

SHOW DAILY

THE OFFICIAL SHOW DAILY OF GOVWARE CONFERENCE AND EXHIBITION 2023

BRANDED CONTENT

Tackling the Dynamic Threat Landscape with XDR

Around the world, public sector organisations and large enterprises are wrestling with a constant barrage of sophisticated cyber threats. On the one hand, the rapidly changing tactics of cyber attackers make it difficult for them to stay ahead of emerging threats.

On the other, the situation is often exacerbated by a lack of agility in their cybersecurity strategies. Specifically, bureaucratic processes and the need for extensive approvals can hinder the timely implementation of security measures, leaving organisations vulnerable to cyberattacks.

The dynamic threat landscape

Cybercriminals are adapting and developing advanced techniques to infiltrate both public sector and corporate networks. For instance, fileless malware attacks leverage native, legitimate tools to execute a cyber attack, making them difficult to detect with traditional security measures.

Ransomware attacks show no signs of abating globally, with the time from breach to encryption as short as seven minutes. Meanwhile, supply chain attacks continue to make headway against third-party vendors and service providers, exploiting the trust relationships between organisations to gain unauthorised access.

Finally, multi-vector attacks have also become more prevalent, combining different methods and entry points to exploit vulnerabilities. This can include phishing emails, social engineering, and unpatched software.



“Organisations are using an average of 25 individual security solutions. A third say a top hurdle is having too many pieces of technology without a sole source of truth.”
– Harold Rivas, CISO, Trellix

Against this backdrop, there is a heightened sense of urgency for public sector organisations and businesses to strengthen their cybersecurity defences to proactively identify and mitigate risks.

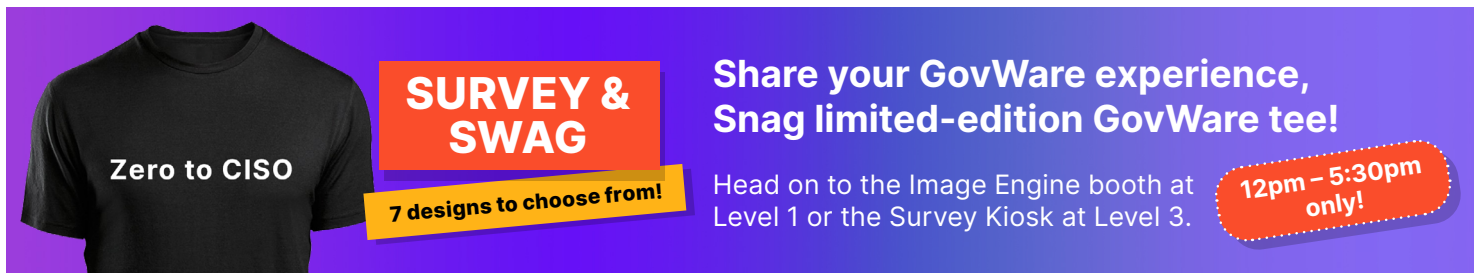
Why XDR, why now?

Traditional security tools often operate in silos, making it difficult for organisations to piece various alerts together for a complete picture of their security environment.

Indeed, a Trellix study earlier this year found both public and private organisations are using an average of 25 individual security solutions. Unsurprisingly, 30% of respondents say a top hurdle is having too many pieces of technology without a sole source of truth.

As organisations grapple with an....
Continue to page 04

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




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 or the Survey Kiosk at Level 3.

12pm – 5:30pm only!



The Trellix logo is rendered in a white, bold, sans-serif font. The letter 'X' is stylized with a diagonal slash through it. The background of the entire page is a blue-to-green gradient with a pattern of small, white, diagonal dashes.

UNTANGLING XDR

Trellix's Take on
the 2023 Gartner[®]
Market Guide

Welcome Messages

Welcome to Singapore International Cyber Week 2023

“Building Trust and Security in the Emerging Digital Order”

2023 marks yet another pivotal year for technological developments globally. Since ChatGPT was launched in November 2022 by OpenAI, there has been an explosion of interest in the use of generative artificial intelligence (GenAI) tools to augment and improve various aspects of our daily lives. Globally, businesses and governments are swiftly leveraging GenAI tools to provide enhanced customer and citizen support services.

