

HITACHI



LATAM Partner Summit FY26

Built to Grow. Powered by Data.

The background of the slide is a vibrant, artistic illustration of a tropical beach. In the foreground, the sand is depicted with concentric, wavy lines in a rainbow of colors, transitioning from purple and blue on the left to red and orange on the right. The ocean waves are also rendered with similar rainbow-colored lines, creating a sense of movement and energy. The sky is a soft, pastel mix of pink, orange, and blue, suggesting a sunrise or sunset. A few palm trees are visible on the left and right edges of the frame, adding to the tropical atmosphere.

HITACHI

The Resilient Enterprise:

Protecting Brand Reputation, Revenue & Growth at the Board Level

Resiliency: Board-Level Risk Agenda

The risks that most threaten brand reputation, revenue and growth



Cyber & data breach



Third-party & supply chain



Technology & AI adoption



Business continuity



Regulatory & compliance



Data governance & privacy



Talent & key-person risk



Brand & reputation

How AI Is Changing Cyber Attacks

AI has moved from a drafting aid to an operator inside the attack chain – raising volume, speed and credibility all at once.

Shift	What the evidence shows	What it means for the board
AI is now in the attack	IBM: one in four breaches between March 2025 and February 2026 was AI-enabled, up 56% year over year	Assume AI involvement in the next incident and plan controls accordingly
Identity is no longer proof	Gartner: 62% of organisations report a deepfake incident; documented global deepfake fraud losses exceed US\$3.7B, almost all since 2025	Payment and access approvals need verification that a cloned voice or face cannot pass
Phishing at machine scale	Phishing remains the top initial access vector; median time from email to click is 21 seconds, against 28 minutes to report	Detection and response speed matters more than awareness training alone
Autonomous intrusion has arrived	Anthropic disclosed a state-sponsored group using AI agents to run 80–90% of intrusion tradecraft against ~30 organisations	Attack tempo now outpaces manual defence; automation is required on both sides
Ransomware has industrialised	Publicly listed ransomware victims rose 213% year over year in Q1 2025, with most attacks never reported	Resilience and tested recovery, not prevention alone, determine the loss

