

Solution Profile

Hitachi Vantara's 7-Layer Defense Strategy: Identify

Identify Using Pen/Patch/Upgrade Testing and DevSecOps.

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. Identifying and managing cybersecurity risk to systems, assets, data and capabilities can also be challenging.

IT needs to balance protecting and recovering data in a timely and budget-friendly manner with the need to run the business. Losses can and do add up to millions of dollars. That's why hundreds of the world's most security conscious enterprises turn to Hitachi Vantara and our ecosystem of partners for support.

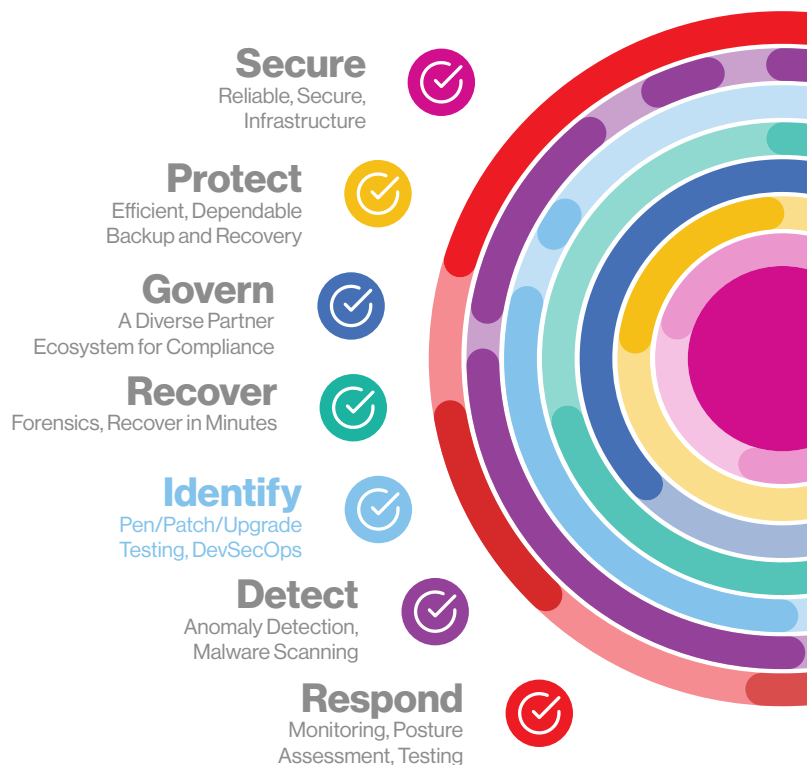
Hitachi helps organizations of all sizes and industries confidently identify address the threats from today's cyber criminals by offering a proactive defense strategy that expands on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

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. It delivers identify functionality, 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.

Quickly Identify Sophisticated and Costly Security Events

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. Identifying anomalies quickly helps. A report by Hitachi partner Veeam¹ found that in 93% 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

AI-powered Anomaly Detection Quickly Identifies Risk Exposure

The Identify layer serves as the foundation of the NIST framework. It necessitates the awareness of an organization's systems, assets, data and capabilities to effectively manage cybersecurity threats and ensure that current cybersecurity risks are understood.

Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers and related risks enables an organization to prioritize its efforts and resources effectively and adapt its security strategies to protect critical assets and manage vulnerabilities more efficiently.

This function is divided into six categories — asset management, business environment, governance, risk assessment, risk management strategy and supply chain risk management. It also includes identifying improvement opportunities for the organization's policies, plans, processes, procedures and practices that support cybersecurity risk management to inform efforts under all NIST functions.

Understanding Your Cybersecurity Posture

The Identify layer is about knowing your organization's cyber strengths and weaknesses. Hitachi Vantara offers a wide range of services including monitoring, posture assessment, testing and analysis to assess the strengths and weaknesses of your cybersecurity posture, help you gain deeper knowledge of vulnerabilities and threats through proactive risk management, understand where you are, where you need to go, and what needs to be done to get there.

Hitachi Vantara—100% Data Availability, Guaranteed

Hitachi has decades of experience ensuring reliable, secure storage that incorporates immutability, encryption, retention and versioning to prevent tampering, deletion, loss, theft or data exposure. We bring AI-powered anomaly detection and malware scanning, to identify threats quickly.

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.
- 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. It has 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