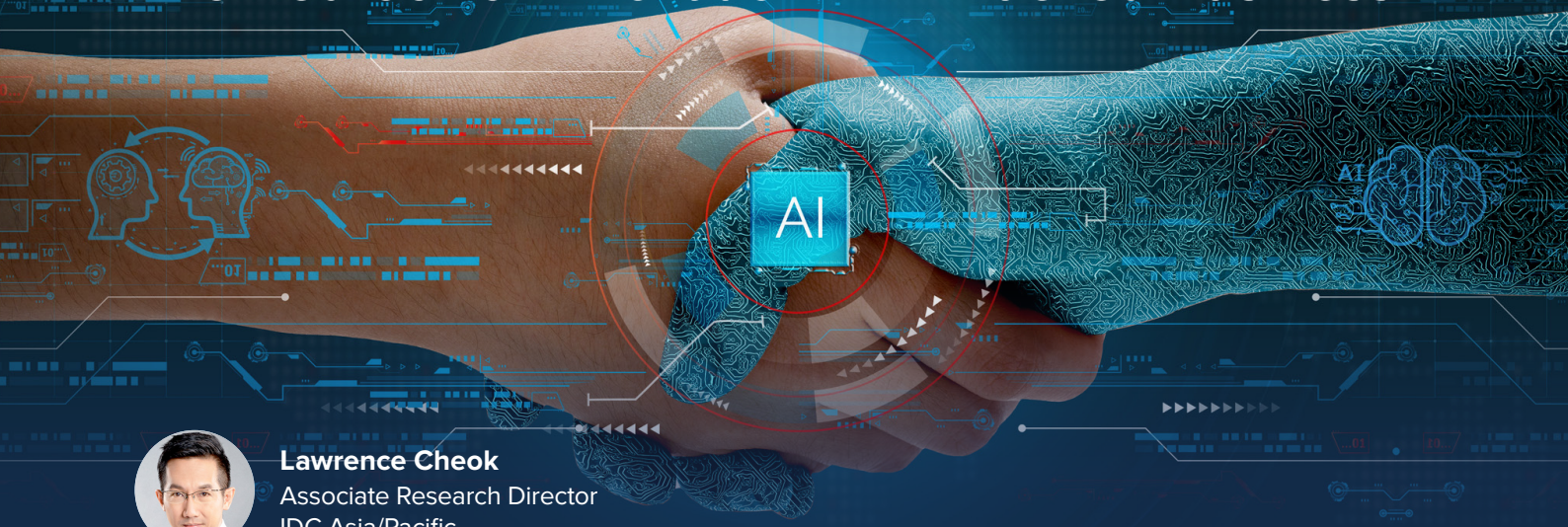
Analyst Brief, sponsored by Telstra
FEBRUARY 2025

Hyperconnected Digital Trust:
The Bedrock of Innovation in AI-Fuelled Business



Lawrence Cheok
Associate Research Director
IDC Asia/Pacific

The ability to continuously protect, improve, and respond against bad actors in an ever-evolving threat landscape is essential for AI-fuelled innovation to thrive. This report provides a perspective on digital trust in a hyperconnected world and recommends actions organisations must take for AI-fuelled businesses to thrive in this new era.

Digital Trust in the Future of AI and Digital Business

Digital trust is the cornerstone of resilient digital business models, ensuring secure, reliable, and ethical interactions within digital ecosystems. For CIOs and chief information security officers (CISOs), the mandate is to enable end-to-end security postures, processes, and controls to protect organisational and customer assets across a myriad of platforms residing both inside and outside corporate boundaries. This includes the use of data in motion and data at rest that feeds into artificial intelligence (AI) algorithms and models for AI-powered digital experiences for both employees and customers.

In 2025, IDC expects that Asia/Pacific will pivot from generative AI (GenAI) experimentation to AI at scale. This marks the transition to an era which is defined by a hyperconnected landscape of distributed workforces, decentralised application, external ecosystems, and increasing machine-to-machine and human-to-machine digital interactions that are fuelled by AI/ML algorithms and models. In 2025 and beyond, the ability for businesses to effectively construct, contextualise, and consume data in a secured and trusted manner will determine disruptors from those that are disrupted.

KEY STATS

- In 2025, 15% of organisations in APeJ will move from proof of concept (PoC) to production in specific generative AI (GenAI) use cases without a comprehensive risk-based assessment of their trust capabilities, thus creating a house of cards.
- According to IDC's *Digital Business and AI Survey*, 2024, 63% of Asia/Pacific enterprises lack readiness in their cybersecurity and compliance capabilities to take AI initiatives into production.

