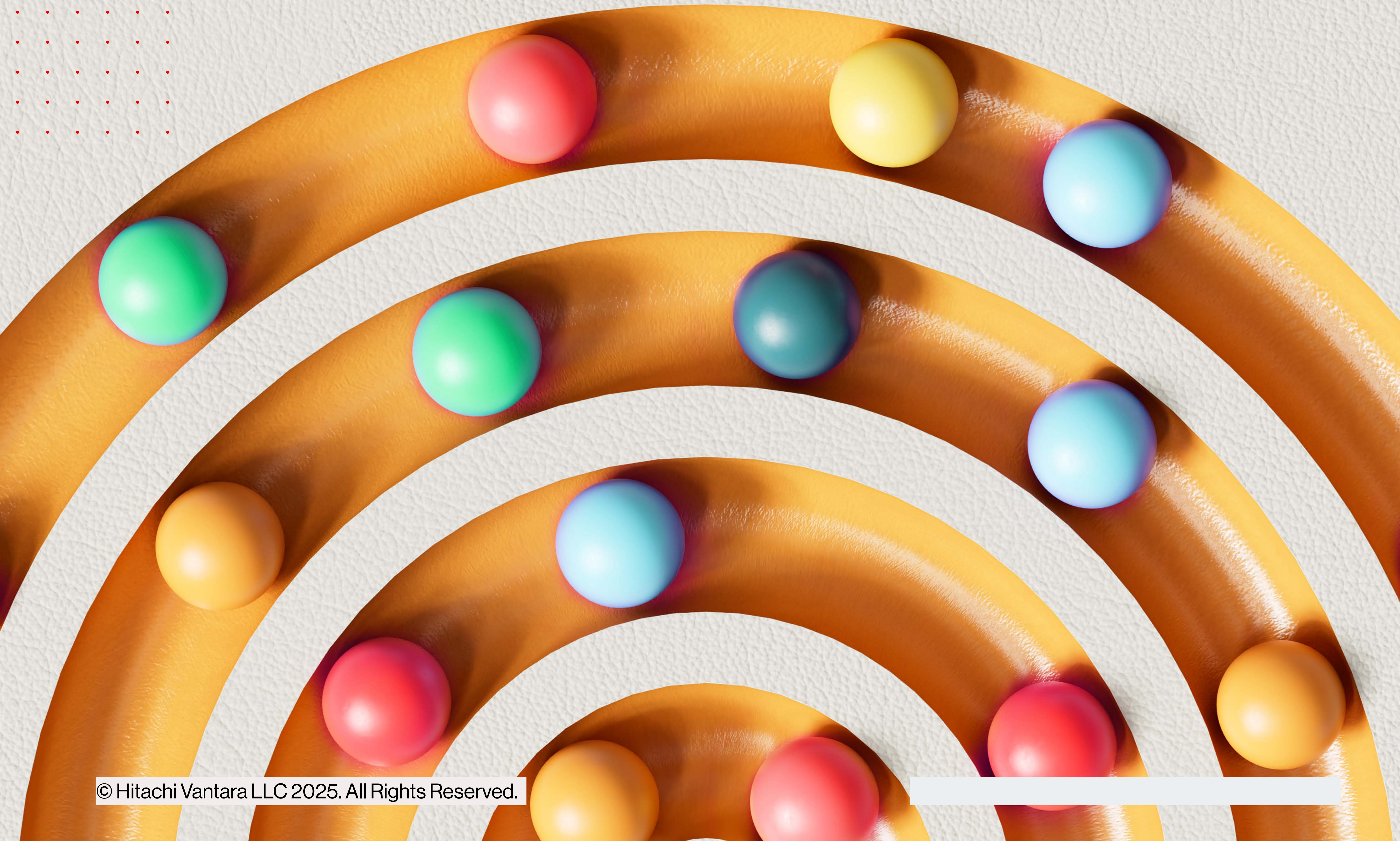
