distributors, emt takes immense pride in its robust commitment to service offerings. Unlike its counterparts, emt boasts a dedicated service division, providing not only support for vendor technologies but also vendor-neutral services. This distinctive approach underscores emt's role as a service distributor, facilitating seamless delivery through its extensive network of channel partners, with the flexibility to white-label services as per individual branding preferences.

Furthermore, emt has made significant strides in cloud management and security, aligning itself with the burgeoning trend of cloud adoption across various sectors. While the benefits of cloud solutions are undeniable, emt remains acutely aware of the paramount importance of ensuring the security of cloud environments. To this end, the company has forged strategic alliances with new vendors and implemented robust security measures in line with industry standards, such as

AI IS A GAME CHANGER AND emt HAS LEVERAGED THE POWER OF AI TO ACHIEVE ITS OBJECTIVES AND PROPEL GROWTH.

CIS controls. By prioritising security in the cloud, emt reaffirms its commitment to providing comprehensive, end-to-end solutions that inspire confidence in an increasingly digital world.

Meanwhile, expanding into Africa remains another significant area of focus for the company. "We've established resources in South Africa and Morocco, with plans to open additional offices in 2024. The African market presents exciting opportunities for training, technology sales, and services, which align with our strategic focus on service offerings."

BRIDGING THE SKILLS GAP

emt Distribution is actively involved in skilling and training the future generation. Recognising the ever-widening cybersecurity skills gap, the company has collaborated with organisations like the Dubai World Trade Centre and the UAE Cybersecurity Council to provide training in cybersecurity, IoT, and data science. "Additionally, we're now delving into office gaming platforms to create environments for blue and red teams to practice real-world scenarios," Mo points out.

"On a national level, we're working in multiple initiatives to expand our cooperation with the respective authorities in cybersecurity awareness campaigns and initiatives focused on IT asset and cost optimisation. By customising solutions for ministries and government entities, we aim to help them redirect funds towards cybersecurity investments," he adds.

WITH A SPOTLIGHT ON SECURITY MANAGEMENT WITHIN THE OT DOMAIN, emt IS POISED TO MAKE SIGNIFICANT STRIDES IN THIS ARENA THROUGHOUT 2024.

POWERED BY AI

AI is a game changer and emt has leveraged the power of AI to achieve its objectives and propel growth. Mo underscores the pivotal role played by Artificial Intelligence (AI) in navigating the contemporary business landscape. "AI has evolved into a cornerstone of our operational strategies," he states. "While numerous platforms harness AI capabilities, we acknowledge the unique significance of generative AI, especially within cybersecurity frameworks." To foster understanding and proficiency in this specialised domain, we've conducted extensive workshops and training sessions focused on generative AI. These initiatives serve as a prelude to the integration of this cutting-edge technology into our suite of offerings. He stresses the company's commitment to empowering both individuals and organisations through certified training programs, envisioning a future where the full potential of AI is harnessed to address evolving challenges in the industry.

THE WAY AHEAD

The Middle East region stands as a promising arena for the company's growth trajectory, particularly with the UAE, Saudi Arabia and Qatar emerging as steadfast

hubs for expansion. Mo highlights that despite occasional global turbulence, these markets have demonstrated resilience, remaining robust, appealing, and primed for development. "While challenges like payment issues persist, we've adeptly maneuvered through them by implementing service-centric solutions and flexible payment structures," he explains. Moreover, the competitive landscape has evolved into a more professional and stable environment, fostering healthier market dynamics. Says Mo, "Considering the challenges faced in other regions, the Middle East presents a wealth of opportunities, positioning it as a strategic focal point for our investment and expansion endeavors." This sentiment underscores the company's commitment to leveraging the region's growth potential and consolidating our presence in key markets.

In an era marked by unprecedented digital transformation and ever-evolving cyber threats, emt Distribution emerges as a beacon of innovation and resilience within the IT sector. It is not just a distributor; rather, it is a strategic partner equipped to help businesses navigate the complex challenges of today's rapidly changing business landscape.

At the heart of emt's mission lies a steadfast commitment to enhancing information security and mitigating cyber threats effectively. Its focus on innovation is evident in its proactive approach to cybersecurity. Rather than merely reacting to threats as they arise, emt anticipates and prepares for future challenges. Through strategic partnerships and ongoing research and development, emt stays at the forefront of cybersecurity trends, ensuring that its clients have access to the most advanced tools and technologies available.

AT THE HEART OF emt'S MISSION LIES A STEADFAST COMMITMENT TO ENHANCING INFORMATION SECURITY AND MITIGATING CYBER THREATS EFFECTIVELY.

As the IT sector continues to evolve at breakneck speed, businesses must adapt quickly to stay ahead of the curve. emt Distribution stands poised to guide organisations through this dynamic landscape, providing the expertise, resources, and support needed to thrive in an ever-changing world. With its unwavering commitment to innovation, collaboration, and excellence, emt is not just a distributor; it is a trusted partner for businesses seeking to secure their digital future.

emt Distribution's proactive approach, comprehensive solutions, and commitment to education position it as a leader in the IT sector. As businesses navigate the challenges of an increasingly interconnected world, they can rely on Emt to provide the tools, expertise, and support needed to safeguard their digital assets and thrive in a rapidly evolving landscape.

CARELESS EMPLOYEES ARE UAE ORGANISATIONS' BIGGEST DATA LOSS PROBLEM: PROOFPOINT

Proofpoint, Inc., a leading cybersecurity and compliance company, released its inaugural Data Loss Landscape report, which explores how current approaches to data loss prevention (DLP) and insider threats are holding up against current macro challenges such as data proliferation, sophisticated threat actors, and generative artificial intelligence (GenAI). The findings reveal that data loss is a problem stemming from the interaction between humans and machines — "careless users" are much more likely to cause those incidents than compromised or misconfigured systems.

Emile Abou Saleh, Senior Regional Director at Proofpoint Middle East, Turkey & Africa, said: "Data loss poses a severe threat, where a simple oversight can lead to the loss of critical data. It is, therefore, crucial for employees to understand the role they play in data protection and that it is not just an IT problem. As work models evolve,

organisational strategies for securing data across all platforms must also adapt. By enhancing data loss prevention policies and insider risk strategies across the board—from endpoints and cloud apps to email and the web—organisations will be able to bolster their defenses against the modern security landscape, ensuring a secure digital future for everyone involved."

The 2024 Data Loss Landscape report examines third-party survey responses from 600 security professionals at organisations with 1,000 or more employees across 17 industries from 12 countries. These insights were supplemented with data from Proofpoint's Information Protection platform and Tessian, which Proofpoint acquired last fall, to convey the scale of the data loss and insider threats that organisations face.