The Impact Is Financial, Political & Real

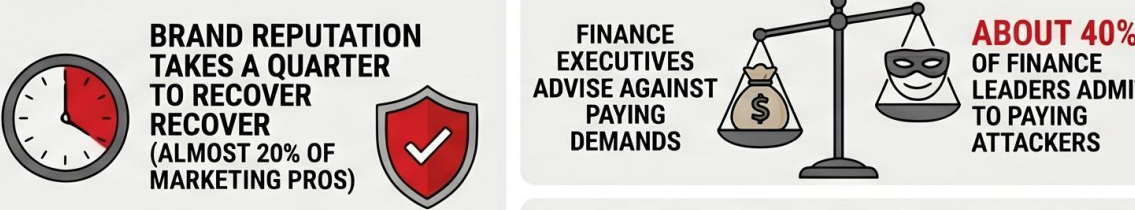
GLOBAL COST



COSTS INCREASES SINCE 2024



CHALLENGES & PERCEPTIONS



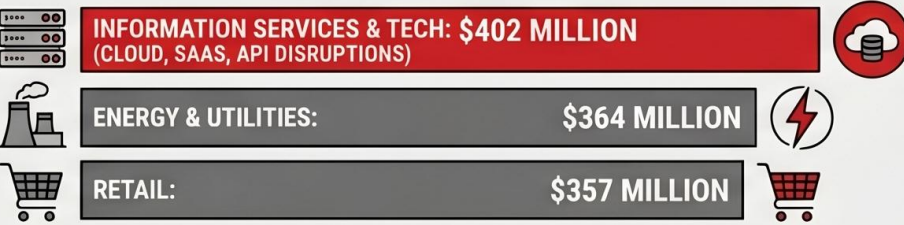
CHALLENGE & PERCEPTIONS