Despite the capabilities of GenAI and its potential, many cybersecurity experts have also warned of threat actors exploiting the same technology for purposes such as malicious cyber activities, the creation of deepfake content, and development of phishing emails. Emerging technologies like these are double-edged, as with digitalisation.

This year, as we gather once again for the 8th edition of the Singapore International Cyber Week (SICW), and the 31st year of GovWare, we must be cognisant of how technological advancements can both benefit and threaten our digital way of life. While we should be optimistic about the many opportunities that the latest technologies may confer, we must be prepared to mitigate the accompanying risks and challenges to our safety and security. Cybersecurity will be critical to building trust in the ever-evolving digital domain; hence, the theme for SICW 2023 is “Building Trust and Security in the Emerging Digital Order”.

The SICW provides a platform for policy makers, industry leaders, and top academics from around the world to have extensive and diverse discussions, exchange ideas, and forge partnerships.



We are pleased to organise SICW and GovWare once again and would like to thank all our partners who helped make this possible.

Welcome to SICW 2023 and Singapore, and I hope to see you soon!

David Koh
Commissioner of Cybersecurity and
Chief Executive
Cyber Security Agency of Singapore

Welcome to GovWare Conference and Exhibition 2023

“Fostering Trust Through Collaboration in the New Digital Reality”

Welcome again, everyone!

As we meet once again, it is remarkable how two seemingly conflicting truisms come to the fore; 1) the pace of change in so many areas is stunning, and 2) yet indeed some things never seem to change.

For the first, it is easy to forget that it is only a year ago that being able to meet like this was such a privilege after years of deprivation, even isolation. COVID seems a distant memory, and our focus now is indeed on meeting friends, colleagues, and experts and driving the cause of cyber collectively. When we met in GovWare 2022, AI was already nothing new, but many noted the immense potential and excitement surrounding this field. However, few if any, could have foreseen the jaw-dropping advent of gen AI and the sheer acceleration of its impact in every aspect of life as we know it – all in just a few short months. The discussions we will have over the next few days on this subject is well nigh on a different planet from just a year ago.

And yet, we are faced with a sense of the old and familiar in so many ways as well. From the ancient times of the punch card in mainframe computing, a cliché has consistently been how technology moves at blinding speed. We marvelled at so many things, as cards gave way to 5.25 and 3.5-inch diskettes, from COBOL to object orientation, from the Apple II to the iPhone 15. The pace of change is

itself unchangeable. 30 years ago, it was said that key issues in IT security were not so much just pure technology but also about the human element and the need for collaboration. This has hardly changed – the narrative is exactly the same today as we approach with anticipation and trepidation of modern issues ranging from the complexity of ASM to the staggering force of AI. The human dimension and the need to work together – the more things change, the more they stay the same.

We are honoured to be once again event partners for the Singapore International Cyber Week (SICW), and to bring GovWare as the industry base event for the Week. In past years, we have at times used the same themes for both, and at times used slightly different focus areas as a reflection of the topical areas of discussion for the policy and industry perspectives. The second is true for 2023, but you will have perhaps noted how similar the two themes are; they were indeed developed independently. It is validation, if any is needed, that trust and digitalisation are so important today.

Like so much in life, GovWare has changed, is changing, and yet is also still the GovWare we all know, and I would trust and love. We are still the go-to for the entire ecosystem in cybersecurity and beyond, a platform developed with, for, and by all of us. But we have also embraced the convergence that has been looming for so long, the reality that cyber is so much about security,



and also so much more, as a key force for transformation and our digital future. We have expanded from serving the technology informational needs of the government-linked sectors, into serving the hyper-connected ecosystems of today, while remaining very much true to our cybersecurity roots.

You see a new, and old GovWare today, powering cybersecurity, but also helping secure our collective digital journey. Still the premier information source on public sector issues but encompassing the critical infrastructure and business ecosystems comprehensively too. We are GovWare – where cyber means business.

