

SHOW DAILY

THE OFFICIAL SHOW DAILY OF GOVWARE CONFERENCE AND EXHIBITION 2023

BRANDED CONTENT

Embracing AI-Powered Security and Zero Trust in a Dynamic Threat Landscape

The threat landscape is exploding as significant cyber incidents continue to increase at a record pace. Threat actors are exploiting misconfiguration and vulnerabilities, sometimes in mere minutes with a CVE announcement. In our latest [Unit 42 Cloud Threat Report](#), 60% of organisations take longer than four days to resolve security issues.

As cyber threats grow in sophistication, organisations can no longer rely on worn old strategies, but must adapt their security strategies to stay ahead. This includes understanding the latest threats and defending against them, securing their cloud environments, and consolidating their cybersecurity defences.

The threat story today

Cybersecurity continues to evolve in response to new trends and emerging technologies, such as sophisticated malware variants designed to evade detection. In this ever-changing threat landscape, several key trends have arisen.

For a start, malware continues to be the top concern across more than half of the region's organisations. Account takeovers and identity access issues are also among the main concerns, as cybercriminals employ various tactics like phishing and credential stuffing to compromise user accounts.

“With AI and automation, security analysts can process and analyse large volumes of data more quickly and identify patterns to indicate potential threats before an attack occurs. It significantly increases efficiency by automating repetitive and time-consuming tasks.”

– Steven Scheurmann, Regional VP for ASEAN, Palo Alto Networks


Attacks on critical infrastructure and operational technology (OT) networks are growing, however. According to a Unit 42 Network Threat Trends Research Report, organisations have experienced a 238% increase in attacks aimed at industries using OT technology from 2021 to 2022.

While attacker continue to use old vulnerabilities so long as it proves lucrative, there comes a point where the creation of newer, more complex attack techniques is necessary to achieve their objectives. As basic evasions are commoditised and more security vendors successfully deflect them, expect attackers to respond by moving toward more *Continue to page 03*

This article is also available online on the [GovWare Knowledge Hub](#).



Steven Scheurmann
Regional Vice President for ASEAN, Palo Alto Networks



SURVEY & SWAG
7 designs to choose from!

Share your GovWare experience, Snag limited-edition GovWare tee!

Head on to the Image Engine booth at Level 1 for more information.

12pm – 5:30pm only!

Introducing Medical IoT Security, the most comprehensive Zero Trust solution for medical devices

Palo Alto Networks **Medical IoT Security** is the **most comprehensive Zero Trust security for medical devices**. It is the only solution to accurately discover and assess every medical device on your network, **quickly implement Zero Trust security, stop highly evasive zero-day attacks, and simplify your security operations**, all in a single platform.

Proven. Trusted. Award-Winning.



Automate Zero Trust and protect IoT devices better and faster

70X SECURITY
EFFICIENCY

15X FASTER
DEPLOYMENT

20X FASTER
POLICY
CREATION

Medical IoT Security – designed to secure healthcare devices



Zero Trust Security for Medical Devices

Zero Trust security is a concept – trust nothing, validate everything. Medical IoT Security makes it easy to deploy a Zero Trust approach to your medical devices. Let Medical IoT Security do the work; find all devices, assess all risks, monitor behavior anomalies, prevent known and unknown threats, and secure every digital interaction.



Network Segmentation

Use Medical IoT Security to confidently segment connected clinical and operational devices and apply Zero Trust least-privilege policies to prevent attacks and lateral movement of threats. Get contextual device segmentation through deep profiling, assessment, and policy enforcement of managed and unmanaged devices. Enhance your NAC-led segmentation with native integrations.



Vulnerability Management

Understand the attack surface by assessing device vulnerabilities your VM can't find and scan. Strengthen your vulnerability management strategy with Medical IoT Security to get a true device risk score, including passively and actively discovered vulnerability data on managed and unmanaged clinical and operational devices.



Asset Management

With Medical IoT Security, organizations can transform a static medical device inventory into a dynamic inventory with complete medical and IoT visibility and risk context. Medical IoT Security can also share the device information with your existing asset management solutions such as ITSM and CMMS to keep them up to date.

... Continued from page 01

advanced techniques. Organisations must hence be ready for a threat landscape of more complex attacks.

Securing the cloud

Organisations have rapidly turned to the cloud to meet their growing needs and stay competitive, lured by their unmatched agility and scalability. However, the fast evolution and growth of cloud workloads, on top of the complexity of managing hybrid and multi-cloud environments, has caused many organisations to fall behind the curve and inadvertently introduce security weaknesses into their environments.

This is evident in the numerous legacy resources, vulnerabilities, and insecure configurations still utilised by organisations. These gaps provide threat actors with ample opportunities to infiltrate the cloud. Indeed, 80% of security exposures were observed in the cloud, while personally identifiable information (PII), financial records, and intellectual property are found in 63% of publicly exposed storage buckets.

As the attack surface of organisations expands in line with their increased use of the cloud, securing the cloud becomes an essential aspect of an organisation's cybersecurity strategy. To effectively secure their public cloud environments, organisations can focus on:

- **Continuous visibility:** Gain continuous visibility over all Internet-accessible assets, including cloud-based systems and services, to effectively manage the attack surface.
- **Secure remote access services:** Implement strong authentication methods and monitor remote access services for signs of unauthorised access or brute-force attacks.

- **Prioritise remediation and critical vulnerabilities:** Focus on areas with a high Common Vulnerability Scoring System (CVSS) score and an Exploit Prediction Scoring System (EPSS) score.
- **Address cloud misconfigurations:** Regularly review and update cloud configurations to ensure they align with best practices and address potential security risks.

Cybersecurity Consolidation – reduce complexities

Ever since the first cybersecurity product, cyber defenders have designed a rich array of solutions to defend against various attack vectors and mitigate risks associated with new threats. Over time, organisations have adopted a multitude of these products, layering security measures to create a more resilient infrastructure.

However, the practice of harnessing disparate cybersecurity point products has led to inefficiency and complexity in procurement, implementation, and operations. Relying on threat-specific point products is not a scalable or viable strategy for modern cybersecurity, as using different cybersecurity tools may lead to coverage gaps that hackers can exploit.

