JUL – SEP 2023

SECURITY SOLUTIONS TODAY

HOMELAND & CRITICAL
INFRASTRUCTURE SECURITY
DATA PROTECTION SOLUTIONS

IN THIS ISSUE

CONTACT

ASSOCIATE PUBLISHER Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

EDITOR Navkiran Kaur (sst@tradelinkmedia.com.sg)

MARKETING MANAGER Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

HEAD OF GRAPHIC DEPT / ADVERTISEMENT CO-ORDINATOR
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

CIRCULATION Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)

Vectors/Images Credit: Freepik.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
1 Paya Lebar Link, #04-01, Paya Lebar Quarter 1 (PLQ 1), Singapore 408533
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)

Disclaimer: The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

For advertising interests, please email us at **info@tradelinkmedia.com.sg.**

ZYXEL'S LATEST ROUTER PROVIDES SMALL BUSINESSES AND REMOTE WORKERS WITH A SIMPLER APPROACH TO WIFI 6E AND SECURITY

The SCR 50AXE router brings security, WiFi 6E, and cloud management together in one device, offering a simple and affordable solution for running small business networks.

Hsinchu, Taiwan – Zyxel Networks, the leader in delivering secure and cloud-powered networking solutions, has announced the release of its new SCR 50AXE - AXE5400 Tri-band WiFi 6E Secure Cloud-managed Router. The device is designed for small and home office users, remote workers, and small business owners looking for a network with best-in-class security and superfast WiFi.

While there are many security and WiFi devices currently on the market, small businesses and home office workers often struggle to find a cost-effective network management option that is simple, fast, secure, and easy to manage. The SCR 50AXE alleviates this pain, by bringing together everything needed in a small business network in one device, at an affordable price.

Subscription-free network security

The SCR 50AXE has been designed with security in mind, offering best-in-class security as part of the product, without any extra subscription or licensing costs. In-built and comprehensive threat management features help protect small businesses from ransomware, malware, mail fraud, phishing, intrusion, exploitation, and other attacks, using reputation-based technologies that deliver on performance while consuming less computing power. Additional security features, such as firewalling, country restrictions, IPsec VPN, and guest SSID are also available. Users looking for even more security and management options can choose to opt-in to the SCR Pro Pack licence, including real-time threat intelligence insights, web filtering (DNS) powered by Trellix, 30-day log retention, AI-assisted smart network management, and more.

All threat management features are presented in a graphical security dashboard showing threat insights and providing information on how devices connected to the router are behaving.

Superfast WiFi, simply managed

Alongside comprehensive security measures, the SCR 50AXE also includes the latest tri-band AXE5400 WiFi 6E, granting businesses access to the newly opened 6GHz radio with super-wide channels*. This allows them to take advantage of maximum speeds and low latency across multiple connections simultaneously. Additionally, the SCR 50AXE is cloud-native, meaning it has been created to be cloud-manageable through Zyxel's Nebula platform. By simply using the Nebula app, customers can finish onboarding the SCR 50AXE in just a few clicks and provision the WiFi name to the whole network, including the router and any additional access points. The app also allows users to seamlessly manage their connectivity and security from anywhere, via a single pane of glass, and receive an up-to-date view of their network security posture at a glance.

Having been through seventeen major updates since 2016, including the most recent version released in April 2023, Nebula has been transformed to incorporate real-world feedback, making it easier to access key features with a new menu structure and user interface enhancements. It is the most comprehensive cloud networking solution for SMBs, supporting 100 different models in its product portfolio. This includes the recently launched NWA90AX Pro WiFi 6 APs for small businesses, WiFi 6E APs, multi-gigabit switches, firewalls, and 5G mobile routers.

Mr. Crowley Wu, Vice President of Sales and Marketing at Zyxel Networks, says, “The small business market is often overlooked when it comes to network security and management, so we are proud to be offering an affordable solution that brings the best of both together in one device. Combining best-in-class security, superfast WiFi, and cloud management, the SCR 50AXE is the perfect solution for businesses looking to simplify their network management without sacrificing security or quality.”

For more information, please visit: https://www.zyxel.com/SCR_50AXE. ■

OKTA CUSTOMER IDENTITY CLOUD ADDS SECURITY CENTER TO ENTERPRISE PLAN

The new feature provides real-time monitoring of potential identity security events and threat response efficacy.

Singapore – Okta, Inc. (NASDAQ: OKTA), the leading independent identity provider, today announced the general availability of Security Center, a new feature that helps enterprise customers optimise their identity security posture by leveraging insights from Okta Customer Identity Cloud to provide a single view of authentication events, potential security incidents, and threat response efficacy. It includes real-time data on companies' current state of attack protection, out-of-the-box threat monitoring on major identity attack vectors, and application-level visibility into authentication traffic.

Image by Freepik

Determining whether an organisation's identity security posture is too restrictive or too lax is not trivial. Customers currently need to parse through logs of third-party tools or build their own, which requires expert-level experience to effectively identify attacks and be ready to respond to them. Security Center provides an improved way to visualise this type of data directly from the Okta Customer Identity Cloud.

Security Center leverages Okta Customer Identity Cloud security insights to provide CISOs, Security Operations professionals, and Identity teams a faster way to detect and respond to identity threats. It provides a streamlined view of authentication events, potential incidents, and threat response efficacy, allowing them to optimise their security posture without having to risk their bottom line after going through the learning curve themselves.

“Accurate detection alone doesn't ensure threat response is appropriate to the level of risk, given other business objectives like customer acquisition, retention, and growth,” said Jameeka Aaron, Chief Information Security Officer, Customer Identity at Okta. “As attacks against identity flows get more sophisticated and evolve to bypass detection, security teams often have to go through a learning curve on their own production environments, which can mean delayed detection of attacks and consequent business losses. Security Center leverages our focused expertise in identity security and packages it in a way that security operations professionals can understand and take action.”

Account takeover attacks targeting everything from sensitive healthcare data to loyalty points are one of the most common and costly cyber threats. Verizon's 2022 Data Breach Investigations Report (DBIR) found that 80% of corporate breaches involve compromised identity solutions. Security Center takes the work out of building your own tooling to identify and be able to respond to identity threats in a timely manner. Customers can understand their identity security landscape with a summary visualisation of major attack types, authentication events, and threat monitoring.

Security Center also allows companies to measure user experience impacts of Attack Protection features. Consumer-facing apps must balance security with user experience by minimising friction while maintaining appropriate protection against identity attacks. Security Center shows app owners in near-real time UX effects of defence tactics, allowing them to adjust security and friction as appropriate to their situation. Companies can fine-tune their attack protection strategy by seeing in near real-time how defence tactics like MFA, rate limiting, and CAPTCHA affect their applications. ■

TRENDNET LAUNCHES TAA AND NDAA COMPLIANT SURVEILLANCE SOLUTIONS

Torrance, California – TRENDnet®, a global leader in reliable SMB and consumer networking and surveillance solutions, has launched a new set of PoE surveillance cameras and network video recorder (NVR) that are both TAA and NDAA compliant. TAA and NDAA compliance allow these TRENDnet cameras and NVR to be used for federal government projects (in the US and other parts of the world).

The Indoor/Outdoor 5MP H.265 WDR PoE IR Network Cameras are available in bullet or fixed turret form factors, models TV-IP1514PI and TV-IP1515PI respectively. Each new PoE camera supports 5MP HD video, night vision, one-way audio, and an outdoor IP66 weather rating. They also support Wide Dynamic Range technology, which improves image quality and focus when the camera is exposed to high contrast lighting by enhancing dark areas of the image to make them more visible.

The two new cameras launch with an 8-Channel H.265 4K PoE NVR (TV-NVR1508), a comprehensive camera management solution with advanced video playback. It supports concurrent 4K camera streams and video recording on all channels. It can support up to over a month of continuous 4K HD video recording. The NVR will auto-recognize and power the TV-IP1514PI and TV-IP1515PI PoE cameras once they are connected.

The new TRENDnet surveillance cameras and NVR support easy cloud P2P QR code installation via the free Sentinel mobile apps available on the App Store® or Google Play™. You can also view live surveillance video on your mobile device. The cameras also come with a complimentary PC software, View Manager, to manage TRENDnet cameras.

Indoor/Outdoor 5MP H.265 WDR PoE IR Bullet Network Camera, TV-IP1514PI

- 5MP HD video (2592 x 1920) at 20 fps
- Night vision IR LEDs for night vision up to 30m (98 ft.)
- Built-in microphone for one-way audio
- Programmable motion detection recording and email alerts
- Micro SD card slot (up to 256GB)
- MSRP: $134.99 USD
- Product page

Indoor/Outdoor 5MP H.265 WDR PoE IR Fixed Turret Network Camera, TV-IP1515PI

- 5MP HD video (2592 x 1920) at 20 fps
- Night vision IR LEDs for night vision up to 30m (98 ft.)
- Built-in microphone for one-way audio
- Programmable motion detection recording and email alerts
- Micro SD card slot (up to 256GB)
- MSRP: $134.99 USD
- Product page

8-Channel H.265 4K (8MP) PoE NVR, TV-NVR1508

- 8MP (4K) concurrent camera streams up to 240fps
- Supports H.265 video encoding for high quality & low bandwidth streams
- One 3.5" SATA internal drive bay supports up to a 12TB of storage (HDD sold separately)
- External USB port supports up to 128GB
- Rackmount hardware included
- PoE power budget: 56W
- ONVIF certified

The Indoor/Outdoor 5MP H.265 WDR PoE IR Bullet Network Cameras (TV-IP1514PI and TV-IP1515PI), and the 8-Channel H.265 4K PoE NVR (TV-NVR1508) are available now for purchase worldwide. They can be found online on the TRENDnet Store, or through TRENDnet's worldwide authorised distribution network and retail partners.

For more information, please visit: www.trendnet.com. ■

CYBERATTACKERS LEVERAGED MORE THAN 500 UNIQUE TOOLS AND TACTICS IN 2022, SOPHOS' ACTIVE ADVERSARY REPORT FOR BUSINESS LEADERS FINDS

The Most Common Root Causes of Attacks Were Unpatched Vulnerabilities and Compromised Credentials, While Ransomware Continues to Be the Most Common "End Game". Dwell Time—Time From the Start of an Attack to When it's Detected—Decreased From 15 to 10 Days.

Singapore – Sophos, a global leader in innovating and delivering cybersecurity as a service, today released its Active Adversary Report for Business Leaders, an in-depth look at the changing behaviours and attack techniques that adversaries used in 2022. The data, analysed from more than 150 Sophos Incident Response (IR) cases, identified more than 500 unique tools and techniques, including 118 "Living off the Land" binaries (LOLBins). Unlike malware, LOLBins are executables naturally found on operating systems, making them much more difficult for defenders to block when attackers exploit them for malicious activity.

In addition, Sophos found that unpatched vulnerabilities were the most common root cause of attackers gaining initial access to targeted systems. In fact, in half of the investigations included in the report, attackers exploited ProxyShell and Log4Shell vulnerabilities—vulnerabilities from 2021—to infiltrate organisations. The second most common root cause of attacks was compromised credentials.

"When today's attackers aren't breaking in, they're logging in. The reality is that the threat environment has grown in volume and complexity to the point where there are no discernible gaps for defenders to exploit. For most organisations, the days of going at it alone are well behind them. It truly is everything, everywhere, all at once. However, there are tools and services available to businesses that can alleviate some of the defensive burdens, allowing them to focus on their core business priorities," said John Shier, field CTO, Sophos.

Image by Freepik

More than two-thirds of the attacks that the Sophos IR team investigated (68%) involved ransomware, demonstrating that ransomware is still one of the most pervasive threats for companies. Ransomware also accounted for nearly three-quarters of Sophos' IR investigations over the past three years.

While ransomware still dominates the threat landscape, attacker dwell time decreased in 2022, from 15 to 10 days, for all attack types. For ransomware cases, the dwell time decreased from 11 to 9 days, while the decrease was even greater for non-ransomware attacks. The dwell time for the latter declined from 34 days in 2021 to just 11 days in 2022. However, unlike in past years, there was no significant variation in dwell times between different sized organisations or sectors.

"Organisations that have successfully implemented layered defences with constant monitoring are seeing better outcomes in terms of attack severity. The side effect of improved defences means that adversaries have to speed up in order to complete their attacks. Therefore, faster attacks necessitate earlier detection. The race between attackers and defenders will continue to escalate and those without proactive monitoring will suffer the greatest consequences," said Shier.

The Sophos Active Adversary Report for Business Leaders is based on 152 incident response (IR) investigations spanning the globe across 22 sectors. Targeted organisations were located in 31 different countries, including the U.S. and Canada, the U.K., Germany, Switzerland, Italy, Austria, Finland, Belgium, Sweden, Romania, Spain, Australia, New Zealand, Singapore, Japan, Hong Kong, India, Thailand, the Philippines, Qatar, Bahrain, Saudi Arabia, the United Arab Emirates, Kenya, Somalia, Nigeria, South Africa, Mexico, Brazil, and Colombia. The most represented sectors are manufacturing (20%), followed by healthcare (12%), education (9%), and retail (8%). The Sophos Active Adversary Report for Business Leaders provides organisations with actionable threat intelligence and insights needed to optimise security strategies and defences.