We are thankful once again to CSA, our partners, sponsors, and to you the cyber warrior for staying the course with us on this journey.

I look forward to meeting you again.

Ian Monteiro
Executive Director
Image Engine

... Continued from page 01

increasingly complex cybersecurity landscape, they need a solution that can keep up with the ever-changing threats and provide a comprehensive view of their security posture.

Extended Detection and Response (XDR) has gained prominence in the cybersecurity landscape in recent years. Collecting and correlating data from multiple security layers, XDR can detect threats that may go unnoticed by standalone security tools.

With XDR, organisations can consolidate their security tools, gain better visibility into their environment, and respond to threats more effectively. This not only improves their overall security posture but can reduce the complexity and cost associated with managing multiple security solutions.

Benefitting from XDR

XDR allows companies to simplify cybersecurity, offering customers a holistic view of what's happening across security controls.

Organisations that can benefit from XDR include:

- **Financial institutions:** Financial institutions are a prime target for cyberattacks because they have valuable customer data. XDR can help financial institutions detect and respond

to threats quickly and effectively, protecting their customers' data and their own financial well-being.

- **Healthcare organisations:** Healthcare organisations have access to sensitive patient data, making them a target for cyberattacks. XDR can help healthcare organisations to protect their patient data and ensure the continuity of care.
- **Critical infrastructure operators:** Critical infrastructure operators, such as power plants and water utilities, are essential to the functioning of society. XDR can help critical infrastructure operators to protect their systems from cyberattacks, preventing disruptions to essential services.
- **Large enterprises:** Large enterprises have a large and complex attack surface, making them a target for cyberattacks. XDR can help large enterprises to detect and respond to threats quickly and effectively, protecting their valuable assets.

Trellix, the leader in XDR

When evaluating XDR solutions for your organisation, it is crucial to consider several key factors. For a start, prioritise comprehensive integration with native security controls and third-party data sources, contextual threat prioritisation, real-time threat detection and response, and adaptability to a specific environment – whether on-premises, cloud-based, or hybrid.

In addition, the glue that ties an effective XDR solution together is advanced threat intelligence and analytics. On this front, the availability of advanced threat intelligence helps to better analyse threat patterns and predict future attacks and can ultimately help to better deliver the desired security outcomes.

As a cybersecurity industry leader, Trellix is dedicated to fortifying the digital defences of our over 40,000 customers, including governments and 80% of the global Fortune 500.

Trellix offers an open, integrated XDR that ingests data from the largest array of native, best-of-breed security controls spanning today's critical threat vectors as well as more than 1,000 third-party data sources.

Leveraging more than a billion global threat sensors, Trellix can correlate and enrich data to deliver timely insights to improve detection, investigation, and remediation response times.

Trellix is exhibiting at GovWare 2023, Asia's premier cybersecurity event. Visit us at booth L12 to learn more about our XDR solution and to schedule product demonstrations.

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

Rethinking App Architecture for Enhanced Resilience and App Security in Hybrid, Multi-Cloud Environments

Modern applications have evolved rapidly to meet the growing demands of the digital landscape, with the emergence of architectural patterns designed to deliver a new generation of responsive and sophisticated services that customers expect. Using these patterns, developers can create powerful applications that are more scalable, resilient, and adaptable to change.

The evolving cloud paradigm

But as new applications are rolled out on the disparate mix of systems employed by organisations today, the inevitable complexity has culminated in new challenges. Invariably, businesses find themselves grappling with hurdles in areas such as deployment, monitoring, and security.

“Customers might think that leveraging the auto-scaling capabilities in the public cloud would mean that they don't have to think about application resiliency. But the reality is that public clouds can also go down. In addition, existing application security often do not provide adequate protection for APIs and mobile app against, for example, supply chain attack and mobile device takeover.”

– Chin Keng Lim, Strategic Sales Director, F5

More than 15 years since the first public cloud platform was released, the cloud has become an integral part of

IT deployments around the world. But despite its numerous advantages, the cloud isn't always the best option for powering the incredibly diverse range of applications and use cases found across enterprises.