This is where a strategically designed solution portfolio based consolidation could be superior to a disparate pool of solutions organically acquired over the years. As cybersecurity solutions are consolidated, new technologies such as automation and artificial intelligence (AI) can be introduced that benefit the entire platform.

Using AI, a consolidated security solution can play a crucial role in mitigating

personnel shortages by allowing machines to bridge knowledge gaps. This can also free up security teams for higher-value tasks like risk assessment and mitigation.

Palo Alto Networks: Zero Trust, AI-driven approach

Cyber attackers will continue to evolve, incorporating recent technology innovations into their repertoire of tricks. This is already happening with generative AI, as the technology is used to democratise cybercrimes. The onus is on enterprise defenders to stay a step ahead by utilising a best-of-breed, consolidated platform to secure their environments.

Regardless of the environment, Palo Alto Networks is committed to leveraging AI across our entire portfolio and harnessing precision AI to deliver unparalleled detection and response for near real-time security. Since 2020, machine learning (ML) has been incorporated into our next-generation firewall.

Today, every Palo Alto Networks security subscription comes with advanced AI capabilities: DNS security, Advanced URL Filtering, Advanced Threat Prevention, and Advanced WildFire all harness ML technology for inline detection and prevention of zero-day attacks.

Palo Alto Networks will be present at GovWare 2023, Asia's premier cybersecurity event. Do visit us at booth G06 if you are attending. You can also sign up for our upcoming Prisma Cloud Workshop (02 Nov) [here](#), or SASE Masterclass (Webinar) [here](#) to learn more.

This article is also available online on the [GovWare Knowledge Hub](#).

BRANDED CONTENT

Beyond Traditional PCs - How Mobile Devices Are Changing the Game

The world is evolving, and so are our work tools. Mobile devices have become indispensable in the workplace, as workers increasingly favour them over laptops and desktops.

In this new era of remote work, mobile devices have become a lifeline for many office workers. Acting as always-connected digital gateways, these devices readily connect them to colleagues and

put access to crucial work resources at their fingertips.

The changing role of mobile devices

This shift in preference can be attributed to the sheer convenience and portability of mobile devices. The increasing power and sheer capabilities of these gadgets also play a role, as they can now handle tasks once reserved for traditional PCs.

“Mobile devices were used more as a supplementary device in the past but that has changed. While the use of laptop and mobile devices was split 75%-25% before the pandemic, it is now more of a 50%-50% split today.”

– Hendra Wiratno, Knox Product Lead - Solution Architect, Samsung

... Continue to page 04

... Continued from page 03

The pandemic arguably accelerated the transition by proving that knowledge work can happen outside the four walls of the office. The result is a massive surge in demand for mobile devices in the enterprise, as companies rushed to equip their employees with the mobile tools they need to work from anywhere and at any time.

The uptake was swift. Where knowledge workers had previously looked to mobile devices as supplementary devices to their laptops, they are now turning to smartphones and tablets for many of the tasks they used to boot up their laptops for.

For instance, smartphones are used heavily for video calls or for staying in the loop through various collaboration software. Tablets, with their larger, more comfortable screens are starting to replace PCs for productivity apps or enterprise software, which are increasingly available from mobile apps or a web-based interface.

It is hence no surprise that enterprises are now taking a closer look at mobile devices not just for front-liners in industries that rely on fieldwork or in industries such as manufacturing, logistics, or warehousing, but also for knowledge workers in the office. This broadening of mobile device usage across various departments highlights the growing importance of these tools in today's work environment.

Securing mobile devices

While mobile technology has undoubtedly enhanced productivity, management and security remain the biggest challenges. It is hardly surprising, considering how mobile devices are used to access the same resources as a corporate laptop - from confidential documents to internal correspondence, as well as sensitive ERP and CRM systems.

Mobile Device Management (MDM) is essential to address these concerns. By providing centralised control over devices, an MDM enables IT administrators to enforce security policies, remotely wipe lost or stolen devices, and monitor usage patterns across all devices. Additionally, MDMs can help ensure that company data is encrypted and compliant with industry regulations.

Yet not every MDM integrates with existing solutions used to manage and secure the PCs that are currently deployed. As enterprises adapt to this new landscape, IT departments must find ways to manage and secure both mobile

devices and traditional PCs. This is vital if organisations were to implement the same IT policies across various devices and minimise gaps in defences that can be exploited.

Finally, another often-overlooked aspect of mobile device management is firmware management. While upgrading to the latest firmware is typically a good idea, new firmware updates must first be tested to ensure compatibility with enterprise applications.

In the same vein, users who continually defer an update also put the corporate network at risk. For these reasons, the ability to monitor and manage firmware is an important capability that enterprises should not overlook.

Segregating work and play

Experienced security managers know that the best security measures are moot if stifled users actively seek to circumvent them. To prevent this, it is crucial to strike a balance between security measures and user experience by creating a separate, secure workspace on enterprise mobile devices.

By segregating and keeping work-related data and apps isolated from their personal data, enterprises ensure enterprise data security management and prevent enterprise data leakage. On their part, employees can continue using their favourite apps and services without fear of compromising the security of the company's sensitive information.

Moreover, the implementation of a separate workspace on personal devices allows IT departments to enforce security policies and manage work-related apps



SAMSUNG

Samsung at GovWare

Oct 17 - 19, 2023
MBS Convention Centre: Booth F17

Discover how you can empower your frontline and IT teams with the latest military-grade rugged devices, protected from chip up by KNOX security solutions. Trusted by the governments, designed to keep you safe.

Schedule a meeting with one of our experts, and learn about priority access to GovWare deals!



Is Zero Trust Vision Achievable?
Oct 18 Wed, 5pm - 5.30pm
MBS Convention Centre, Level 3, Room GW3

Joon Hong
Director, Product Management
Samsung Electronics

Where is your organisation at with respect to implementing Zero Trust security? Hear from Joon as he uncovers the importance of robust endpoint security foundation, with rollout and management to allow for a balance of security and user experience in order to achieve your Zero Trust Vision.

and data without interfering with the user's personal space. This approach not only enhances security but also respects the privacy of employees, fostering a more positive work environment.

Samsung Knox: An enterprise platform for devices

The Samsung Knox platform is an industry-leading ecosystem designed to provide best-in-class security, policy management, and compliance capabilities to enterprise mobile devices. First launched in 2013, there are over 70 million devices managed under Knox today.