Key global findings include:

- **Data loss is a widespread yet preventable problem:** organisations experienced the equivalent of two incidents per month (a mean of 24 data loss incidents per UAE organisation in the past year), and 75% of respondents said the main cause was careless users. Carelessness includes misdirecting emails, visiting phishing sites, installing unauthorised software, and emailing sensitive data to a personal account. These all-preventable behaviors that could be mitigated with practices such as implementing data loss prevention policy rules for email, web uploads, cloud file synching, and other common data exfiltration methods.
- **Misdirected email is one of the simplest and most significant sources of data loss:** According to 2023 data from Tessian, about one-third of employees sent one or two emails to the wrong recipient. That means a business of 5,000 employees can expect to deal with around 3,400 misdirected emails per year. A misdirected email containing employee, customer or patient data can potentially trigger a significant fine under GDPR and other legal frameworks.
- **Generative AI is the fastest growing area of concern:** tools such as ChatGPT, Grammarly, Bing Chat and Google Gemini are increasing in power and utility, and more users are inputting sensitive data into these applications. "Browsing gen AI sites" has become one of the top five DLP and insider threat alert rules configured by organisations using Proofpoint's Information Protection platform.
- **Consequences of malicious actions can be costly:** 19% of respondents said malicious insiders such as employees or contractors were behind data loss incidents. Malicious actions and departing employees who seek to harm the organisation can have even greater implications than careless insiders because these individuals are motivated by personal gains.
- **Departing employees were identified as one of the riskiest users (22%):** departing employees do not always think they are acting maliciously—some simply feel entitled to leave with information they have produced. Proofpoint data shows that 87% of anomalous file exfiltration among cloud tenants over a nine-month period was caused by departing employees, underscoring the need for preventative strategies such as implementing a security review process for this user category.
- **Privileged users are the riskiest:** Almost three-quarters (72%) of UAE respondents identified employees with access to sensitive data, such as HR and finance professionals, as representing the greatest risk of data loss. Additionally, Proofpoint data shows that 1% of users are responsible for 88% of data loss events. These findings indicate that organisations must prioritise best practices such as using data classification to identify and protect business-critical data and the "crown jewels," as well as monitoring people with access to sensitive data or admin privileges.
- **Organisations' data loss prevention programs are maturing:** Many DLP programs in the UAE are initially implemented in response to legal regulations, with more than one-third (36%) of survey participants citing meeting regulatory compliance standards as the primary driver. Protecting the privacy of employees and customers and minimising costs associated with data loss came in as the top drivers for UAE organisations (both at 50%).

ENSURING A PROACTIVE APPROACH TO CYBERSECURITY SKILLS TRAINING

ANITA JOSEPH CAUGHT UP WITH **NED BALTAGI**, MANAGING DIRECTOR, META AT SANS INSTITUTE, TO LEARN HOW COMPANIES CAN EFFECTIVELY IMPLEMENT AND MAINTAIN AN IN-DEPTH DEFENCE STRATEGY IN THE CONTEXT OF ESCALATING CYBERATTACKS, AND HOW SKILLS AND KNOWLEDGE COME IN HANDY.

In the context of a defense-in-depth strategy, what are the key advantages of this approach for companies, and how can they effectively implement and maintain this approach in their cybersecurity framework?

The defence-in-depth strategy offers multiple layers of security controls and measures across the various components of a company's information systems. This approach is advantageous because it provides redundancy in the event of a control failure and encompasses a comprehensive range of protective measures to address different vectors of attack. It not only helps in preventing security breaches but also minimizes the impact of a breach should one occur.

Companies can effectively implement and maintain a defence-in-depth strategy by first conducting thorough risk assessments to identify critical assets and vulnerabilities. Following this, they should adopt a layered security approach that includes physical security, network security, application security, and data security measures. Regularly updating and testing security controls, alongside continuous monitoring for threats, are crucial for maintenance. Employee training and incident response plans are key components of a robust defense-in-depth strategy.

Human error is often cited as a significant cybersecurity risk. How can companies address and reduce the risk of human error through education, awareness, and upskilling of their employees, and what role does a proactive response play in mitigating such errors?

Human error is a significant risk factor in cybersecurity. Companies can address this by implementing comprehensive cybersecurity awareness programs that educate employees on the importance of security practices and the common tactics used by adversaries. Regular training sessions, phishing simulations, and the promotion of a security-conscious culture are effective ways to reduce the likelihood of human error.

A proactive response plays a critical role in mitigating errors by quickly identifying and correcting them before they can be exploited by attackers. This includes having mechanisms in place to detect potential security incidents, conducting regular audits and assessments, and fostering an environment where employees feel comfortable reporting mistakes without fear of retribution.

Considering the multifaceted nature of cybersecurity, how can organizations ensure that they are not solely focused on technical issues but also actively addressing the human element? What strategies can be employed to balance technical solutions with human skills and awareness?

Organizations can ensure a balanced focus on both technical issues and the human element by implementing a holistic cybersecurity strategy that includes technical defenses alongside human-centered approaches like regular training and awareness programs. Engaging employees in security practices and fostering a culture of security are essential. Strategies such as gamification of training, personalized learning paths, and promoting security as a shared responsibility can enhance engagement and awareness.

Looking ahead to 2024, do you anticipate the cyber skills gap to continue growing, and what implications might this have for organizations? Additionally, how can ongoing education and training, such as SANS' 2024 courses and events, contribute to shrinking the cyber skills gap?

The cyber skills gap is likely to continue growing into 2024, driven by the rapid evolution of technology and increasing sophistication of cyber threats. This gap presents significant implications for organizations, including increased vulnerability to cyber-attacks and challenges in protecting critical information assets.

Ongoing education and training, such as the courses and events offered by SANS in 2024, are crucial for addressing the cyber skills gap.

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics offers an in-depth exploration of advanced threat hunting and forensic analysis, teaching participants to effectively detect, contain, and remediate cyber threats through a well-defined incident response plan. Leadership and governance in cybersecurity, critical for narrowing the skills gap, are emphasized in courses like LDR514: Security Strategic Planning, Policy, and Leadership, focusing on strategic planning, policy formation, and legal aspects. For securing critical infrastructure, ICS410: ICS/SCADA Security Essentials is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats. SEC497: Practical Open-Source Intelligence (OSINT) is a top choice for mastering safe and effective open-source intelligence research.

Additionally, considering the unprecedented integration of GenAI in the workplace, our recently launched online course, AIS247: AI Security Essentials for Business Leaders, is tailored to empower leaders with the knowledge and tools to navigate the complexities of AI in the business world. AIS247 also addresses the critical aspect of AI policy development, equipping participants with the skills needed to craft and implement effective AI strategies to manage its risks and opportunities within their organizations.

A PROACTIVE APPROACH TO EDUCATION AND TECHNICAL TRAINING IS ESSENTIAL FOR DEVELOPING A RESILIENT DEFENSE AGAINST EMERGING CYBER THREATS.

These programs provide current and aspiring cybersecurity professionals with the skills and knowledge needed to tackle emerging threats. By investing in education and training, organizations can build a more skilled workforce capable of defending against sophisticated cyber-attacks.