Considerations range from inadvertent over-provisioning of resources to hidden fees or unpredictable costs. As a result, some enterprises have started leveraging the cloud to quickly conceptualise, develop, and test applications, before moving it on-premises for long-term deployments. This effectively allows them to benefit from the flexibility and capabilities of the cloud, while enjoying the fixed cost overheads of on-premises systems.

Data residency is another concern that is now a key factor in many industries,...

Continue to page 05

... Continued from page 04

with the spotlight also falling on data privacy in the face of stricter regulatory requirements. Moreover, regulations such as GDPR and HIPAA have led to enterprises seeking alternative solutions that offer greater control over their data while still benefiting from the advantages of the public cloud.

For these reasons, a multi-cloud, hybrid cloud strategy has emerged as the preferred choice for many enterprises. While cloud adoption continues to grow, organisations are gravitating towards the best combination of cloud and on-premises infrastructure for the best of both worlds. The result is a complicated web of interconnected systems, each with its own set of benefits.

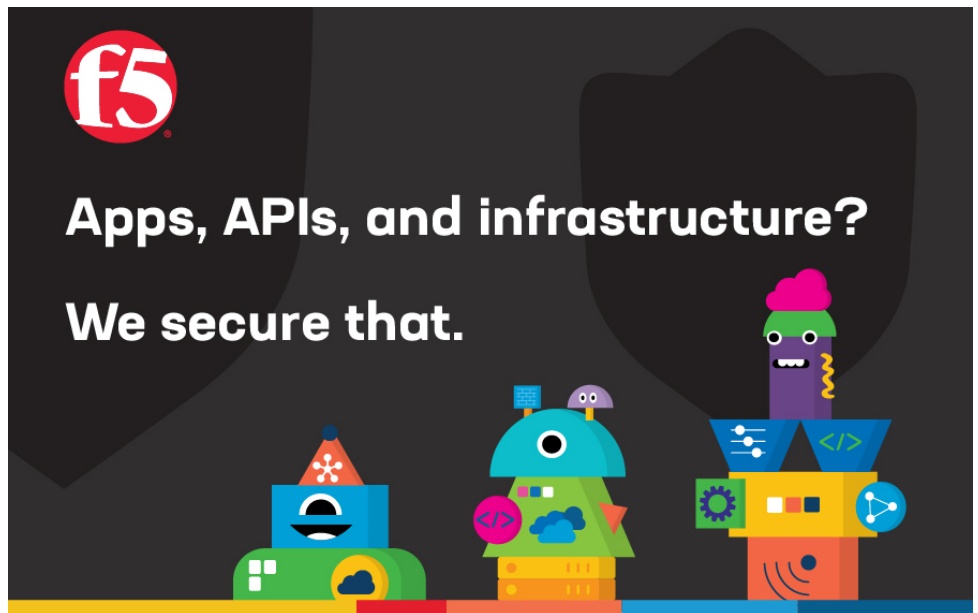
Rethinking app architecture

As apps become more fragmented and distributed across different environments, how can enterprises bridge the gap between legacy systems, on-premises deployments, and cloud-native applications? The solution lies in a rethink of app architecture and the implementation of a more structured approach through conceptual tiers focused on application orchestration, communication, security, and management.

- **Global Site Shared Services Tier:** Centralise app orchestration, secure web apps and APIs, and deliver high-performance connectivity.
- **Site Shared Services Tier:** Ensure secure app-to-app communication, support traditional and modern apps, and monitor system health.
- **App Services Tier:** Protect app segmentations, address Kubernetes challenges, and fortify against lateral movement vulnerabilities.
- **Management and Ops Tier:** Cohesive force that connects all tiers with automation, adopts Infrastructure as Code, and delivers rapid, reliable app deployment.

A well-structured framework not only facilitates scalability but enables the dynamic allocation of additional resources as required. For instance, an organisation could deploy more server instances during periods of high user activity, and conversely, optimise cost-efficiency by removing unnecessary resources during periods of low demand.

With a centralised management platform, enterprises can consolidate app orchestration across multiple sites. It also gives a unified perspective of workloads and applications for real-time performance monitoring, enabling application teams to promptly identify underperforming clusters and enact automated processes and scripts to proactively address performance issues.