Apart from features such as firmware management (Knox E-FOTA) and unified endpoint management (Knox Suite), Knox offers key features to support Zero Trust that conform to the key pillars as outlined in Singapore's Government Zero Trust Architecture (GovZTA) framework.

To ensure support for the greatest range of devices including PCs, Samsung works with multiple partners such as Microsoft, VMware, and Dell, and even other MDM solutions to support enterprise deployments.

Samsung will be present at GovWare 2023, Asia's premier cybersecurity event. Learn more about Knox and check out Samsung's range of rugged mobile devices designed for frontline workers at Booth F17.

This article is also available online on the [GovWare Knowledge Hub](https://www.govware.sg/knowledge-hub).

Safeguarding Innovation in Critical Infrastructure - A Spotlight on Healthcare

Imagine a future where smart medical devices monitor our health around the clock, leveraging AI to detect health issues early. These devices provide timely intervention, helping us stay healthy from the comfort of our homes.

Across Asia and the world, digitalisation is revolutionising the healthcare ecosystem. In this fast-paced landscape, telemedicine is flourishing, while the incorporation of new technologies is streamlining healthcare delivery, cutting costs, and enhancing patient outcomes.

Yet the healthcare sector is arguably more vulnerable than others to cyber threats. And as we become more dependent on connected devices and systems, the potential for medical data manipulation and even physical harm grows exponentially. What can we do to address cyber threats in healthcare?

The digitalisation of healthcare

It's no secret that patient access to care and the way healthcare workers operate in healthcare institutions have evolved, thanks to digitalisation and advancements in technology.

[Yong Yih Ming](#), CEO of Mount Elizabeth Hospital, pointed out that the days of hardcopy "case cards" stored in metal cabinets are fast disappearing. In Singapore, medical records are typically digitalised.

"It has brought a lot of efficiencies and improved accessibility to care for the patients. And in some way, it has also reduced the cost of health care," he said. "The visuals, the patient information, their medical conditions, the medication prescribed, even the cost of treatment, are all part of this digital system."

Such sensitive information falling into the wrong hands would be a huge problem. Fully securing the systems that host clinical information is no walk in the park, however, considering the diversity of healthcare environments and technology infrastructures.

"Everyone has different financial investment, different logistics support, and different infrastructure. I think that's where the new challenges will come from because it's not a homogeneous care or technology environment," observed Yong.

"It is also not a homogeneous technology knowledge environment – the doctors and healthcare professionals using these systems vary in terms of their cyber security awareness and understanding of technology and information sharing."

A rising tide of threats

Medical devices are the weakest link on the hospital network as they bear critical vulnerabilities, says [Alex Nehmy](#), the director of Industry 4.0 for Japan & Asia Pacific at Palo Alto, citing research by his firm's threat intelligence and incident response team, Until 42.

Imaging devices, such as X-ray, magnetic resonance imaging (MRI) and computed tomography (CT) scanners, are particularly vulnerable. Specifically, one in five (20%) common imaging devices are running an unsupported version of Windows, and 44% of CT scanners and 31% of MRI machines were exposed to high-severity vulnerabilities.

"[Today], medical devices critical in providing positive health outcomes for patients are now computer systems performing complex and life-saving medical functions – like digital ventilators, advanced pacemakers with implantable defibrillators, and robotic surgical systems – and they're getting smarter," said Nehmy.



"Vulnerabilities to cyberattacks have increased with digitalisation. The closer a medical device is to a patient, the more likely it is to impact patient safety and that a threat actor will weaponise it."

– **Alex Nehmy, Director Industry 4.0, Japan & Asia Pacific, Palo Alto Networks**

Vulnerabilities to cyberattacks have increased with digitalisation, Nehmy explained. He noted that the closer a medical device is to a patient, the more likely it is to impact patient safety and that a threat actor will weaponise it.

"A security breach in health care is of critical concern because security lapses in these devices have the potential to put lives at risk or expose sensitive patient data. Ensuring the cyber security of Internet of Medical Things (IoMT) [devices] has never been more important for patient safety," he said.

Charting the road ahead

Legacy, perimeter-based security is no longer adequate, says Nehmy. "Healthcare service providers will need an ironclad strategy that offers complete visibility on

how people will interact with them and ensures that security is baked in all steps of their approach, from the planning stages through the running phase."

Ultimately, healthcare CISOs must prepare for the worst. "Preparedness is key, and having an incident response plan is no longer a 'nice to have' but a must to manage growing cyber threats and minimise the impact of cyberattacks on business operations," said Nehmy.

One thing that IHH Healthcare Singapore did was introduce restrictions to patients' information, limit the use of portable storage devices, and keep general Internet access to dedicated terminals, says Yong. Moreover, new employees are expected to pass a compulsory cybersecurity onboarding quiz, which must be retaken annually with updated questions.

Yong suggests that new equipment purchases should be viewed through the lens of cyber security. A connected robot for the operating theatre should be acquired together with relevant systems to mitigate potential cyber security threats. A project-based approach like this keeps cyber security investments manageable and progressively improves the organisation's security posture, he says.

And when more investments are needed, such as additional security systems to secure the growing fleet of hypothetical robots, this could be amortised across the lifespan of the system: "If we can do it on a bite-sized level, in simple investment terms, then I think it's probably easier for the board or the senior management to accept."

"Boards need to understand that beyond providing healthcare services, good healthcare in the future is really how we manage digitalisation and patient information in a digital context," said Yong.

"And when it comes to allocating the budget, it needs to go beyond just the tools for healthcare operations. There must be another layer of dedicated investments for cyber security protection. Like it or not, this is the new normal," he summed up.

Remember to join us at the by-invitation-only GovWare Healthcare Forum in Room GW7 at 12pm today if you have registered.

Explore "Strengthening Cybersecurity of Medical Devices - A Team Sport Approach" by Dr Alvin Lee, Deputy Director (Analytics and Capacity Building), Health Regulation, Ministry of Health, on 18 Oct 2023 at 2:30pm - 3:00pm. Don't miss the Health Innovation Showcase as well at the GovWare Exhibition at Level 1.

This article is also available online on the [GovWare Knowledge Hub](#).