INVESTOR CONCERNS ON RESILIENCE



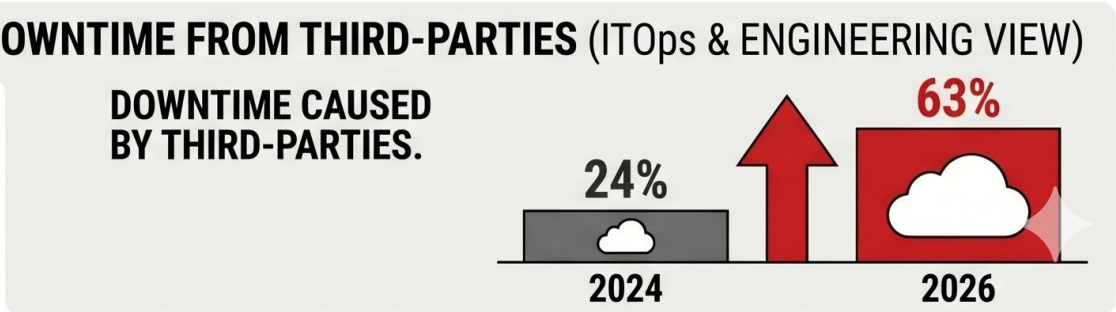
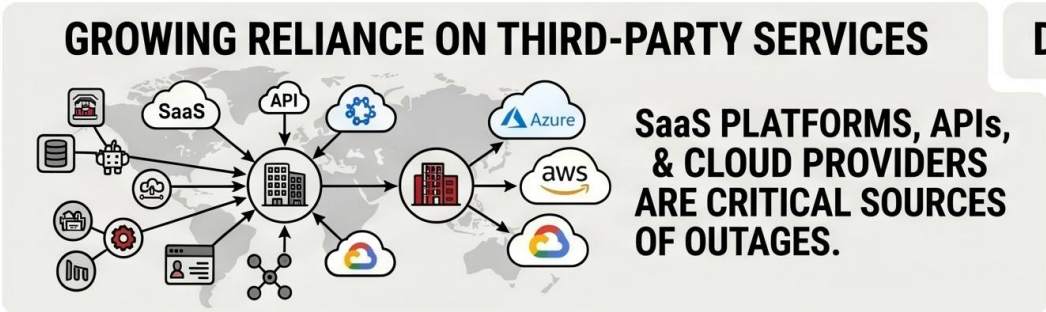
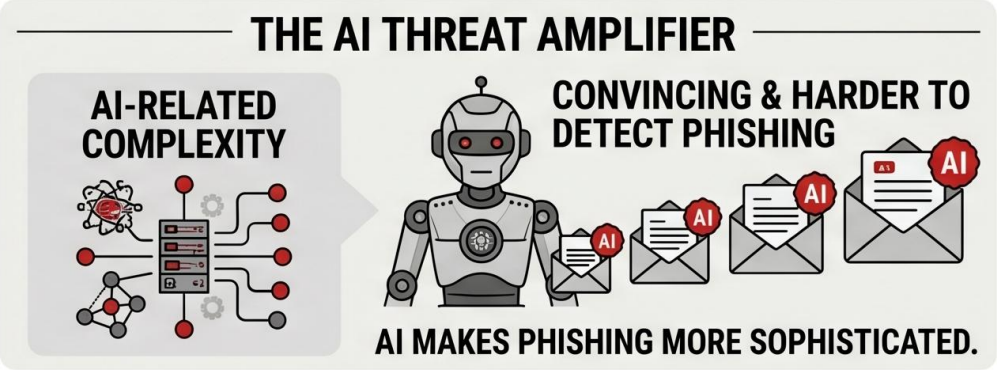
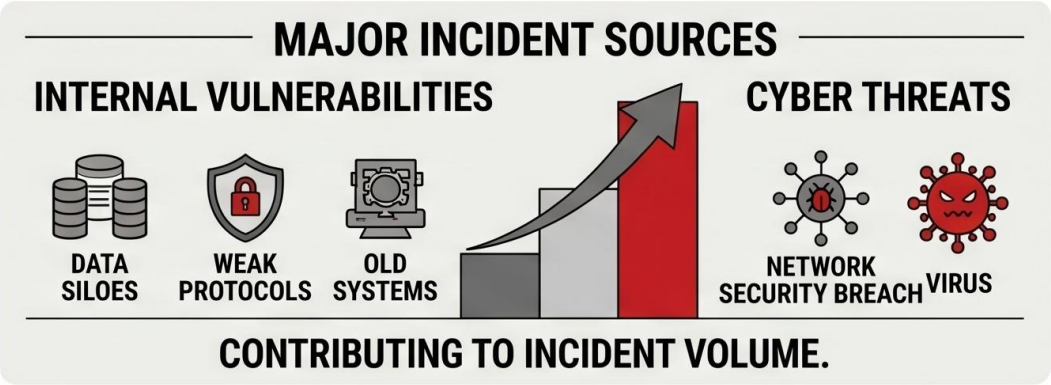
INDUSTRY COST BREAKDOWN (HIGHEST DOWNTIME COSTS)