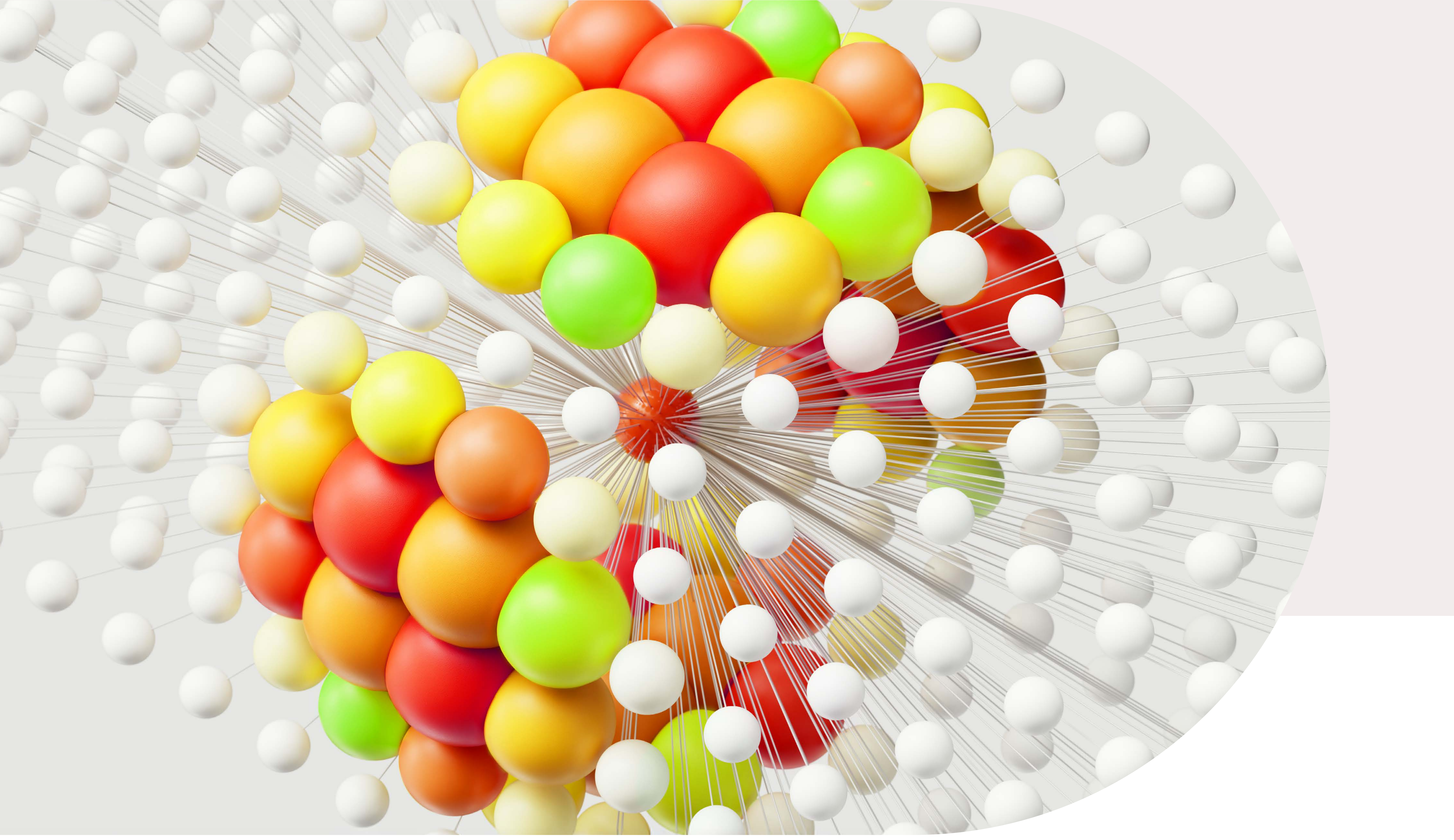
Hitachi Vantara