A foundation for holistic apps with API security and delivery

Building on a distributed cloud platform using a structured approach is key to achieving true application portability, resilience, and security. This gives enterprises more flexibility in delivering any type of application in any environment, while also putting them in a better position to negotiate prices with public cloud providers.

The responsibility lies with enterprises to regain control over their application architecture. This starts with a thorough understanding of their current infrastructure and identifying commonalities across their existing applications. By leveraging the four tiers mentioned earlier and ensuring alignment across the organisation, CIOs can create a robust foundation for even the most complex deployments.

In addition to these benefits, adopting a unified approach to application architecture enables organisations to streamline their development processes, reduce time to market for new features and services, and holistically secure their apps and APIs with Zero-trust security. WAAP (Web App and API Protection) and Anti-Abuse for distributed apps and APIs can be easily implemented through a consistent configuration and operational model, fortifying defences against web/API attacks and ensuring overall robust protection.

As organisations transit from traditional virtual machines (VMs) to Kubernetes-based environments, this structured app architectural approach can also ensure app segments are properly safeguarded. Dedicated API gateways and DevSecOps microgateways can be deployed at service endpoints that are containerised or in traditional VMs, strengthening security

for app segmentations in Kubernetes environments and fortifying the overall security within Kubernetes clusters.

Securing what matters with F5 Distributed Cloud Services

The F5 Distributed Cloud Platform offers a common platform that unifies the cloud, data centre, and edge to connect, protect, and run apps anywhere. The result is a unified solution for managing infrastructure and workloads across diverse environments while ensuring consistent policy enforcement and seamless integration with existing systems.

CIOs and CISOs are freed from the burden of having to deploy, integrate, and secure disparate technologies so that they work together. Crucially, integrated security capabilities which range from DDoS protection, network and web app firewalls, and static and dynamic API security, keep threats from reaching applications.

Ultimately, a modern app architecture helps enterprises navigate the complexities of today's multi-cloud and hybrid cloud landscape. This allows businesses to optimise performance, scalability, and security, delivering exceptional user experiences and driving digital success.

F5 is exhibiting at GovWare 2023, Asia's premier cybersecurity event. To learn more about F5 and how we can help you in securing, simplifying, and innovating your applications, visit us at our GovWare booth or visit our Distributed Cloud Services solution page [here](#).

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

Smoothing the Intersection of Cybersecurity and Innovation

“CISOs cannot be the only [party] responsible for security,” said [Stéphane Duguin](#), the CEO of the CyberPeace Institute.

As the digital world rapidly evolves, CISOs around the world face the tough challenge of defending their organisations from a constantly expanding range of cyber threats. So how should CISOs balance forging ahead with innovation and maintaining security?

Duguin was univocal that cybersecurity should be a collective responsibility. In his view, the desire to innovate is all good and well. But why must the ball invariably end up in the CISO’s court?

The same side of the fence: Innovation and cyber security

“To disrupt and innovate is fine. However, it needs to be clearly understood by each and every manager that cybersecurity issues can potentially arise from new initiatives. This should be on every one of their performance evaluations – no one should get a bonus or a raise if they are not meeting their cybersecurity KPIs,” he said.

“CISOs are too often the end of the chain; tons of decisions are often made without the CISO. And at the end of the day, someone simply goes to the CISO and says: ‘Oh, can you secure this by the way?’”

Early involvement in a project is vital, says [Alexander Antukh](#), the CISO of AboitizPower. He notes that supporting digital innovation without sacrificing security starts with early involvement in projects to integrate “Security by Design” principles, ensuring that security initiatives are aligned directly with business goals.

“CISOs must understand the systemic nature of digital risk and contextualise innovation within this landscape. Regular communication between security and innovation teams ensures that both agendas progress cohesively, minimising vulnerabilities while maximising business value,” he said.

“CISOs are too often the end of the chain; tons of decisions are often made without the CISO.”