In the realm of cybersecurity, what steps should companies take to prepare for the evolving threat landscape, specifically in terms of upskilling and training their workforce? How can a proactive approach to education and technical training contribute to a more resilient defense against emerging cyber threats?

Companies should take proactive steps to continuously upskill and train their workforce to prepare for the evolving threat landscape. This includes offering regular training sessions, workshops, and certifications that cover the latest cybersecurity trends, technologies, and best practices.

A proactive approach to education and technical training is essential for developing a resilient defense against emerging cyber threats. This approach should involve equipping employees with the necessary technical skills and fostering a culture of continuous learning and adaptability. By staying ahead of the latest cybersecurity developments, companies can better anticipate and mitigate potential threats.

A multi-faceted approach encompassing defence-in-depth strategies, addressing human error through education, balancing technical and human elements, preparing for the cyber skills gap, and adopting proactive education and training initiatives is essential for enhancing cybersecurity resilience. As the cybersecurity landscape continues to evolve, organizations must prioritize these aspects to safeguard their digital assets effectively.


معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC
GLOBAL
23-25 APR 2024
DUBAI WORLD TRADE CENTRE
A BOLD
NEW FUTURE
AI-DRIVEN
CYBER RESILIENCE
MIDDLE EAST AND AFRICA'S
LARGEST CYBERSECURITY EVENT
SCAN HERE
GET INVOLVED
gisec@dwtc.com | Tel: +971 4 308 6469
#gisecglobal | gisec.ae
HOSTED BY
مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
OFFICIAL GOVERNMENT CYBERSECURITY PARTNER
مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER
OFFICIALLY SUPPORTED BY
وزارة الداخلية
MINISTRY OF INTERIOR
شرطة دبي
DUBAI POLICE
OFFICIAL DISTRIBUTION PARTNER
SPIRE
LEAD STRATEGIC PARTNER
HUAWEI
DIGITAL TRANSFORMATION PARTNER
du
STRATEGIC PARTNER
Microsoft
PLATINUM SPONSOR
PENTERA
GOLD SPONSOR
CLOUDFLARE
emt
sg
MENLO SECURITY
NOKIA
Qualys.
BRONZE SPONSOR
bugcrowd
CLAROTY
Honeywell
sekoia
ITSEC

CYBERSECURITY IN 2024: TOWARDS EVER GREATER SOPHISTICATION OF TACTICS

CHESTER WISNIEWSKI, DIRECTOR GLOBAL FIELD CTO, SOPHOS

The year 2023 was marked by persistence in the tactics of cybercriminals, with the predominance of ransomware, the exploitation of vulnerabilities, theft of credentials and even attacks targeting the supply chain. The common point in all his attacks is their formidable effectiveness.

It is therefore essential to ask what trends will persist in 2024 and what strategies businesses should adopt to deal with these future cyber threats.

Between persistent trends and evolving cybercrime tactics

In 2024, the threat landscape is not expected to change radically, particularly with regard to attack typologies and criminal tactics and procedures. Criminal groups still primarily focus their attention on financial gains and ransomware remains their weapon of choice. These cybercriminals tend to take the easy way out by opportunistically attacking unpatched security vulnerabilities.

The recent Citrix Bleed attack demonstrated the agility of cybercriminals when it comes to quickly and effectively exploiting these new vulnerabilities. However, once patches are applied to these vulnerabilities, cyberattackers tend to revert to more common strategies of stealing credentials or, failing that, cookies or session cookies, which, while slightly slower, constitute always a proven means that allows them to penetrate within a system.

In 2024, however, we should expect increased sophistication in defense evasion tactics, particularly due to the generalisation of certain technologies such as multi-factor authentication. These attacks will combine malicious proxy servers, social engineering techniques and repeated authentication request attacks or "fatigue attacks".

AI and regulations will continue to shape cybersecurity

In 2024, the development of AI will have a positive impact on the efficiency of IT teams and security teams by enabling them to strengthen defenses and work more efficiently, including through the processing of vast volumes of data in the aim of detecting anomalies. It should make it possible to respond more quickly in the event of an incident.

Indeed, analysis of attacks in 2023 showed a shortening of the time between network penetration and the triggering of a final attack – using malware or ransomware. The need for rapid detection and response tools to prevent costly incidents is therefore essential.

Finally, regulatory developments could have a major influence on measures taken against ransomware. The need to take more substantial measures could push some states to penalise the payment of ransoms, which would represent a brake on malicious actors and change the perspective of companies in the event of an attack. Other stricter legislation, such as the implementation of the European NIS2 Directive, is also expected to force companies to take additional measures, particularly regarding their abilities to collect data sets.

To protect themselves against increasingly rapid, effective and costly attacks, companies will need to strengthen their defenses by equipping themselves with tools that allow them to detect and respond to incidents more quickly. The worsening cybersecurity talent shortage does not appear to be as serious as some studies claim. On the contrary, companies have implemented more lax hiring criteria and more open-mindedness in the recruitment process.

From this perspective, to guarantee their survival in a constantly evolving threat landscape, companies have every interest in establishing partnerships with cybersecurity experts whose main mission is to make the hyperconnected world safer, to advise and assist them. in setting up effective defenses.

IN 2024, THE THREAT LANDSCAPE IS NOT EXPECTED TO CHANGE RADICALLY, PARTICULARLY WITH REGARD TO ATTACK TYPOLOGIES AND CRIMINAL TACTICS AND PROCEDURES.

DEMYSTIFYING TECHNOLOGY

ENG. **BADAR ALI SAID AL SALEHI**, CHAIR OF OIC-CERT AND DIRECTOR GENERAL OF OMAN NATIONAL CERT (OCERT), DISCUSSES THE EVOLVING LANDSCAPE OF CYBERSECURITY AND DIGITAL TRANSFORMATION.

The OIC-CERT has established working groups for 5G Security and Cloud Security over the past few years and released related frameworks. What are the key missions of these two working groups, which were discussed during the recent roundtable?

The 5G Security and Cloud Security Working Groups (WGs) are among the more developed within OIC-CERT, addressing essential technological concerns critical to any nation's digital transformation roadmap. As the industry advances towards 5.5G, the OIC-CERT 5G Security WG will assist in demystifying and facilitating the adoption of this technology by the OIC-CERT member countries and OIC community. The 5G WG developed a 5G Security Framework to establish a sustainable security and resilience of 5G ecosystem through standardise, impartial, and non-discriminatory manner for regulatory authorities of the member countries.

The OIC-CERT 5G Harmonised and Unified Cybersecurity Certification System (HUCCS) is a cross-recognition assurance methodology with the plan to establish critical 5G evaluation and certification facilities.

Meanwhile, the Cloud Security WG will develop a cloud security framework providing work towards a high-level guidance on direction and strategy base on common open certifiable standards. The framework will be technical operating procedures and technical specifications that aligned with national strategies and regulatory compliance requirement. To kicking off, the WG is planning a pilot implementation for the OIC-CERT Cloud Security Framework, with a Central Asia Cloud Security whitepaper, alongside a series of Cloud Security roundtables, which is replicating what had been done last year for the Middle East region.