eBook

Cyber Resilience

Beyond Traditional Security in the Age of Inevitable Breaches





The Fundamentals of Cyber Resilience

Cyber threats today are a relentless, shape-shifting challenge.

Traditional cybersecurity – focused solely on prevention – is no longer enough. Cyber resilience is a strategic evolution, acknowledging a critical truth: breaches are not just possible, they're inevitable.

Imagine your organization as a high-performance team in an unpredictable game where the rules constantly change. Cybersecurity is one component: your defensive playbook, blocking immediate threats. **Cyber resilience is your entire game strategy. It's the ability to adapt, respond, and continue playing, no matter what unexpected challenges emerge.**

Cyber resilience transforms how organizations approach digital risk. It's a comprehensive strategy that goes beyond prevention, focusing on rapid detection, swift response, and maintaining critical operations during and after cyber incidents.

Cybersecurity *vs.* Cyber Resilience

	Cybersecurity	Cyber Resilience
Focus	• Prevention and protection	• Identification, protection, detection, response and recovery
Primary Goal	• Blocking and preventing cyber threats	• Anticipate, withstand and recovery operations quickly from cyber incidents
Approach	• Defensive, static strategy	• Adaptive, proactive strategy
Key Characteristics	• Emphasis on technical controls • Reactive threat management • Primarily technology-driven • Aims to create impenetrable barriers	• Holistic organizational approach • Anticipates and adapts to evolving threats • Balances prevention with recovery capabilities • Includes people, processes, and technology • Focuses on business continuity and rapid response
Key Differentiator	Cybersecurity asks, **"How do we stop threats?"**	Cyber Resilience asks, **" How do we reduce risk to business operations from inevitable attacks?**

Why Cyber Resilience Matters

Cyber resilience is the cornerstone of modern organizational strategy.

It ensures that your operations remain secure, adaptive, and functional, even in the event of a cyberattack, system failure, or significant digital disruption. A robust cyber resilience strategy encompasses key elements:

- **Cybersecurity:** Measures which prevent unauthorized access, use, disclosure, disruption, modification, or destruction of digital assets.
- **Backup and Recovery:** Measures which ensure the regular backing up of data and ability to restore it quickly and efficiently in case of data loss.
- **Adaptive Response:** Measures which ensure the organization can quickly detect, respond to, and recover from cyber incidents while maintaining critical operations.