To learn more about attacker behaviours, tools and techniques, Everything Everywhere All At Once: The 2023 Active Adversary Report for Business Leaders on Sophos.com.■

TENABLE ONE TO SUPPORT ON-PREMISES AND HYBRID DEPLOYMENTS WITH INTEGRATION OF TENABLE SECURITY CENTER

Increased deployment flexibility makes exposure management more accessible for customers.

Tenable®, the Exposure Management company, today announced that its Tenable One Exposure Management Platform now supports on-premises and hybrid deployments via a new integration with Tenable Security Center 6.1. Tenable One streamlines exposure management for hybrid vulnerability management deployments and may help on-premises customers transition to the cloud more quickly. Tenable is now the only vendor to offer exposure management for both on-premises and hybrid deployment models. With the introduction of this new integration, all Tenable One customers get access to both Tenable Vulnerability Management and Tenable Security Center, which gives them the flexibility to choose where they deploy their vulnerability management assets - in the cloud, on-premises or both, for a hybrid approach.

At the same time, Tenable Security Center customers can now explore the value of Tenable One's path into exposure management. This enables organisations to take full advantage of advanced exposure management features like Lumin Exposure View, Attack Path Analysis and Asset Inventory analytics to aid in cyber risk analysis and unified visibility of all exposures across the attack surface.

Tenable One combines vulnerability management, cloud security, external attack surface management (EASM), identity exposure, web app scanning and attack path analysis data to discover the most critical weaknesses before attackers can exploit them. It continuously assesses environments – from traditional IT assets to cloud resources and identity systems – delivering the broadest vulnerability coverage available.

Tenable Security Center customers can use Tenable One for a single view of all of their exposure data across the attack surface, with cyber risk analytics that enables organisations to easily prioritise remediation activity and communicate cyber risk to executive stakeholders. Both Tenable Security Center Plus and Security Center Director have been integrated to deliver additional enhanced visibility and simplified management value.

"Visibility into cyber risk factors should be a right and not a privilege, and yet for too many organisations who only deploy on-premises vulnerability management solutions, there's no way to truly see the full picture of where the greatest threats exist," said Glen Pendley, chief technology officer, Tenable. "Tenable's platform approach with Tenable One is continuing to expand its reach throughout the security stack and not only creating economies of scale but flexibility for customers as well."

For more informatio, please visit: https://www.tenable.com/lp/events/2023/rsac/. ■

DARKTRACE ADDRESSES GENERATIVE AI CONCERNS WITH THE INTRODUCTION OF AI MODELS THAT HELP PROTECT DATA PRIVACY AND INTELLECTUAL PROPERTY

New Darktrace data indicates 74% of active customer deployments have employees using generative AI tools. Darktrace introduces new risk and compliance models to help CISOs as they balance the opportunity and risk of inadvertent IP loss and data leakage from the use of generative AI and LLM-based tools.

Cambridge UK – In response to growing use of generative AI tools, Darktrace today announces the launch of new risk and compliance models to help its 8,400 customers around the world address the increasing risk of IP loss and data leakage. These new risk and compliance models for Darktrace DETECT™ and RESPOND™ make it easier for customers to put guardrails in place to monitor, and, when necessary, respond to activity and connections to generative AI and large language model (LLM) tools.

This comes as Darktrace's AI observed 74% of active customer deployments have employees using generative AI tools in the workplace[1]. In one instance, in May 2023 Darktrace detected and prevented an upload of over 1GB of data to a generative AI tool at one of its customers.

New generative AI tools promise increases in productivity and new ways of augmenting human creativity. CISOs must balance the

continue on page 8

desire to embrace these innovations to boost productivity while managing risk. Government agencies, including the UK's National Cyber Security Centre have already issued guidance about the need to manage risk when using generative AI tools and other LLMs in the workplace. In addition, regulators in a variety of jurisdictions (including the UK, EU, and US) and in various sectors are expected to lay out guidance to companies on how to make the most of AI without exacerbating its potential dangers.

"Since generative AI tools like ChatGPT have gone mainstream, our company is increasingly aware of how companies are being impacted. First and foremost, we are focused on the attack vector and how well-prepared we are to respond to potential threats. Equally as important is data privacy, and we hear stories in the news about potential data protection and data loss," said Allan Jacobson, Vice President and Head of Information Technology, Orion Office REIT. "Businesses need a combination of technology and clear guardrails to take advantage of the benefits while managing the potential risks."

At London Tech Week, Darktrace's Chief Executive Officer Poppy Gustafsson will be interviewed by Guy Podjarny, CEO of Snyk, in a fireside chat on 'Securing Our Future by Uplifting the Human,' where they'll discuss how can we future-proof organisations against cyber compromise and prepare teams to fend off unpredictable threats. Commenting ahead of London Tech Week, Poppy Gustafsson said, "CISOs across the world are trying to understand how they should manage the risks and opportunities presented by publicly available AI tools in a world where public sentiment flits from euphoria to terror. Sentiment aside, the AI genie is not going back in the bottle and AI tools are rapidly becoming part of our day-to-day lives, much in the same way as the internet or social media. Each enterprise will determine their own appetite for the opportunities versus the risk. Darktrace is in the business of providing security personalised to an organisation, and it is no surprise we are already seeing the early signs of CISOs leveraging our technology to enforce their specific compliance policies."

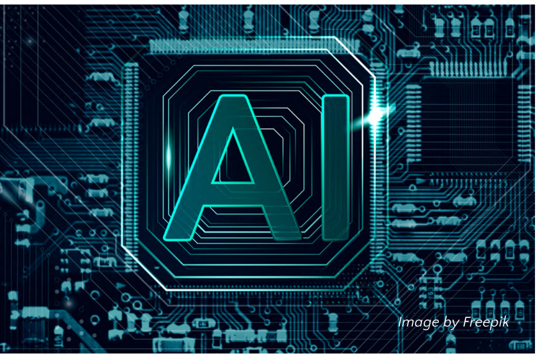


Image by Freepik

Image by Freepik

"At Darktrace, we have long believed that AI is one of the most exciting technological opportunities of our time. With today's announcement, we are providing our customers with the ability to quickly understand and control the use of these AI tools within their organisations. But it is not just the good guys watching these innovations with interest - AI is also a powerful tool to create even more nuanced and effective cyber-attacks. Society should be able to take advantage of these incredible new tools for good, but also be equipped to stay one step ahead of attackers in the emerging age of defensive AI tools versus offensive AI attacks."

To complement its core Self-Learning AI for attack prevention, threat detection, autonomous response, and policy enforcement, the Darktrace Cyber AI Research Center continually develops new AI models, including its own proprietary large language models, to help customers prepare for and fight back against increasingly sophisticated threats. These models are used across the products in Darktrace's Cyber AI Loop™.

"Recent advances in generative AI and LLMs are an important addition to the growing arsenal of AI techniques that will transform cyber security. But they are not one-size-fits-all and must be applied with guardrails to the right use cases and challenges," said Jack Stockdale, Chief Technology Officer, Darktrace. "Over the last decade, the Darktrace Cyber AI Research Center has championed the responsible development and deployment of a variety of different AI techniques, including our unique Self-Learning AI and proprietary large language models. We're excited to continue putting the latest innovations in the hands of our customers globally so that they can protect themselves against the cyber disruptions that continue to create chaos around the world." ■

IMPERVA® AND FORTANIX PARTNER TO PROTECT CONFIDENTIAL CUSTOMER DATA

Imperva Data Security Fabric and Fortanix Data Security Manager combine to provide end-to-end data security.

Singapore – Imperva, Inc., (@Imperva) the cybersecurity leader that protects critical applications, APIs, and data, anywhere at scale, and Fortanix, Inc. (@Fortanix), the Data Security company powered by Confidential Computing, announce that they have signed a partnership agreement, and have each joined the other's strategic partner program.

This partnership brings together two of the most innovative and trusted cybersecurity companies focused on multicloud data protection. The joint offerings from Imperva and Fortanix will provide the ability to manage the entire data security workflow for customers ensuring data privacy and compliance.

Imperva now offers Fortanix Data Security Manager (DSM), a highly scalable data security platform that delivers unified cryptographic and privacy services such as encryption, tokenization, dynamic data masking (DDM), secrets management, and enterprise key management. The solution works across multiple cloud service providers (CSPs) and provides an "easy button" to secure over 100 services. Fortanix DSM is simple to deploy and is offered in two editions — on-premises and a cloud-based SaaS solution — providing data security controls with both backed by FIPS 140-2 Level 3 certification.

"We're thrilled to partner with Imperva and take a best-in-class solution to the market together," says Anand Kashyap, CEO of Fortanix. "With Imperva's data discovery and classification capabilities and the Fortanix Data Security Manager SaaS and multicloud offering, customers have an end-to-end solution for securing workloads across the entire Data Lifecycle. This solution will help customers accelerate their data journey to the cloud while meeting the highest level of compliance."

Imperva Data Security Fabric (DSF) is a robust and scalable hybrid, multicloud platform for data discovery and classification, activity monitoring, access controls, security analytics, threat detection, and compliance reporting. Imperva DSF provides protection for unstructured, semi-, and structured data — both on-premises and in the cloud.

Organisations continue to seek the most efficient and effective data security solutions to address multiple use cases such as sensitive data protection, insider threat detection, and data risk management. They must also meet compliance and privacy requirements while operating diverse ecosystems at scale and consolidating legacy tools, all without impacting the speed and agility of the application development team to achieve the highest level of ROI.

With the combined strength of Imperva DSF and Fortanix DSM, this data security partnership will benefit organisations that find their traditional controls are no longer sufficient as they move data workloads and applications to the cloud. These data security solutions address data security and privacy regulations such as GDPR, CCPA, PCI DSS, and HIPAA by employing methods to help protect and control data confidentiality, data integrity, and data access across the hybrid multicloud environment.

"With the unprecedented explosion of data over recent decades and every day, unknown sensitive data might be anywhere — potentially exposed, and unsecured. But with this new partnership between Imperva and Fortanix, companies can now discover, classify, and secure their data using encryption and tokenization wherever it resides," says Dan Neault, SVP and GM of Data Security at Imperva. "Using the intelligence and flexibility of Imperva DSF combined with the power of the Fortanix DSM, finding sensitive data and taking the right steps to secure it is now easier than ever."

Additionally, Imperva is now able to provide customers with Fortanix DSM via the Imperva End-User Licence Agreement (EULA) providing streamlined procurement via a single vendor for sales, implementation, training, support, and services.

Building a complete cybersecurity technology ecosystem dedicated to data security and compliance

The Imperva Technology Alliance Program (TAP) enables technology companies, security vendors, and cloud service providers to co-market, sell, and integrate their products and platforms with the award-winning Imperva cybersecurity portfolio to create solutions that deliver added value for customers and generate revenue growth for TAP partners.

Imperva DSF continues to deliver more value to customers through these alliances. Additionally, Fortanix also supports the Imperva Web Application Firewall (WAF) by being able to store WAF encryption keys. ■

GOOGLE WORKSPACE EXTENDS ENTERPRISE-GRADE SECURITY AND DEVICE MANAGEMENT FOR HYBRID WORK WITH OKTA AND VMWARE

Industry-leading identity and device management solutions can be combined with Google Workspace, enabling secure, hybrid work at enterprise scale. JumpCloud is also integrating with Google Workspace to extend enterprise-quality security capabilities to small and midsize organisations.

Google Cloud today announced a series of new security alliances to bring more choice, capability, and simplicity to enterprise and public sector IT teams tasked with managing hybrid work at large scale, often for tens of thousands of users.

Google Workspace comes with industry-leading security built-in to its cloud-native, zero trust architecture. These capabilities combine threat defences powered by Google AI, client-side encryption, data privacy controls, and simple access to Google Cloud cybersecurity products like BeyondCorp Enterprise and Chronicle Security Operations, to automatically stop the vast majority of online threats before they emerge and support customers' regulatory and sovereignty needs. Through its ecosystem of cybersecurity partners, Google Workspace can extend these capabilities further by combining them with tools from the industry's leading security companies, enabling customers to adopt comprehensive, secure collaboration solutions to meet their specific security needs as part of a single Google Workspace offering.

"Global enterprises want to provide their workforces with more effective and secure ways of collaborating, with tools that increase productivity and avoid the vulnerabilities of older communications systems," said Sunil Potti, VP of cloud security, Google Cloud. "Through its growing ecosystem of security partners, Google Workspace offers the most enterprise-ready platform for hybrid work, providing organisations with confidence and flexibility to work securely with advanced capabilities from Okta, VMware, and more."

Securing Enterprise Workforces with VMware and Okta

Today, Google Cloud is extending the built-in identity, device, and access management capabilities of Google Workspace through new alliances with VMware and Okta, enabling large-scale businesses and public sector organisations to provide their workforces with FedRAMP-authorised collaboration and communication tools. Google Workspace works seamlessly with the enterprise-grade device and application management capabilities in VMware Workspace ONE, and the identity and access management capabilities in Okta Workforce Identity Cloud, providing organisations with more choice and flexibility in how they enable safer collaboration for their workforce.