THE CLOUD SECURITY WG WILL DEVELOP A CLOUD SECURITY FRAMEWORK PROVIDING WORK TOWARDS A HIGH-LEVEL GUIDANCE ON DIRECTION AND STRATEGY BASE ON COMMON OPEN CERTIFIABLE STANDARDS.

In addition to those existing WGs, some new activities, such as AI study groups and supply chain working groups, were proposed at a recent roundtable discussion. Can you please elaborate further on those points?

The OIC-CERT recognised the emerging of new technologies and the security threats they post such as AI security, AI governance, supply chain security, post-quantum cryptography, and data security governance that were well covered during MWC. We've had expert group workshops discussing these issues in December 2023, and OIC-CERT plans to form study groups and WG to facilitate OIC-CERT member countries and OIC community in mitigating security issues of these technologies in digital transformation journey. It's encouraging to see more OIC-CERT members are leading these new areas of work, tapping into the collective expertise from the 57 OIC member countries globally, ranging from Africa to the Middle East and from Central Asia to Southeast Asia.

AI & CYBERSECURITY

In this feature, we delve into the dynamic intersection of Artificial Intelligence and Cybersecurity, where cutting-edge technology meets the imperative of protecting our interconnected world. As the digital landscape evolves, so do the threats we face. Explore how AI is revolutionising cybersecurity strategies, from predictive threat analysis to autonomous response systems. Uncover the latest advancements in machine learning, natural language processing, and neural networks, shaping the battle against cyber threats.

Q1. In the realm of cybersecurity, how are machine learning algorithms and artificial intelligence technologies transforming traditional approaches to threat detection, and what specific advantages do these advancements bring to the table?

Q2. As AI continues to play a pivotal role in enhancing cybersecurity defenses, could you elaborate on real-world examples where your organisation has helped businesses successfully leverage AI/machine learning to proactively identify and respond to emerging cyber threats, ultimately strengthening their overall security posture?

Abdullah Abu-Hejleh

Director of Cyber Security, CNS Middle East

Machine learning algorithms and artificial intelligence (AI) technologies are revolutionising traditional approaches to threat detection in cybersecurity by enabling more proactive and adaptive defenses. Machine learning algorithms can analyze vast amounts of data to identify patterns and anomalies that may indicate potential threats. This helps in detecting previously unknown attacks or unusual behavior that might evade traditional rule-based systems.

AI technologies can learn normal user and system behaviors and detect deviations from these patterns. AI-powered systems can automate the response to certain types of threats, such as isolating compromised systems, blocking malicious traffic, or applying patches. This reduces the response time

to incidents, minimizing the impact of attacks.

Machine learning algorithms can analyze large datasets of threat intelligence information to identify emerging threats and prioritize security measures accordingly. This helps organisations stay ahead of evolving cyber threats.

AI can also be used to detect adversarial attacks aimed at undermining machine learning models themselves. By deploying AI-based defenses, organisations can better protect against such attacks and ensure the integrity of their security systems.

Overall, AI and machine learning are increasingly being integrated into cybersecurity strategies to help businesses stay ahead of evolving threats and safeguard their digital assets.

Ali Moghnieh

Sales Manager, Ruckus Commscope

Machine learning and artificial intelligence have revolutionized the cybersecurity landscape, enabling organisations to instantly identify and respond to threats by analysing large volumes of real-time data. AI and ML algorithms uncover hidden relationships and indicators by examining complex patterns of potential threats, reducing reliance on signatures and threat intelligence updates. These advancements nonetheless address the challenges of limited cybersecurity resources.

RUCKUS AI is a next-generation solution that leverages artificial intelligence and machine learning to overcome the challenges faced by IT in managing network incidents and optimising network performance. By utilising advanced AI technologies, RUCKUS AI quickly identifies and resolves network issues by uncovering hidden patterns and relationships, reducing the Mean Time to Identify (MTTI) and improving overall network stability. This comprehensive AI solution extends to both wired and wireless networks, providing IT Leadership with a streamlined incident management process. With RUCKUS AI, CIOs can allocate more resources to strategic planning and focus on driving organisational growth, while maintaining a secure and resilient network infrastructure.

Ben Gelman

Senior Data Scientist, Sophos

AI has made critical transformations to threat detection, analysis, and resolution. For threat detection, AI is focused on classifying telemetry. The amount of data that even a relatively small customer base can generate is tremendous. Discovering patterns and bringing it to the attention of human analysts is indispensable in modern cybersecurity solutions. With the addition of large language models, we are seeing significant changes in analysis and resolution. Security copilots and natural language interfaces are creating a new dynamic between human

analysts and the underlying security data.

AI is integral to the Sophos product itself. We use AI to identify threats within everything from office files, PDFs, executables, and command lines to emails and Android devices. Our wide range of AI models generate credible indicators of threats, and, in turn, our human analysts leverage our custom security copilot to understand and respond to incidents more efficiently. Businesses can reinforce their security posture through our AI-powered systems, without needing to delve into the intricate operations of AI themselves.

Biju Unni

Vice President, Cloud Box Technologies

Hackers use ML techniques coupled with AI to increase the potency of their attacks and this can only be countered by equivalent or better technology. Much as attackers adopt AI and machine-learning techniques, cybersecurity teams will need to evolve and scale up the same capabilities. Organisations can use these technologies and outlier patterns to detect and remediate noncompliant systems. Teams can also leverage machine learning to optimise workflows and technology stacks so that resources are used in the most effective way over time. Most of the vendors

We follow the best practices starting with a Digital Resilience Assessment to understand the "As is" situation, then there is Cyber Risk insights followed by a Simulated attack on the client environment. We have onboarded Security vendors utilising Generative AI coupled with active machine learning and Advanced algorithms for their security solutions. We also operate a 24/7 Security Operating Centre which is meant to be a bulwark against security threats. Our SOC is a fully automated entity integrating the latest Generative AI along with ML to constantly improve the security posture of the clients.

David Hoelzer

SANS Fellow and AI Expert, SANS Institute

Machine learning and artificial intelligence can truly act as force multipliers in a cybersecurity organisation. There are two big problems with traditional approaches; our ability to look at large volumes of traffic efficiently as humans and being overly reliant on solutions that rely on known-bad (signature-based solutions). AI solutions that we teach people to build in our course allow us to go beyond these barriers.

A gentleman from a US National Laboratory attending our SEC595 course approached me during the second day with a problem he was trying to solve. He had vast amounts of DNS log data and felt certain that there was useful threat intelligence that could be harvested from this data. He had spoken to data scientists at his facility who had told him that the best he could do was leverage known-bad lists for domains known to be associated with phishing and malware. On the morning of the third day of class, we built a system that was able to find critical threat indicators in DNS log data in seconds... without using a known-bad list. Another group from a defense organisation was able to take what they learned on Day 2 and apply it to their own systems overnight. By the next day, they had found multiple previously unknown compromises in their networks using this new technique.