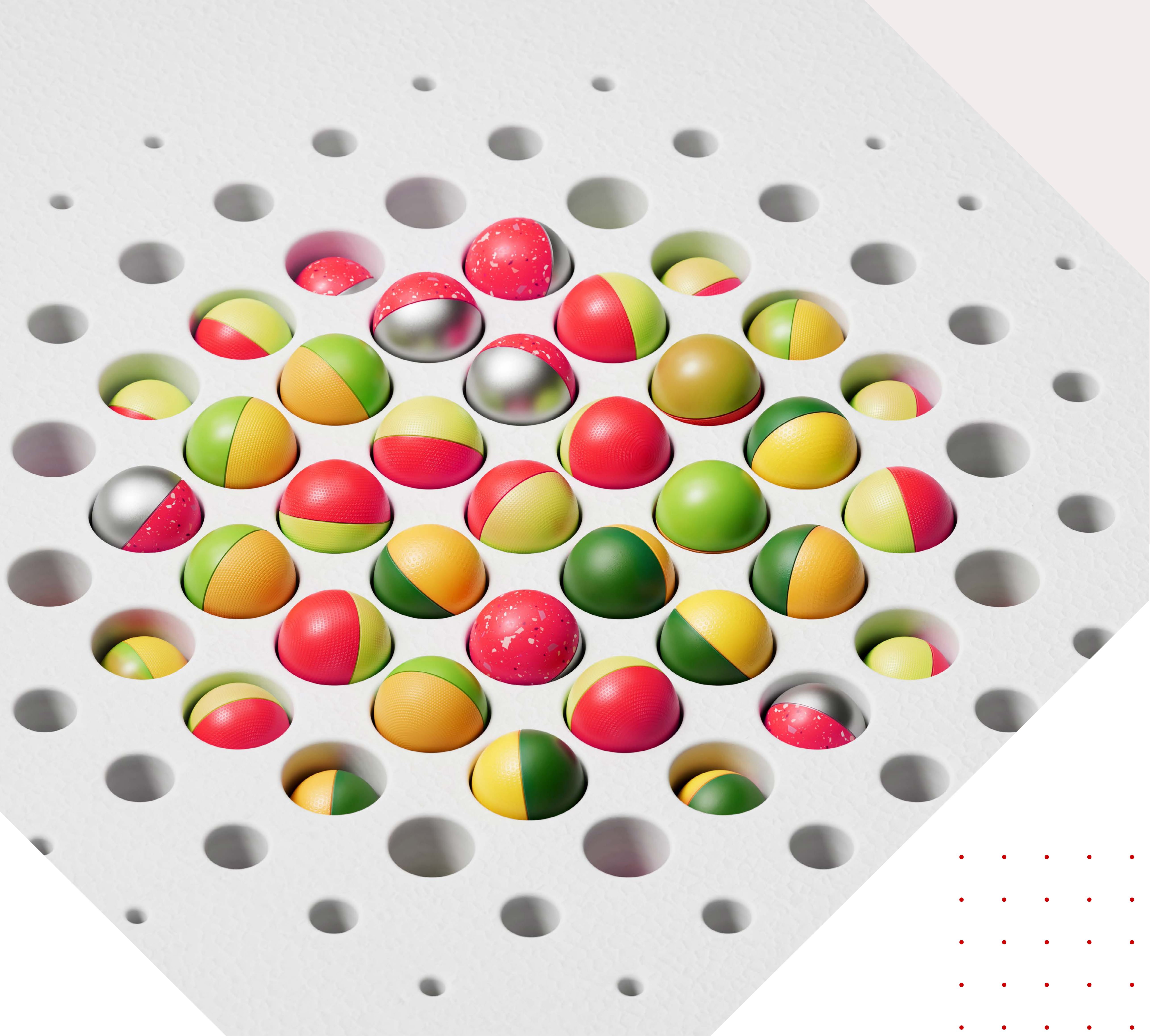
Building a Strong Cyber Foundation

Organizations which master the basics can build a strong foundation for cyber resilience.

Some basics include, but are not limited to:

- **Strong Passwords and Multi-Factor Authentication:** Using unique, complex passwords and enabling multi-factor authentication to add an extra layer of security to their user accounts.
- **Vulnerability Management:** Regularly identifying and remediating software and infrastructure vulnerabilities to reduce the attack points that threat actors can exploit.
- **Robust Network Architecture:** Leveraging advanced technologies like next-generation firewalls, intrusion detection and prevention systems, and zero-trust network designs to create adaptive defensive perimeters.
- **Antivirus and Anti-Malware Software:** Tools which detect and quarantine or remove malicious software found on servers and user endpoints that can compromise the organization's data.
- **Employee Education:** Continuous training of the organization's employees on cyber resilience best practices, including recognizing sophisticated phishing attempts, understanding social engineering tactics, and maintaining operational security.

Organizations often make the critical mistake of becoming over-reliant on tools and technology, while ignoring the fact that effective cyber resilience requires a holistic, multi-layered approach involving a combination of technologies, processes, human skills, and adaptive strategies.



Let’s Talk Recovery and Response

Data loss can still occur even after implementing the very best cyber resiliency measures. This is where the need for robust backup, recovery, and response comes in.

At a rudimentary level, a comprehensive backup and recovery plan should include:

- **Regular Backups:** Data should be backed up regularly, with the frequency depending on the criticality of the organization’s operations and its data.
- **Offsite and Vaulted Backups:** Storing backups in a separate location and/or in an air-gapped vault protects against data loss due to physical disasters or ransomware attacks that encrypt local data.
- **Testing and Recovery:** Regular testing of the backup and recovery process to ensure it is working as expected, and that the organization can restore data quickly in an emergency.

