White Paper

Ensure Business Continuity Across the Enterprise

Employ Hitachi Vantara's 7-layer defense-in-depth strategy to achieve end-to-end resilience and protection.

Hitachi Vantara

It's no longer a matter of 'if' but 'when' your organization will be impacted by intricate, sophisticated, nefarious ransomware and cyberattacks. This imminent threat underscores the need for CIOs and CISOs to prioritize threat protection and mitigation. In a recent study, 94% of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack.[1]

Hitachi helps organizations of all sizes and industries confidently address the threats from today's cyber criminals by offering a proactive defense for an ever-evolving threat landscape.

Hitachi Vantara's 7-layer defense-in-depth strategy, spanning hardware, software and services, delivers immutable safeguards, operational resilience and compliance without the overwhelming complexity found in other solutions.

This unique approach helps our customers address rampant data growth and sprawl, cyber threats, downtime costs and regulatory oversight by delivering continuous, comprehensive protection for apps and data across their ecosystems.

[1] Ransomware Payments Increase 500% In the Last Year, Finds Sophos State of Ransomware Report

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

Ransomware Attacks are Taxing IT Systems and Infrastructure.

Today's threat landscape makes it difficult for organizations to be continuously operational. The sophistication and impact of modern attacks, combined with expanding attack surfaces, a growing list of security risks and increasing regulatory scrutiny, require teamwork and a new, comprehensive approach. Increasing threats like ransomware make the job of protecting the enterprise a challenging one. Bad actors target and corrupt data backup copies, unleashing malicious and unpredictable attacks. Successful intrusions result in downtime, system failures and devastating financial losses. The damage adds up quickly.[1]

- Media losses are estimated 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 losing **$2 million per hour**
- The energy industry **$2.48 million per hour**
- Automotive bleeding **$3 million per hour**
- Brokerage service industries hemorrhaging **$6.48 million per hour**

Solidify Your Defense with Hitachi Vantara

Data resiliency is the backbone of operational resilience, combining traditional data protection and disaster recovery (backup/recovery, replication/failover, etc.) with cyber readiness.

While just about every IT shop has some data protection in place, cyber readiness is a different animal. But as cyberattacks become more frequent and sophisticated, the path to operational resiliency becomes increasingly difficult. Hitachi Vantara's solutions are designed to enhance cyber readiness and ensure your organization is prepared for any cyber threat with an integrated, incremental approach to enhancing traditional data protection toward robust cyber readiness.

100%

Data availability guarantee.

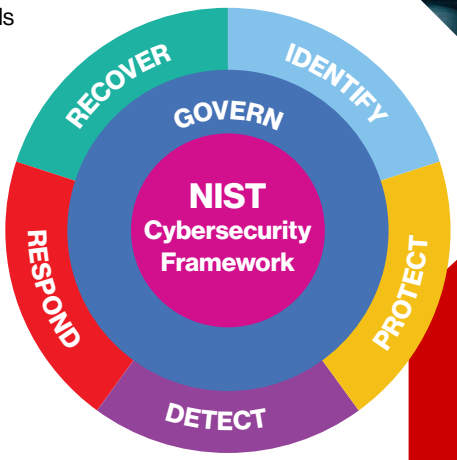
Our reliable, secure, immutable infrastructure comes with the only 100% data availability guarantee in the market—and creates impregnable fortress that protects the integrity of your data and enables rapid recovery.

[1] Average Cost of Downtime per Industry

Ensure Resilience and Compliance Without Complexity

Hitachi Vantara's 7-point defense-in-depth integration, which expands on the NIST Cybersecurity Framework, is designed to deliver on its Secure, Protect, Govern, Recover, Identify, Detect and Respond plan without the overwhelming complexity of other solutions. Hitachi Vantara delivers on these functions with:

- **The world's fastest recovery** of VM and bare metal environments
- **The only 100% data availability** guarantee in the market
- **Robust cyber resilience** from end-to-end
- **Comprehensive compliance** across the information lifecycle
- **Reusable protection and data** for other workloads
- **A single source** for purchase and support



Expanding on the NIST Cybersecurity Framework, Hitachi Vantara offers your organization:

- Peace of mind knowing that your data is safe and sound in an isolated, encrypted, versioned and secure storage environment designed for scale and speedy recovery.
- Robust protection of data where it lives to reduce the cost of traditional data protection and reduce the risk of data loss.
- Assurance of continuous operations for mission-critical applications with nonstop, uninterrupted data access to achieve strict zero RTO and RPO objectives makes it more scalable, affordable, faster, easier to manage and more reliable.
- Fortified defenses with built-in features bolster data durability, automated retention, massive scalability, immutability, versioning, performance and more.
- The ability to deliver the same robust protection to edge offices and remote workers you provide in your data centers.