Fady Younes

Managing Director, Cybersecurity MEA, Cisco

The integration of machine learning algorithms and artificial intelligence has revolutionised traditional threat detection methods through enabling proactive identification and response to evolving threats.

At Cisco, we lead by leveraging AI to analyse vast data volumes, detect threats, and ensure seamless operations. Our Cisco Talos security team, leveraging AI for years, processes approximately 550 billion security events daily and blocks around nine million emails per hour, showcasing our commitment to proactive threat mitigation, smoother workflows, and safeguarding digital ecosystems.

Cisco has been at the forefront of leveraging AI and machine learning to enhance cybersecurity defenses. One notable example is our AI Assistant for Security, which reframes how organisations think about cybersecurity

outcomes and tip the scales in favor of defenders by helping make informed decisions, augment existing capabilities and automate complex tasks through extensive integrations and unmatched visibility across the network and security.

Additionally, Cisco combines AI with its breadth of telemetry across the network, private and public cloud infrastructure, applications, internet, email, and endpoints. Our predictive AI capabilities in Advanced Malware Protection (AMP) enable statistical modeling and threat analysis, while Cisco Talos and cloud security products utilise AI and ML to detect malware samples and identify email threats efficiently. These advancements underscore Cisco's commitment to making AI pervasive in cybersecurity, empowering organisations to navigate the evolving threat landscape confidently.

Jiten Sil

VP Strategic Initiatives, Bahwan CyberTek

The last few years were a period of dynamic transformation. Bold and rapid recalibration helped progressive enterprises reduce costs, optimise processes, and create new products and markets. This shift, however, also exposed vulnerabilities putting these enterprises at risk. Instances of phishing, ransomware, and malware increased significantly last year, with some reports claiming 20% increase in data breaches from 2022 to 2023. In the Middle East alone, 77% of organizations witnessed ransomware activity.

Decision makers, in the age of AI, are no longer struggling to cope with these challenges. They're building cyber security strategies with AI at the crux of it, keeping their enterprises a step ahead of threats. AI has the capacity to automate time-consuming redundant processes, enabling analysts to focus a lot more on mitigation and prevention than monitoring. Powered by humans, AI can effortlessly sift and analyse huge volumes of data, quickly and accurately saving precious amount of time.

Using our product engineering expertise, we've created a cutting-edge Managed Security Services and Threat Intelligence Platform. This platform not only tackles current threats but also empowers organisations to stay ahead of cybercriminals proactively. With a strong implementation of 'intelligent threat hunting and investigation' alongside automated incident response, we help businesses keep pace with the constantly evolving cybercrime landscape. This ensures their security and preparedness for the future.

Lev Matveev

Chairman of the Board of Directors, SearchInform

AI and neural networks help specialists worldwide to deal with a wide range of tasks, reduce the probability of human error and optimise work processes. However, not all fields are in dire need of AI implementation.

Regarding insider threat prevention, we at SearchInform don't believe that AI deals with information security (IS) tasks better than already developed algorithms and solutions. The fact is that AI does not yet possess the universal cognitive functions that are so crucial for IS, in particular, for prevention of data breaches.

Until AI and neural networks have such functions, they won't replace existing IS solutions.

It is too early to say that AI plays a pivotal role in information security. However, functions, such as image and face recognition and audio-to-text conversion, help to prevent data leaks.

We've added these functions to our DLP for determining whether the legitimate user or unauthorised person is at a PC and for detecting attempts to take a picture of the monitor. The implementation of AI has also simplified audio transcription in messengers and reduced the number of data leaks through this channel.

Other developers' experience shows that machine learning is effective in detecting phishing, bullying, and other violations.

Majid Ahmed Khan

Director – Service Design & Architecture, HelpAG

ML algorithms and AI technologies have transformed threat detection, enhancing accuracy and speed by analysing vast datasets for patterns and anomalies. This proactive approach, coupled with AI-driven automation, reduces the time between detection and mitigation. ML's role in establishing automatic baselines and triggering events when deviations occur elevates detections from static logic to dynamic, automated processes. Integration of AI with threat intelligence feeds strengthens detection by correlating internal data with external threat intelligence. Additionally, generative AI streamlines the creation of threat detection content, enabling rapid deployment in relevant technologies like SIEM systems. At Help AG, we employ intelligent automation in our security operations to ensure timely, consistent, and intelligent detection and response, ultimately ensuring effective incident handling.

Help AG has been pioneering the integration of AI and ML into cybersecurity strategies for years, recognising the necessity to combat evolving threats with advanced technologies. In a recent incident, our ML-driven threat detection system flagged an alarming anomaly: a user within a specific department began accessing a new system, deviating from their established behavioral patterns. Further investigation confirmed unauthorised access by an adversary. This immediate detection showcases our precision and dynamic adaptability to recognize patterns rather than settle on static logic, minimising false positives and efficiently

allocating resources. This rapid response mitigated potential risks, preventing breaches. Our scalable AI-driven solutions cater to organizations of all sizes, future-proofing defenses against evolving threats.

Meriam El Ouazzani

Regional Director, META, SentinelOne

Machine learning algorithms and artificial intelligence (AI) technologies are revolutionising traditional threat detection methods in cybersecurity by enabling faster and more accurate identification of threats. These advancements empower security teams to analyse vast amounts of data in real-time, detecting anomalies and potential attacks with greater precision. AI-driven systems can adapt and learn from new data, continuously improving their ability to identify and mitigate threats. Specifically, they provide advantages such as enhanced threat-hunting capabilities, quicker response times, and the ability to detect previously unseen patterns of malicious behavior.

SentinelOne has demonstrated its efficacy in bolstering cybersecurity defenses through AI and machine learning. As pioneers in applying AI to cybersecurity, our threat-hunting platform employs AI algorithms to analyse diverse datasets, including endpoint, network, cloud, and user data, enabling proactive threat identification. By leveraging natural language processing, security teams can swiftly query and receive actionable insights, facilitating rapid response to potential threats. Our AI-driven approach has enabled businesses to detect and neutralize emerging cyber threats before they escalate, fortifying their security posture. This proactive stance not only enhances defense mechanisms but also instills confidence in organisations, mitigating risks in today's dynamic cybersecurity landscape.

Nizar Elfarra

Regional Sales Engineering Leader, SEEMEA, Commvault

The volume, variety and velocity of data resulting from the pools of cyber security and advance warning systems are overwhelming traditional data analytics. However, AI and ML make it easier to identify patterns and anomalies, enabling faster, more accurate and more cost-effective detection of potential threats. Such capability allows for the swift analysis of complex and evolving threats, thereby enhancing security posture. ML algorithms continuously learn and adapt, also aiding in reducing dwell time by providing early warning insights. ML and AI also has an often overlooked benefit of helping analysts learn - a continual process to improve the 'Observe - Orient - Decide - Act (OODA)' loop.