– Stéphane Duguin, CEO, CyberPeace Institute



CISOs should also focus on business outcomes: “The key to communicating this delicate balance is to use the language of business outcomes. Instead of detailing technical risks or security measures, CISOs need to focus on financial metrics such as potential impact – revenue loss, brand damage, and regulatory penalties.”

Risk or compliance?

Should CISO adopt a risk-based approach or compliance approach? Is there a middle ground?

“If you just want to be compliant, I will say that I don’t think this works. Because just being compliant [alone] is going to put you behind the curve,” observed Duguin.

On that front, Duguin cautioned that the regulatory environment is changing very quickly, citing new regulations such as the Cyber Resilience Act which came into effect last year and the Digital Services Act in August.

“And that is just in Europe. Multiply this by the number of different regulations that are popping out left and right around the world – for CISOs operating in global companies, it’s already a legal headache,” he said.

What would a risk-based approach look like? “The first question that we need to ask is, who wants to target me? What would be the intent? And then what kind of capabilities do they have? Knowing this makes it easier to design your defences and more importantly, to prioritise, because you cannot defend everything at the same time.”

“Cyber security is an operational field, so it’s better to start with risk. Start with a flat landscape analysis to identify measures, and then to investigate whether these measures will enforce compliance. Is there something missing? If that’s the case, work to address that,” summed up Duguin.

“While both risk-based and compliance approaches have merits, a risk-centric strategy offers a dynamic framework

that adapts to evolving threats. In this view, compliance failures are treated as yet another category of risk, potentially leading to financial and reputational losses,” said Antukh.

“This approach, along with robust risk quantification processes, allows [us] to consolidate the message and appeal to the executive audience. With that said, once the risk of non-compliance is deemed unacceptable, it is certainly possible to use compliance requirements as a baseline.”

Preparing for the future

When it comes to preparing for the road ahead, Antukh recommends adopting a multi-faceted approach to upskilling. This means formal training, workshops, and real-world exercises, as well as fostering a culture of learning and curiosity in the team.

“CISOs should encourage team members to attain certifications, connect with their peers and participate in industry events, organise learning sessions within the company, and, if possible, contribute to open-source projects,” he said.

For Duguin, the key is creating an environment where failing is not a name-and-shame game and ensuring diversity in cyber security teams.

“Everyone in cybersecurity fails. Everyone is going to make a mistake. The whole point is to empower people to feel safe, that they can admit that they failed and learn from their mistakes. And then you can improve your security as fast as possible.”

“Think also about diversity, including gender. You don’t end up leading a team of guys all from the same part of the planet. Because in front of you, you have a very diverse crowd of attackers – it takes a very diverse brain to engineer a response.”

Join Alexander Antukh at his upcoming panel session titled “Artificial Intelligence: Friend, Foe or a Bit of Both for Cybersecurity” on 17 October at 4:00pm.

Stephane Duguin will be moderating the panel discussion “How can Collaborative Partnerships Forge Impactful Synergies in Cybersecurity?” on 17 October at 4:00pm as well.

Flip over to the Conference Programme page to check out today’s agenda!

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	 Menlo 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