Our Sponsors

CORNERSTONE



Ensign InfoSecurity	Booth J02
---------------------	-----------

PLATINUM PLUS

	Cisco Systems (USA) Pte Ltd	Booth J08		CrowdStrike Singapore Pte Ltd	Booth J12		Huawei International Pte Ltd	Booth H08		M.Tech Products Pte Ltd	Booth M08		Mandiant	Booth M12		NCS	Booth P06
	Palo Alto Networks	Booth G06		PCS Security	Booth L02		Singtel	Booth M02		ST Engineering	Booth M12		Trellix	Booth L12		Trend Micro	Booth H02

PLATINUM

	Check Point Software Technologies Ltd.	Booth L18		F5	Booth R06		Fortinet	Booth J18		HPE Aruba Networking	Booth G02		IBM Corporation	Booth H18
	Lenovo Singapore Pte Ltd	Booth P02		Menio Security	Booth G10		NTT	Booth M18		SentinelOne	Booth N18		Tanium Singapore Pte Ltd	Booth P10

GOLD

	Aqua	Booth E14		Cloudflare, Pte. Ltd.	Booth E22		Eclipsium	Booth Q02		ExtraHop	Booth F05		Imperva	Booth F01		Infoblox Inc	Booth E05
	LogRhythm	Booth P14		National Cyber Security Agency - Qatar	Booth C10		Rubrik	Booth P18		Samsung	Booth F17		ServiceNow	Booth B12		SolarWinds	Booth Q14
	Symantec by Broadcom	Booth E01		VMware Singapore Pte. Ltd.	Booth B01		Votiro Cybersec Ltd.	Booth Q10		XM Cyber	Booth E09		Zscaler	Booth E10			

Agenda Overview

17 OCTOBER 2023

8:30am – 5:00pm	Singapore Cyber Conquest 2023		
8:30am – 6:00pm	DFRWS APAC 2023 (Workshops) @ Suntec Singapore		
9:00am – 9:30am	SICW Opening Ceremony		
9:30am – 12:30pm	SICW High-Level Panels – Opening Plenary		
12:00pm – 1:00pm	Lunch Break		
12:30pm – 3:20pm	CXO Plenary (By-invite-only)		
1:00pm – 1:10pm	GovWare Opening Remarks		
1:10pm – 1:55pm	GovWare Keynote Panel		
2:00pm – 3:30pm	Track 1: Developments in the Zero Trust Environment	Track 2: Cybersecurity Ops Centre	Track 3: Recent Developments in ML/ AI Engines
3:30pm – 4:00pm	Tea Break		
4:00pm – 5:30pm	Track 1: How Can Collaborative Partnerships Forge Impactful Synergies in Cybersecurity? (Panel Session)	Track 2: Endpoint, Mobile & Network Security	Track 3: Artificial Intelligence: Friend, Foe or a Bit of Both for Cybersecurity (Panel Session)
5:30pm – 7:30pm	GovWare Opening Reception		

18 OCTOBER 2023

9:00am – 11:00am	GovWare Keynote Sessions		
9:00am – 6:00pm	DFRWS APAC 2023 (Conference)		
11:00am – 11:30am	Tea Break		
11:30am – 1:00pm	GovWare x ICE71 Innovation Hour		
11:30am – 1:00pm	GovWare Keynote and Panel Sessions		
12:00pm – 3:30pm	GovWare Healthcare Forum (By-invite-only)		
1:00pm – 2:00pm	Lunch Break		
2:00pm – 3:30pm	Track 1: Cybersecurity and Digital Transformation	Track 2: Organisational Cybersecurity Culture; The Role of Leadership and Management	Track 3: Managing Crossroads of Data Security, Data Privacy and AI Adoption (Panel Session)
2:00pm – 3:30pm	Tech Talk Sessions		
3:30pm – 4:00pm	Tea Break		
4:00pm – 5:30pm	Track 1: Cybersecurity as an Essential Enabler: Who, What, Where, When and How (Panel Session)	Track 2: Developing the Cybersecurity Ecosystem, Talent Pipeline and Professionalism	Track 3: Security by Design: Risk Assessment, Avoidance and Mitigation
4:00pm – 5:30pm	Tech Talk Sessions		
5:30pm – 7:30pm	GovWare Happy Hour		

19 OCTOBER 2023

8:15am – 5:15pm	Cyber Secure Singapore 2023		
9:00am – 6:00pm	DFRWS APAC 2023 (Conference)		
9:00am – 10:30am	GovWare Keynote Sessions		
9:50am – 10:30am	Tech Talk Sessions		
10:30am – 11:00am	Tea Break		
11:00am – 1:00pm	CLOUDSEC @GovWare 2023		
11:00am – 1:00pm	Tech Talk Sessions		
1:00pm – 2:00pm	Lunch Break		
2:00pm – 4:00pm	Government Closed Door Session (Open to SG Civil & Public Servants only)		
2:00pm – 5:30pm	GovWare FSI Forum (By-invite-only)		
2:00pm – 3:30pm	Track 1: Cyber Threat Landscape & Intelligence	Track 2: Cloud Native Security	Track 3: Operational Technology Threat and Vulnerabilities Landscape
2:30pm – 3:30pm	Tech Talk Sessions		
3:30pm – 4:00pm	Tea Break		
4:00pm – 5:30pm	Track 1: Cyber Threat Landscape & Intelligence	Track 2: Darkweb, Cybercrime, Cyberwarfare	Track 3: Building Resilience: Securing Critical Infrastructures and IT Supply Chains (Panel Session)
4:00pm – 5:00pm	Tech Talk Sessions		
6:00pm – 9:00pm	GovWare Appreciation Night (By-invite-only) @ PARKROYAL COLLECTION Marina Bay, Singapore		