The NIST Cybersecurity Framework is a set of industry standards and best practices designed to help organizations manage cybersecurity risks. Developed by the National Institute of Standards and Technology (NIST), the framework provides a flexible and cost-effective approach to enhancing cybersecurity infrastructure and risk management processes. It is structured to be applicable across diverse sectors and organizations of all sizes, from small businesses to large enterprises and government agencies.

Hitachi's Powerful Defense: VSP One, HCP, and HCP Anywhere Enterprise

Learn more about:

Hitachi Vantara Data Protection and Cyber Resiliency →

Hitachi Vantara Data Governance →

This trio of engines are at the heart of Hitachi Vantara's 7-point defense-in-depth integration. Hitachi Virtual Storage Platform One (VSP One) is a hybrid cloud data platform that's designed to simplify infrastructure for mission-critical applications.

VSP One ***provides 100% data availability, modern storage assurance, and immutable snapshots***. The Hitachi Content Platform (HCP) delivers 15 nines of data durability with 10 nines of data accessibility and allows IT organizations and cloud service providers to securely and cost-effectively store, share, protect, preserve and analyze data.

HCP Anywhere Enterprise allows organizations to implement advanced content collaboration and data protection solutions without compromising on security or performance.

Learn more about Data Protection, Cyber Resiliency and Data Governance.

99.999999999

The Secure Layer
Reliable, Manageable, Immutable Infrastructure

The Secure layer of Hitachi Vantara's 7-point defense-in-depth integration is an enhancement and specific application of the Protect function. While the Protect layer focuses on implementing appropriate safeguards to ensure the delivery of critical infrastructure services, the Secure layer delves deeper into the technical and procedural elements necessary to harden systems against threats.

In addition, the Secure layer provides detailed practices for fortifying hardware and software with encryption, immutability, versioning, data integrity checking and enforcing security policies that protect sensitive information from unauthorized access and leaks.

Other features include next-generation cybersecurity technologies such as endpoint detection and response (EDR), and artificial intelligence in cybersecurity defenses. Integrating the Secure layer within the framework involves enhancing the existing Protect layer with a more proactive and advanced set of tools and methods to keep data and assets safe.

The Protect Layer
Efficient, Dependable Backup and Recovery

The Protect layer covers traditional data protection techniques such as backup and replication and outlines appropriate safeguards to ensure the delivery of critical infrastructure services. It includes the necessary access control to limit exposure to cyberattacks, data security measures to protect information and maintenance of security protection technologies to provide resilience against threats.

The Protect layer functionality extends beyond prevention tactics by incorporating education and awareness programs. Training is essential for creating a security-conscious culture within your organization as it significantly reduces the risk of security breaches from internal sources.

The Govern Layer
A Diverse Partner Ecosystem for Compliance

The Govern layer offers an overarching functionality that ensures all cybersecurity activities are aligned with the organization's business requirements, risk tolerances and regulatory environment. The Govern layer complements and overlaps several of the NIST framework's functions, particularly the Identify and Protect layers.

Effective governance involves establishing policies, procedures and controls that guide the implementation and ongoing management of cybersecurity practices. It ensures that cybersecurity strategies comply with applicable laws and regulations, along with regular reviews and audits, to remain current and compliant. This layer helps an organization map out its risk management processes and decide on the allocation of resources.

The Digital Operational Resilience Act (DORA) is an EU regulation that came into effect on January 16, 2023, and will be applicable starting January 17, 2025. Its purpose is to enhance the IT security of financial entities, including banks, insurance companies and investment firms, ensuring that the financial sector in Europe remains resilient during severe operational disruptions. DORA standardizes the rules related to operational resilience for the financial sector, encompassing 20 different types of financial entities and ICT third-party service providers.

The Recovery Layer

Forensics, Restoration in Minutes

The Recovery layer identifies appropriate activities to maintain resilience plans and reestablish capabilities or services impaired due to a cybersecurity incident. The process ensures timely restoration of systems or assets affected by the events, with efforts focused on reducing adverse outcomes and making the necessary improvements to policies and procedures.

This layer emphasizes the ability to quickly adapt and restore critical functions to minimize downtime and mitigate the impact on business operations. Recovery planning includes IT restoration and managing public relations and customer communications to maintain trust and confidence.

The Identify Layer

Pen, Patch, Upgrade Testing, DevSecOps

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.

The focus is on understanding the business context, the resources that support critical functions, and the related cybersecurity risks. By clearly recognizing the baseline, organizations can prioritize their efforts and resources effectively and adapt their security strategies to protect critical assets and manage vulnerabilities more efficiently.

The Detect Layer

Anomaly Detection, Malware Scanning

The Detect layer facilitates the timely discovery of cybersecurity events. Detection processes assist in identifying anomalies and events quickly and ensure they are understood well enough to enable timely response.

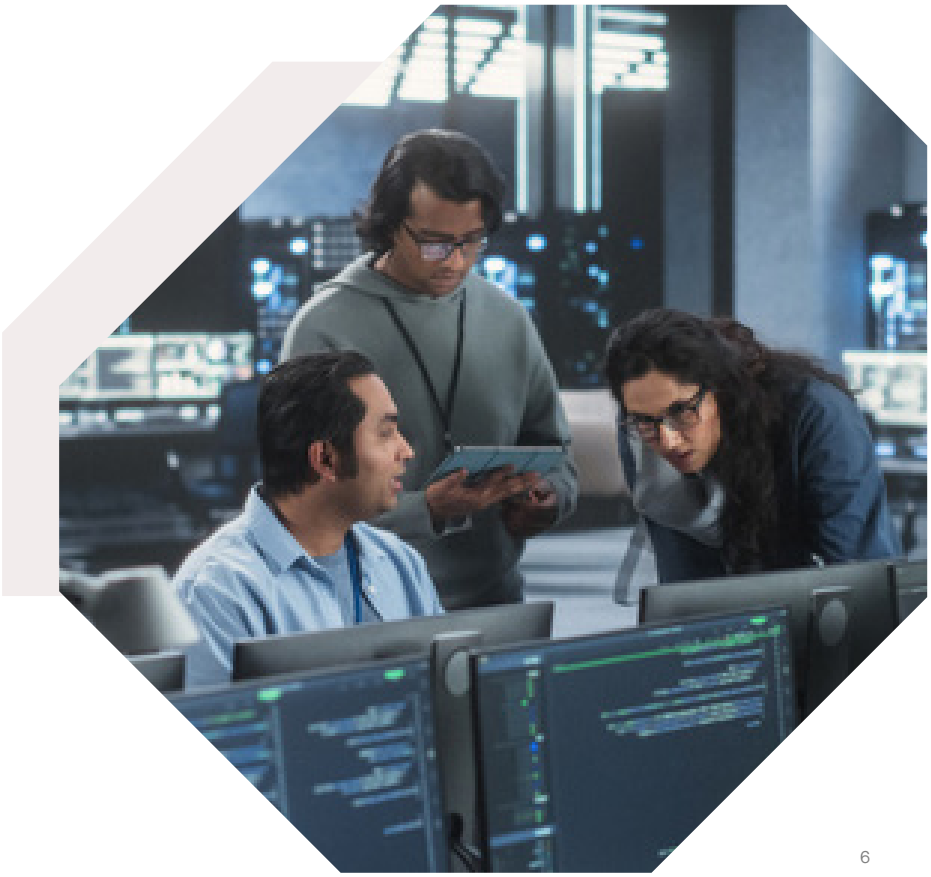
Implementing advanced detection systems and continuous monitoring practices helps recognize potential threats before they cause significant harm. This function emphasizes the importance of an adaptive protection and detection strategy that evolves with emerging threats and changing tactics by attackers, ensuring that detection mechanisms are always aligned with current threat landscapes. AI anomaly detection uses artificial intelligence and machine learning algorithms to identify irregularities in data that deviate from the norm.

The Respond Layer

Monitoring, Posture Assessment, Incident Response

The Respond layer supports the ability to contain the impact of a potential cybersecurity incident. Effective response strategies require a coordinated effort across different organizational levels and incorporates communication plans, an incident analysis and activities to prevent expansion or recurrence.

Intertwined with recovery processes, the Respond layer empowers IT to expedite the return to normal operations. It improves incident response plans and strategies based on lessons learned and forensic analysis following an event.



A Multi-Faceted Defense

Superior Expertise, Partnerships and Technology

The Hitachi Vantara 7-layer, defense-in-depth strategy, based on the NIST Cybersecurity Framework layers of functionality, combines hardware, software and services to achieve operational resilience and compliance without complexity. This unique approach helps mitigate the issues surrounding data growth, sprawl, cyber threats, downtime costs and regulatory oversight.

Cyber Security Without Compromise

Leverage Hitachi Vantara solutions to ensure comprehensive cyber resilience and business continuity across your environment with:

- The only 100% data availability guarantee in the marketplace
- Partnerships with the most respected and up-and-coming names in cybersecurity and backup
- A community with 100s of software partners to help maintain comprehensive compliance across the information lifecycle
- The tools and forensics to find the right recovery point and enable rapid recovery at scale of VMware, bare metal and file serving environments
- Software and service allies that make comprehensive, end-to-end testing a reality with thin digital twins of production environments
- AI-powered anomaly detection and malware scanning to identify threats quickly

Solve Your Data Protection Challenges with Hitachi

Trust Hitachi Vantara to protect your enterprise and enjoy a single source of consumption and support with service-level guarantees. We have expert services to help fill skills or staffing gaps, provide 24/7/365 monitoring, assess and test customer environments and even aid incident response.

Ready to get started?

Learn more →

Connect with a Hitachi Vantara cybersecurity expert. →

Hitachi Vantara
A Hitachi Group Company

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

HV-BTD-WP-DPRC-7-Layer-Defense-7Nov24-B