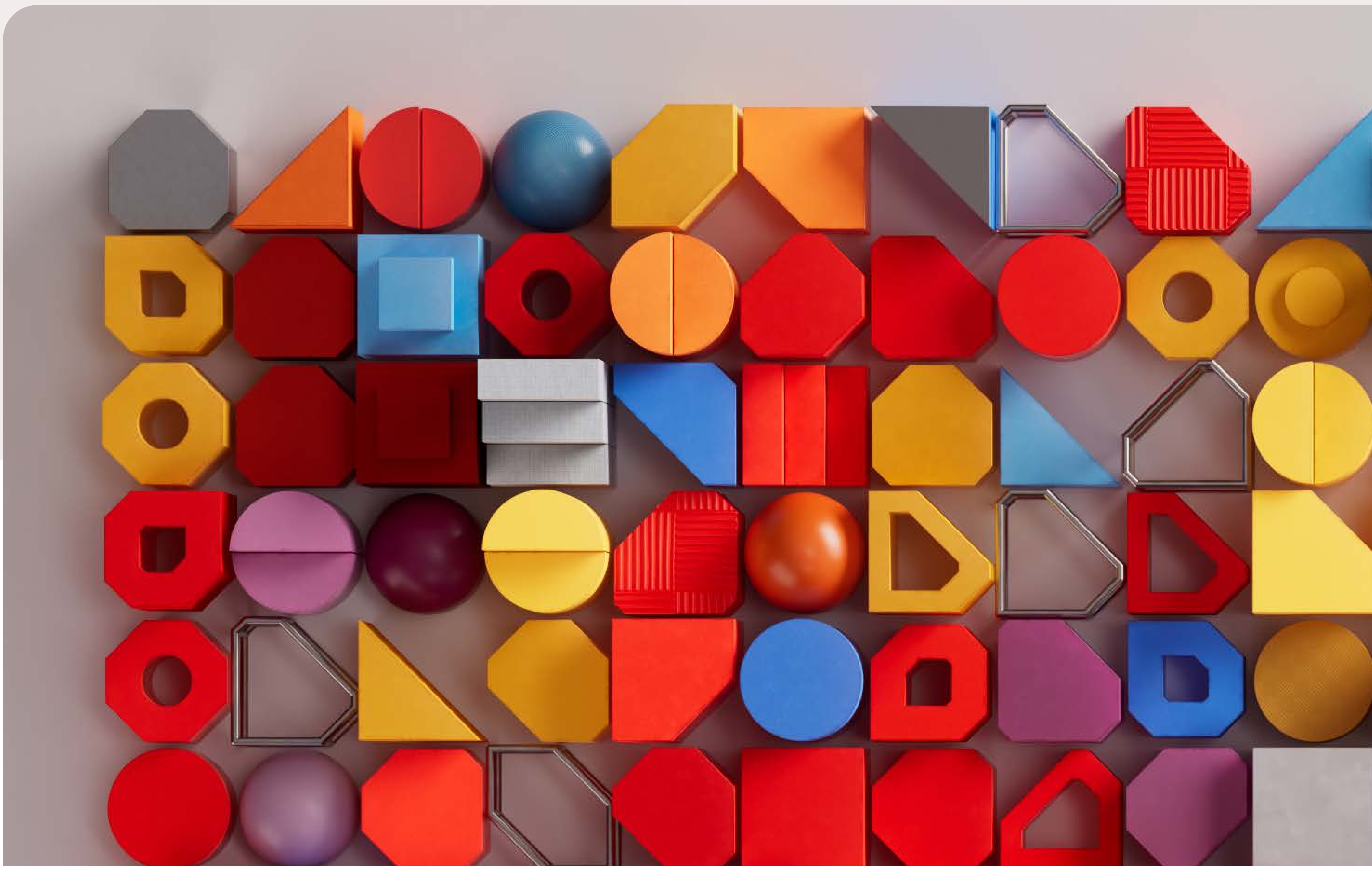
Regulations Driving Cyber Resilience

As our complex, operating environment changes, and the interconnectedness of the globe increases, regulators worldwide have taken notice and put greater emphasis on the need for operational resilience, especially where data is concerned.

The **Digital Operational Resilience Act (DORA)**, a new regulation in the European Union, sets out requirements for global financial entities to manage and mitigate Information Communication Technologies (ICT) risks. DORA emphasizes the need for:

- **ICT Risk Management:** Impacted organizations must implement a comprehensive framework to identify, assess, and manage ICT risks.
- **Incident Reporting:** Strict and timely reporting of major ICT-related incidents to relevant authorities. This highlights the need for a robust organizational incident response process.
- **Digital Operational Resilience Testing:** Regular testing of the resilience of ICT systems and processes to ensure that the organization's people, processes, and technologies are aligned to ensure continuation of services.

This regulation is just one example of the expanding regulatory focus on cyber resilience. The purpose for DORA is essentially to protect the consumer and maintain financial stability in the face of an IT disruption. Under the regulation, an institution must be able to identify, withstand and recover quickly from operational failure and be able to "fail forward."



Cyber Resilience: A Shared Responsibility

Cyber resilience is not only the responsibility of IT, IT Operations, or IT Security departments. It is an organizational responsibility, requiring the collective effort from everyone within the organization, particularly the Board and C-Suite.