Leveraging AI and machine learning through our Commvault Cloud platform helps our customers monitor operational activity, such as backup jobs and unusual file activity changes in backups. For example, by analysing anomalies such as backup job status, irregular backup sizes, MIME type mismatches, and unusual file extensions, our platform can proactively detect and alert on potential threats, including malware infiltration or unauthorised data access to backups. Moreover, we utilise ML behavioural analytics to identify patterns indicative of malicious activity, enabling swift response measures. Such measures significantly enhance our clients' cyber resilience, ensuring quick detection, clean recoveries, and robust protection against emerging threats while minimising downtime and data loss.

Toni El Inati

RVP Sales, META & CEE, Barracuda Networks

AI can be used to enhance the volume, speed and quality of threat detection and intelligence. Among other things, AI-based algorithms can be used to detect anomalies, analyse behavioural data, recognize patterns and for predictive analysis. This collectively empowers organisations to identify and respond to emerging threats more effectively. AI's ability to analyse vast amounts of unstructured data from varied sources and native formats, current and historical data helps to establish baselines and it can learn and adapt all the time.

These capabilities are rounded out by the ability of AI systems to enable the automation and enhancement of incident response. With the right AI tools, security teams can detect, contain and neutralise attacks quickly and more effectively, reducing human error and accelerating incident triage.

By integrating AI, Security Operation Centers (SOCs) can significantly improve threat detection and response platforms, creating flexible defence mechanisms against advanced threats.

Barracuda has empowered businesses to harness AI and machine learning in safeguarding against cyber threats. For example, through

Barracuda Email Protection, our AI-driven models combat 13 email threat types, bolstering gateway and API-enabled defences. Our SecureEdge SASE platform, part of Barracuda Network Protection, ensures comprehensive network security with Zero Trust Access capabilities, while Barracuda Application Protection leverages AI to safeguard applications and APIs seamlessly. Additionally, Barracuda Data Protection offers secure backup solutions, shielding against ransomware attacks targeting backups. Our Managed XDR services further enhance cybersecurity with comprehensive capabilities and a cutting-edge Security Operations Center. Through integrated platform components and ongoing advancements, Barracuda enables businesses to proactively identify and respond to emerging threats, fortifying their overall security posture. These are just a few of the real-world examples of how our AI powered solution delivers real world protection to businesses on a daily basis.

Walid Gomaa

CEO, Omnix International

ML algorithms and AI technologies are transforming traditional approaches to threat detection in cybersecurity. They facilitate the automated analysis of extensive data volumes, pinpointing patterns, and anomalies indicative of malicious behavior. They adapt and learn from emerging threats, progressively enhancing detection precision. Moreover, they expedite response times by automating specific tasks, alleviating the workload on human analysts.

AI excels in discerning intricate attack patterns across varied data sources, even when attackers attempt to conceal their actions. It automates real-time threat response by promptly flagging and neutralising suspicious activities. Continuously learning from past incidents and feedback, AI/ML systems consistently refine their effectiveness, remaining one step ahead of evolving threats. Additionally, ML and AI streamline proactive threat hunting, empowering organisations to proactively address emerging threats.

Within endpoint security, ML algorithms are deployed to scrutinise endpoint data, swiftly identifying potential threats and responding promptly to prevent breaches. Similarly, in Network Traffic Analysis, AI algorithms actively monitor network traffic patterns, rapidly detecting abnormal behaviors and autonomously mitigating risks.

In threat intelligence, AI analyses extensive threat intelligence data, empowering organizations to identify emerging threats and adapt their defenses. Furthermore, within User Behavior Analytics, ML examines user behavior patterns, assisting in uncovering insider threats and unauthorised access attempts. AI/ML detects and classifies malware by training algorithms to recognise diverse malware characteristics, thereby enabling the real-time identification of new malware variants.

Finally, in fraud detection, AI algorithms analyse transaction data, facilitating the detection of fraudulent activities and empowering organisations, particularly financial institutions, to block suspicious transactions in real-time.

WHY DNS EXPLOITS CONTINUE TO BE A TOP ATTACK VECTOR IN 2024

TERRY YOUNG, DIRECTOR OF SERVICE PROVIDER PRODUCT MARKETING, A10 NETWORKS

The world of IT security has become more sophisticated and complex; as threats have grown exponentially, they have also become more blended, obscure, and harder to remediate. Today, most organisations have experienced some kind of attack, with many experiencing multiple attacks, and it is no longer a matter of if, but when, an attack will take place.

The growth of cybercrime-as-a-service, especially DDoS-as-a-service, has enabled criminals to purchase or rent tools and services that enable them to carry out attacks without having to develop expertise themselves. Combining such tools with attractive financial incentives and a wide collection of ready-made victims, it is easy to see why this is such a lucrative industry for criminals.

Top attack techniques

The cost of a network, website or service being down or unavailable can be probative. The average cost of downtime across all industries has historically been about $5,600 per minute, but recent studies have shown this cost has grown to about $9,000 per minute. For higher risk industries such as finance, government, healthcare, manufacturing, media, retail, and transportation their average cost of downtime tends to be over $5 million per hour.

One of the most popular attack

techniques involves the domain name system (DNS). The DNS protocol is essential to every internet-based service and is used to translate alphabetic domain names into a set of numerical internet protocol addresses. DNS is one of the key protocols that makes the internet work.

Why DNS is a favourite attack vector

Today, many organisations provision their own DNS infrastructure to ensure uninterrupted operations of their IT infrastructure and business applications. For example, in many organisations, work computers default to using the organisation's own DNS servers. This helps internal users access internal websites while keeping such domain names confidential and secure. However, DNS still remains one of the favourite attack vectors for cyber criminals for two main reasons:

- It is an inherently insecure protocol, and easier to target.
- DNS is fundamental to the operations of the internet and applications, and therefore bringing it down can have a much greater impact compared to simply targeting individual applications or services.

As more organisations rely on online applications, DNS exploits have become more common. In a 2023 IDC study, 88% of organisations have experienced one or more DNS attacks on their network, with an average of seven per year and each successful attack costs the business, on average, $942,000.

Delving into DNS attack techniques

There are several different DNS-based attack techniques including: DNS tunneling, DNS phishing, DNS hijacking or credential attacks, DNS spoofing, and DNS malware. DNS attacks are also used as the basis for both DDoS and more advanced phishing attacks.

Many DDoS attacks rely on ways to abuse DNS protocols, including traffic amplification, subdomain attacks, DNS floods and DNS recursion attacks. DNS hijacking, for example, allows attackers to re-route queries from an organisation's servers to destinations that they control, and it is often used to insert malware into endpoints. With DNS spoofing, malware is injected into DNS caches, or directly via DNS tunneling, so hackers can redirect DNS query traffic. DNS NXDomain flood attacks send spurious queries to nonexistent domain names with requests for invalid or non-existent records, tying up servers.