Image by Freepik

- VMware Workspace ONE extends VMware's industry-leading unified endpoint management and zero trust access capabilities to Google Workspace. IT teams can manage all Google Workspace apps through VMware's comprehensive platform, which provides users with quick and easy access to business applications and makes it simple for administrators to onboard devices, change configurations, push automated OS updates, and more, without requiring a combination of disjointed third-party solutions. Workspace ONE administrators can also access a collection of device-health dashboards and reports, along with multi-tenancy for management across geographies, organisations, and use cases.
- Okta's Workforce Identity Cloud brings Okta's leading identity and access management capabilities to Google Workspace customers, securely connecting employees, contractors, and business partners from any device and any location. Workforce Identity Cloud's flexible rules and policies ensure employees have just the right level of access they need to get their work done. With Okta, employees can use their Google Workspace credentials across more than 7,000 pre-built apps in the Okta Integration Network to reduce password sprawl for increased security.

"The rapid shift to hybrid work has highlighted the need for IT teams to do more with less, while simultaneously balancing the increasing demands of security and productivity," said Renu Upadhyay, VP of product marketing, End-User Computing, VMware. "This VMware and Google partnership unlocks a transformative approach to end-user computing by creating an automated, unified, and secure experience across all endpoints, apps, and enterprise services, no matter where employees work."

continue on page 11

"Identity is the connective tissue between a business's ecosystem of people and the technologies they need to be successful in hybrid and remote work," said Arnab Bose, Chief Product Officer, Workforce Identity Cloud at Okta. "This partnership allows us to bring identity-powered security to Google Workspace customers while giving them an easy button to optimise their employee experiences and increase operational efficiency."

"In APAC, Okta is helping enterprises to leverage customer and workforce identity as new business assets in the same league as cash, working capital, reserves and property," said Ben Goodman, Senior Vice President and General Manager, Okta Asia Pacific and Japan. "Today's announcement is a veritable step towards helping organisations adopt next-generation workplace and collaboration toolsets, so that they can be much more responsive to client needs to deliver business impact."

Helping Small and Midsize Organisations Replace Legacy Directory Services with JumpCloud

JumpCloud Open Directory Platform provides customers with an alternative directory service to replace ageing Microsoft Active Directory servers with a modern cloud-based solution. The platform works seamlessly with Google Workspace, enabling identity workflows and synchronisation to thousands of applications, HRIS systems, and cloud infrastructure. It also combines these features with desktop and mobile device fleet management capabilities to ensure secure, frictionless access to applications and other resources from any operating system or location an employee chooses to work from.

"IT teams are looking for solutions that centralise access, device, and identity management. They need easier and more effective ways to secure how work happens," said Greg Keller, CTO and co-founder, JumpCloud. "The Google Cloud and JumpCloud bundle gives IT teams a modern and affordable solution to securely manage today's work on-prem, in the cloud or on the go. This partnership and bundled offering provides IT teams, and channel IT solution providers, a more affordable, best in class alternative to expensive, legacy Microsoft packages."

Google Workspace's Flexible, Secure Ecosystem

Google Workspace is committed to offering more choice by providing organisations of any size with the ability to combine purpose-built security tools from its ecosystem of cybersecurity partners, such as CrowdStrike, Palo Alto Networks, and now VMware, Okta, and JumpCloud. Over the coming year, deeper technical integrations with these partners will expand the joint capabilities available to Google Workspace customers, making it even easier to adopt Google Workspace for organisations with the most rigorous security and regulatory requirements. ■

VERIZON 2023 DATA BREACH INVESTIGATIONS REPORT: FREQUENCY AND COST OF SOCIAL ENGINEERING ATTACKS SKYROCKET

Human error continues to play a significant role in breaches across all industries.

- Cost per ransomware incident doubled over the past two years, with ransomware accounting for one out of every four breaches.
- Pretexting (Business Email Compromise) has more than doubled since the previous year.
- The human element is involved in 3 out of 4 breaches.
- Analysis of the Log4j incident illustrates the scale of the incident and the effectiveness of the coordinated response.

Basking Ridge, New Jersey – Verizon Business today released the results of its 16th annual Data Breach Investigations Report (2023 DBIR), which analysed 16,312 security incidents and 5,199 breaches. Chief among its findings is the soaring cost of ransomware – malicious software (malware) that encrypts an organisation's data and then extorts large sums of money to restore access. The median cost per ransomware more than doubled over the past two years to $26,000, with 95% of incidents that experienced a loss costing between $1 and $2.25 million. This rise in cost coincides with a dramatic rise in frequency over the past couple of years when

Image by Freepik

continue on page 12

the number of ransomware attacks was greater than the previous five years combined. That prevalence held steady this year: Representing almost a quarter of all breaches (24%), ransomware remains one of the top cyberattack methods.

The human element still makes up the overwhelming majority of incidents and is a factor in 74% of total breaches, even as enterprises continue to safeguard critical infrastructure and increase training on cybersecurity protocols. One of the most common ways to exploit human nature is social engineering, which refers to manipulating an organisation's sensitive information through tactics like phishing, in which a hacker convinces the user to click on a malicious link or attachment.

"Senior leadership represents a growing cybersecurity threat for many organisations," said Chris Novak, Managing Director of Cybersecurity Consulting at Verizon Business. "Not only do they possess an organisation's most sensitive information, but they are also often among the least protected, as many organisations make security protocol exceptions for them. With the growth and increasing sophistication of social engineering, organisations must enhance the protection of their senior leadership now to avoid expensive system intrusions."

Like ransomware, social engineering is a lucrative tactic for cybercriminals, especially given the rise of those techniques being used to impersonate enterprise employees for financial gain, an attack known as Business Email Compromise (BEC). The median amount stolen in BECs has increased over the last couple of years to $50,000 USD, based on Internet Crime Complaint Center (IC3) data, which might have contributed to pretexting nearly doubling this past year. With the growth of BEC, enterprises with distributed workforces face a challenge that takes on greater importance: creating and strictly enforcing human-centric security best practices.

"Globally, cyber threat actors continue their relentless efforts to acquire sensitive consumer and business data. The revenue generated from that information is staggering, and it's not lost on business leaders, as it is front and centre at the board level," said Craig Robinson, Research Vice President at IDC. "Verizon's Data Breach Investigations Report provides deep insights into the topics that are critical to the cybersecurity industry and has become a source of truth for the business community."

Image by Freepik

In addition to the increase in social engineering, other key findings in the 2023 DBIR include:

- While espionage garners substantial media attention, owing to the current geopolitical climate, only 3% of threat actors were motivated by espionage. The other 97% were motivated by financial gain.
- 32% of yearly Log4j vulnerability scanning occurred in the first 30 days after
- its release, demonstrating threat actors' velocity when escalating from a proof of concept to mass exploitation.
- External actors leveraged a variety of different techniques to gain entry to an organisation, such as using stolen credentials (49%), phishing (12%) and exploiting vulnerabilities (5%).

One of the ways that enterprises can help safeguard their critical infrastructure is through the adoption and adherence of industry-leading protocols and practices. Verizon recently became the first nationwide telecom provider to become a participant of

Mutually Agreed Norms for Routing Security (MANRS): a global initiative that provides crucial fixes to reduce the most common routing threats that can be exploited by attackers. Participation in MANRS demonstrates Verizon's commitment to implementing industry-best fixes to common routing threats and best practices geared at helping to prevent cyber incidents for customers on the network. ■

MEGAMATCHER ABIS USED FOR ID CREDENTIALS ISSUANCE IN MADAGASCAR

Neurotechnology partnered with MOSIP to provide a MOSIP-compliant ABIS for an ID credentials issuance pilot project in Madagascar.

Image by Freepik

Vilnius, Lithuania – Neurotechnology, a provider of deep learning-based solutions and high-precision biometric identification technologies, today announced its participation in a pilot project jointly executed by MOSIP and the government of the Republic of Madagascar using Neurotechnology's MegaMatcher ABIS.

The Madagascar Ministry of Digital Development, Digital Transformation, Posts and Telecommunications (MNDPT) has partnered with MOSIP to implement a pilot program for the issuance of ID credentials, using technology components that include a MOSIP-compliant Automatic Biometric Identification System (ABIS). The pilot will see an end-to-end demonstration of MOSIP, covering some registrations and ID generation. The MOSIP-compliant ABIS from Neurotechnology (MegaMatcher) is currently being used in the pilot.

MegaMatcher is an ABIS that includes a highly accurate and fast multi-biometric matching engine for managing enrollment, identification and verification transactions in identity management systems. The MegaMatcher ABIS features fingerprint, face, iris, palm-print and voice biometrics, as well as a ready-to-use interface for the operator to manage several other functionalities of the system. It is compliant with MOSIP's API specifications, and includes an adjudication module (under compliance) among other capabilities.

"We see MOSIP standards widely adopted in our industry, and we believe that in the future it will be required even more by different countries for their identity projects," said Antonello Mincone, Business Development Director for Neurotechnology. "MegaMatcher ABIS has already demonstrated its accuracy and speed capabilities in many large-scale national projects worldwide, and we consider it very important to have proven in the field that it is also fully compliant with MOSIP specifications."

Krishnan Rajagopalan, Head – Country Implementations in MOSIP, said, "MOSIP believes in working with our partners to ensure that adopting countries can choose from a variety of cutting-edge, MOSIP-compliant technology solutions. As more technology providers continue to join our growing ecosystem, we look forward to a long, fruitful partnership with Neurotechnology to help accelerate MOSIP's efforts with their vast experience in the field of biometric solutions."

The MOSIP implementations for MegaMatcher ABIS and MegaMatcher SDK are available on request for government institutions and system integrators who aim to test and use Neurotechnology's capabilities through this open standard.

About MOSIP

The Modular Open Source Identity Platform (MOSIP) was incubated at IIIT Bangalore as a global Digital Public Good. The platform enables digital-identity-led development and transformation for countries.

MOSIP offers adopters the flexibility to design, build and own critical software infrastructure for ID. The open-source and open-standard platform comes with a modular, configurable and customizable architecture, built on the principles of security and privacy by design. In addition to use cases, reference integrations and additional technology modules, the MOSIP project offers adopters an interoperable solution for putting ID to use.

The platform is currently being adopted by the Republic of the Philippines, Morocco, the Togolese Republic and Ethiopia in addition to being piloted in Sri Lanka, Guinea, Sierra Leone, Madagascar, Burkina Faso and Niger. ■

ESET ANNOUNCES SIGNIFICANT UPDATES FOR ESET PROTECT PLATFORM TO HELP BUSINESSES OF ALL SIZES KEEP AHEAD OF ATTACKERS

The addition of Vulnerability and Patch Management powered by OPSWAT, enables businesses to tighten their defences.

Singapore – ESET, a global leader in cybersecurity, today announces the upcoming availability of a significant enhancement to its unified cybersecurity platform, ESET PROTECT. The enhancement is designed to address both current and future digital security challenges for businesses worldwide. ESET has partnered with OPSWAT, a global leader in IT, OT and ICS critical infrastructure cybersecurity solutions, to bring integrated vulnerability and patch management into the ESET PROTECT Platform. ESET Vulnerability and Patch Management have been added to existing ESET PROTECT Complete along with a brand-new tier – ESET PROTECT Elite – to better safeguard organisations struggling to keep up with a constantly evolving threat landscape and ensure their systems are correctly patched.*

With centralised management from the ESET PROTECT Cloud console, organisations can easily assess security threats and manage patches across the entire network, ensuring timely detection and remediation of the latest zero-day vulnerabilities. Automated scanning and a wide range of filtering options enable organisations to quickly identify and focus on the security issues that mean the most to them. Further, with automatic and manual patching options, businesses can ensure that their endpoints are updated with the latest security patches in a timely manner.

“Threat actors are taking advantage of unpatched vulnerabilities as many businesses continue to struggle with managing patches and updates across their entire network, leaving their endpoints vulnerable to attacks. It can also be difficult for them to identify and prioritise vulnerabilities based on severity,” comments Pamela Ong, Sales Director – APAC, ESET. “Many organisations want solutions that will keep them safe, but not all know what to look out for. At ESET, we strive to provide easy-to-use, enterprise-grade security solutions to businesses of all sizes. The addition of ESET Vulnerability and Patch Management will give our customers flexibility and control so that their endpoints can be optimally patched promptly through customisable patching policies. This helps them minimise the risk of attack and disruption, keep costs down and at the same time meet various regulatory, ISO and cybersecurity insurance requirements.”

Image by Freepik

ESET Vulnerability and Patch Management scans thousands of popular applications, such as Adobe Acrobat, Mozilla Firefox, and Zoom Client, for over 35,000 common vulnerabilities and exposures (CVEs). Vulnerabilities can be filtered and prioritised based on exposure score, severity, and score over time. ESET Vulnerability and Patch Management provide a constantly evolving inventory of patches with patch name, version of the app, CVE, patch severity/importance, and affected applications. Businesses can launch immediate updates and begin patching via customisable options or manually when a patch has been identified. They can simplify the patching process further by prioritising critical assets and scheduling the remainder to off-peak times to avoid disruption. Organisations can take advantage of the Vulnerability and Patch Management multitenancy functionality to enjoy full visibility over the entire network yet be focused on a dedicated area.

