

Solution Profile

Hitachi Vantara's 7-Layer Defense Strategy: Govern

Employ Governance to Deliver Transparency and Visibility.

Digital business transformation, generative AI and emerging cyber threats are creating unprecedented security risks. Protecting data from tampering, deletion, loss and theft isn't easy. What's worked in the past is falling short, leaving gaps in many companies' security posture.

In response, organizations are searching for new and immutable cybersecurity approaches. That's why hundreds of the world's most security conscious enterprises turn to Hitachi Vantara and our ecosystem of partners for support.

Hitachi helps organizations of all sizes and industries confidently address the threats from today's cyber criminals by offering a proactive defense strategy that expands on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

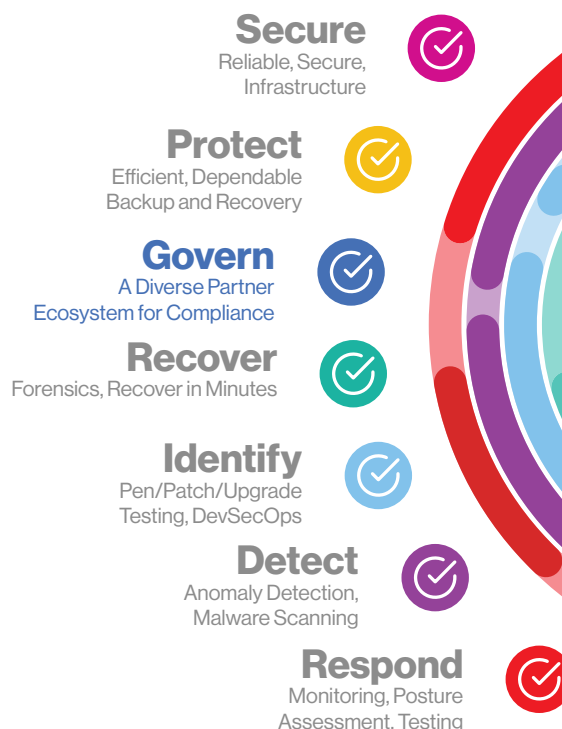
The [NIST Cybersecurity Framework](#) is a set of industry standards and best practices designed to help organizations manage cybersecurity risks and provides a flexible and cost-effective approach to enhancing cybersecurity infrastructure and risk management processes.

Hitachi Vantara's 7-layer defense-in-depth integration with the NIST Cybersecurity Framework spans hardware, software and services and delivers immutable safeguards, operational resilience and compliance without overwhelming complexity. This unique approach helps our customers address rampant data growth and sprawl, cyber threats, downtime costs and regulatory oversight.

The recently added function, Govern, complements and overlaps with several of the NIST framework's functions, particularly Identify and Protect. It signifies a strategic shift from viewing risk management as a task to recognizing it as an integral part of governance that informs and shapes policy, strategy and operational decisions.

Monitoring Security Risks, Mitigating Loss

Whether an intrusion or other breach, the total cost of an event is often more than the ransom—it also includes the recovery of impacted systems and the losses incurred by downtime. A report by Hitachi partner Veeam¹ found that in 94% of ransomware incidents, threat actors actively targeted backup repositories. Seventy-five percent of victims lost some of their backups, and 39% of backup repositories were completely lost.



Downtime is Detrimental and Expensive

System failures, user errors, and malicious attacks are unpredictable and unavoidable. According to Pingdom², the cost of downtime for these industries can amount to the cost of downtime for these industries can amount to:

- Media at **\$90,000** per hour
- Health care at **\$636,000** per hour
- IT at **\$450,000** per hour
- Retail at **\$1.1 million** per hour
- Telecommunications at **\$2 million** per hour
- The energy industry at **\$2.48 million** per hour
- Auto at **\$3 million** per hour
- Brokerage service industry at **\$6.48 million** per hour

Hitachi Vantara's 7-Layer Defense Strategy

A More Comprehensive Approach to Management

The Govern layer of Hitachi's 7-layer defense-in-depth strategy provides an overarching function that ensures all cybersecurity activities are aligned with the organization's business requirements, risk tolerances and the regulatory environment.

Governance involves establishing policies, procedures and controls that guide the implementation and ongoing management of cybersecurity practices. It ensures cybersecurity strategies support business objectives and comply with applicable laws and regulations.

Effective governance also helps an organization map out its risk management processes and decide on resource allocation, which are crucial steps in the Identify function.

Governance activities are critical for incorporating cybersecurity into an organization's broader risk management strategy. Govern directs the understanding of organizational context, which involves establishing cybersecurity supply chain risk management, roles, responsibilities, authorities, policies, processes and procedures and the oversight of cybersecurity strategy.

Increased Visibility, Maintaining Compliance

Hitachi has decades of experience establishing and monitoring compliance and securing storage that incorporates immutability, encryption, retention and versioning to prevent tampering, deletion, loss, theft or exposure of data. We work with hundreds of software partners to help maintain comprehensive compliance across the information lifecycle in an ever-changing regulatory landscape.

As a result, you gain the peace of mind that comes with:

- The only 100% data availability guarantee in the market and the impregnable fortress that protects data integrity.
- Data that is safely stored in an isolated, encrypted, versioned and secure storage environment designed for scale and speedy recovery.
- Built-in advanced data management capabilities such as retention, legal hold, encryption auditing, e-discovery reduce risk of non-compliance.

- The robust protection of data where it lives reduces the cost of traditional data protection and the risk of data loss.
- Ensuring continuous operations for mission-critical applications with nonstop, uninterrupted data access to achieve strict zero RTO and RPO objectives.

The Hitachi Advantage: VSP One, HCP and HCP Anywhere Enterprise

Hitachi Vantara solutions deliver reliable, scalable and secure storage solutions so organizations can manage their data effectively.

The Hitachi Virtual Storage Platform One (VSP One) is built with resiliency in mind. It provides 100% data availability, modern storage assurance and adequate capacity. The Hitachi Content Platform (HCP) allows IT organizations and cloud service providers to securely and cost-effectively store, share, protect, preserve and analyze data.

Adding VSP One and/or HCP will make your environment more scalable, affordable, faster, easier to manage and reliable, with built-in features for data durability, automated retention, massive scalability, immutability, versioning, performance and more.

HCP Anywhere Enterprise is an enterprise-level file synchronization and sharing platform that brings edge offices and remote workers under the same robust protection you can deliver in your data centers.

Click here to learn how we can help you build an unbreakable data infrastructure powered by Hitachi Vantara's technology.

[Learn more →](#)

¹ Backup Repositories Targeted in 93% of Ransomware Attacks

² Average Cost of Downtime per Industry



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