All of these types of attacks can have short- and long-term implications. In the immediate aftermath of an attack, an organisation may experience downtime or loss of productivity as a result of systems being taken offline. This can lead to revenue loss, reputational damage, and regulatory fines. Long-term impacts include damage to brand reputation, loss of customers, and decreased market share.

The challenge with multiple products to protect DNS

With the emergence of each new threat and the technology to counter it, organisations have traditionally responded by deploying a new security product to remediate the immediate threat at hand. Over time, this has led to the deployment of numerous security devices in the network, resulting in the following challenges:

- **Increased complexity:** With many security devices in the network, the task of deploying, managing, and troubleshooting has become increasingly complex. Each device has its own separate management interface and configuration commands that require specialised knowledge to deploy and troubleshoot.
- **Increased cost:** Upgrading DNS infrastructure to meet growing traffic needs requires upgrading most, if not all devices. This results in the need to purchase multiple different products, resulting in high purchase and licensing costs.
- **Slow performance:** Some of the newer DNS technologies, such as DNS over HTTPS (DoH) and DNS over TLS (DoT) require TLS decryption/encryption processing, which is highly CPU-intensive. However, DNS servers were not originally designed for such processing, therefore adding DoH/DoT can lead to a severe slowdown in overall performance.
- **Unsuitable for hybrid cloud:** All these problems are further compounded by the growing adoption of hybrid cloud. This is because many of the legacy security products that have been deployed in private data centres may either not be available or may not be optimally suited for such a deployment. This leads to adoption of cloud-specific offerings, adding to the complexity and cost of deployment.

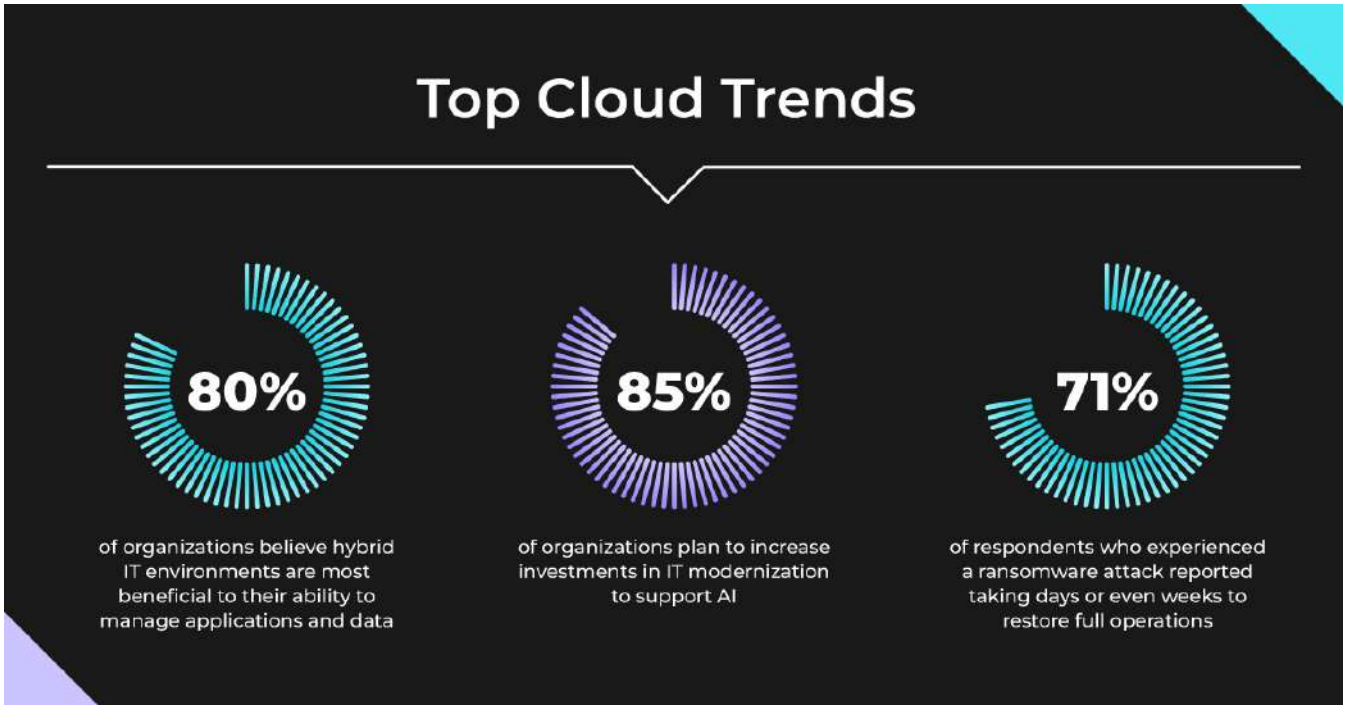
DNS STILL REMAINS ONE OF THE FAVOURITE ATTACK VECTORS FOR CYBER CRIMINALS

Securing and simplifying your DNS infrastructure

DNS is a critical component of the internet infrastructure, and it is important that DNS is always up and running to ensure normal business operations. However, DNS is also susceptible to a range of attacks and unfortunately no single security method can prevent all the different types of attacks. Therefore, an all-encompassing approach is required, including DNS load-balancing, DNSSEC, DoH/DoT, and DNS caching to ensure DNS infrastructure is constantly available and performing optimally.

Only with a comprehensive set of DNS security solutions can organisations secure and simplify their DNS infrastructure without compromising on performance or the user experience.

AI SECURITY, SUSTAINABILITY MAJOR DRIVERS FOR IT MODERNISATION: NUTANIX



Nutanix, a leader in hybrid multicloud computing, has announced the findings of its sixth global Enterprise Cloud Index (ECI) survey and research report, which measures enterprise progress with cloud adoption. This year's ECI report revealed the use of hybrid multicloud models is forecasted to double over the next one to three years as IT decision makers are facing new pressures to modernise IT infrastructures because of drivers like AI, security, and sustainability.

As organisations continue to grapple with the complexities of moving applications and data across environments, the ECI report highlighted the growing importance of hybrid multicloud infrastructure. The report found that security and innovation were the top drivers for moving applications from one environment to another over the past year. As AI takes center stage for businesses, ECI respondents identified increasing investments to support AI strategy as their #1 priority, followed closely by investment in IT modernisation.

"Whether it be because of AI, sustainability, or security imperatives, IT organisations are facing ever-increasing pressure to modernise their IT infrastructure quickly," said Lee Caswell, SVP, Product and Solutions Marketing at Nutanix. "80% of ECI respondents are planning to invest in IT modernisation, with 85% planning to increase their investments specifically to support AI. What this year's ECI reveals is that organisations need to support the technologies of tomorrow by future proofing their IT infrastructure today. Hybrid multicloud continues to emerge as the infrastructure standard of choice because of the flexibility it provides to support traditional VM and modern containerised applications and movement between clouds and on-prem."