ESET’s unified cybersecurity platform, ESET PROTECT, is a single-pane-of-glass cloud console that provides centralised visibility, management, and insight. The ESET PROTECT Platform integrates balanced breach prevention, detection, and response capabilities with the company’s industry-leading managed and professional services and threat intelligence. It is simple, modular, adaptable, and continuously innovated. With the launch of ESET PROTECT Elite, there are now four subscription tiers to the ESET PROTECT Platform for businesses of all sizes:

- **ESET PROTECT Entry** – an entry-level solution with competitive pricing that includes endpoint protection, server security, and the ESET PROTECT Cloud console.
- **ESET PROTECT Advanced** – providing first-class endpoint protection with advanced threat defence

continue on page 15

technology and full disk encryption.

- **ESET PROTECT Complete** – includes the new ESET Vulnerability and Patch Management capability, cloud application protection, and mail security to minimise cyber risks.
- **New ESET PROTECT Elite** – provides increased visibility and decreased cyber risks, ESET Vulnerability and Patch Management, ESET's native extended detection and response (XDR) capability, plus robust multifactor authentication.

"As cyberattacks keep evolving and the industry becomes increasingly complex, our offerings have transitioned to reflect changing business needs and a transitioning threat landscape. With the launch of ESET Vulnerability and Patch Management, we provide a pathway to swift remediation, helping keep disruption, and costs, down to a minimum for businesses," added Pamela Ong.

For more information, please visit: www.eset.com. ■

NETAPP APPOINTS ANDREW SOTIROPOULOS AS SENIOR VICE PRESIDENT AND GENERAL MANAGER FOR ASIA PACIFIC

Industry veteran joins cloud data management leader to chart its next lap of growth in Asia Pacific

Singapore – NetApp® (NASDAQ: NTAP), a global, cloud-led, data-centric software company, today announced that it has appointed IT industry veteran and senior business executive Andrew Sotiropoulos as Senior Vice President and General Manager for Asia Pacific (APAC).

Based in Singapore, Andrew will preside over NetApp's business and spearhead the company's expansion plans in the region. Reporting to NetApp President Cesar Cernuda, his priorities include growing NetApp's enterprise storage and cloud business, strengthening its partner ecosystem, and extending its leadership in regional markets.

Andrew has over three decades of experience in the technology industry, leading pan-regional teams to drive business growth and capture emerging opportunities. He most recently served as VP of Asia Pacific and Japan at Pure Storage. Andrew has also led teams at IBM and Lenovo. At IBM, he led the Global Technology Services division in Asia Pacific. He has extensive experience leading organisations in Asia Pacific and Global roles across both product and technology services segments.

Image by Freepik

Andrew takes over from Sanjay Rohatgi, who will be departing the company to pursue opportunities outside of the company, after nearly four years of leading NetApp's sales teams in Asia Pacific.

"As a global company, and having spent many years in APAC myself, we appreciate the importance of building and strengthening our long-standing relationships with business communities in the region," said Cesar Cernuda, President at NetApp. "I am delighted to have Andrew join us to continue the growth of our business as we empower our customers wherever they are on their respective cloud transformation journeys."

"NetApp is resolute in helping APAC organisations mitigate complexities to accelerate their digital transformation journeys, across on-premises and hybrid multicloud environments," said Andrew Sotiropoulos, Senior Vice President and General Manager, NetApp Asia Pacific. "I am excited to build on the 30-year foundation that NetApp has laid down, letting customers further boost their innovation speed, lower costs, and improve agility."

For more information, please visit www.netapp.com. ■

IBM LAUNCHES NEW QRADAR SECURITY SUITE TO SPEED THREAT DETECTION AND RESPONSE

Modernised, unified interface streamlines analyst response across the full attack lifecycle. Sophisticated AI and automation capabilities shown to speed alert triage by an average of 55%.

Singapore – IBM (NYSE: IBM) unveiled its new security suite designed to unify and accelerate the security analyst experience across the full incident lifecycle. The IBM Security QRadar Suite represents a major evolution and expansion of the QRadar brand, spanning all core threat detection, investigation and response technologies, with significant investment in innovations across the portfolio.

Delivered as a service, the IBM Security QRadar Suite is built on an open foundation and designed specifically for the demands of a hybrid cloud. It features a single, modernised user interface across all products – embedded with advanced AI and automation designed to empower analysts to work with greater speed, efficiency and precision across their core toolsets.

Today's Security Operation Center (SOC) teams are protecting a fast-expanding digital footprint that extends across hybrid cloud environments – creating complexity and making it hard to keep pace with accelerating attack speeds. They can be slowed down by labour-intensive alert investigations and response processes, manually stitching together insights and pivoting between disconnected data, tools and interfaces. SOC professionals say they spend around one-third of their day investigating and validating incidents that turn out to not be real threats, according to a recent survey.

Built on the company's existing leadership in 12 security technology categories, IBM has rearchitected its market-leading threat detection and response portfolio to maximise speed and efficiency and to meet the specific needs of today's security analysts. The new IBM Security QRadar Suite includes EDR/XDR, SIEM, SOAR, and a new cloud-native log management capability – all built around a common user interface, shared insights and connected workflows, with the following core design elements:

- **Unified Analyst Experience:** Refined in collaboration with hundreds of real-world users, the suite features a common, modernised user interface across all products: designed to dramatically increase analyst speed and efficiency across the entire attack chain. It is embedded with enterprise-grade AI and automation capabilities that have been shown to speed alert investigation and triage by 55% in the first year, on average.
- **Cloud Delivery, Speed & Scale:** Delivered as a service on Amazon Web Services (AWS), QRadar Suite products allow for simplified deployment, visibility and integration across cloud environments and data sources. The suite also includes a new, cloud-native log management capability optimised for highly efficient data ingestion, rapid search and analytics at scale.
- **Open Foundation, Pre-Built Integrations:** The suite brings together the core technologies needed across threat detection, investigation and response - built around an open foundation, an extensive partner ecosystem, and more than 900 pre-built integrations that provide strong interoperability between IBM and third-party toolsets.

"In the face of a growing attack surface and shrinking attack timelines, speed and efficiency are fundamental to the success of resource-constrained security teams," said Mary O'Brien, General Manager, IBM Security. "IBM has engineered the new QRadar Suite around a singular, modernised user experience, embedded with sophisticated AI and automation to maximise security analysts' productivity and accelerate their response across each step of the attack chain."

Co-innovation for Real-World Security Demands
The QRadar Suite is the culmination of years of IBM investment, acquisitions and innovations in threat detection and response. It features dozens of mature AI and automation capabilities that have been refined

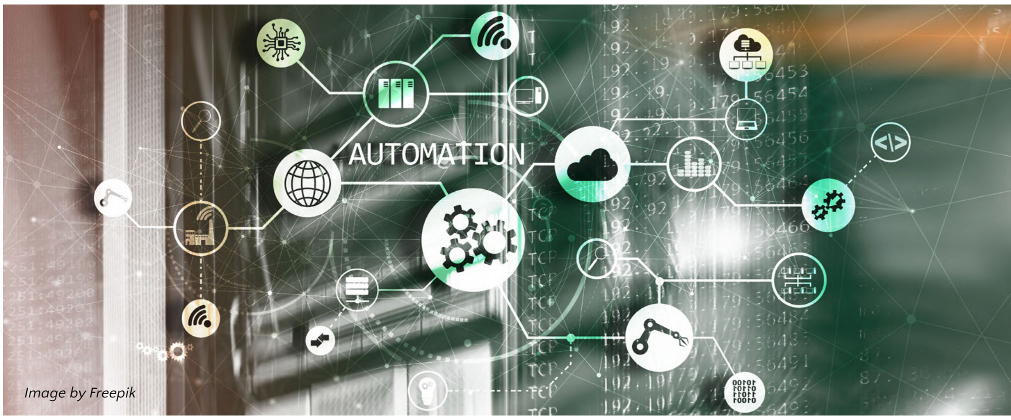


Image by Freepik

continue on page 17

over time with real-world users and data, including IBM Managed Security Service engagements with more than 400 clients. It also includes innovations developed in collaboration with IBM Research and the open source security community.

These AI-powered capabilities have been shown to significantly improve the speed and accuracy of SOC operations: For example, allowing IBM Managed Security Services to automate more than 70% of alert closures and reduce its alert triage timelines by 55%2 on average within the first year of implementation.

Bringing these capabilities together via the unified analyst experience, the QRadar Suite automatically contextualises and prioritises alerts, displays data in visual format for rapid consumption, and provides shared insights and automated workflows between products. This approach can drastically reduce the number of steps and screens required to investigate and respond to threats. Examples include:

- **AI-Powered Alert Triage:** Automatically prioritises or closes alerts based on AI-driven risk analysis, using AI models trained on prior analyst response patterns, along with external threat intelligence from IBM X-Force and broader contextual insights from across detection toolsets.
- **Automated Threat Investigation:** Identifies high-priority incidents that may warrant investigation, and automatically initiates investigation by fetching associated artefacts and gathering evidence via data mining across environments. The system uses these results to generate a timeline and attack graph of the incident based on the MITRE ATT&CK framework and recommends actions to speed response.
- **Accelerated Threat Hunting:** Uses open-source threat-hunting language and federated search capabilities to help threat hunters discover stealthy attacks and indicators of compromise across their environments without moving data from its original source.

By helping analysts respond faster and more efficiently, QRadar technologies can also help security teams improve their productivity and free up analysts' time for higher value work.

Open, Connected and Modernised Security Suite
The QRadar Suite leverages open technologies and standards across the portfolio alongside hundreds of pre-built integrations with IBM Security ecosystem partners. This model enables deeper shared insights and automated actions across third-party clouds, point products, and data lakes, which can reduce deployment and integration times from months to days or weeks.

The IBM QRadar Suite includes the following core products, initially delivered as SaaS and updated with the new unified analyst experience:

- **QRadar Log Insights:** A new, cloud-native log management and security observability solution providing simplified data ingestion, sub-second search and rapid analytics. It leverages an elastic security data lake optimised to collect, store and perform analytics on terabytes of data with greater speed and efficiency. It is designed for cost effective security log management alongside federated search and investigation.
- **QRadar EDR and XDR:** Helps companies protect their endpoints against previously unknown, zero-day threats – using automation and hundreds of machine learning and behavioural models to detect behavioural anomalies and respond to attacks in near-real time. It leverages a unique approach that monitors operating systems from the outside, helping avoid manipulation or interference by adversaries. For companies looking to extend their detection and response capabilities beyond the endpoint, IBM also offers XDR with alert correlation, automated investigation, and recommended responses across the network, cloud, email, and more, as well as managed detection and response (MDR).
- **QRadar SOAR:** Recent winner of a Red Dot Design Award for interface & user experience; helps organisations automate and orchestrate incident response workflows and ensure their specific processes are followed in a consistent, optimised and measurable way. It includes 300 pre-built integrations and offers out-of-the-box playbooks for responding to 180+ global data breaches and privacy regulations.
- **QRadar SIEM:** IBM's market-leading QRadar SIEM has been enhanced with the new unified analyst interface, which provides shared insights and workflows with broader security operations toolsets. It offers real-time detection, leveraging AI, network and user behaviour analytics, and real-world threat intelligence built to provide analysts with more accurate, contextualised and prioritised alerts. IBM also plans to make QRadar SIEM available as a service on AWS by the end of Q2 2023.

The IBM Security QRadar Suite is available today via individual SaaS offerings. **For more information, please visit: https://www.ibm.com/qradar.** ■

VIVOTEK CREATES INTERNATIONAL SMART SECURITY SOLUTION FOR CHI-HAI CULTURAL PARK IN TAIWAN

Towards a Future of New Smart City Paradigm.

Yet another successful case of cultural landmarks in Taipei, Taiwan! VIVOTEK (3454-TW), the global leading IP surveillance solution provider, has introduced international standard security solution to Ching-Kuo Chi-Hai Cultural Park (hereinafter referred to as "Chi-Hai Cultural Park") in Taipei to offer citizens a safe environment and experience when they visit the park and protect the park's important cultural heritage and historical displays from damage, while also strengthening the park's security under the premise of effective management of manpower and operating cost.

"With its great historical significance, Chi-Hai Cultural Park has now transitioned into a new cultural landmark. With upgraded security services, a balance is achieved between revitalization and preservation of historical heritage, creating new values for the park. VIVOTEK has over 20 years of industry experience and has recently undergone rebrand to transition from a surveillance equipment manufacturer to a comprehensive security solution brand, just like Chi-Hai Cultural Park's successful transformation that presents historical heritage and an image of revival," said Allen Hsieh, VIVOTEK Spokesperson and Director of Global Marketing Division. "In response to the market trend of AI, VIVOTEK will continue to introduce AI smart analysis capability to existing product lines and strive for integration of software and hardware and upgrade of services, proactively building safer and smarter security services for diverse places."