Conference Programme

18 OCTOBER 2023

<p>9:00am – 9:30am</p>	<p>Keynote: The Evolving Challenges in Cybersecurity Lee Fook Sun Chairman <i>Ensign InfoSecurity</i></p>				
<p>9:30am – 10:00am</p>	<p>Keynote: Navigating the Crossroads of AI and Cybersecurity Sam Rubin Vice President, Global Head of Operations, Unit 42 <i>Palo Alto Networks</i></p>				
<p>10:00am – 10:30am</p>	<p>Keynote: The Forgotten Last Layer of Securing Digital Transformation Poornima DeBolle Co-Founder & Chief Product Officer <i>Menlo Security</i></p>				
<p>10:30am – 11:00am</p>	<p>Keynote: Cyber Security Myth-understanding: Demystifying OT Cybersecurity Goh Eng Choon President, Cyber <i>ST Engineering</i></p>				
<p>11:00am – 11:30am</p>	<p>Tea Break</p>				
<p>11:30am – 12:00pm</p>	<p>Keynote: Defying Cybercriminals: Trust, Innovation, and Resilience in the Digital Age Eva Chen Chief Executive Officer & Co-Founder <i>Trend Micro</i></p>				
<p>12:00pm – 1:00pm</p>	<p>Keynote Panel: Digital Transformation - When the Tyre Hits the Road Moderator: Ng Hoo Ming Advisor & President for Cybersecurity & Governance Chapter <i>ASEAN Chief Information Officer Association (ACIOA)</i></p>				
	<p>Stephen Fogarty Senior Executive Advisor <i>Booz Allen Hamilton</i></p>	<p>Foo Siang-Tse Senior Partner, Cyber <i>NCS</i></p>	<p>Eddie Hau Chief Information Security Officer <i>Sunway Group</i></p>	<p>Steve Ledzian Chief Technology Officer <i>Mandiant - Google Cloud</i></p>	<p>Ong Chin Beng Chief Information Security Officer <i>Maritime and Port Authority of Singapore</i></p>

Conference Programme

	Track I: Cybersecurity and Digital Transformation	Track II: Organisational Cybersecurity Culture; The Role of Leadership and Management	Track III: Managing Crossroads of Data Security, Data Privacy and AI Adoption
2:00pm – 2:30pm	Cybersecurity in the Digital Era Tham Mei Leng Ministry Chief Information Security Officer <i>Government Technology Agency</i>	Leading in the Talent Warfare: Empowering Leaders to Securely Harness GenAI for a Resilient Future Ed Soo Hoo WW Chief Technology Officer Global Account Innovation & Transformation Executive <i>Lenovo Singapore</i>	Moderator: Jenny Tan President <i>ISACA Singapore Chapter</i> Panellists: Chen Kin Siong Chief Information Security Officer & Co-Founder <i>InsiderSecurity</i> Dr Richard Searle Vice President of Confidential Computing <i>Fortanix</i> Dr Vrizlynn Thing Senior Vice President <i>ST Engineering</i> Yeong Chee Wai Area Vice President, APJ <i>Rubrik</i>
2:30pm – 3:00pm	Strengthening Cybersecurity of Medical Devices - A Team Sport Approach Dr Alvin Lee Deputy Director (Analytics and Capacity Building), Health Regulation <i>Ministry of Health</i>	Duty of Care: The Convergence of Remote Working, Cyber-Safety Culture & Insider Risk Nick Savvides Field Chief Technology Officer & Head of Strategic Business APAC <i>Forcepoint</i>	
3:00pm – 3:30pm	What Keeps CISOs Up at Night - CISO World Cup 2023 Vivek Gullapalli Chief Information Security Officer, APAC <i>Check Point Software Technologies</i>	Managing Which Cyber Risks to Accept, Mitigate or Transfer for Complex National Eco-Systems Evelyn Anderson Distinguished Engineer <i>IBM</i>	
3:30pm – 4:00pm	Tea Break		
	Track I: Cybersecurity as an Essential Enabler: Who, What, Where, When and How	Track II: Developing the Cybersecurity Ecosystem, Talent Pipeline and Professionalism	Track III: Security by Design: Risk Assessment, Avoidance and Mitigation
4:00pm – 4:30pm	Moderator: Johnny Kho President <i>Association of Information Security Professionals (AiSP)</i> Panellists: Rashmy Chatterjee Chief Executive Officer <i>ISTARI</i>	Exploring CISO Challenges and the Government CISO Ecosystem Soh Zhi Qi Assistant Director <i>Government Technology Agency</i>	Why Increasing Exposure Management Maturity is the Key to Closing the Remediation Deficit Stree Naidu Vice President, APAC <i>XM Cyber</i>
4:30pm – 5:00pm	Qiang Huang Vice President, Product Management <i>Palo Alto Networks</i> Jim Richberg Head of Cyber Policy & Global Field CISO <i>Fortinet</i>	Future of Cyber Workforce: Harnessing Non-traditional Talent Benjamin Tan Chief Executive Officer <i>Red Alpha Cybersecurity</i>	Make Better Risk Decisions to Prevent Future Cyber Attacks Nathan Wenzler Chief Security Strategist <i>Tenable</i>
5:00pm – 5:30pm	Karan Sondhi Chief Technology Officer, Public Sector <i>Trellix</i> Richie Tan Partner, Cyber & Forensics GTM <i>PWC</i> Chris Thomas Senior Security Advisor <i>ExtraHop</i>	From Ethical Hacker to Professional: Professionalising the Cybersecurity Ecosystem Rowland Johnson President <i>CREST</i>	Is Zero Trust Vision Achievable? Joon Hong Director, Product Management <i>Samsung Electronics</i>

Tech Talk Programme

18 OCTOBER 2023

GovWare x ICE71 Innovation Hour

11:30am – 11:50am	<p>Keynote: Cybersecurity Acumen Through Startup Growth</p> <p>Ian Lim Field Chief Security Officer JAPAC <i>Palo Alto Networks</i></p>		
11:50am – 12:30pm	<p>Panel Session: If I Were a Hacker Now: Perspectives from a Venture Capitalist, Chief Information Security Officer, and Founder</p> <p>Moderator: Rayson Ng Programme Manager <i>ICE71 (NUS Enterprise)</i></p>		
	<p>Beenu Arora Chief Executive Officer and Co-Founder <i>Cyble</i></p>	<p>Huang Shao Fei Chief Information Security Officer <i>SMRT Corporation</i></p>	<p>Tan Yi Shu CapVista Investment Associate <i>Cap Vista</i></p>

