Digital Business
Building with Trust

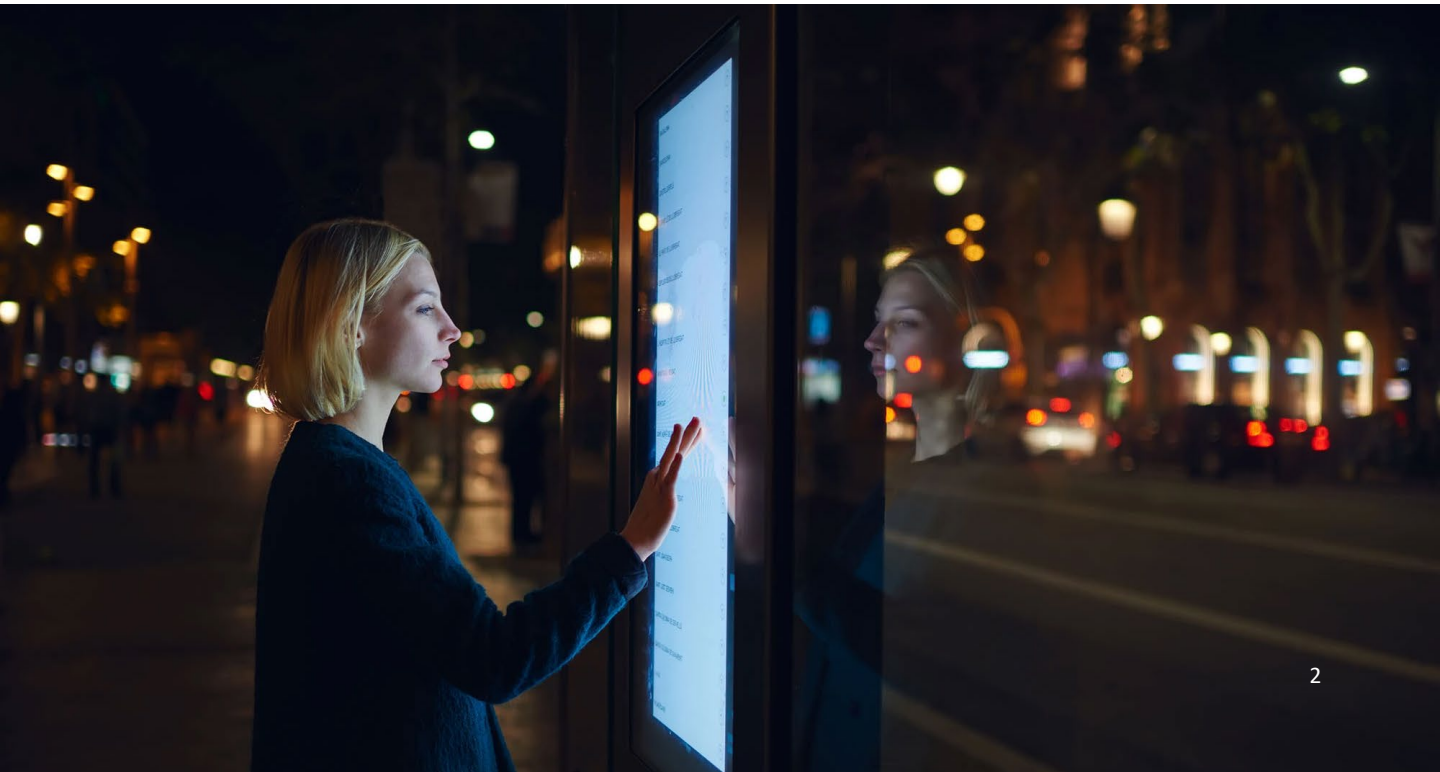
Digital Businesses

The shift towards digital-first business is fundamentally reinventing how organisations operate and deliver value. Businesses are looking at new operating models, lowering costs to serve, while identifying ways to better support customers across channels and employees with the right tools to be productive in their roles. Many businesses want to innovate at scale, expand into new markets, comply with regulations while supporting customers with an 'always on' mindset in a continuum of data collection for better insights, understanding current sentiments, identifying next-best actions, and creating value in session and context at the point of sale.

But there is also a realisation that businesses need to crawl or walk before they run. For most businesses, they will need to consider their digital infrastructure, especially the interrelationship between hybrid cloud, networking, and security to ensure it is secure, scalable, dynamic, and responsive to the needs of the market.