Key findings from this year's report include:

- Hybrid multicloud infrastructure deployments will become an infrastructure standard. 90% of ECI respondents are taking a "cloud smart" approach to their infrastructure strategy – leveraging the best environment (e.g., data center, public cloud, edge) for each of their applications. Given the pervasiveness of this approach, it is no wonder that hybrid and multicloud environments have become the de facto infrastructure standard. Furthermore, over 80% of organisations believe hybrid IT environments are most beneficial to their ability to manage applications and data.
- Ransomware protection is top of mind for both CXOs and practitioners but most organisations continue to struggle in the wake of attacks. Ransomware and malware attacks will remain existential threats to modern enterprises, with the cat-and-mouse game between malicious actors and enterprise security professionals set to continue throughout 2024. Yet, data protection and recovery remain a challenge, as 71% of ECI respondents who experienced a ransomware attack reported taking days or even weeks to restore full operations. To help address this, 78% of organisations say they plan to increase investments in ransomware protection solutions throughout this year.
- As organisations seek equilibrium driven by security and innovation, application and data movement remains a complex challenge. Enterprise workloads – including their applications and data – often find their way into the IT environment which best suits their needs, whether that environment is an on-premises data center, the public cloud, a smaller edge location, or a mix of all three. This diversity of application placement is part of the reason why 95% of ECI respondents say they moved applications from one environment to another over the past year, with security and innovation as the top drivers for this movement. Enterprises should expect application and data movement to remain constant, and plan infrastructure choices accordingly – emphasising flexibility and visibility.
- IT teams aren't just planning their sustainability programs, they are actively implementing them starting with IT modernisation. 88% of ECI respondents agree that sustainability is a priority for their organisation. However, unlike in the previous report where action was limited, many organisations indicate they are already taking active steps to implement sustainability initiatives, with the most common being modernising IT infrastructure. This is a fascinating result, and one that shows the direct impact of IT infrastructure on sustainability.
- Infrastructure modernisation is becoming an imperative, driven by AI, modern applications and data growth. ECI respondents identified increased investment to support AI strategy as their #1 priority, followed closely by investment in IT modernisation. Furthermore, 37% of ECI respondents indicate running AI applications on their current IT infrastructure will be a "significant" challenge. In order to mitigate and overcome this challenge, organisations are prioritising IT modernisation and edge infrastructure deployments, which can facilitate faster processing and access to data. This, in turn, can help improve their ability to link data from multiple environments to give better visibility into where data resides across their sprawling ecosystems

SECURITY AND INNOVATION WERE THE TOP DRIVERS FOR MOVING APPLICATIONS FROM ONE ENVIRONMENT TO ANOTHER OVER THE PAST YEAR

For the sixth consecutive year, Vanson Bourne conducted research on behalf of Nutanix, surveying 1,500 IT and DevOps/Platform Engineering decision-makers around the world in December 2023. The respondent base spanned multiple industries, business sizes, and geographies, including North and South America; Europe, the Middle East and Africa (EMEA); and Asia-Pacific-Japan (APJ) region.

MOBILE IDS, MFA AND SUSTAINABILITY EMERGE AS TOP TRENDS: HID

HID, a worldwide leader in trusted identity solutions, announces its 2024 State of the Security Industry Report, which gathered responses from 2,600 partners, end users, and security and IT personnel worldwide, across a range of job titles and organization sizes representing over 11 industries.

The 2024 State of Security Report delves into the underlying concerns driving upcoming innovations and the technologies that underpin them, helping security leaders to be proactive in adapting to evolving challenges. Conducted in the fall of 2023, this year's survey reveals six themes, as follows:

1. Mobile identity is expected to be ubiquitous in the next five years

Given the widespread use of mobile devices, momentum continues to build around their use in support of identity. Within the next five years, surveyed end users state that nearly 80% of organisations will deploy mobile IDs. Industry partners are even more optimistic in their outlook, stating that 94% of their customers will have deployed mobile IDs.

2. Multi-Factor Authentication is widespread, despite slow but growing implementation of Zero Trust

More than 83% of end users respondents said their organisation currently uses Multi-Factor Authentication (MFA), mainly due to the vulnerabilities of passwords. For many, this represents the first step on the longer journey toward Zero Trust, an approach to security that calls for organisations to maintain strict access controls and to never trust, always verify anyone – internal or external – by default. Zero Trust has been implemented in 16% of organisations with over 100,000 employees and 14% in those with up to 10,000 employees, according to the survey.

With MFA being widespread, the eventual end of passwords is imminent. The creation of new standards such as FIDO (Fast Identity Online), which uses "standard public key cryptography techniques to provide phishing-resistant authentication," will pave the path to new and more secure authentication options that will be part of a more robust Zero Trust architecture.

3. Sustainability becomes a growing driver in business decisions

Among HID's survey respondents, sustainability continues to rank high as a business priority, with both end users and partners rating its importance at a "4" on a 1-to-5 scale. Additionally, 74% of end users indicate the importance of sustainability has grown over the past year, and 80% of partners reported the trend growing in importance among their customers.

4. Biometrics continues its impressive momentum

In this year's survey, 39% of installers and integrators said their customers are using fingerprint or palm print, and 30% said they're using facial recognition. The momentum continues to build as 8% plan to test or implement some form of biometrics in the next year and 12% plan to do so in the next three to five years.

5. Identity management points up to the cloud

Nearly half of end users are moving to cloud-based identity management, with 24% already using it and another 24% in the process of implementing such systems. Industry partners say their customers face several hurdles here, including existing reliance on legacy/on-prem equipment (28%), lack of budget (24%), and cloud-based identities simply not being a business priority (21%).

6. The rise of artificial intelligence for analytics use cases

Conversations about AI have come to dominate the business landscape, and many security professionals see AI's analytic capabilities as the low-hanging fruit to enhance identity management. Rather than looking to AI to inform the entirety of the security system, it's possible to leverage data analytics as a way to operationalise AI in support of immediate outcomes.

رقميات
Raqmiyat

Secure Your Digital Future

Simple. Secure. Resilient.

Secure Your Enterprise IT Footprint For A Safer Digital Journey

www.raqmiyat.com

UAE | KSA | INDIA

Keep an eye on your home from anywhere

Video doorbells, security cameras and alarm system

Ring lets you monitor every corner of your property.
With a Video Doorbell at your door and Security Cams around the house, you can create a Ring of Security around your entire home.

Ring... smart security for every home.

ring
an amazon company

For more information, contact mea@ring.com or visit www.ring.com

Available at:

Dubai	MYZ Tel: +971 4 351 1825	DSR Tech Tel: +971 4 238 0921	AL Ershad Tel: +971 4 359 8896	Hyper X Tel: +971 4 352 8820	Innox Tel: +971 4 386 1418	Al Muhairi General Trading LLC Tel: +971 4 393 2107
Abu Dhabi	Royal Phone Center Tel: +971 2 491 8888	Empower / Apple Plus Computers Tel: +971 2 445 3222	Asia Mobile Palace Tel: +971 55 652 3400			