Tech Talk

2:00pm – 2:20pm	<p>A Giant Leap of (Offensive) AI</p> <p>Andy Thompson Offensive Security Research Evangelist <i>CyberArk Labs</i></p>		
2:20pm – 2:40pm	<p>Advancing Cyber Analytics Via a Multi-disciplinary Approach</p> <p>Lee Joon Sern Director (ML and Cloud Research), Labs <i>Ensign InfoSecurity</i></p>		
2:40pm – 3:30pm	<p>Panel: AI in Cybersecurity: Promise or Reality of the Ideal Human-Machine Partnership?</p> <p>Moderator: David Siah Vice President, South East Asia-Australia <i>Centre for Strategic Cyberspace + International Studies (CSCIS)</i></p>		
	<p>Dr Magda Chelly Managing Director, Chief Information Security Officer <i>Responsible Cyber</i></p>	<p>Mark Johnston Director, Office of the CISO <i>Google</i></p>	<p>Lee Joon Sern Director (ML and Cloud Research), Labs <i>Ensign InfoSecurity</i></p>
3:30pm – 4:00pm	<p>Tea Break</p>		
4:00pm – 4:20pm	<p>The Cyber Threats from the Supply Chain: Best Practices in Addressing Third-Party Risk at Scale</p> <p>Brendan Conlon Chief Operating Officer of Supply Chain Defense <i>BlueVoyant</i></p>		
4:20pm – 4:40pm	<p>AI - Boon or Bane for AppSec?</p> <p>Julian Totzek-Hallhuber Director Solution Architects <i>Veracode</i></p>		
4:40pm – 5:30pm	<p>Panel Session: AI & Cybersecurity: Threats, Risks and Opportunities</p> <p>Moderator: Dr Carrine Teoh Vice President, Cybersecurity Chapter <i>ASEAN CIO Association (Cybersecurity & Governance Chapter)</i></p>		
	<p>Brendan Conlon Chief Operating Officer of Supply Chain Defense <i>BlueVoyant</i></p>	<p>Audrey Teoh Chief Information Security Officer <i>Singapore Post</i></p>	<p>Julian Totzek-Hallhuber Director Solution Architects <i>Veracode</i></p>

ABP SECURITE

A Company of ABPGroup

VISIT US AT BOOTH M22

Learn about our latest **CyberRange** and **Solutions** to equip yourself ahead of potential cyber threats



www.abpsecureite.com

BeyondTrust

Leader in Intelligent Identity & Access Security

Visit Booth N22

athena dynamics

Disrupt the **THOUGHT**, Address the **CAUSE**

Join us for actionable disruptive IT and OT cyber protection technologies to address the causes of attacks, not just their effect.

BOOTH J28

Visit us and stand a chance to win attractive prizes in our lucky draw!



For more details, [CLICK HERE TO FIND OUT MORE](#)

aqua

We stop cloud native attacks

we guarantee it



Stay Informed, Join the GovWare Community!

JOIN NOW



www.govware.sg

LogRhythm®

Security Made Easy



Axon



NDR



SIEM

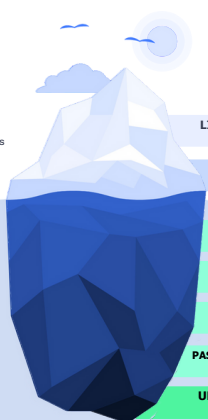


UEBA

Visit us at **Booth P14** to find out more.