Solving the Conundrums of Revitalization and Preservation of Historical Sites, VIVOTEK Tailors for Chi-Hai Cultural Park Three Security Highlights

Opening up a cultural heritage to the public often faces two conundrums—difficulty of revitalization and preservation; moreover, most surveillance equipment has not been replaced or upgraded for years and many sites still use traditional analog cameras, where image resolution is affected by transmission distance. Also, these cameras only have the function of passive recording and lack real-time preventive mechanisms. Thus, during the preparatory period of Chi-Hai Cultural Park, VIVOTEK was tailored for the park's international standard smart security solution. For example, VIVOTEK has installed diverse products, such as fixed dome and bullet cameras and network video recorders, at important spots like Chiang Ching-Kuo Presidential Library, the first of its kind in Taiwan, and Exhibition Halls according to their specific needs, responding to the rigid demands of preservation of historical relics, prevention of incidents, and control of personnel access. Furthermore, for the park's perimeters and entrances with busy traffics, VIVOTEK's smart image analysis technology can also be utilised to detect abnormalities like intrusion, loitering, or line crossing detection, and notify the management through the system's real-time alerting function, significantly enhancing efficiency of the park's security management procedure and building a comprehensive smart security system.

On the Foundation of Smart Surveillance Service, VIVOTEK Builds Cross-Scene Security Solutions

As the leading global smart security brand, VIVOTEK has implemented the rebrand project since 2021. In addition to continued optimization and R&D of technologies, VIVOTEK also utilises existing surveillance products as carriers for horizontal introduction of applications and smart surveillance technology. VIVOTEK not only applies AI deep learning technology to image detection and analysis, but also develops different application scenes for object tracking, behaviour analysis, and facial or licence plate recognition; moreover, VIVOTEK's three major advanced search functions of attribute search, scene search, and re-search, enables one-key screening that precisely targets tags like gender, age, and clothes colour. The recently launched smart cloud surveillance service and system, VORTEX and VAST Security Station, are VIVOTEK's answer to the past pain points of untimely surveillance and protection and inaccessibility to security data. In the future, VIVOTEK will continue to optimise products and technologies and develop innovative technological applications, building for companies more smart solutions with greater efficiency, while also expanding diverse vertical applications in the areas of smart city, building automation, and transportation.

For more information, please visit www.vivotek.com. ■

HITACHI VANTARA, CISCO SIGN NEW STRATEGIC PARTNER AGREEMENTS TO HELP CUSTOMERS SIMPLIFY HYBRID CLOUD MANAGEMENT

Hitachi Vantara joins Cisco's Solution Technology Integrator and Service Provider Partner programs to offer customers complete data solutions and best-in-class managed services.

Singapore – Hitachi Vantara, the modern infrastructure, data management and digital solutions subsidiary of Hitachi, Ltd. (TSE: 6501), today announced two new global partnership agreements with Cisco. The agreements bring Hitachi Vantara into Cisco's Service Provider and Solution Technology Integrator (STI) partner programs, respectively, enabling Hitachi Vantara to seamlessly integrate Cisco technologies with its storage products and position the company as a leading data centre infrastructure and hybrid cloud managed services provider.

Many businesses are grappling with the complexities of data management and intelligence as they manage their expanding hybrid cloud footprints. According to IDC, 40% of companies will depend on multi-partner technology agreements by 2024 to address these concerns. Coinciding with the STI agreement, Hitachi Vantara now includes the Cisco UCS X-Series servers in its offerings to deliver a complete converged infrastructure (CI) solution. The server line becomes part of the "Cisco and Hitachi Adaptive Solutions" portfolio which pairs Cisco compute and networking with Hitachi Vantara's Energy Star-certified Virtual Storage Platform (VSP) to offer customers one of the most reliable, resilient and environmentally friendly IT infrastructure solutions on the market. The solution is now available for Hitachi Vantara customers, helping address a growing market need for converged data centre infrastructure.

As a member of Cisco's Service Provider program, Hitachi Vantara offers consumption-based managed services to Cisco customers looking for data centre and hybrid cloud services. The services can help address a critical shortage of skilled workers in the IT industry, enabling enterprises to adopt new and emerging technologies more effectively and rely on a trusted organisation in Hitachi Vantara to streamline their hybrid cloud operations.

Image by Freepik

"Hitachi Vantara and Cisco have been trusted partners for more than two decades, and these agreements are important additions to the innovative relationship these global technology leaders have built," said Kimberly King, senior vice president of strategic partners and alliances at Hitachi Vantara. "Successful partners adjust to meet customers' needs, both for today and for the future, and these developments do just that by offering the data-driven solutions and services they need the most."

"As customers seek to simplify their data centre operations, providing converged infrastructure solutions with managed services capabilities from two trusted global vendors can help them reduce risk and optimise their business outcomes," said Nick Holden, vice president of global strategic partners and co-sell at Cisco. "Together, Hitachi Vantara and Cisco make it easier for customers to navigate complex hybrid data centre and storage solutions."

"We're seeing a clear shift in market dynamics and consumer preferences that calls for integrated solutions, particularly from industry leaders like Hitachi Vantara and Cisco," said Steve White, vice president of channels & alliances, IDC. "These types of alliances are crucial to address a growing list of enterprise challenges that include sustainable practices, solution complexities, governance and supply chain issues, among others."

For more information, please visit: https://www.hitachivantara.com/en-us/partners/become-partner.html. ■

SAP AND GOOGLE CLOUD EXPAND PARTNERSHIP TO BUILD THE FUTURE OF OPEN DATA AND AI FOR ENTERPRISES

The new offering will unite SAP with Google Cloud's data and analytics technology, making enterprise data more open and valuable while advancing enterprise AI development

Singapore – SAP SE (NYSE: SAP) and Google Cloud announced an extensive expansion of their partnership, introducing a comprehensive open data offering designed to simplify data landscapes and unleash the power of business data. This offering enables customers to build an end-to-end data cloud that brings data from across the enterprise landscape using the SAP® Datasphere solution together with Google's data cloud, so businesses can view their entire data estates in real-time and maximise value from their Google Cloud and SAP software investments.

Data is the cornerstone of digital transformation and artificial intelligence (AI) development. Organisations spend significant resources building complex data integrations, custom analytics engines, and generative AI and natural language processing (NLP) models before they start to realise value from their data investments. Data originating from SAP systems, in particular, are among organisations' most valuable assets and can contain critical information on supply chains, financial forecasting, human resources records, omnichannel retail, and more. SAP Datasphere combines this mission-critical data with data from across the enterprise landscape, regardless of its origin. The ability to easily combine SAP software data and non-SAP data on Google Cloud, from virtually any other data source, means organisations can dramatically accelerate their digital transformation with a fully-defined data foundation that retains complete business context.

Christian Klein, CEO and member of the Executive Board of SAP SE, said: "Bringing together SAP systems and data with Google's data cloud introduces entirely new opportunities for enterprises to derive more value from their full data footprints. SAP and Google Cloud share a commitment to open data and our extended partnership will help break down barriers between data stored in disparate systems, databases, and environments. Our customers not only benefit from the business AI already built into our systems, but also from a unified data foundation."

Thomas Kurian, CEO, Google Cloud, said: "SAP and Google Cloud now offer an incredibly comprehensive and open data cloud, providing a foundation for the future of enterprise AI. Few resources are as important to digital transformation as data. By deeply integrating SAP data and systems with our data cloud, customers will be able to utilise our analytics capabilities, as well as advanced AI tools and large language models to find new insights from their data."

Image by Freepik

Enterprises in Southeast Asia, such as Blue Bird Group, JB Cocoa, Kopi Kenangan, Link Net, NTUC Enterprise, Ocean Network Express, Siam Cement Group, and Vingroup, just to name a few, have been leveraging Google Cloud and SAP's joint offerings to help them run their businesses more intelligently and sustainably, and achieve impactful results.

Yeo Yean Mei, Group Project and IT Manager, JB Cocoa, said: "SAP on Google Cloud centralises our business processes, from sales to logistics, and incorporates internal and external data for greater traceability and financial transparency. Our use of Google Cloud powered by renewable energy will enable us to meet our environmental, social, and governance (ESG) goals and, more broadly, contribute to our customers' emission reduction targets. With SAP on Google Cloud, we can automate complex intercompany transactions with a customised pricing engine to track commodity price fixing and forex hedging. We can analyse the changing risk exposure and position on a daily basis with real-time data. Our goal is to build a centralised production dashboard to perform more analytics directly on Google Cloud in the future, combining data sources from [our] Supervisory Control and Data Acquisition (SCADA) and SAP systems."

Zeng Fengping, Chief Technology Officer, Kopi Kenangan, said: "The combination of SAP and Google Cloud is a no-brainer. The cloud model brings a lot of advantages. It is an agile way to scale the business and an easy way to optimise operational costs. It also provides better service availability. RISE with SAP enables us to enjoy all the benefits of Google Cloud without the extra effort. Together, they serve one offering, which makes it an easy

continue on page 21

decision for us. It simplifies all efforts regarding running and maintaining SAP, and it also gives us the same level of service quality and data privacy protection that we can get in a traditional implementation."

Alan Sze, Deputy General Manager, BPIT, Ocean Network Express, said: "One advantage of running SAP on Google Cloud is the business continuity on a highly available platform. Google Cloud provides failover between sites so we can keep accounting tasks running even if a disaster occurs. This enables us to continue our operations without compromising on service quality to our customers.
The flexibility and scalability of Google Cloud made our upgrade easy – not to mention the reduction of operational costs and also the reduction of CO_2 emissions, which is in line with our corporate sustainability policy. We are in the midst of building our BigQuery cloud data warehouse and using Looker as our new business intelligence (BI) tool.
We are also planning to build our data lake in BigQuery, so that we can have the data analytics capability to achieve operational excellence and provide a better customer experience."

SAP and Google Cloud's new open data offering complements the RISE with SAP solution and will enable customers to:

- **Access business-critical data in real-time:** The integration between SAP Datasphere and Google Cloud BigQuery allows customers to easily access their most critical data in real-time without data duplication. This joint offering can unify data from SAP software systems, such as SAP S/4HANA® and SAP HANA® Cloud, providing organisations with a comprehensive view of their most important data on Google's data cloud.

- **Simplify data landscapes:** SAP and Google Cloud have co-engineered powerful data replication and federation technologies, which allow businesses to easily integrate SAP software data with BigQuery environments and leverage SAP and Google Cloud's leading data analytics capabilities. Now, customers can federate queries across SAP Datasphere and BigQuery to blend data from SAP and non-SAP software. This eliminates common data silos from sources that span marketing, sales, finance, supply chain, and more. For example, customers with wholesale business distribution models can now have full visibility into their products as they go through the sales pipeline and reach customers.

- **Create trusted insights with Google Cloud's advanced AI and machine learning (ML) models:** Businesses will be able to use Google Cloud's AI and ML services to train models on data from SAP and non-SAP systems.

- **Perform advanced analysis:** Organisations can utilise the analytics capabilities of the SAP Analytics Cloud solution in Google Cloud to analyse financial and business outcomes while improving the accuracy of models. With a simple integration to data in BigQuery with SAP Datasphere, customers can plan with a single, comprehensive view of their businesses.

- **Utilise joint solutions for sustainability:** SAP and Google Cloud are exploring ways to combine SAP Datasphere with broader ESG data sets and insights powered by Google Cloud to accelerate sustainability journeys with actionable insights.

- **Use SAP Business Technology Platform (SAP BTP) on Google Cloud globally:** SAP will advance its multi-cloud offerings by expanding regional support of SAP BTP and SAP HANA Cloud on Google Cloud, which includes support for SAP Analytics Cloud and SAP Datasphere. SAP and Google Cloud intend to launch SAP BTP in five new regions this year, building to a total of eight regions supported by 2025.

The companies also plan to partner on joint go-to-market initiatives for enterprises' largest data projects, enabling customers to adopt data products from both SAP and Google Cloud.

For more information, please visit www.sap.com. ■

ZYXEL WINS ITALIAN CHANNEL AWARDS FOR THREE YEARS IN A ROW

Honour reflects comprehensive support for channel partners.

Hsinchu, Taiwan – Zyxel Networks, the leader in delivering secure and cloud-powered networking solutions, has outperformed fellow international networking enterprises to receive an Italian Channel Award for the third consecutive year in the latest recognition of its outstanding channel services. Presented to Zyxel last month in Milan, the Best Channel Program Award recognized the comprehensive support the company offers its channel partners, which ranges from pre-sale support to ongoing training. The prize is the latest in a string of such honours for Zyxel,

continue on page 22

which last year bagged its second consecutive Channel Excellence Award in Germany and won the Best PSA/RMM Vendor Award at the European MSP Innovation Awards in the U.K.

"We know that being a leading brand requires more than just offering good products – it also means having a well-designed, symbiotic program that supports sales channel partners," Crowley Wu, Zyxel Network's vice president of sales and marketing, said. "Zyxel's consistent success in winning channel awards in major European markets shows the trust that we have earned by investing in our channel program over the long run."

A trusted partner

The Italian Channel Awards, now in their ninth year, are organised by industry media outlet ChannelCity and voted on annually by thousands of channel partners across Italy. Zyxel's success at the awards follows its impressive performance over recent years in Italy, where it has emerged as a top choice for local channel partners. Notably, in 2022, the company secured a role in the government's education network upgrade project and the National Recovery and Resilience Plan. It has also earned particular praise from Italian channel partners for the pre- and after-sale support, education, and training it offers to help them achieve sustainable growth.

No better time for Nebula

According to Wu, recent global challenges have highlighted Zyxel's strengths in innovation and customer service, particularly its Nebula cloud management solution.
"We've used Nebula to help our partners weather the storm brought by the pandemic, supply chain, and inflation crises," he said.