WHAT'S IMPORTANT

- Establishing a trusted digital foundation across data and digital infrastructure is essential for the success of AI initiatives as organisations begin to pivot beyond GenAI experiments and scale AI initiatives in production environments.
- AI plays a dual role in cybersecurity, enhancing threat detection and response while also requiring robust security measures to protect AI systems themselves from specific threats.

Hyperconnected Digital Trust: A Dynamic Framework for Hyperconnected Businesses

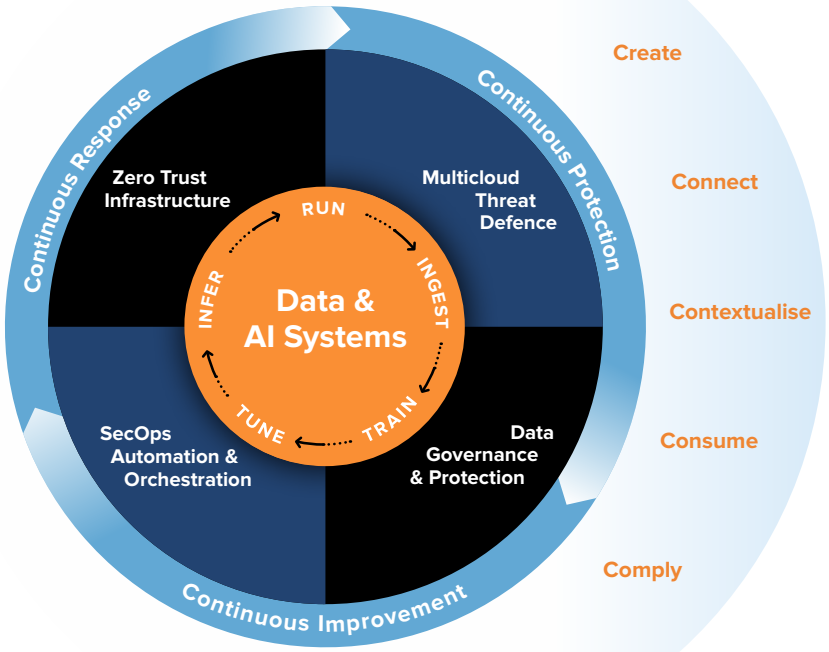
Digital trust is the confidence users and customers have in the ability of people, processes, and technology to create a secure digital environment. With the rapid proliferation of AI, including GenAI, the traditional concept of digital trust must evolve to meet the way data is leveraged across AI systems.

In the era of AI, data in motion and data at rest are continuously consumed by machines and algorithms that power digital products, services, and experiences. This dynamic nature has rendered traditional point solutions and passive threat responses inadequate for protecting data across the ever-expanding number of endpoints and platforms.

Conventional cybersecurity can no longer keep up with the fluidity of data in motion, the increasingly sophisticated threat landscape, and the growing number of interconnected systems that create, connect, contextualise, consume, and comply with data.

FIGURE 1

Enabling Trusted Data & AI Systems in Digital Products and Services



Source: IDC Digital Business Research, 2024

To address these challenges, organisations must evolve from static and isolated trust measures to Hyperconnected Digital Trust, a framework that integrates cybersecurity, privacy, transparency, and compliance across the entire digital ecosystem.

This approach focuses on continuous protection, continuous improvement, and continuous response — to enable end-to-end security postures, processes, and controls that continuously safeguard both organisational and customer data across a myriad of platforms, both inside and outside corporate boundaries, including AI-infused applications and AI-enabled endpoints and devices (Figure 1).

Evolving Risk Postures with Hyperconnected Digital Trust

In short, organisations must shift from reactive risk models to dynamic, proactive strategies encompassing the following:

- **Continuous protection**. Moves beyond static, point-in-time cybersecurity model to an always-on approach that continuously monitors and safeguards systems throughout every phase of data interaction — creating a dynamic defence rather than a reactive one.
- **Continuous improvement**. Traditional cybersecurity measures often rely on periodic updates, leaving organisations vulnerable to emerging threats. Hyperconnected digital trust incorporates real-time data-sharing and insights to adapt security and governance frameworks continuously, staying one step ahead of adversaries.

- **Continuous response**. Organisations can no longer afford to wait for security incidents to fully unfold before responding. With continuous response, organisations can detect, react to, and mitigate potential risks or breaches immediately — ensuring threats are contained without disrupting business operations.

Together, these three elements form a dynamic, proactive framework that ensures trust in digital and AI-driven ecosystems. As organisations increasingly rely on AI to create, connect, contextualise, consume, and comply with data, they must continuously monitor data, digital interactions, and transactions for threats, respond in real time, and build compliance transparency across all areas as shown in Table 1.