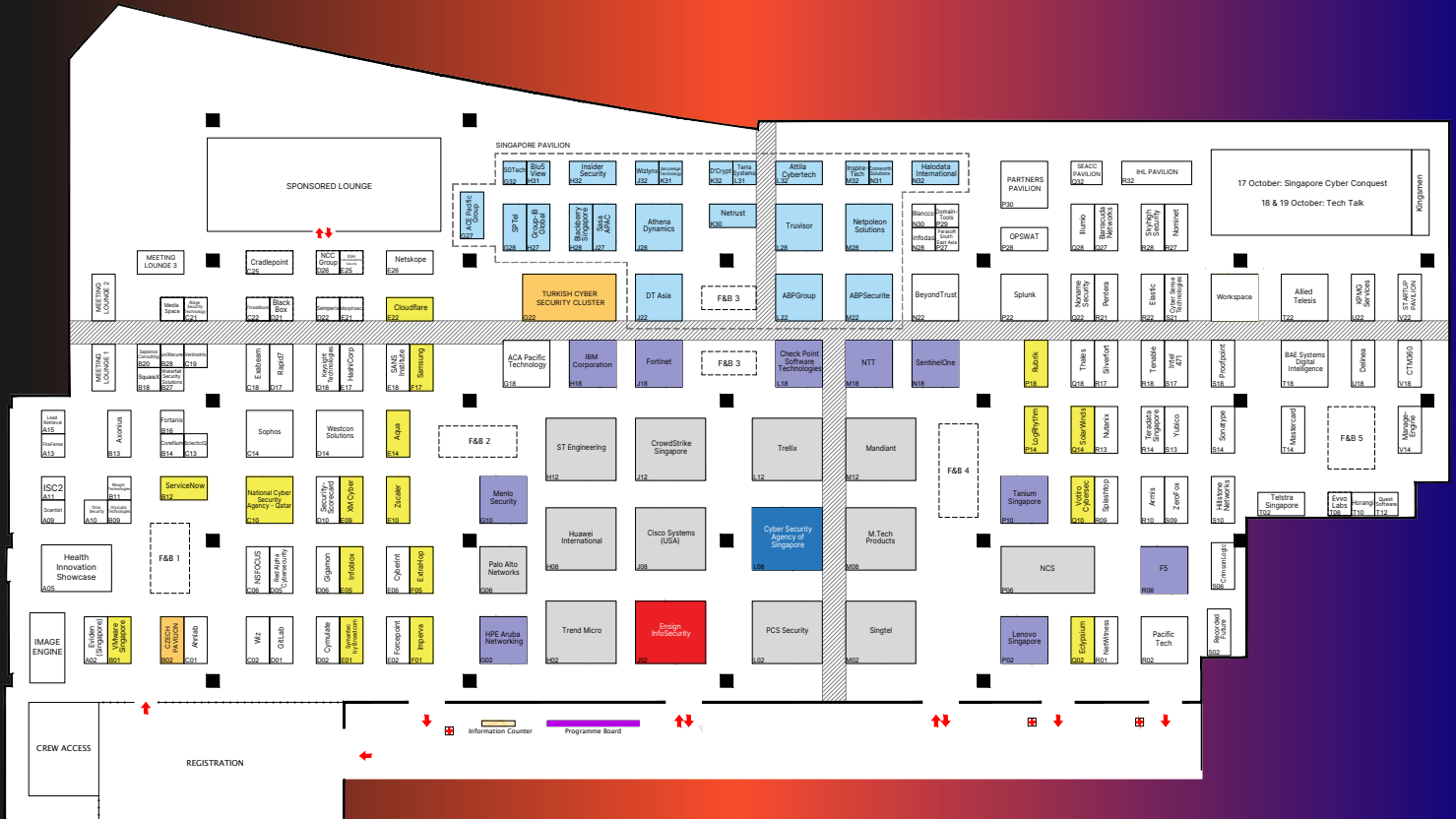
8:15am – 5:15pm	Cyber Secure Singapore 2023		
9:00am – 6:00pm	DFRWS APAC 2023 (Conference)		
9:00am – 10:30am	GovWare Keynote Sessions		
9:50am – 10:30am	Tech Talk Sessions		
10:30am – 11:00am	Tea Break		
11:00am – 1:00pm	CLOUDSEC @GovWare 2023		
11:00am – 1:00pm	Tech Talk Sessions		
1:00pm – 2:00pm	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

