GovWare 2025
Conference and Exhibition

About GovWare Conference & Exhibition 2025

Cyberspace: Of Starbursts, Black Holes, and Last Frontiers

The environment defining tech has barely retained its footing amidst widespread and involuntary realignment and seems destined to continue roiling under a systemic barrage of disruptions. Cyberspace and cybersecurity are no strangers to innovation, adaptation, and great agility in an arena synonymous with advancement and progress over the last half century. Although cliched, the bare fact is that the pace of change over the last year is truly unprecedented, and seemingly a herald of a new normal.

There can be 3 broad categories from which these changes can be examined, namely – 1) within pureplay cybersecurity, 2) cybersecurity and the interplay with adjacent tech, notably AI, and 3) the social and real-world environment within which tech resides and serves. An added challenge is the interplay between these ecosystems is itself a complex and shifting dynamic.

GovWare 2025 will attempt to frame a conversation on topical issues given the above, with a thematic nod to the historical narrative of the primacy of science and the unknowns that science dissects and yet is limited by. The focus will remain on a cybersecurity core, with appropriate segues into the policy orientation of other discussions at the Singapore International Cyber Week (SICW).

The imagery of cyber and deep space is framed by the spectacular and spectacularly constant impact of explosive progress in AI and its associated effects on security, the perils and downsides of implosions and loss of control, and the reality of frontiers being just artificial structures or limits defined by current understanding and appetite for risk.

GovWare 2025
Conference and Exhibition

1) Pureplay Cybersecurity

I. A Relook of Identity and Data as Key Underpinnings of Cybersecurity
   a. *Are identity posture tools too static for current environments?*
   b. *NHI and HI vulnerabilities as organisational stacks evolve and scale*
   c. *Emergence and validity of identity attack surface management as a means of integrating access control, governance, and privilege management to improve visibility, posture, and protection mechanisms*

II. Agentic AI and Securing AI
   a. *Agentic functionality: historical development and the new generative landscape*
   b. *Security tooling and limitations in dedicated AI security*
      i. *Firewalls and SASE limitations for prompt injection and backdoor manipulation*
      ii. *WAFs and AI model misuse*
      iii. *Cloud access security that helps in detection but don't protect AI models*
      iv. *Constraints of DSPM tools on LLM leakage*
      v. *Fit / misfit of CNAPP / CSPM / EDR against adversarial AI inputs*
      vi. *Browser security postures functioning as UI control, but again not securing the underlying AI model*
      vii. *AI Security as a dedicated new domain?*
      viii. *Securing Model Context Protocol (MCP) against prompt injections*
      ix. *Is LLM Firewall the panacea to GenAI attacks and leakages?*
      x. *Regulatory landscape and standards for AI*

III. Zero Trust as Applied to the Converged AI / Digital Trust Landscape
   a. *Is ZT a viable objective given the rise of ephemeral data and agents?*
   b. *Prompt engineering, vibe constructs, and the emergence of model context protocol – layering ZT principles across heterogenous data sources and rapidly changing environments*

IV. Cloud Native Security / Cloud-Enabled Cybersecurity
V. Cyber Threat Landscape & Intelligence
VI. Cybersecurity Ops Centre: Methodologies & Operations
VII. Darkweb, Cybercrime, Cyberwarfare
VIII. Endpoint Security / Mobile Security / Network Security
IX. Incident Response, Investigations, Forensics, and Recovery in IT and OT Environments
X. Cybersecurity in OT Environments: Threats, Intelligence and Automation
XI. Security by Design: Risk Assessment, Avoidance and Mitigation
XII. Cybersecurity Risk Management / Risk-based Frameworks

2) Cybersecurity and the Interplay with Adjacent Tech

I. Data Security and the DPSM Matrix
II. Sec Ops and Cloud Native Convergence
III. Differentiation and Overlaps in AI and Cybersecurity Visibility
IV. Governance and Assurance in AI
V. Quantum Computing and its Impact on Trust and Security Infrastructure
VI. Recent Developments in ML / AI Engines
VII. Privacy, Trust, and Compliance in the Digital Economy
VIII. Cybersecurity and Digital Transformation
IX. Distributed Security in General and IoT Environments / Internet of Things
X. Cybersecurity and IT Resilience: Bridging Protection with Recovery
XI. Tech Convergence for Cyber Defence: AI, Quantum, and the Human Factor
XII. Cybersecurity in the Age of Industry 5.0
XIII. Navigating the Quantum Shift: Preparing for a Post-Quantum Era

3) Social and Real-World Environment

I. Consolidation in the Cybersecurity Market and the Ecosystem VS Best of Breed Approach
   a. *Trade-offs, challenges, and budget rationalisation*
   b. *Impact on GTM and runway for smaller scale players*
   c. *Channel, distribution, and partnership models*
   d. *Viability of sustained innovation and talent flow*

II. Geopolitics and the Weaponisation of Critical Infrastructure
   a. *CVE disruption as a recent example*

III. Concepts of Trust and the Spillover of General Ecosystem Dynamics into Cyber Specific Supply Chains
   a. *Integrating systems parallel to integrating business objectives*
   b. *Tech bifurcation realities in cross border deployment*

IV. Re-charting the CISO and Head of Security Footprint
   a. *Ongoing debate over skillsets, remit, and responsibilities*
   b. *The 'head of security' posture and conflation with leadership alignment on setting / achieving business objectives*
   c. *Who is responsible for risk, compliance, AI?*

V. Customer Protection by Design – Perspectives from Regulatory and Technical Engineering Viewpoint
VI. People, Partnerships and Culture: Building a Sustainable Cybersecurity Ecosystem
VII. Cybersecurity in Developing Economies and Underserved Communities