TABLE 1

Hyperconnected Digital Trust Measures Across the Data Life Cycle

Life-Cycle Stage	Continuous Protection	Continuous Improvement	Continuous Response
Create	• Ensures data integrity at the point of creation by securing and identifying AI-enabled endpoints.	• Uses AI-powered analytics to identify vulnerabilities in data sources and strengthen security protocols continuously.	• Detects suspicious or abnormal data creation patterns and initiates immediate remediation.
Connect	• Secures data as it moves across networks, hybrid/multicloud environments, and between stakeholders.	• Continuously adapts access policies based on real-time threat intelligence.	• Automatically restricts access or reroutes data to avoid compromised connections.
Contextualise	• Ensures data, including synthetic/generated data, is classified and secured based on context and sensitivity.	• Improves real-time data classification accuracy, ensuring appropriate security for each type of data.	• Ensures real-time adjustments to contextual classification, preventing potential breaches.
Consume	• Ensures the consumption of accurate, validated, and secure data by AI models and users.	• Improves data privacy protocols to better safeguard sensitive information in business decisions.	• Detects anomalies in data consumption and initiates immediate response to mitigate risks.
Comply	• Ensures compliance with global privacy, security, and data protection laws throughout the entire data life cycle.	• Enhances governance and reporting tools to maintain transparency and regulatory adherence.	• Detects and corrects non-compliance incidents before they escalate into larger legal or reputational risks.

Source: IDC Measuring Future IT & IDC Digital Business Research, 2024

Developing Hyperconnected Trust for AI Innovation

Hyperconnected digital trust is increasingly the bedrock of successful digital businesses. In an era where AI and machine learning underpin key business processes, trusted data is vital to ensuring the effectiveness of AI-driven decision-making and AI-orchestrated processes.

By developing a framework based on hyperconnected digital trust, organisations can ensure that AI-driven customer interactions and operational processes are secure, compliant, and resilient.

The principles of continuous protection, improvement, and response must be applied across areas comprising zero trust infrastructure, multicloud threat defence, data governance, and operational automation and orchestration as follows:

- **Zero trust infrastructure**: In a hyperconnected world, every digital entity, from AI-powered systems to human users, is a potential security risk. CIOs and CISOs must adopt a zero trust architecture that continually verifies identities and authorisations, ensuring secure access to critical data and systems at all times.

- **Multicloud threat defence**: AI/MLOps leverage multisourced data streams that cut across multi/hybrid cloud environments, making traditional perimeter-based security measures obsolete. Multicloud defence takes a holistic approach encompassing security across clouds, networks, and applications, and identity and access management to ensure a resilient and secure data stack.

- **Data governance and protection**: Digital businesses traverse organisational and national boundaries and must be transparent to comply with a myriad of evolving data and AI legislations. Safeguarding data in its entirety, respecting privacy, and ensuring compliance bolster trust that underlies ecosystem engagements and AI initiatives.

- **Automation and orchestration**: The fast-expanding attack surface and emergence of new threat vectors make automated security operations essential for handling uncategorised, disparate, and duplicated alerts to reduce alert fatigue. By orchestrating automated responses to known threat vectors, businesses can respond in real time, scale their security operations, and focus security experts in investigating high-priority anomalies and new emerging threats.

To guide the development of hyperconnected digital trust, CIOs and CISOs should leverage key performance indicators (KPIs) that measure both operational effectiveness and business impact. Table 2 shows examples of KPIs organisations can use to assess their progress in building a trust-driven digital foundation.

TABLE 2

Sample KPIs for Developing the Hyperconnected Digital Trust

Pillar	Business KPIs	Operational KPIs
Zero trust infrastructure	● Reduction in security breaches resulting from unauthorised access. ● Improvement in audit compliance rates for access control policies. ● Reduction in downtime due to security incidents involving unauthorised users.	● Number of unauthorised access attempts blocked. ● User authentication success rate (e.g., multifactor authentication [MFA]). ● Time to revoke access upon detection of unauthorised access.
Multicloud threat defence	● Reduction in data breaches across cloud environments. ● Business continuity through better cloud security. ● Improvement in regulatory compliance across cloud platforms.	● Time to detect and respond to multicloud security threats. ● Percentage of encrypted data across cloud environments. ● Decrease in security misconfigurations across cloud infrastructure.
Data governance and protection	● Increase in customer trust index (as measured by customer survey and feedback). ● Decrease in data-related compliance fines and legal penalties. ● Improvement in data quality driven by effective governance.	● Data classification accuracy, percentage of data classified correctly by sensitivity and compliance. ● Data encryption coverage, percentage of sensitive data encrypted both in motion and at rest. ● Time taken to detect and address data governance-related issues.
Automation, orchestration, and response	● Reduction in response times for security incidents. ● Increase in operational efficiency by automating routine tasks. ● Improvement in incident management outcomes.	● Percentage of security incidents managed automatically. ● Mean time to resolve incidents using automated workflows. ● Reduction in false positives detected by security automation systems.