Since launching it in 2016, Zyxel has constantly upgraded Nebula and expanded its support for cloud-managed devices, allowing users to deploy networks more efficiently and providing more intelligent services to simplify complex network management and operations.

Nebula now supports 100 product models, including WiFi 6/6E APs, network switches, firewalls, and 5G mobile routers. This makes it the industry's most comprehensive cloud networking solution for small and medium-sized businesses.

For more information, please visit: https://www.zyxel.com/nebula. ■

GIGAOM RADAR NAMES HITACHI VANTARA A LEADER AND FAST MOVER IN UNSTRUCTURED DATA MANAGEMENT FOR THIRD CONSECUTIVE YEAR

Industry recognition highlights Hitachi Vantara's continued leadership and innovation in unstructured data, delivering cyber resiliency, compliance, and cost efficiencies

Singapore – Hitachi Vantara, the modern infrastructure, data management, and digital solutions subsidiary of Hitachi Ltd. (TSE: 6501), announced today its Hitachi Content Platform (HCP) has been recognized as a leader and fast mover in the latest GigaOm Radar Report for Unstructured Data Management for Infrastructure-focused Solutions. The report evaluated 12 vendors in the market and rated them on their capabilities to address the complex challenges of managing unstructured data in large-scale infrastructure environments. This is the third consecutive year HCP has received GigaOm recognition for leadership in the unstructured data management radar for infrastructure solutions.

The report highlights the exceptional performance of HCP across a wide range of metrics and criteria. HCP was rated exceptional in five out of six evaluation metrics.
The exceptional metrics include architecture, scalability,

continue on page 23

flexibility, performance and efficiency, and ecosystem. Furthermore, HCP was also rated exceptional in five out of seven key criteria, including metadata analytics, global content & search, big data analytics, compliance, and security. HCP was also rated exceptional in both deployment models – user-managed and SaaS.

“To be a GigaOm radar leader, a company must distinguish itself across several key criteria, such as the ability to deliver high performance, scalability across data, and strong compliance and security capabilities,” said Arjan Timmerman, analyst, GigaOm. “Hitachi Vantara’s HCP platform delivers ease of use, with the ability to help customers optimise and secure their object storage performance. HCP delivers fast data processing and insights into data, meeting the most pressing demands of today’s modern cloud-native workloads. This is why HCP is considered a leader in managing unstructured data.”

Solutions in a complex cloud environment

Managing unstructured data in complex multicloud and multi-vendor infrastructure environments is one of the numerous data management challenges many organisations encounter. According to the report, enterprises face several operational and business risks including dark and orphaned data, security, infrastructure cost, and compliance risks if they do not have a data strategy in place. Additionally, the report highlights that while storage for structured data (or primary storage) is still one of the most significant items of expenditure in any IT budget, unstructured data storage now accounts for 80% to 90% of the total capacity and is growing more quickly than any other form of storage. Infrastructure solutions defined by GigaOm are designed to target data management at the infrastructure level and metadata. Hitachi Vantara has demonstrated exceptional capabilities in these areas, making it a preferred choice for customers.

Vector by Freepik

Image by Freepik

“This recognition is a testament to the company’s commitment to innovation and its ability to cater to the dynamic needs of customers in the infrastructure solutions market,” said Dan McConnell, senior vice president, product management-storage, Hitachi Vantara. “As data management becomes increasingly important, companies must address expanding requirements such as performance, scalability, and data intelligence. Data-aware products like HCP are critical in managing costs, gaining insights, supporting new applications, and meeting regulatory requirements for privacy and security, particularly as unstructured data continues to grow at an unprecedented rate. Hitachi Vantara remains dedicated to delivering exceptional data management solutions to its customers.”

The GigaOm Radar weighs vendors based on their ability to execute and innovate and their product roadmap. The radar chart shows HCP is well-positioned to meet the evolving needs of customers in the infrastructure-focused solutions market.

HCP offers a broad ecosystem of solutions, including comprehensive, intelligent data management to unlock the full value of data assets. Hitachi’s HCP portfolio has been rated as exceptional for metadata analytics, big data analytics, and compliance and security. HCP delivers comprehensive data management for IoT, big data, and unstructured data, whether it is on-premises or in the cloud.

This latest recognition adds to the strong performance portfolio for Hitachi Vantara. In addition to this latest GigaOm acknowledgement, Hitachi Vantara recently announced results from TechTarget’s Enterprise Strategy Group (ESG) technical review of the Hitachi Content Platform (HCP), validating the platform’s scalable, high performance. The Hitachi Content Platform: High-performance Object Storage for Cloud-native Applications Report also assessed the cost-effectiveness customers can achieve in their data centre modernization and data-driven. analytics initiatives.

For more information, please visit: www.hitachivantara.com. ■

POLYGON LABS AND GOOGLE CLOUD JOIN FORCES TO PROVIDE DEVELOPERS WITH TOOLS AND ENTERPRISE INFRASTRUCTURE TO ACCELERATE GROWTH ON POLYGON PROTOCOLS

Google Cloud will support all Polygon protocols, including Polygon PoS, Polygon Supernets, and Polygon zkEVM.

Singapore – At Consensus 2023, Google Cloud and Polygon Labs announced a multi-year strategic alliance to accelerate adoption of core Polygon protocols, including Polygon PoS, Polygon Supernets, and Polygon zkEVM, with Google Cloud infrastructure and developer tools. Together, they are embarking on joint engineering and go-to-market initiatives to make it easier for developers to build, launch, and grow their Web3 products and decentralised applications (dApps) on Polygon protocols.

Google Cloud to become the strategic cloud provider for Polygon protocols

Companies like Starbucks, Mercedes-Benz, Reddit, Flipkart, and Nexon are already leveraging Polygon protocols as their entry points to Web3 to deliver new experiences to their brand communities.

To help developers overcome the time-intensive processes and costly overheads associated with provisioning, maintaining, and operating their own dedicated blockchain nodes, Google Cloud will bring Blockchain Node Engine, its fully managed node hosting service, to the Polygon ecosystem, thereby diversifying the usage of cloud services across the Polygon ecosystem. Once Blockchain Node Engine support for Polygon is made available, developers using Blockchain Node Engine will no longer have to worry about configuring or running their Polygon Proof of Stake (PoS) nodes; they can instead focus on growth while retaining complete control over where their nodes are deployed.

The Google Cloud Marketplace is already offering developers simple one-click deployment of a Polygon PoS node to power their dApps quickly and easily. The Polygon blockchain dataset was listed on the Google Cloud Marketplace under the Google Cloud Public Dataset Program in 2021. With that dataset, developers can combine their use of BigQuery, Google Cloud's serverless enterprise data warehouse, and Polygon PoS or Polygon Supernets to analyse real-time on-chain and cross-chain data to inform decision-making.

Polygon Supernets is a dedicated app chain providing enterprises and other developers of specific applications with the ability to customise and extend blockspace based on their needs. By the end of Q3 2023, Polygon Labs will enable one-click developer net (DevNet) deployments on Google Cloud. Developers who are interested in deploying a Supernet will be able to provision a three to five node network with a simulated bridge in their virtual private cloud (VPC) for the purpose of rapid evaluation of the Supernets stack for their projects.

Optimising Polygon zkEVM scaling performance

Polygon zkEVM is an Ethereum Virtual Machine (EVM) equivalent scaling solution that integrates seamlessly with existing Ethereum functions, smart contracts, developer tools, and wallets by leveraging zero-knowledge proofs, an advanced form of cryptography. Polygon zkEVM benefits decentralised finance (DeFi) developers and users by enabling faster and cheaper transactions, leading to increased efficiency and lower costs. With Google Cloud as a strategic cloud provider, and Searce facilitating technical implementation, Polygon Labs will advance its zero-knowledge innovation strategy and enable Web3 developers to avoid trade-offs between three key properties: decentralisation, scalability, and security. Initial tests to run Polygon zkEVM's zero-knowledge proofs on Google Cloud, for instance, resulted in significantly faster and cheaper transactions as compared to the existing setup.

Fuelling the next wave of Web3 ecosystem innovation

To provide founders in the Polygon ecosystem with more resources to scale their innovative Web3 products and dApps, eligible early-stage startups backed by Polygon Ventures can now receive newly announced Web3-specific benefits through the Google for Startups Cloud Program. This includes up to US$200,000 in credits for their Google Cloud and Firebase usage for up to two years, early access to Google Cloud's Web3 products and roadmap, invitation to a gated Discord channel with Google Cloud's Web3 product and engineering teams, free access to hands-on learning labs focused on Web3 and the latest Google Cloud technology, and more.

continue on page 25

"Google Cloud supporting all of Polygon's protocols is a step in the right direction to help onboard more people into Web3," said Ryan Wyatt, President, Polygon Labs. "Today's announcement with Google Cloud aims to increase transaction throughput, enabling use cases in gaming, supply chain management, and DeFi. This will pave the way for even more businesses to embrace blockchain technology through Polygon."

"The industry is experiencing a flight to quality as corporations seek to minimise risk when exploring new possibilities in Web3. Building on our work over the past few years, Google Cloud is helping the industry achieve escape velocity by directing our engineering efforts toward areas like improving data availability and enhancing the resilience and performance of scaling protocols like zero-knowledge proofs," said Mitesh Agarwal, Managing Director, Customer Engineering and Web3 Go-to-Market, Asia Pacific, Google Cloud. "Alongside Searce as our implementation partner, we look forward to deepening our collaboration with Polygon Labs to deliver the enterprise-ready Web3 infrastructure and developer-friendly tools that businesses need to offer fast, frictionless, and secure access to dApps for consumers."

"At Searce, we are passionate about building a decentralised future, and our partnership with Polygon Labs and Google Cloud reinforces our commitment to this vision. Together, we will offer cutting-edge cloud solutions that help businesses harness the power of Web3 and create new opportunities in the digital economy. We are excited to work with our partners to drive innovation in the Web3 space," said Rahul Shah, Senior Vice President and Head of Business, Japan and Asia Pacific, Searce. ■

INDUSTRY ANALYST DCIG AFFIRMS ARCSERVE UDP 9.0 AS THE OBVIOUS SOLUTION TO SIMPLIFY BACKUP COMPLEXITIES AND DEFEAT RANSOMWARE THREATS

Singapore – Arcserve, the world's most experienced provider of backup, recovery, and immutable storage solutions for unified data protection against ransomware and disasters, today announced the results of a comprehensive review conducted by independent research firm DCIG of its Arcserve UDP 9.0 backup solution. The study found that Arcserve UDP 9.0 offers organisations a clear edge in protecting against ransomware while tackling the persistent challenges of managing backup and recovery complexities. Arcserve UDP 9.0 delivers a cloud-based, multi-tenant Cloud Console that centrally manages UDP and Cloud Direct, enhancing its protection of enterprise applications such as Oracle and MS SQL Servers. The solution includes architectural and user interface enhancements to improve performance, simplify management, and improve data resilience, availability, and durability through its support for multiple cloud object storage providers. These features, combined with Arcserve's existing integration with Sophos, provide organisations with a reinforced beachhead against ransomware threats.

Image by Freepik

Jerome Wendt, CEO & Lead Data Protection Analyst of DCIG, commented on Arcserve UDP's multiple backup and DR capabilities, stating that "Arcserve UDP has for some time delivered advanced data protection features at its core that organisations routinely use. Arcserve offers both agent-based and agentless backup options, which give organisations the flexibility to use the best backup approach to meet specific application data protection requirements."

Arcserve UDP offers multiple disaster recovery (DR) options, including DRaaS, Instant Restores, and Virtual Standby (VSB). DRaaS is available via its fully managed cloud services extension, Cloud Hybrid. Its DRaaS service keeps critical data and workloads protected offsite and available and positions organisations to continue operations during or after unplanned on-premises outages. The Instant Restore feature allows IT personnel to spin up a VM directly from a backup quickly. At the same time, VSB offers a highly available configuration for data and applications for even faster recoveries than its Instant Restore feature.

"As ransomware attacks become more sophisticated and frequent, a weak backup solution is no longer an option. With Arcserve UDP 9.0, organisations empower themselves to defend against the latest ransomware threats and overcome the complexity inherent in IT environments," said Patrick Tournoy, executive vice president of operations at Arcserve. "DCIG's review confirms that Arcserve UDP 9.0 is a robust backup solution that can effectively protect organisations against these threats." ■

DIGICERT ANNOUNCES PARTNERSHIP WITH ORACLE TO MAKE DIGICERT® ONE AVAILABLE ON ORACLE CLOUD INFRASTRUCTURE

Partnership provides joint customers with fast time to value for their digital trust initiatives.

Singapore – DigiCert, a leading global provider of digital trust and a member of Oracle PartnerNetwork (OPN), today announced a partnership to provide DigiCert ONE, the platform for digital trust, on Oracle Cloud Infrastructure (OCI). Customers will benefit from DigiCert ONE's fast time to value combined with OCI's high-performance and security-first architecture for single and multi-cloud deployments. Moving forward, DigiCert and Oracle will collaborate on further integration into the OCI ecosystem to help joint customers manage their digital trust initiatives in a unified architecture.