VOTIRO

Zero Trust Content Security



ANTIVIRUS

Only prevents what's already detectable
System slowdowns and file limitations

LIMITED DETECTION CAPABILITIES

KNOWN THREATS WITH SIGNATURES

VOTIRO

Prevents threats hiding under the surface

Retain full file functionality
Transparent, frictionless, signatureless

Reduce time spent by SOC team on investigating files

Reduce risk, reduce costs, and increase business productivity

URLS & ACTIVE CONTENT

HIDDEN EXECUTABLES

STEGANOGRAPHY

PASSWORD-PROTECTED ELEMENTS

UNKNOWN THREATS & ZERO DAYS

votiro.com

TRUVISOR

VISIT US @ **BOOTH L28**

AUTOMATING YOUR CYBERSECURITY DEFENCE

TRUVISOR'S SHOWCASE AT BOOTH L28



00011

ABP GROUP

Elevating Security Excellence

Enhance your security posture with our **Managed Security Suite**

VISIT US AT BOOTH L22

Companies of ABPGroup

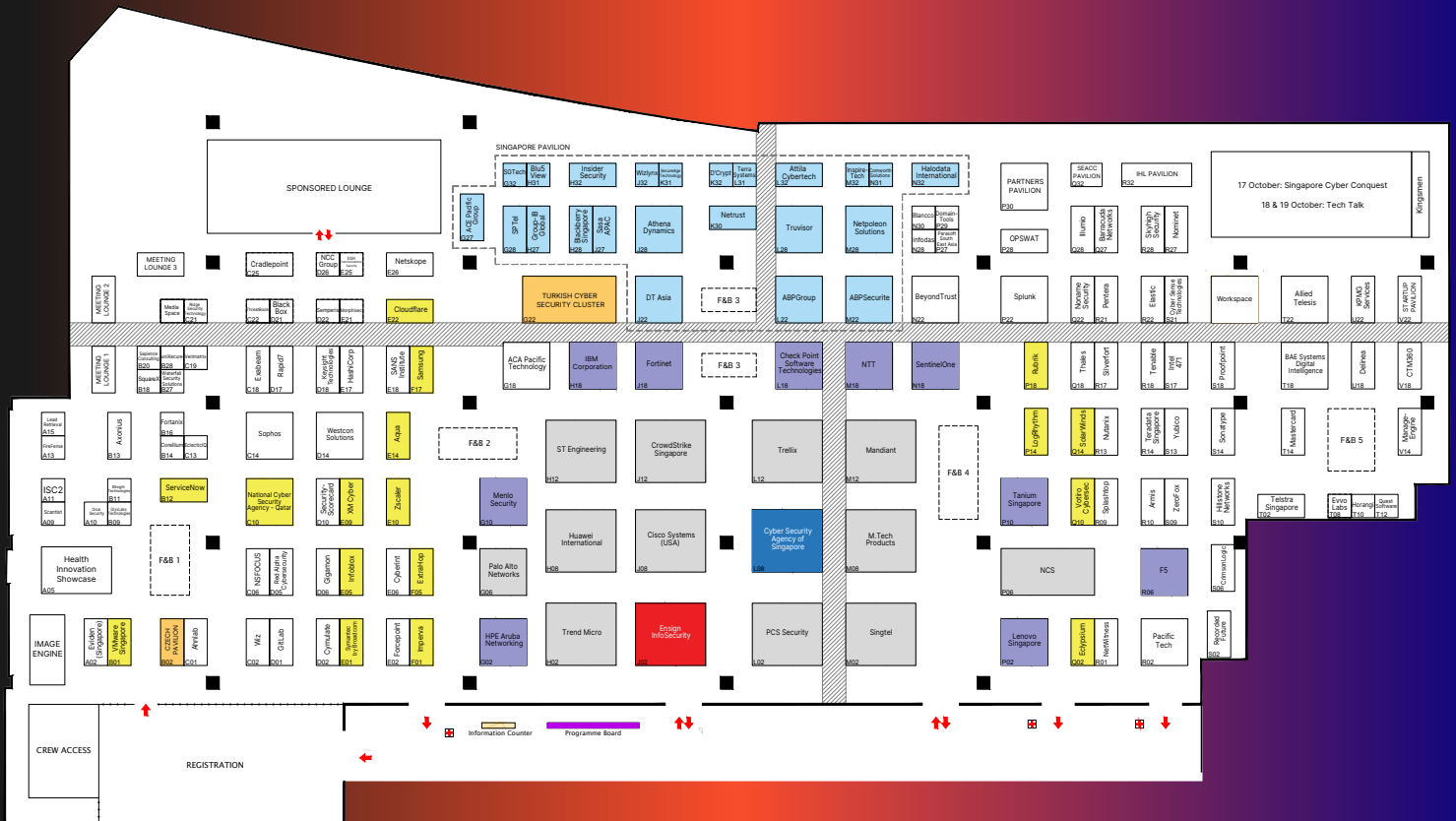
SUNNIC
A Company of ABPGroup

ABPCYBER
A Company of ABPGroup

ABPSECURITE
A Company of ABPGroup

www.abpgroup.com

Exhibition Floor Plan



Legend

- Cornerstone
- Platinum
- Exhibitor
- Country Pavilion
- Platinum Plus
- Gold
- Singapore Pavilion
- Information Counter

Exhibitors Listing

SPONSORS	BOOTH
Aqua	E14
Check Point Software Technologies Ltd.	L18
Cisco Systems (USA) Pte Ltd	J08
Cloudflare, Pte. Ltd.	E22
CrowdStrike Singapore Pte Ltd	J12
Eclyspium	Q02
Ensign InfoSecurity	J02
ExtraHop	F05
F5	R06
Fortinet	J18
HPE Aruba Networking	G02
Huawei International Pte Ltd	H08
IBM Corporation	H18
Imperva	F01
Infoblox Inc	E05
Lenovo Singapore Pte Ltd	P02
LogRhythm	P14
M.Tech Products Pte Ltd	M08
Mandiant	M12
Menlo Security	G10
National Cyber Security Agency - Qatar	C10
NCS	P06
NTT	M18
Palo Alto Networks	G06
PCS Security	L02
Rubrik	P18
Samsung	F17
SentinelOne	N18
ServiceNow	B12
Singtel	M02
SolarWinds	Q14
ST Engineering	H12
Symantec by Broadcom	E01
Tanium Singapore Pte Ltd	P10
Trellix	L12
Trend Micro	H02
VMware Singapore Pte. Ltd.	B01

Votiro Cybersec Ltd.	Q10
XM Cyber	E09
Zscaler	E10

Cyber Security Agency of Singapore **L08**

EXHIBITORS	BOOTH
ACA Pacific Technology (S) Pte Ltd	G18
AhnLab, Inc	C01
Allied Telesis	T22
Armis	R10
Axonius Inc	B13
BAE Systems Digital Intelligence	T18
Barracuda Networks Inc	Q27
BeyondTrust	N22
Bitsight Technologies, Inc	B11
Black Box	D21
Blanco	N30
Corellium	B14
Cradlepoint	C25
CrimsonLogic Pte Ltd	S06
CTM360	V18
Cyber Sense Technologies	S21
Cyberint	E06
Cymulate	D02
Delinea	U18
DomainTools	P29
EclecticlQ	C13
Elastic	R22
Eviden (Singapore) Pte Ltd	A02
Evvo Labs	T08
Exabeam	C18
FireFense	A13
Forcepoint	E02
Fortanix	B16
Gigamon	D06
GitLab	D01

HashiCorp	E17
Health Innovation Showcase	A05
Hillstone Networks	S10
Horangi Pte Ltd	T10
Illumio Inc	Q28
infodas	N28
Intel 471	S17
ISC2	A11
Keysight Technologies	D18
KPMG Services Pte Ltd	U22
ManageEngine	V14
Mastercard	T14
Morphisec	E21
NCC Group	D26
Netskope	E26
NetWitness	R01
Nominet	R27
Noname Security	Q22
NSFOCUS	C06
Nutanix	R13
OPSWAT	P28
Orca Security	A10
OryxLabs Technologies	B09
Pacific Tech	R02
Parasoft South East Asia	P27
Pentera	R21
Proofpoint, Inc.	S18
Quest Software	T12
Rapid7	D17
Recorded Future	S02
Red Alpha Cybersecurity	D05
Ridge Security Technology	C21
SANS Institute	E18
Sapience Consulting	B20
Scantist Pte Ltd	A09
SecurityScorecard Inc	D10
Semperis	D22
Silverfort	R17
Skyhigh Security	R28
Sonatype	S14

Exhibitors Listing

EXHIBITORS	BOOTH
Sophos Pte Ltd	C14
Splashtop	R09
Splunk	P22
SquareX Pte Ltd	B18
SSH Communications Security	E25
Telstra Singapore	T02
Tenable	R18
Teradata Singapore Pte Ltd	R14
Thales	Q18
ThreatBook	C22
uniXecure	B28
Verimatrix, Inc.	C19
Waterfall Security Solutions Ltd	B27
Westcon Solutions Pte Ltd	D14
Wiz	C02
Yubico	S13
ZeroFox	S09

PAVILIONS	BOOTH
Singapore Pavilion	
ABPGroup Pte Ltd	L22
ABPSecureite Pte Ltd	M22
ACE Pacific Group Pte Ltd	G27
Athena Dynamics Pte Ltd	J28
Attila Cybertech Pte Ltd	L32
Blackberry Singapore Pte Limited	H28
Blu5 View Pte Ltd	H31
Comworth Solutions Pte Ltd	N31
D'Crypt Pte Ltd	K32
DT Asia Pte Ltd	J22
Group-IB Global Private Limited	H27
Halodata International Pte Ltd	N32