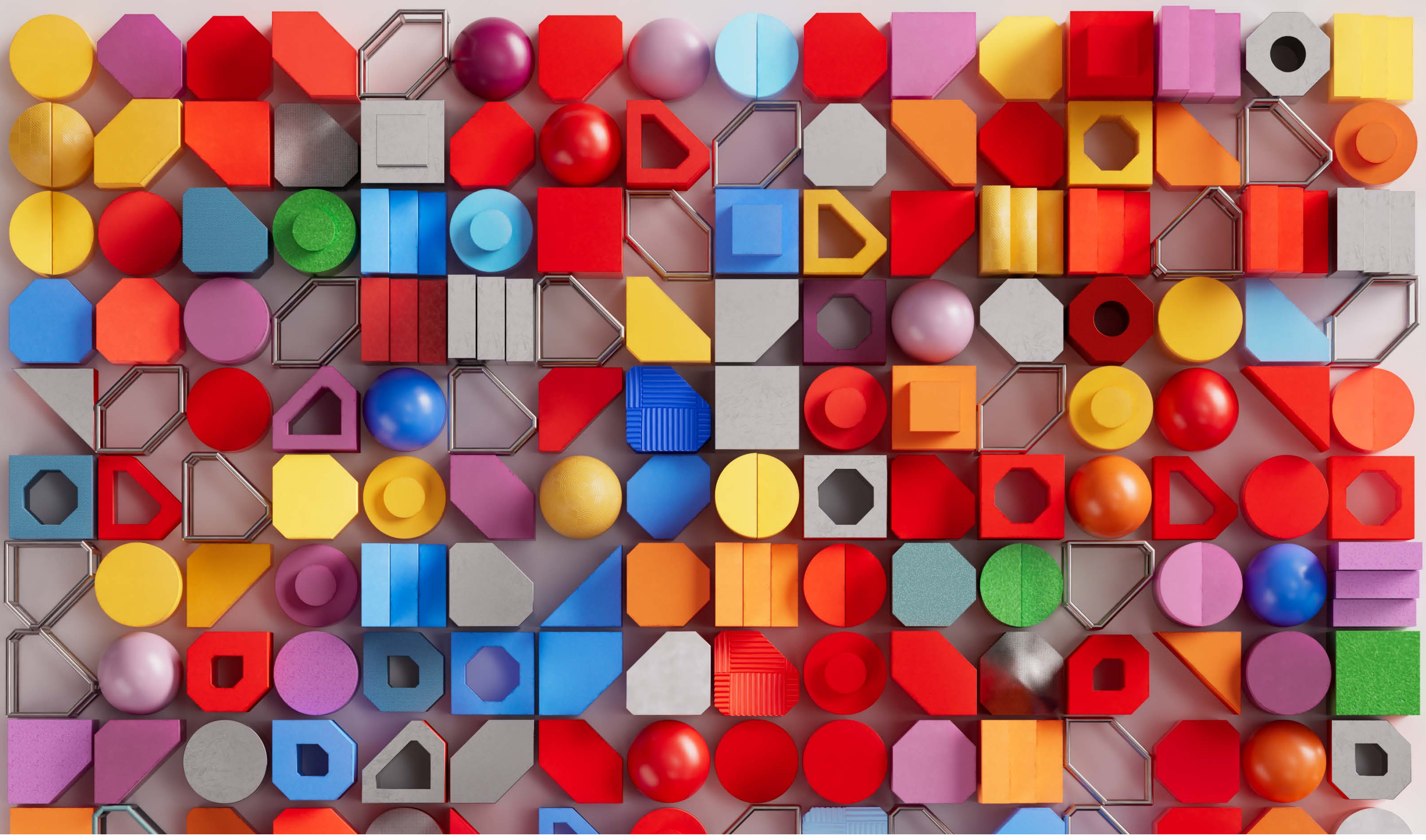
Why?

Because the tone is set from the top and must be reinforced from there. Business leaders must prioritize cyber awareness training as part of their cyber resilience strategy, recognizing the need for sustained investments in necessary resources and processes. An educated and highly aware employee becomes a critical player in the ongoing challenge of maintaining organizational cyber resilience.

A Trusted Partner in Cyber Resilience

Nothing beats having a trusted partner to help you in this journey. Reach out to Hitachi Vantara today to gain expert advice and guidance on the approach you should take in navigating your cyber resilience strategy.

Get Resilient →



Hitachi Vantara

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

HV-GBS-EB-Cyber-Resilience-Beyond-Traditional -24Feb25-A

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact