Solution Profile

Hitachi Vantara's 7-Layer Defense Strategy: Detect

Detect — Anomaly Detecting, Malware Scanning

Digital business transformation, generative AI and emerging cyber threats create unprecedented security risks. Protecting data from tampering, deletion, loss and theft can be challenging. Business continuity and resiliency rely on the rapid recovery of data, which 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.
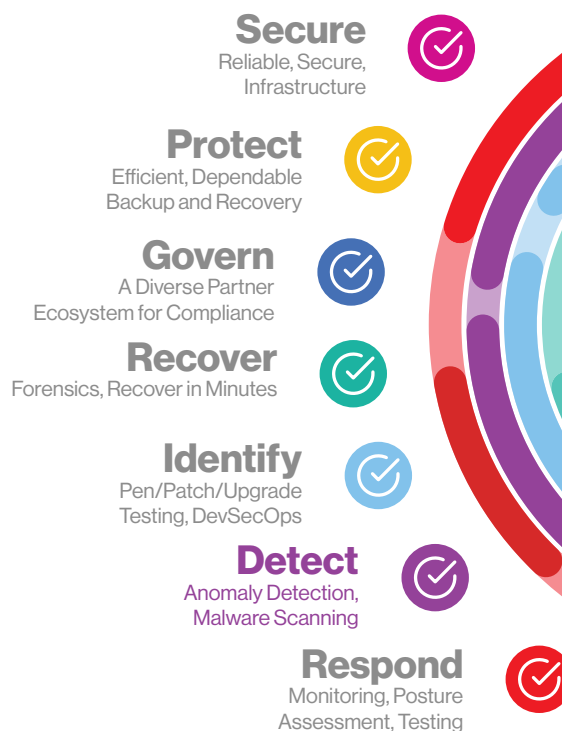
Hitachi helps organizations of all sizes and industries confidently address the threats from today's cyber criminals by offering a proactive defense strategy that expands on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

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 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.

Rapid Detection is Key to Mitigating Losses

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. Quickly detecting the anomaly helps. A report by Hitachi partner Veeam[1] 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.

Secure
Reliable, Secure, Infrastructure

Protect
Efficient, Dependable Backup and Recovery

Govern
A Diverse Partner Ecosystem for Compliance

Recover
Forensics, Recover in Minutes

Identify
Pen/Patch/Upgrade Testing, DevSecOps

Detect
Anomaly Detection, Malware Scanning

Respond
Monitoring, Posture Assessment, Testing

Downtime is Detrimental and Expensive

System failures, user errors, and malicious attacks are unpredictable and unavoidable. According to Pingdom[2], 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

Detection Strategies Speed Time-to-Response

The detect pillar focuses on developing and implementing strategies promptly to identify cybersecurity events and threats. It emphasizes the importance of continuous monitoring and proactive detection to ensure that organizations can rapidly detect and respond to potential incidents.

Detection is one of the most important functions of the NIST CSF core framework, as it defines important detection roles, responsibilities and processes and where they are conscientiously implemented within the organization.

The detect functionality of Hitachi's 7-layer defense-in-depth strategy is crucial for the timely discovery of cybersecurity events. Detection processes help identify anomalies and events quickly and ensure they are understood well enough to enable timely response. Implementing advanced detection systems and continuous monitoring practices helps identify potential threats before they cause significant harm.

This layer emphasizes the importance of an adaptive protection and detection strategy that evolves with emerging threats and attackers' changing tactics, ensuring that detection mechanisms are always aligned with current threat landscapes.

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 provide the tools to aid with forensics to find the right recovery point and the fastest recovery of virtual machine and bare metal environments to get operational again. We also enable rapid recovery at scale of file system environments.

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 and rapid recovery at scale that 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

HV-BTD-PV-7-Layer-Detect-7Nov24-B