Insider Security Pte Ltd	H32
Inspire-Tech Pte Ltd	M32
Netpoleon Solutions Pte Ltd	M28
Netrust Pte Ltd	K30
Sasa APAC Pte Ltd	J27
SecureAge Technology Pte Ltd	K31
SGTech	G32
SPTel Pte Ltd	G28
Terra Systems Pte Ltd	L31
Truvisor Pte Ltd	L28
Wizlynx Pte Ltd	J32

Czech Pavilion	
Blindspot Technologies	B02
GoodAccess	

Turkish Cyber Security Cluster	
Arksoft	G22
Cyberwise	
FileOrbis	
Labris Networks	
Secunnix	
STM Defence International	
TR7 Load Balancer & WAF	
Ulak Communications Inc.	

South-East Asia Cybersecurity Consortium (SEACC) Pavilion	
Association of Information Security Professionals (AISP)	Q32
Association of National Information and Communication Technology Entrepreneurs (APTIKNAS)	
Brunei Cyber Security Association (BCSA)	
Women in Security Alliance Philippines (WiSAP)	

Startup Pavilion	
Aires A.T.	V22
AxisNow	
PolyDigi	
Reperion	
Wissen International Pte. Ltd.	

Partners Pavilion	
ASEAN Chief Information Officer Association (ACIOA)	P30
Center for Strategic Cyberspace & International Studies (CSCIS)	
Cyber Youth Singapore	
IASA APAC	
ICE71	
ISACA Singapore Chapter	
iTnews	
Operational Technology Information Sharing and Analysis Center (OT-ISAC)	

IHL Pavilion	
Cyber-Hardware Forensics & Assurance Evaluation R&D Programme (CHFA), NTU	R32
ITE College Central	
ITE College East	
iTrust, Centre for Research in Cyber Security, SUTD	
Nanyang Polytechnic	
National Cybersecurity R&D Laboratory (NCL), NUS	
National Integrated Centre for Evaluation (NICE), NTU	
Republic Polytechnic	
Strategic Centre for Research in Privacy-preserving Technologies and Systems (SCRIPTS), NTU	
Temasek Polytechnic	

General Information

GovWare Exhibition and Networking

Exhibition Hours	17-18 October, 9:00am – 5:30pm 19 October, 9:00am – 5:00pm
GovWare Opening Reception	17 October, 5:30pm – 7:30pm
GovWare Happy Hour	18 October, 5:30pm – 7:30pm
Location	GovWare Exhibition Hall, Level 1 Halls A-C, Sands Expo and Convention Centre

SICW 2023 Open Sessions

All GovWare pass holders can also access SICW 2023 Open Sessions, including the SICW Opening Ceremony, SICW High-Level Panels – Opening Plenary, Women in Cyber, International IoT Security Roundtables, and more. For more information, view the SICW calendar of events [here](#).

Media Centre

The Media Centre offers complimentary internet access exclusively for verified media personnel.

Location	Begonia 3110, Level 3, Sands Expo and Convention Centre
Hours	17-19 October 2023, 8:30am-6:00pm

For any media enquiries, please reach out to HKGovWare2023@hkstrategies.com.

Data Collection

GovWare does not share your information with Sponsors and Exhibitors without your explicit consent. Do note that when you permit the scanning of your badge by any Sponsor or Exhibitor, you are granting consent for them to collect your personal data. The sponsors and exhibitors may use this information to send you information about products, content, and services that might interest you and for internal analytical and business development purposes. Please note that the sponsors and exhibitors have their own privacy policies, you should check their privacy policies or opt-out from their communications directly with the respective organisations.

Unofficial Partners & Fraudulent Emails Alert

Watch out for false claims of GovWare partnerships and fraudulent emails selling attendee lists. GovWare has no such partnerships, and we never sell attendee data. Legitimate partnerships are announced through GovWare's official channels. Before committing or purchasing, verify with us. For concerns or official partnerships, contact us at enquiries@govware.sg or your GovWare representative.

Photography and Filming Notice

By attending this event, you agree to be photographed, filmed, and otherwise recorded. Please be aware that these images and recordings may be used for promotional, educational, and informational purposes by the event organisers and their partners. Your participation in the event implies your consent to the use of your likeness and voice in these materials, without any further notification or compensation. If you have any concerns about your image being captured, please notify the event staff or organisers. We appreciate your understanding and cooperation in helping us document and share the experience of this event.

Registration Counters and Name Badge Collection

Registration Counter Location	GovWare Exhibition Hall, Level 1 Hall C, Sands Expo and Convention Centre
-------------------------------	---

To collect your badge at the registration counter, follow these steps:

- Go to the registration counter and queue at one of the kiosks.
- Scan the QR code from the 'Know Before You Go' email to print your badge.
- Receive your printed name badge, badge pouch, and lanyard.
- Verify the badge details for accuracy before leaving the registration area.

For a smooth badge collection process, please have the following items with you:

- Any government-issued identification
- Registration confirmation email with your unique QR code
- Your business card
- Singapore Public Service Card or Civil Service Card (if applicable)

Should you require any assistance, please do not hesitate to contact our Registration Support at registration@govware.sg.

Parking Coupon

From 17-19 October, you can obtain a discounted **SGD8.56** parking ticket for a single exit with your event pass. Visit the Sands Expo and Convention Center Event Services Concierge along the foyer of the Exhibition Hall at Level 1 between 8:00am and 6:00pm to redeem it. Please present your event pass to be eligible for redemption.

Upon exiting the car park, simply scan the coupon at the car park exit to lower your parking fees to SGD8.56.

Important: Remove your cash card before reaching the exit gantry to prevent any additional deductions from it.

Our Partners

HELD IN



A PART OF



ORGANISED BY



KEY SUPPORTING PARTNER



SUPPORTING ORGANISATIONS



SUPPORTING ASSOCIATIONS



MEDIA PARTNERS





GovWare 2024

Conference and Exhibition

Where Cyber Means Business

Save the Date!

15-17 October 2024

Sands Expo and
Convention Centre,
Singapore

REGISTER INTEREST NOW

www.govware.sg