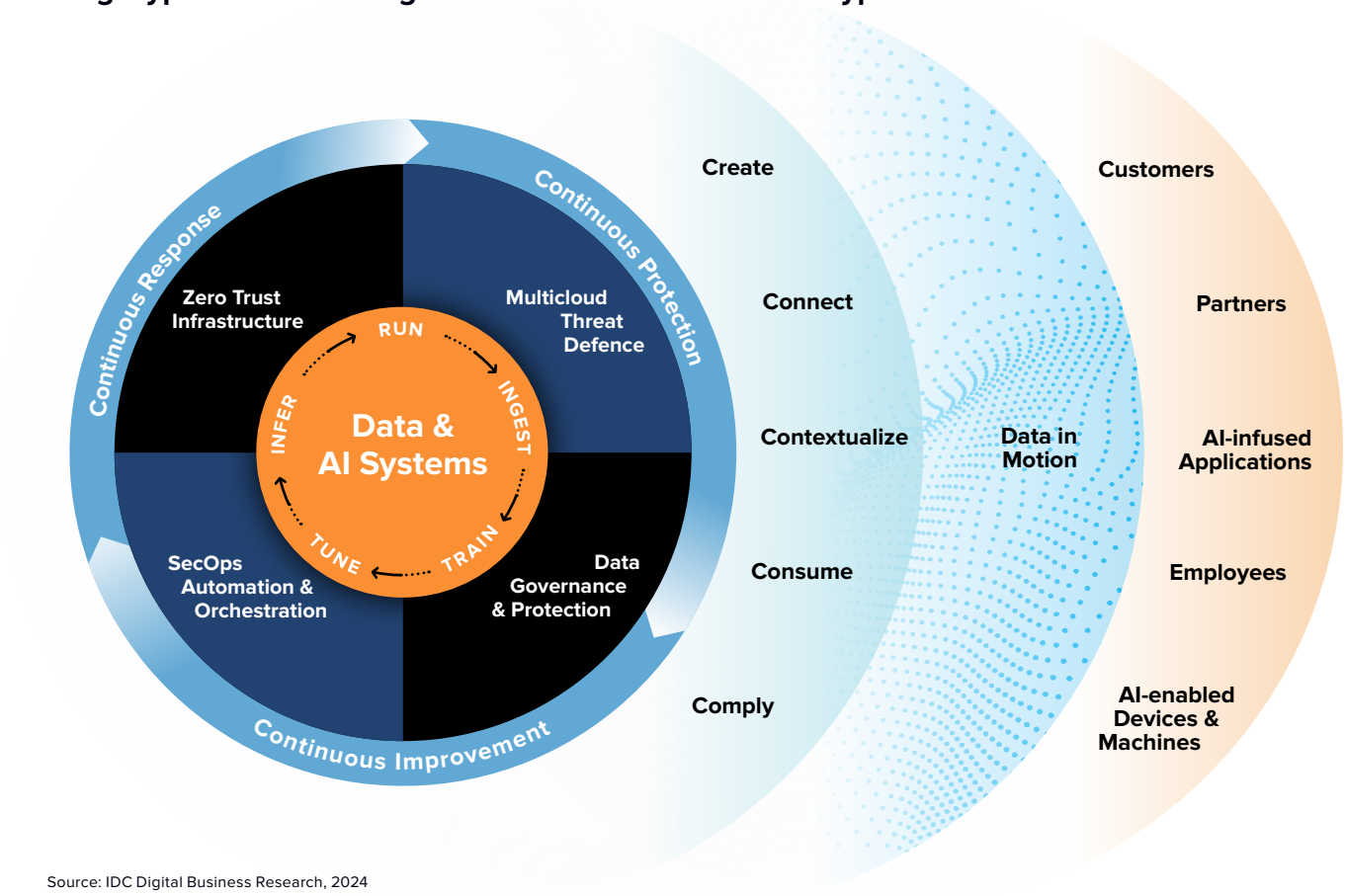
Hyperconnected Digital Trust

The Value Foundation for the Digital Business & AI Era

Lawrence Cheok
Associate Research Director
Digital Business Strategies, IDC Asia/Pacific

Linus Lai
Vice President
Digital Business, Trust and Services Research, IDC Asia/Pacific