"Collaboration and deeply integrated security are a few of the key reasons why many of the world's leading brands turn to OCI to help secure their clouds and data," said Mike Cavanagh, Group Vice President, ISV Cloud for North America at Oracle. "Enabling access to DigiCert's leading digital trust infrastructure on OCI provides customers a powerful combination of solutions to safeguard their data and secure their assets."

"DigiCert's partnership with OCI makes deployment of DigiCert ONE on OCI easy to deploy and scalable within customers' single or multi-cloud environments," said DigiCert Chief Product Officer Deepika Chauhan. "Together we can help our joint customers reduce the risk of business disruption, protect attack surfaces and deliver identity-based digital innovation with ease."

Image by Freepik

With DigiCert ONE, customers can secure users, devices, servers, documents, software and more with a unified architecture that centralises management of digital trust initiatives. DigiCert ONE is a modern, multi-tenant, cloud-native SaaS platform, with the flexibility to be deployed in customers' private cloud or on premises, if required.

Image by Freepik

DigiCert ONE supports organisations across a wide variety of use cases, including securing connected medical devices for improved patient care, improving user trust in election data, protecting collection and analysis of device telemetry for improved retail operations, and automating user and device authentication to corporate IT services.

OCI provides a cloud infrastructure with built-in, always-on security that helps deliver compliance with rigorous security protocols and operations. It also delivers performance and reliability with simplified, transparent pricing, and flexible options to help customers meet their unique business needs, whether on premises or in the public cloud, using multiple cloud vendors or a combination.

OCI cloud regions, including OCI Dedicated Regions, offer all the benefits of public cloud services while allowing secure, high-performance, local environments that can help keep sensitive or regulated data and workloads separate to address data residency requirements based on location or sensitivity.

Oracle and DigiCert will jointly market and co-sell DigiCert ONE in a partnership designed to expand the DigiCert ONE portfolio's existing global footprint.

For more information, please visit: www.digicert.com. ■

TDSI SECURITY TECHNOLOGY SHOWCASE VISITS SAUDI ARABIA AND FEATURES GUEST UK PROVIDERS

TDSi and seven leading UK providers deliver presentations and interactive sessions to security professionals in Riyadh and Dammam

Poole, United Kingdom – Integrated Access Control and Security manufacturer TDSi has hosted another of its popular Security Technology Showcase events in Riyadh and Dammam in Saudi Arabia. In addition to TDSi, attendees also enjoyed presentations and hands-on advice from UK security manufacturers such as integrated perimeter security specialist Harper Chalice Group (presented by Building Defence Systems), secure industrial transmission and power solutions provider KBC Networks, CCTV surveillance camera and control solutions manufacturer 360 Vision Technology Ltd, Control Room furniture manufacturer LundHalsey, specialised server technology provider Secure Logiq, AI-driven video analytics specialist VCA Technology, and integrated security application platform provider Veracity.

The latest Security Technology Showcase events were organised and presented by TDSi's International Business Development Director Phil Tennent, along with his team Hassan Ahmed and Sebastien Botella. Phil commented, "We were excited to take our showcase to Saudi Arabia, a vibrant market that is very receptive to the best of British security technology and services. We were also delighted to share the stage with a number of other specialist providers to deliver a really informative and varied schedule for attendees."

Both the Riyadh and Dammam events were attended by over 50 security professionals each and featured a morning of Security Technology Presentations followed by a Product Showcase afternoon, which provided the opportunity to speak directly with the manufacturers to find out more about their products and to see their solutions up close.

As part of TDSi's Security Technology Showcase event week, Phil also attended a UK Department of International Trade event focusing on Security Technology and had the opportunity to talk to many companies about their Vision 2030 projects in Saudi Arabia, along with their security and access control requirements to support these new infrastructure plans. The Latest Saudi Arabia Security Technology Showcase events follow on from similar events in Dubai and Bahrain last October, which featured a free interactive, hands-on session exploring TDSi's latest Access Control Solutions and featured presentations from its technology partners KBC Networks and SimonsVoss.

For more information, please visit: www.tdsi.co.uk. ■

INFOBLOX LEADS THE INDUSTRY TO UNITE NETWORKING AND SECURITY TEAMS TO BETTER PROTECT AGAINST CYBER ATTACKS

- Infoblox simplifies and unites networking & security across any environment, including complex hybrid, multi-cloud environments
- Infoblox delivers new critical security enhancements to Infoblox BloxOne® Threat Defense, offering Lookalike Domain Monitoring and protection against emerging threats to help prevent cybercrime as phishing attacks make headlines across the globe
- Infoblox's 2023 Global State of Cybersecurity Study found that Singapore organisations increased IT security budgets and enhanced cybersecurity measures and networking concerns in 2022 amidst the growing threat of malicious activities worldwide
- Infoblox rebrand initiatives reflect confidence and business focus, positioning its critical role in securing the networks of some of the world's largest companies, appealing to both networking and security professionals alike

Image by Freepik

Singapore – Infoblox Inc. the company that delivers a simplified, cloud-enabled networking and security platform for improved performance and protection, makes several announcements today, as the company takes a strong position on why networking and security teams must join forces in the fight against cybercrime. New critical security features and a refreshed brand identity reflect the company's strategy, confidence and business focus, empowering customers to detect and respond to critical threats to help their businesses thrive.

"Infoblox is the only company that can provide real-time visibility and control over who and what connects across networks and multi-cloud environments to help customers build safer, more resilient environments," said Scott Harrell, CEO and President, Infoblox. "By bringing NetOps and SecOps teams together with shared visibility, data context, automation and control, they can prevent malware communications and pinpoint the source of threats, taking the performance and protection to new heights," he added.

Phishing and email scams remain rampant in Singapore's cybercrime landscape. 69% of Singapore organisations identified phishing as a top attack vector. In response to this, Infoblox will launch its new Lookalike Domain Monitoring capability. This feature can detect websites trying to mimic identities of company brands, which is becoming increasingly common as a means to deceive partners and customers.

Singapore organisations stepped up cybersecurity capabilities, yet remained concerned

Businesses today are increasingly adopting hybrid and multi-cloud environments to stay competitive, creating additional complexity and expanding attack surfaces. Not surprisingly, 64% of Singapore organisations have suffered at least one data breach in the last 12 months with an

continue on page 29

estimated average value of SGD2.4M loss due to these breaches, according to Infoblox's 2023 Global State of Cybersecurity report by CyberRisk Alliance.

In Singapore, more organisations have accelerated digital transformations (57%) to support remote working, according to the report. To mitigate the increased risk to their networks, 66% of organisations added VPNs and firewalls and are also reporting quicker reaction times to threats – 73% took up to 24 hours to investigate a threat in 2022, an improvement from just 49% in the previous year.

Today's challenging environment and corresponding changes in digital habits have left many systems—and users—exposed. This corresponds to the report finding that 75% of Singapore organisations are expecting bigger security budgets in 2023 to combat known and new threats, an increase from the 68% of organisations that have already expanded their security budgets in 2022. However, while organisations recognise the crucial need to upgrade their cybersecurity infrastructure, they still feel unprepared to defend their networks against insider threats (18%), data leakage (13%) and ransomware (12%), especially as such threats are growing in sophistication and frequency.

Enhancing BloxOne® Threat Defense with New Lookalike Domain Monitoring and more.

Infoblox's new Lookalike Domain Monitoring capability identifies sites attempting to impersonate company brands that are increasingly used to deceive partners and customers with phishing, malvertising and similar attacks. This comes just after introducing Infoblox's new emerging threat intelligence feeds that provide indicators of malicious intent to stop attacks before they happen. With these enhancements, Infoblox delivers a better and safer customer experience. Infoblox analyses over 70 billion DNS queries a day. In a new lookalike domain report, to be released at RSAC 2023, Infoblox demonstrates that while the use of lookalike domains by malicious actors continues to persist, the techniques have substantially advanced in 2022, targeting every sector, playing a key role in complex cyberattacks such as those used to bypass multi-factor authentication (MFA) measures.

"As a best-of-breed DNS layer security solution provider, Infoblox continues to pioneer advancements in the use of DNS as a source of unique threat intelligence and as a powerful enforcement point," said Harrell. "We are the first and only DNS Security vendor to protect against the use of lookalike domains by attackers. These attacks are increasing in sophistication and prevalence, making specialised solutions not just nice to have, but necessary to secure enterprises and their users," he added.

In a world that never stops, Infoblox is focused on helping customers build more responsive networks to keep up with the pace of digital transformation, detect hidden threats and stop attacks earlier, powering security services with context-rich network intelligence.

Vector by Freepik

"Singapore has made tremendous progress in creating a more resilient cyber landscape and the steps businesses have taken are in line with recommendations by the Cyber Security Agency of Singapore and interagency Counter Ransomware Task Force. However, as the digital revolution continues to gain momentum, responsive and reliable networks will be crucial to prevent sensitive data from falling into the wrong hands. Uniting network and security will enable businesses to create better visibility of their networks 24/7, detect critical threats in advance, and better prepare them for an ever-changing cyber landscape," said Jeff Castillo, Senior Regional Director, Southeast Asia, Infoblox.

Castillo adds, "We want to help security professionals discover the most pressing network performance and protection issues and enable them with the right tools to secure networks from ever-evolving, fast-moving cyber threats. With the return of face-to-face events, we hope to do this through our annual cyber security event, Infoblox Exchange, that is coming to Singapore on 19th May 2023."

Infoblox's cloud-first, consultative approach provides customers with specific solutions and actions to help them build more resilient networks and stop critical threats sooner based on their unique business needs.

For more information, please visit: infoblox.com. ■

Homeland & Critical Infrastructure Security Data Protection Solutions

In an increasingly interconnected and digital world, ensuring the security of our homeland and critical infrastructure has become a paramount concern. Protecting sensitive data plays a crucial role in safeguarding these vital systems.

Besides, every sector has become dependent on the information technology sector. This makes it vulnerable to breaches and threats. There has been a rise in cybersecurity threats, including 13% data leakage, 12% ransomware and 18% insider threats. This has led many organisations to upgrade their security budget from 68% to 75%.

Let's explore the concept of homeland security and critical infrastructure and data protection solutions that can help mitigate these risks.

Understanding Homeland Security and Critical Infrastructure

Homeland security encompasses the collective efforts to protect a nation's citizens, territory, and critical assets from various threats. Critical infrastructure is the systems and assets essential for a society's functioning, including energy, healthcare information, cyber network, sensitive online data, and communication networks.

These collective efforts undertaken by the government and the agencies protect its citizens, infrastructure, and borders from various threats. When it comes to cloud and cyber security, it may include data leakage, accidental exposure, digital terrorism, cyberattacks, and other emergencies.

On the other hand, critical infrastructure comprises the essential systems and assets vital for a society, economy, and national security. The critical infrastructure consists of a wide range of sectors, including digital assets, online systems, and networks that provide functions necessary for everyday activities. These interconnected and interdependent sectors form the backbone of a nation's operations and services.

The importance of homeland security and critical infrastructure cannot be overstated, as their disruption or compromise can have severe consequences for public safety, economic stability, and national security. Safeguarding these entities requires a multifaceted approach to addressing physical and digital threats.

Images by Freepik

Physical threats to homeland security and critical infrastructure include malware, terrorist attacks, natural disasters (such as hurricanes and floods), industrial accidents, and pandemics. These events can cause significant damage to online infrastructure, disrupt essential services' normalcy, and pose risks to public safety.

Mitigating these threats involves implementing robust security measures and conducting risk assessments. Moreover, enhancing emergency preparedness and response capabilities and fostering collaboration among various stakeholders can be significant in emergencies.

Current Threats to Homeland and Critical Security

In recent years, the digital landscape has emerged as a critical homeland security and infrastructure protection domain. With the increasing reliance on technology and interconnected systems, the vulnerability to cyber threats has grown exponentially. Cyberattacks targeting critical infrastructure can lead to service disruptions, data breaches, financial losses of about SG$ 660.7 million, and potential harm to public safety. Here are some current threats to the homeland and critical security. Organisations can enhance resilience and protection by understanding these threats and implementing appropriate security measures.

> **Ransomware has become a prevalent threat, where attackers encrypt critical data or systems and demand a ransom to restore access.**

Insider Threats

Insider threats pose a significant risk, as individuals with authorised access to critical infrastructure may intentionally or inadvertently cause harm. Malicious insiders can exploit their privileges to steal or manipulate sensitive information, disrupt operations, or sabotage critical systems. Unauthorised individuals gaining control over user accounts may maliciously manipulate critical infrastructure systems.

Infrastructure Vulnerabilities

The increasing connectivity of critical infrastructure systems makes them susceptible to vulnerabilities. Cybercriminals can exploit software, hardware, or network configuration weaknesses to gain unauthorised access, compromise system integrity, and disrupt essential services.

Ransomware Attacks

Ransomware has become a prevalent threat, where attackers encrypt critical data or systems and demand a ransom to restore access. Ransomware attacks and distributed denial-of-service (DDoS) attacks targeting critical infrastructure can cause significant disruptions, financial losses, and potential risks to public safety. In 2021, ransomware attacks

Image by Freepik

Image by Freepik

mainly affected small-medium organisations, as reported in 137 cases. This number has been reduced to 132 cases in 2022 with appropriate measures.