Distributed Workforces and Decentralised Applications

Many businesses, especially the high street, will continue to reduce the physical branch for operational efficiencies. This is being replaced with a broader digital presence, with a smattering of pop-up locations, kiosks and smart stores for industries that need physical touchpoints to serve customers. Many campus environments are also being downsized to accommodate a growing trend towards remote and hybrid working. Traditional office environments are being revamped with hot-desks, and collaboration rooms. Digitisation is inspiring new ways of working while reducing the physical office space (e.g., lower footprint, increase space utilisation). At the same time, core applications have by and large moved to multiple clouds.



As a result, perimeter-based security, typically an assortment of purpose-built appliances, is no longer suited for the needs of the modern workplace. More traffic is generated outside the traditional firewall in the corporate LAN; more employees transact directly from a branch (or remote location) to a cloud environment; the average organisation deploys five to ten major types of clouds; and many telecom providers, such as Telstra, have redesigned networks to include cloud on-ramps, specifically to support the decentralised and distributed work with highest possible performance thresholds.

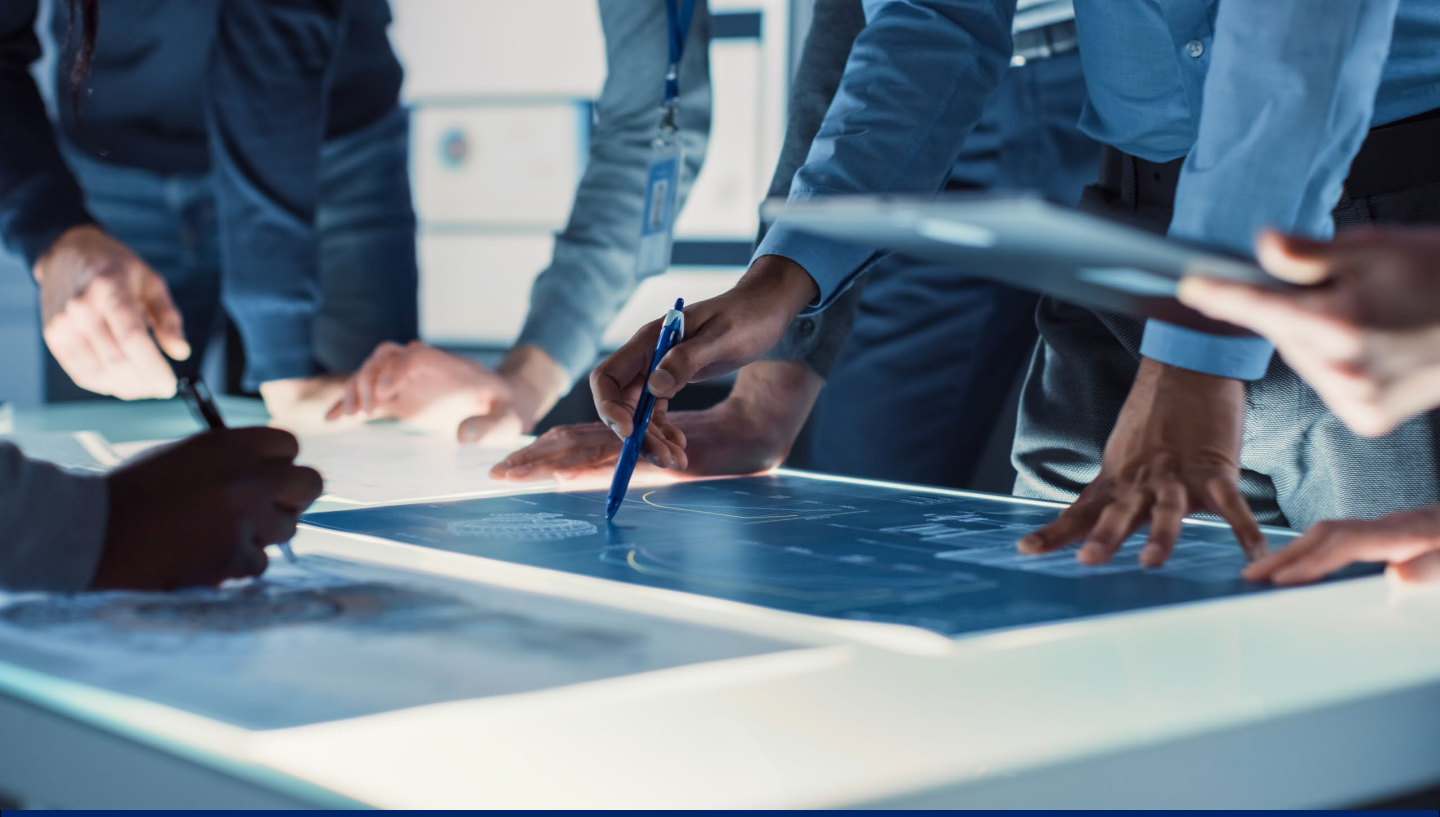
Zero Trust for the Workplace and Digital Ecosystems