Using Hyperconnected Digital Trust as the Bedrock for Hyperconnected Businesses



Source: IDC Digital Business Research, 2024

Digital Trust: The Currency Underpinning The Digital Economy with AI Everywhere

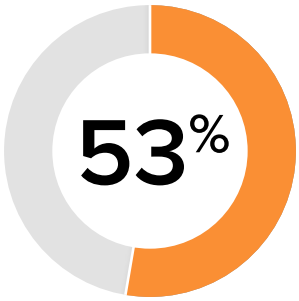
The digital economy and proliferation of AI are transforming the way enterprises do business, creating new ways of connecting with customers, and also uncovering new revenue streams. By 2025, 40% of Asia/Pacific (excluding Japan) organizations will be selling to, engaging with, or provisioning on-demand services through digital ecosystems to enable new business models powered by AI everywhere capabilities (source: IDC FutureScape: Worldwide Digital Business Strategies 2024 Prediction — APEJ Implications). As AI and digital business ecosystems become more intertwined, the essence of shared data across AI-infused applications and AI-orchestrated operations hinges on a singular foundational concept: digital trust. This invisible notion underpins digital transactions, customer interactions, and ecosystem activities as the cornerstone that ensures secured, reliable, and ethical use of data and AI, within and beyond the corporate walls.

Continue reading >

As AI proliferates, digital businesses are increasingly driven and enabled by AI algorithms, and data in motion is the lifeblood that supports value creation activities. The trusted movement of real-time or near real-time data across a complex web of entities to fine-tune and optimize AI models, automate actions, and deliver outcomes, is redefining how businesses create, connect, contextualize, consume, and comply with data:

- **Create**. Data is created by an ever-expanding source of applications, processes, interactions, sensors, and GenAI/AI models as part of their value creation activities. This includes known, unknown, and potentially malicious actors.
- **Connect**. Provide data-in-motion access through hyperconnectivity to employees, partners, customers, and AI-enabled devices and applications while limiting unauthorized access.
- **Contextualize**. Understand and classify the data in motion, including synthetic/generated data, within the conditions of its originating source and circumstances to apply appropriate trust policies within its context.
- **Consume**. Securely consume the data to act and drive business outcomes with full confidence in the data's veracity and efficacy. This includes the use of data for AI model fine-tuning or enhancing GenAI output accuracy using retrieval augmented generation (RAG).
- **Comply**. Using AI-powered data protection measures to ensure that privacy, security, and regulatory requirements are met as data can be created, stored, and computed in disparate locations because of its movement outside of organizations or across national borders.

As value creation continues to shift toward distributed real-time activities driven by AI and automation fueled by data in motion, so too must measures that underlie the trusted use of data.



53% of CEOs across the Asia/Pacific (including Japan) see cybersecurity technology as their top technology investment priority for 2024[1]

Enabling Trusted Data Use Through Continuous Protection, Improvement, and Response

The hyperconnected nature of digital business demands a renewed trust foundation. Prevailing measures of point solutions and passive threat responses can no longer keep pace with the fluidity of data in motion and the ever-evolving threat landscape.

Instead, trusted data use must be built upon continuous protection, response, and improvement measures that encompass the entirety of the digital network, AI systems, and ecosystem participants.

This includes the extension of trust to AI-infused applications and the data that feeds into AI algorithms. At the same time, organizations must embrace AI-enabled trust capabilities (e.g., AI for cybersecurity) to keep up with exponentially growing threat vectors.

Continue reading >

Introducing Hyperconnected Digital Trust

Hyperconnected digital trust is the holistic approach for digital businesses that encompasses cybersecurity, privacy, transparency, and adherence to relevant laws and standards across the entire digital ecosystem. To continuously survey data in motion for potential threats, respond in real time, and build compliance transparency, organizations must develop four digital trust capabilities:

- **Zero trust infrastructure**: Every digital entity, including AI-powered entities, whether inside or outside the organization, can be a potential security risk. Adopting a zero trust posture ensures that every access request across the data stack is continuously monitored, authenticated, authorized, and encrypted before being granted access.

- **Multicloud threat defense**: 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 organizational 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.

- **SecOps automation and orchestration**: The fast-expanding attack surface and emergence of new threat vectors make automated security operations essential for handling uncategorized, 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.

As the digital landscape continues to accelerate, hyperconnected digital trust becomes the bedrock of successful digital businesses in the AI era. Trusted data is central to harnessing GenAI/AI algorithms that underlie business transactions, customer interactions, and operational processes. Through continuous protection, improvement, and response capabilities comprising zero trust infrastructure, multicloud threat defense, data governance, and SecOps automation, businesses can fortify their trust foundation to unlock new value creation in the digital business and AI era.

By 2024, 25% of Asia Top 2000 companies will deploy GenAI on first-party data in their SOCs for detection and response to uplevel analysts while addressing hallucinations, bias, privacy, and reinforced learning concerns.

Source:IDC FutureScape: Worldwide Future of Trust 2024 Predictions — Asia/Pacific Excluding Japan Implications

Produced by: IDC Custom Solutions

Info Snapshot, sponsored by Telstra | July 2024 | IDC #AP249567X