Supply Chain Risks

The globalised nature of supply chains introduces additional cybersecurity risks. Malicious actors may exploit vulnerabilities in the supply chain to infiltrate critical infrastructure systems or insert malicious components. They may also tamper with software or hardware during production or distribution.

Nation-State Threats

Nation-state actors engage in cyber espionage, sabotage, and disruption campaigns targeting critical infrastructure to further their political, economic, or military objectives. These actors possess advanced capabilities and resources, making them formidable adversaries.

Misconfiguration

Improperly configured systems and devices can create vulnerabilities that attackers exploit to gain unauthorised access or disrupt operations.

Data Loss and Leakage

Unintentional or intentional data loss or leakage can lead to significant repercussions, including compromising sensitive information and potential damage to national security.

Data Privacy

Data privacy violations can have severe implications, eroding public trust and exposing individuals to potential harm.

Accidental Exposure of Credentials

Human error or negligence can result in the accidental exposure of sensitive credentials, opening avenues for cyberattacks.

Lack of Visibility

Inadequate monitoring and visibility into critical infrastructure systems can impede timely detection and response to security incidents.

External Sharing of Data

Sharing sensitive information with external entities without adequate security can lead to data breaches and compromises.

Incident Response

The ability to respond to and mitigate security incidents is crucial to minimising the impact of attacks and restoring operations swiftly.

Data Protection Solutions for Homeland & Critical Infrastructure Security

To mitigate these threats, homeland security and critical infrastructure protection efforts focus on implementing robust cybersecurity measures. Collaboration between government agencies, private sector entities, and international partners is vital. They work on sharing information, coordinating responses, and fostering a collective defence against cyber threats.

Public-private partnerships facilitate the exchange of threat intelligence, expertise, and resources.

Implementing robust data protection solutions is crucial to fortify the security posture of homeland and critical infrastructure systems. Some key measures include:

- **Strong Access Controls:** Implementing robust authentication mechanisms, least privilege principles, and privileged access management helps prevent unauthorised access.
- **Encryption:** Applying encryption to sensitive data at rest and in transit ensures that even if data is compromised, it remains unintelligible to unauthorised individuals.

continue on page 36

- **Network Segmentation:** Segmenting critical infrastructure networks helps contain the impact of a breach and prevents lateral movement by attackers.
- **Continuous Monitoring and Threat Detection:** Deploying advanced monitoring and threat detection systems enables early detection of suspicious activities and potential cyber threats.
- **Incident Response Planning:** Establishing comprehensive incident response plans ensures a prompt and coordinated response to security incidents, minimising their impact.
- **Employee Education and Awareness:** Educating employees about cybersecurity best practices and raising awareness about potential threats helps create a security-conscious culture.
- **Regular Security Assessments:** Conducting periodic security assessments and penetration testing identifies vulnerabilities and allows for timely remediation.
- **Data Backup and Recovery:** Regularly backing up critical data and implementing robust data recovery mechanisms mitigate the impact of data loss incidents.
- **Secure Development Practices:** Adopting safe coding practices and conducting thorough security testing while developing critical infrastructure systems reduces the likelihood of vulnerabilities.
- **Collaboration and Information Sharing:** Promoting collaboration and information sharing between government agencies, industry partners, and cybersecurity experts enhances collective defence against emerging threats.

Key Benefits of Data Protection Solutions

Cloud security data protection solutions offer several key benefits in safeguarding sensitive information and mitigating risks. Here are some of the significant advantages:

Image by Freepik

Data Confidentiality and Integrity

Security data protection solutions employ robust encryption techniques to ensure the confidentiality and integrity of data. By encrypting data both at rest and in transit, these solutions prevent unauthorised access and tampering. It gives an additional layer of protection against data breaches and unauthorised modifications.

Access Control and Authentication

The sophisticated access control mechanisms include multi-factor authentication and role-based access control. These measures ensure that only authorised individuals can access sensitive data and perform specific actions, reducing the risk of insider threats and unauthorised access.

Threat Detection and Prevention

Cloud security solutions employ advanced threat detection mechanisms, including intrusion detection and intrusion prevention systems. In real time, these systems continuously monitor network traffic and behaviour patterns to identify and mitigate potential security breaches, malicious activities, and vulnerabilities.

Vulnerability Management

With vulnerability management tools, organisations identify and remediate vulnerabilities in their cloud infrastructure. These security tools scan cloud environments, identify weaknesses, and provide recommendations for patching and securing systems, minimising the risk of exploitation by cybercriminals.

Data Loss Prevention (DLP)

DLP features in cloud security solutions enable organisations to define and enforce policies to prevent

Images by Freepik

sensitive data from being leaked, lost, or exposed. These solutions use content scanning, contextual analysis, and policy enforcement to detect and block the transmission of sensitive data, reducing the risk of data loss or compliance violations.

Regulatory Compliance

Cloud security data protection solutions help organisations meet regulatory requirements and industry standards. They offer features and controls that align with data protection regulations like GDPR, HIPAA, PCI DSS, etc. These solutions facilitate data governance, auditing, and reporting, ensuring organisations comply with relevant regulations and avoid penalties.

Incident Response and Forensics

Cloud security solutions often include incident response and forensic capabilities. In the event of a security breach, these tools may help organisations investigate the root cause, contain the incident, and gather evidence for further analysis and legal purposes. They enable organisations to respond quickly and effectively, minimising the impact of security incidents.

Scalability and Flexibility

Cloud security data protection solutions are designed to scale with organisational needs. They can adapt to changing business requirements, accommodate growing data volumes, and support expanding cloud infrastructures. This scalability and flexibility ensure that security measures remain effective as organisations evolve and expand their cloud footprint.

Image by Freepik

Centralised Management and Visibility

Centralised management consoles that offer comprehensive visibility into security posture, events, and incidents across cloud environments. This centralised management allows organisations to monitor and manage security controls, policies, and compliance requirements from a single interface. As a result, simplifying administration and improving operational efficiency.

Cost Efficiency

Cloud security data protection solutions offer cost advantages compared to traditional on-premises security infrastructure. Organisations can avoid significant upfront investments in hardware, software, and maintenance costs this way.

Parting Words

Protecting the homeland and critical infrastructure requires a multifaceted approach, with cloud data protection playing a central role. With protection solutions and adopting proactive security measures, the resilience of these vital systems can be strengthened.

As threats evolve, continued collaboration and investment in security measures will be crucial for the security and well-being of our nation and its critical infrastructure.

Protecting the homeland and critical infrastructure requires a multifaceted approach, with cloud data protection playing a central role. With protection solutions and adopting proactive security measures, the resilience of these vital systems can be strengthened.

COMING SOON

JUL 19 – 21 2023
Secutech Vietnam 2023
HCMC, Vietnam
https://secutechvietnam.tw.messefrankfurt.com/

SEP 11 – 13 2023
Global Security Exchange 2023
Dallas, USA
https://www.gsx.org

OCT 25 – 28 2023
China Public Security Expo 2023
Shenzhen, China
https://cpse.com

NOV 1 – 3 2023
Secutech Thailand 2023
Bangkok, Thailand
https://secutechthailand.tw.messefrankfurt.com

NOV 14 – 16 2023
ISC East 2023
New York, USA
https://www.discoverisc.com

DEC 7 – 9 2023
IFSEC India 2023
New Delhi, India
https://ifsecindia.com/

JAN 16 – 18 2024
Intersec 2024
Dubai, UAE
https://intersec.ae.messefrankfurt.com

APR 9 – 12 2024
ISC West 2024
Las Vegas, USA
https://www.security-essen.de

SEP 17 – 20 2024
Security Essen 2024
Essen, Germany
https://secutechvietnam.tw.messefrankfurt.com

SECURITY SOLUTIONS TODAY
SECURITY & CROWD MANAGEMENT
DIGITAL TRANSFORMATION
DIGITAL TRANSFORMATION IN PHYSICAL SECURITY INDUSTRY
RT CITIES
TRAVEL SECURITY POST-PANDEMIC
VACCINE PASSPORT
TION SECURITY

SUBSCRIPTION FORM

Email your order to:
yvonne.ooi@tradelinkmedia.com.sg

PRINT

Please (√) tick in the boxes.

□ **Southeast Asia Building**
Since 1974

SOUTHEAST·ASIA
CONSTRUCTION
Cover Story:
Malolos-Clark Railway Project, Philippines
Features:
Trans Sumatra Toll Road
Vermeer pile driver for solar projects
Rockster impact crusher
Mapei underground waterproofing systems

□ **Southeast Asia Construction**
Since 1994

1 year (6 issues) per magazine

Singapore	○ SGD$70.00
Malaysia / Brunei	○ SGD$120.00
Asia	○ SGD$180.00
America, Europe	○ SGD$220.00
Japan, Australia, New Zealand	○ SGD$220.00
Middle East	○ SGD$220.00

DIGITAL

Bathroom + Kitchen Today
Since 2001

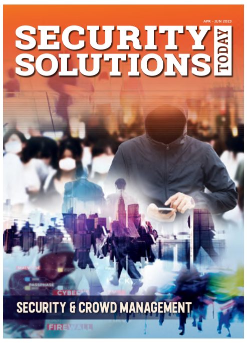
Bathroom + Kitchen Today
is available on digital platform.

http://bkt.tradelinkmedia.biz

Lighting Today
Since 2002

Lighting Today
is available on digital platform.
To download free PDF copy,
please visit:

http://lt.tradelinkmedia.biz



Security Solutions Today
Since 1992

Security Solutions Today
is available on digital platform.
To download free PDF copy,
please visit:

http://sst.tradelinkmedia.biz

Personal Particulars

Name:

Position:

Company:

Address:

Tel: **E-Mail:**

IMPORTANT

Please commence my subscription in
(month/year)

Professionals (choose one):

□ Architect
□ Property Manager
□ Landscape Architect
□ Manufacturer/Supplier
□ Interior Designer
□ Engineer
□ Developer/Owner
□ Others

□ Bank transfer payable to:
Trade Link Media Pte Ltd

<u>Bank Details</u>

Account Name:	Trade Link Media Pte Ltd
Account Number:	033-016888-8
Name of Beneficiary Bank:	DBS Bank
Address of Beneficiary Bank:	12 Marina Boulevard, DBS Asia Central, Marina Bay Financial Centre Tower 3, Singapore 018982
Country:	Singapore
SWIFT Address/Code:	DBSSSGSG

□ PAYNOW to:
Trade Link Media Pte Ltd

PAY NOW

PAYNOW option is applicable for **Singapore companies only.**

Company Registration Number: 199204277K

* GST inclusive (GST Reg. No: M2-0108708-2)

sst.tradelinkmedia.biz

SECURITY SOLUTIONS TODAY

Choose Magazine | Free Signup

SMART CITIES

Q4 / 2022

ASSOCIATE PUBLISHER
Eric Ooi
EDITOR
Navkiran Kaur

Security Solutions Today, published since 1992, is one of the leading security trade publications in Asia. The magazine features industry news, market / technological updates, case studies / application stories on projects, product showcases for new and current security products / devices in available in the market, and security trade show previews and reviews.

Connect with us:
Facebook: @securitysolutionstoday
LinkedIn: @tradelinkmedia
Issuu: @securitysolutionstoday

REQUEST MEDIA KIT

LATEST

Eight Australian international Airports implement IDEMIA's end-to-end border control solution
Jan 05 2023

Texecom launches the Midnight Black Collection
Jan 25 2023

Arcserve unveils Arcserve Unified Data Protection (UDP) 9.0
Jan 20 2023

IDIS expands line up with NDAA-Compliant 8 Channel HD Encoder
Jan 12 2023

Eight Australian international Airports implement IDEMIA's e...
Jan 05 2023

NEWS

Detection Technology expands its manufacturing in Finland to offer ...
Dec 29 2022

ESET named Champion in Canalys Global Security Leadership Matrix...
Dec 21 2022

Alibaba Cloud to Introduce Blockchain Node Service to...
Dec 15 2022

Paessler IT Monitoring Industry Trends for 2023
Dec 12 2022

ESET launches psychometric test to uncover visionary thinkers across...
Dec 07 2022

ESET Research: Bahamut group targets Android users with fake V...
Nov 24 2022

Dortronics Showcases Comprehensive Line of Custom an...
Nov 16 2022

Mimecast Partners With Okta to Safeguard Enterprises from Insid...
Nov 11 2022

Secure-IC acquires Silex Insight's security business to accelerate it...
Nov 04 2022

ESET refreshes its product portfolio to protect consumers wherever th...
Oct 26 2022

ESET to bring its unique cybersecurity solutions to large...
Oct 18 2022

Singapore's Ensign InfoSecurity Steps Up APAC Expansion - Opens...
Oct 12 2022

Securonix Detects New Covert Attack Campaign Targeting Milita...

Prisma Cloud Delivers Context-Aware Software Composition...

Keysight's 224G Ethernet Test Solutions Enable System on a Chi...

UPCOMING EVENTS

Secutech Taipei 2023
Taipei, Taiwan
FROM Apr 26,2023 10:00
TO Apr 28,2023 17:00

Secutech Vietnam 2023
HCM City, Vietnam
FROM Aug 16,2023 10:00
TO Aug 18,2023 17:00

Secutech Thailand 2023
Bangkok, Thailand
FROM Nov 01,2023 10:00
TO Nov 03,2023 17:00

ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website