These demographic shifts, highly likely permanent, require businesses in turn to update and harmonise their security strategy, including policy and processes, to the network, cloud, and workforce. Security strategy, 'never trust, always verify' is evolving to a data-driven approach of becoming policy-based, contextually aware, and policy-enforced. Trust is never assumed, but a concept continuously monitored for base lines (e.g., user identity, behaviour, location, time, etc.) with policy being adapted dynamically based on anomalies detected and associated risk levels. This type of approach is also important for securing vertical supply chains of customers, partners, and suppliers, often interconnected to drive operational efficiency, better control, and visibility. Zero Trust looks to elevate the security posture of the entire supply chain to create uniformity and prevent the possibility of 'island hopping' when an adversary looks to infiltrate a company with a weaker posture to focus on its primary target.

Digitalisation and its Dependencies

The digital economy is flourishing in many countries[1]. However, the success of any digital business is entirely dependent on its ability to manage the continuous threats of cyber-attacks. Each year, businesses face an unprecedented number of cyber-attacks, growing in volume, variety, and sophistication. Unfortunately, each year seems to set a record from the previous. This comes at a time when the attack surfaces increase, especially with the convergence of IT/OT and scaled deployments of IoT. Many other factors come into play such as geo-politics and the rise of state-assisted attacks, through to the weaponisation of AI to enhance the efficacy of existing threat vectors, such as ransomware and social engineering. Based on GlobalData's retail survey in March 2024, 64% of businesses were very concerned about privacy and data integrity risks from AI.