Source: IDC Measuring Future IT (KPIs for Digital Infrastructure/IT Products and Services/Trusted and Secured Enterprise/Innovation and Intelligence)

Digital Trust: Laying the Trust Foundation for Innovation

Digital trust is critical for digital businesses, particularly in financial services where customer data, transactions, and digital interactions must be constantly monitored and protected for regulatory compliance. **GCash**, the leading fintech company in the Philippines, is setting a benchmark in the region with its comprehensive approach to digital trust and cybersecurity.

As a super app providing a broad range of financial services, GCash recognised that its rapid growth could be a double-edged sword, exposing the platform to more security threats as it scaled its operations. In response, GCash implemented a robust multilayered cybersecurity initiative to ensure that customer data and transactions are continuously protected.

GCash's cybersecurity programme focuses on strengthening security across three key areas:

- **Safeguarding customer data**. Implemented end-to-end encryption and advanced data masking techniques to ensure that sensitive customer information remains protected at all times, both at rest and in motion.
- **Securing transactions**. Integrated MFA and transaction monitoring tools to ensure that every transaction on the platform is authenticated and tracked in real time to prevent fraud and unauthorised access.
- **Zero trust platform infrastructure**. GCash fortified its platform infrastructure by deploying a zero trust architecture, continuously verifying all internal and external access requests, and applying strict access control policies to safeguard its digital ecosystem.

In addition, GCash leveraged advanced threat detection tools and integrated AI/ML-based anomaly detection to proactively identify potential risks.

The initiative also addresses broader ecosystem trust, particularly with the inclusion of trusted third-party services integrated into the GCash platform. By reinforcing secure application programming interfaces (APIs) and encryption protocols, GCash ensured that partners could contribute to the platform's ecosystem without exposing sensitive customer data to undue risk.

Collectively, these measures enabled GCash to achieve:

- **Improved trust and confidence**. The security enhancements led to a noticeable increase in user trust, driving higher adoption rates across GCash's financial products, including loans, insurance, and savings.

By 2029, 100% of the A2000[1] will mandate hardware enabled zero trust security in the infrastructure stack as a first line of defence against cyberattacks, increasing IT staff productivity by 5x.

Source: IDC FutureScape: Worldwide Future of Digital Infrastructure 2025 Predictions, APEJ Implications

[1]Asia/Pacific-based Top 2000 organisations

- **Proactive threat management**. With real-time threat detection and automated responses to potential breaches, GCash managed to significantly reduce downtime and prevent critical incidents before they escalated.
- **Ecosystem-wide security**. GCash's efforts extended beyond its platform to secure transactions and interactions with ecosystem partners, reinforcing trust throughout the entire digital financial ecosystem.

GCash's multilayered approach showcases the importance of continuously evolving cybersecurity strategies. By implementing real-time threat detection powered by AI, GCash was able to enhance both its internal security posture and build trust externally with partners and users, and in so doing, demonstrated how digital trust supports innovation and scalability for a digital business.

The Hyperconnected Digital Trust Is Essential for AI-Fuelled Businesses to Thrive

As organisations increasingly adopt AI technologies to drive business innovation, establishing and maintaining digital trust becomes not only a strategic priority but a foundational requirement. The trust users and stakeholders place in an organisation's data, processes, and systems fuels the success of AI-driven initiatives. Without a solid trust framework in place, AI innovations could expose organisations to greater risk and erode stakeholder confidence.

Hyperconnected digital trust focuses on continuously protecting, improving, and responding to threats in real time across complex ecosystems of interconnected systems, platforms, and data streams. In an environment where AI is both a tool for and a target of cyberthreats, businesses need to evolve beyond static security models. AI-fuelled businesses depend on reliable, transparent, and secure data flows, which can only be guaranteed through a trust fabric that spans across endpoints, networks, cloud environments, and external ecosystems.

This dynamic model of digital trust will be essential in the coming years as AI further integrates into critical business operations. By building robust trust capabilities, organisations will not only protect their data but will also enhance their ability to innovate responsibly, ensuring long-term resilience and competitiveness in the AI-driven era.

About the IDC Analyst

Lawrence Cheok
Associate Research Director

Lawrence is an Associate Research Director for IDC's Asia/Pacific Digital Business Strategies research programme. Based in Singapore, Lawrence provides advisory services to technology buyers and suppliers in this role, leveraging primary and secondary research to uncover emerging business and technology trends, the competitive landscape, and buyer adoption.

Message from the Sponsor

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.

Learn More

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.