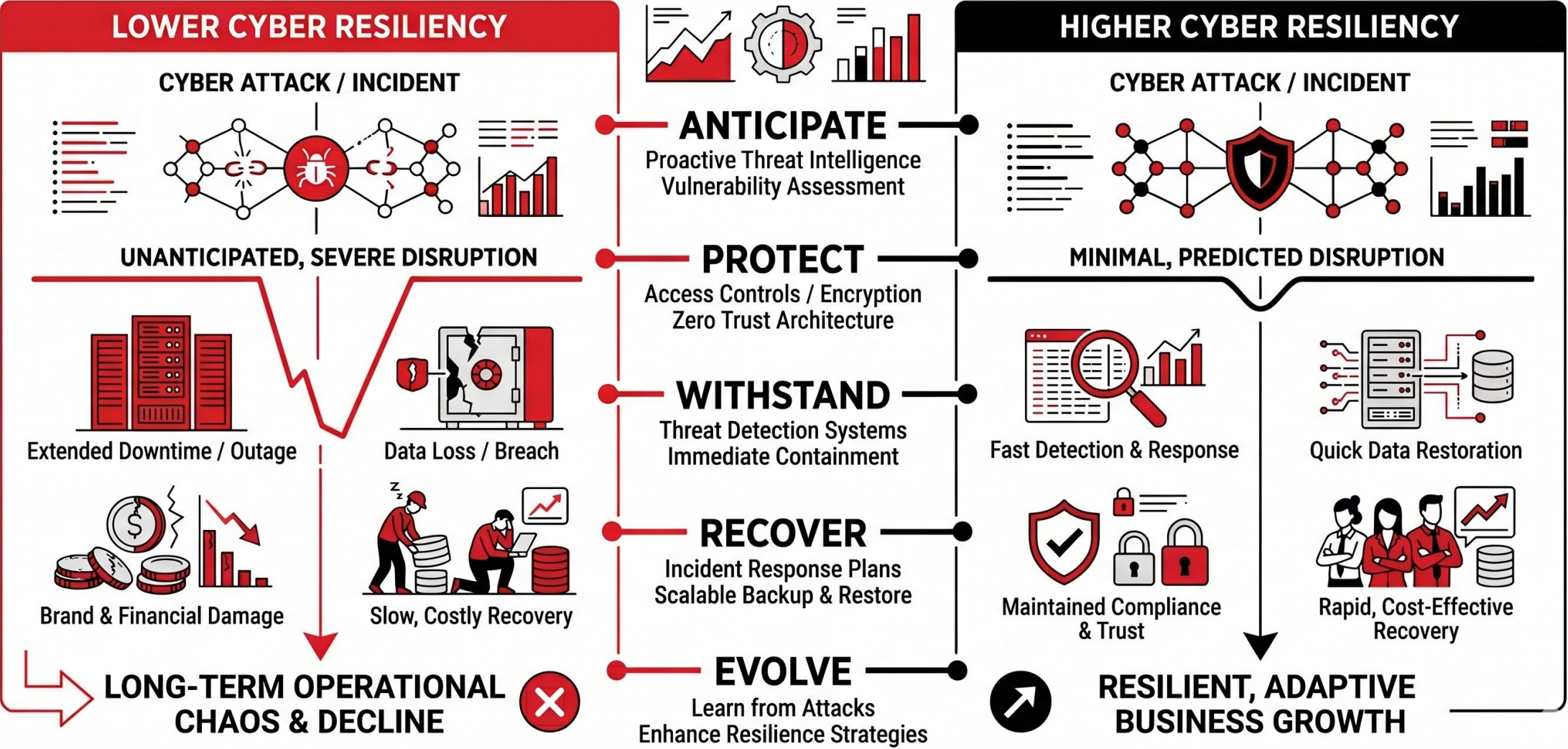


REGIONAL COST DRIVERS



Splunk's The Hidden Costs of Downtime





Case Study: The C&M Software Pix Attack

Brazil, 30 June 2025 – a third-party payments provider was breached through a single insider, and the losses landed on the banks that depended on it.

Dimension	What happened and what it cost
Entry point	Attackers paid a C&M IT operator roughly US\$2,760 for his corporate credentials, then used his help to bypass security controls
Financial	About R\$800 million (roughly US\$140 million) drained from the reserve accounts of six institutions in under three hours; only ~R\$270 million was later frozen
Operational	Brazil's Central Bank suspended all institutional access to C&M's platform during the investigation, cutting the provider off from its customers
Reputational	Reported as the largest digital heist in Brazil's history, triggering arrests, criminal investigation and regulator scrutiny of third-party providers
Board lesson	Cyber, third-party and continuity risk are one connected exposure – a vendor's insider control gap became the banks' loss

Case Study: The IFX Networks Outage

Colombia, September 2023 – ransomware at a single regional hosting provider took hundreds of organisations offline across four countries.

Dimension	What happened and what it cost
The target	IFX Networks, a Bogotá-based cloud and telecom provider serving clients in 17 countries; ransomware encrypted its virtual machines on 12 September 2023
Blast radius	762 public and private organisations disrupted across Colombia, Chile, Panama and Argentina – none of them breached themselves
Operational impact	At least 30 Colombian government sites down, including the justice, health and culture ministries, hospitals and the judicial branch
Recovery	Colombia stood up an emergency national cyber command post; roughly 90% of clients were restored after about ten days
Board lesson	Concentration risk is real – your continuity plan must assume a critical provider goes dark, not just your own systems

The background of the slide is a vibrant tropical beach scene at sunset. The sky is filled with soft, colorful clouds in shades of orange, pink, and yellow. The sun is low on the horizon, creating a bright glow. The ocean is a deep blue, with waves breaking onto a sandy beach. The waves are uniquely colored with a rainbow gradient, transitioning from purple and blue on the outside to red and orange near the shore. Palm trees are visible on the left and right sides of the frame, their fronds silhouetted against the sky.

HITACHI

The Hitachi approach:

Protecting Brand Reputation, Revenue & Growth at the Board Level

Prevention-First Protection

Strategy
Stop attacks with network, endpoint security

Reality
Attacks bypass perimeter controls

Outcome
Extended downtime, significant data loss, non-compliance

Backup-Centric Recovery

Strategy
Traditional restore-from-backup recovery

Reality
Only 53% achieve full data recovery

Outcome
Days-to-weeks downtime, hours-to-days data loss, compliance gaps

Risk-Optimized Data Resilience

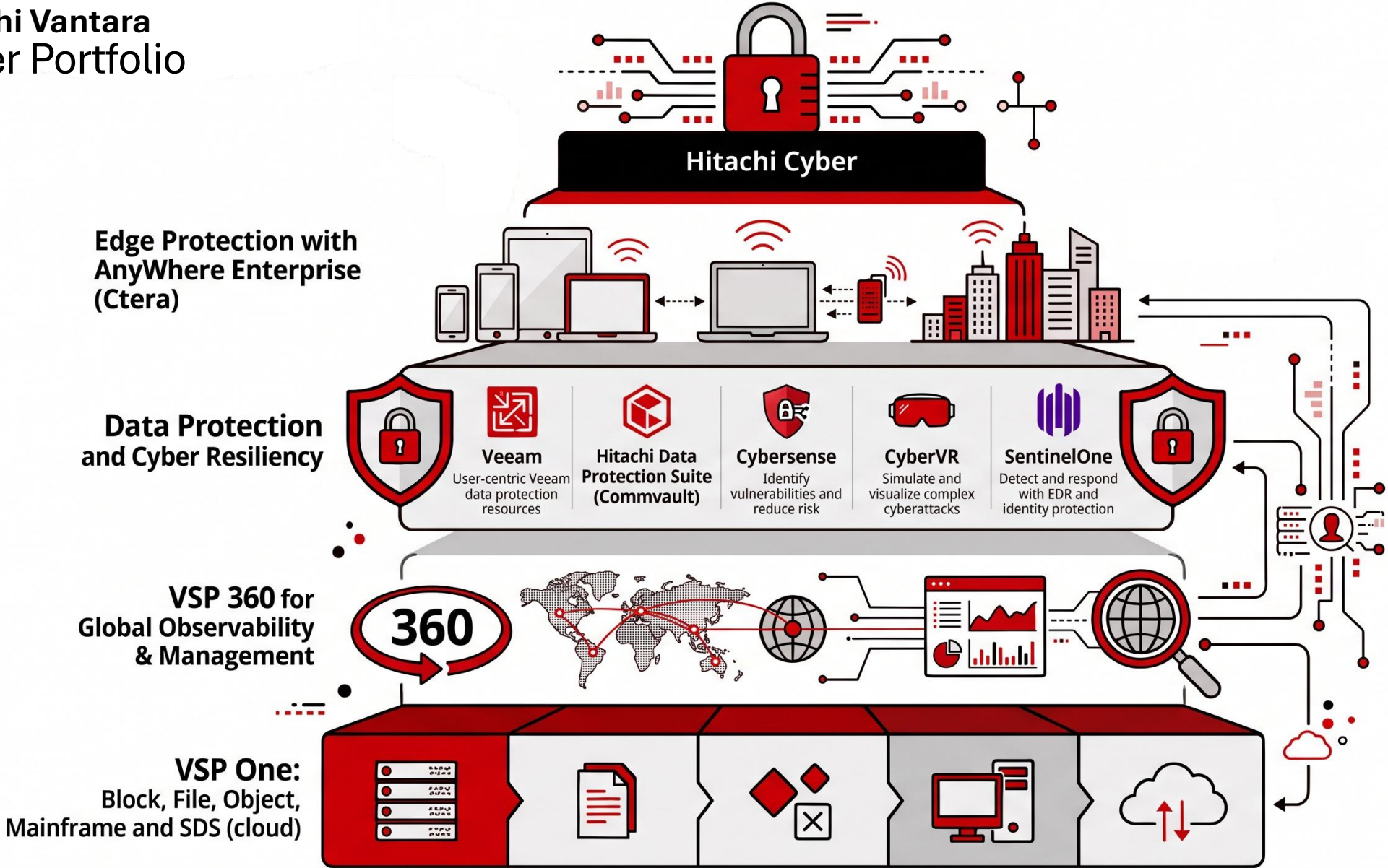
Strategy
Prioritize resilience for critical, regulated data

Reality
Risk-tiered recovery minimizes disruption

Outcome
Hours of downtime, minutes of data loss, supported with governance

Legacy Hardware & Applications

Hitachi Vantara Cyber Portfolio



Action Items: Next Steps with Hitachi Vantara

Cyber resiliency, governance and compliance — a phased path from discovery to measured recovery



> Contact your Hitachi Partner Manager or account team to get started



Gracias