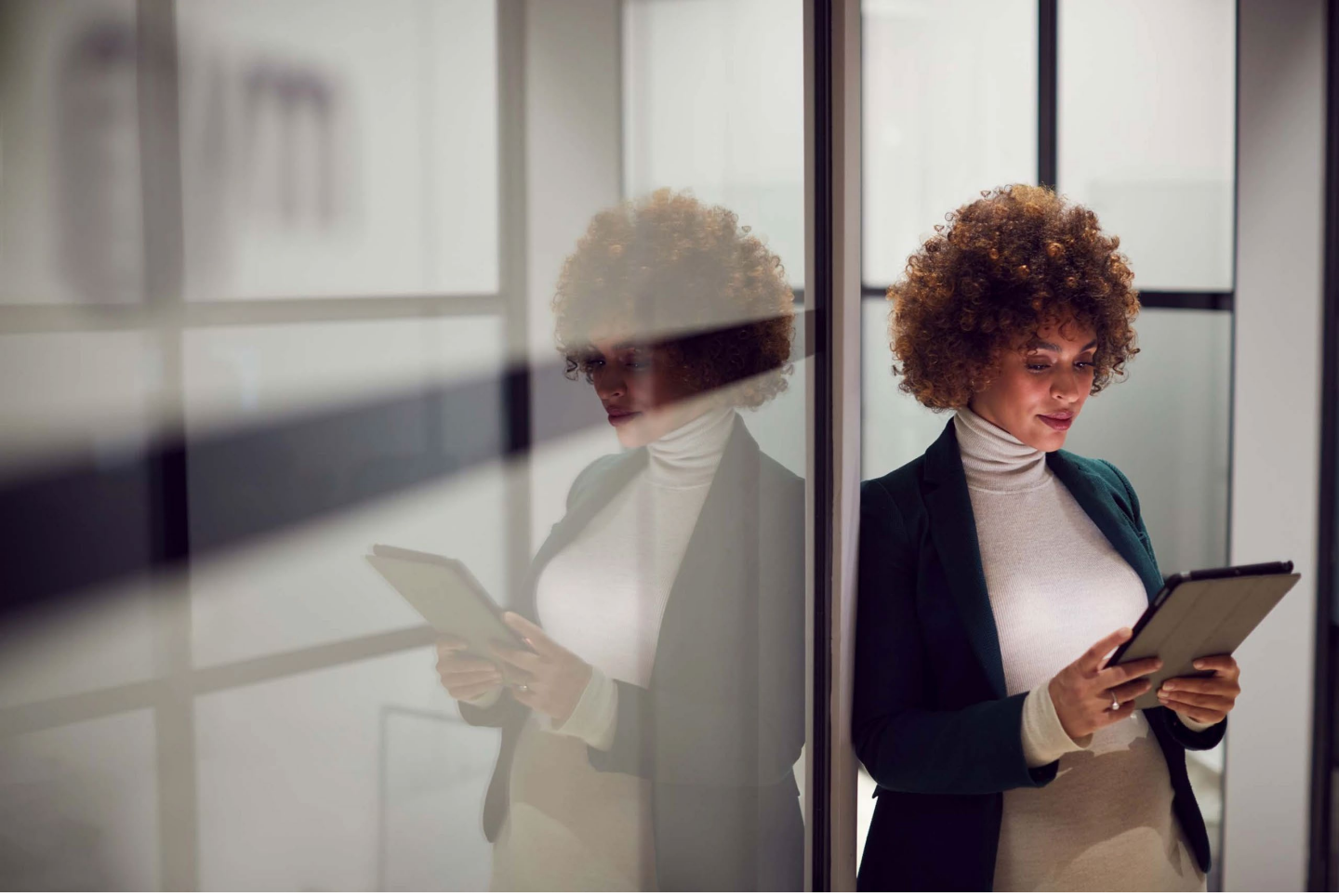
Protecting consumers and employees from the many dangers of cyber-attacks is a form of enterprise risk and threat management. The hyperconnected digital era drives a suite of technologies, typically deployed from the cloud and able to address various aspects to better secure digital infrastructure to secure people, objects, devices and data. There are a growing number of AI-enabled tools and platforms, such as SOAR (Security Orchestration Automation and Response), that play a critical role in helping triage trouble tickets, prioritise alerts, and automate responses (e.g., restrict access, isolate endpoint, force MFA). Threat and risk management increase response times, reduce false positives and often provide proactive threat intelligence to the analysts. They are also credited for providing a uniform security posture, better user experience, performance assurances (via local policy decisioning) and critically less complexity by reducing localised security appliances.



Recommendations

- **Balancing Data Management and Governance:** It is an imperative to protect customer data leveraging data protection methodologies such as Zero Trust approach and Identity Protection. Through effective data management such as reducing risk exposure and meeting compliance obligations (e.g., GDPR), data governance is also important for helping businesses to take an inventory of data assets, understand the value of data sets possessed to further monetisation. Organisations should look to protect and optimise the value of their data sets.
- **Outsourcing Security Operations:** Given the extreme shortages of security analysts, with the high costs for setting up and managing robust cyber defences, businesses should consider the case for outsourcing to third parties which embrace the new concepts like Zero Trust with an array of security vendors and infrastructure, such as SOCs, to scale.
- **Digital Trust is Constant:** In the hyperconnected digital era, security and digital trust is not a one-off investment, but needs to be updated regularly. It is important that architecture reviews, system and vulnerability scans, third-party audits and pen-testing are conducted at regular intervals. Given the fluidity of the market, it is critical to discover vulnerabilities and prioritise fixes continuously.

The IMDA estimates that the digital economy is worth S$106 billion or 17.3% of Singapore's GDP in 2022, up from S$58 billion or 13% of GDP in 2017 (latest figures).



The future of a hyperconnected digital business and AI era necessitates a foundation of digital trust. Delivering cutting-edge security solutions, Telstra International can help you stay ahead of evolving cyber threats, so your business remains resilient and continues to thrive.

For more information, please visit: https://www.telstrainternational.com/en/products/security

About GlobalData

GlobalData employs 3,500 developers, data scientists, analysts, award-winning journalists, editors and researchers, working in 23 offices worldwide and serving 4,500 clients in over 160 countries.

For more information, please visit: www.globaldata.com