17 OCTOBER 2023

1:00pm – 1:10pm	GovWare Opening Remarks Ian Monteiro Executive Director <i>Image Engine</i>		
1:10pm – 1:55pm	Keynote Panel: Balance and Realities in Forging Digital Trust for Critical Infrastructure Moderator: Ian Monteiro Executive Director <i>Image Engine</i>		
	Paul Lek Executive Director, Business Information Security Officer (Japan, China and APAC), Singapore Tech Center <i>MSD</i>	Leonard Ong Director, Cyber Defense Group - Policy, Risk Management & Capability Development <i>Synapse</i>	Clar Rosso Chief Executive Officer <i>ISC2</i>
	Yong Yih Ming Chief Executive Officer <i>Mount Elizabeth Hospital</i>		
	Track I: Developments in the Zero Trust Environment	Track II: Cybersecurity Ops Centre	Track III: Recent Developments in ML/AI Engines
2:00pm – 2:30pm	Building Trust in the Digital Infrastructure Supply Chain is Paramount Dr Yuriy Bulygin Chief Executive Officer and Co-Founder <i>Eclipsium</i>	Distributed Security Monitoring With an Open NDR Architecture - Experiences from Finland Sami Petajasoja Chief Executive Officer <i>SensorFleet</i>	CISO-GPT: Leveraging AI to Augment Corporate Security Posture Kunal Anand Chief Information Security Officer & Chief Technology Officer <i>Imperva</i>
2:30pm – 3:00pm	Moving Towards Zero Trust Architecture in an Era of Change & Uncertainty David Chow Chief Technology Strategy Officer <i>Trend Micro</i>	Building a Sustainable and Scalable SecOps With Agile Engineering Johnny Kho Director, Managed SecOps <i>Singtel</i>	Evolving Modern Tradecraft: How ChatGPT and Analogous AI Engines are Leveraged in Nation State and eCrime Cyber Attacks Scott Jarkoff Director, Intelligence Strategy, APJ & EMEA <i>CrowdStrike</i>
3:00pm – 3:30pm	The Emperor has No Clothes: Why So Many Organisations Aren't Really Doing Zero Trust When They Say They Are Ian Farquhar Security Chief Technology Officer <i>Gigamon</i>	How to Build a World-Class Enterprise Cyber Intelligence Program Cody Barrow Chief Strategy Officer <i>EclecticIQ</i>	AI-Powered Risk Assessment Framework Prof. Yu Chien Siang Chief Innovation and Trust Officer <i>Amaris AI</i>
3:30pm – 4:00pm	Tea Break		
	Track I: How Can Collaborative Partnerships Forge Impactful Synergies in Cybersecurity?	Track II: Endpoint, Mobile & Network Security	Track III: Artificial Intelligence: Friend, Foe or a Bit of Both for Cybersecurity
4:00pm – 4:30pm	Moderator: Stephane Duguin Chief Executive Officer <i>CyberPeace Institute</i> Panellists: Chris Cruz Public Sector Chief Information Officer <i>Tanium</i>	Unraveling Network Observability: From Hype to Actionable Insights Taran Singh Vice President, Network Security Solutions <i>Keysight Technologies</i>	Moderator: Prof. Steven Wong Director, Centre of Digital Enablement (CoDE) <i>Singapore Institute of Technology</i> Panellists: Alexander Antukh Chief Information Security Officer <i>AboitizPower</i>
4:30pm – 5:00pm	Bart Hogeveen Head of Program: International Rules, Norms and Standards in Cyberspace & Capacity Building <i>Australian Strategic Policy Institute</i> Cynthia Lee Vice President, Sales, APJ <i>Cyberint</i>	Safeguarding Mobile Apps in the Wild: Exploring App Security, App Protection, and App Monitoring Priyesh Panchmatia Director, Solutions Consulting <i>i-Sprint Innovations</i>	Ilias Chantzos Global Privacy Officer <i>Broadcom</i> Asha Hemrajani Senior Fellow <i>Centre of Excellence for National Security, RSIS, NTU</i>
5:00pm – 5:30pm	Jeffery Tay Deputy Director, ICT Infrastructure & Cybersecurity <i>Nanyang Polytechnic</i> Juliette Wilcox CMG Cybersecurity Ambassador <i>UK Department for Business and Trade</i>	Automated Moving Target Defense (AMTD): The Evolution of Endpoint Security Michael Gorelik Chief Technological Officer and Head of Malware Research <i>Morphisec</i>	Ian Yip Founder and Chief Executive Officer <i>Averto</i>

Exhibition Floor Plan



Legend

 Cornerstone	 Platinum Plus
 Platinum	 Gold
 Exhibitor	 Singapore Pavilion
 Country 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



automate



Visit Booth D01

- Join us for a live demo!
- Enter the draw to win a Virtual Reality headset



build

secure

Software. Faster.



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