Hitachi Vantara

Solution Profile

Hitachi Vantara's 7-Layer Defense Strategy: Respond

Monitoring, Posture Assessment, Testing, Incident Response.

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. Responding to and managing cybersecurity risks 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.

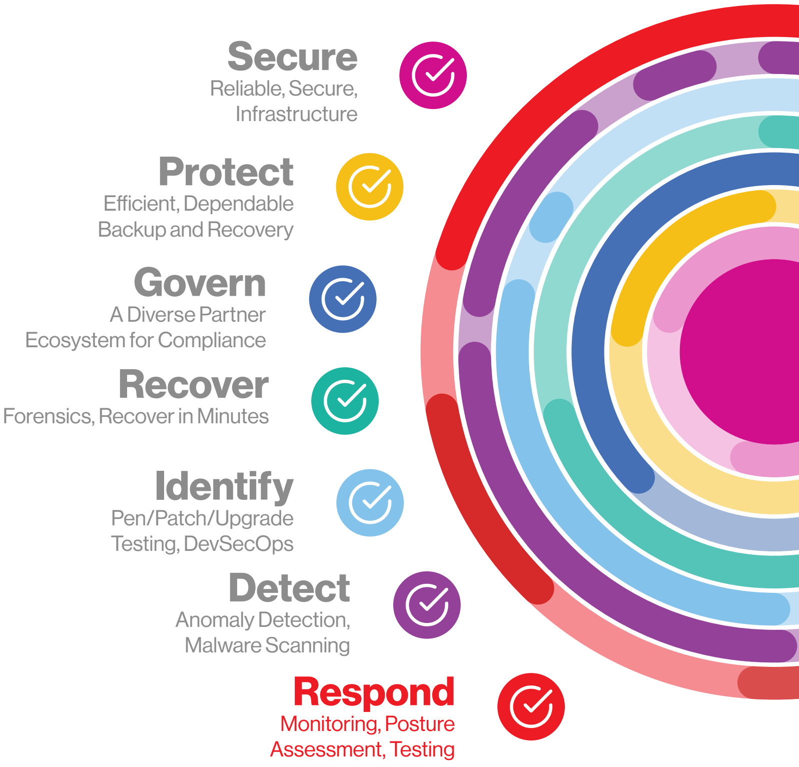
Hitachi helps organizations of all sizes and industries confidently respond to threats from today's cyber criminals by offering a proactive defense strategy that expands on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

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 response functionality, immutable safeguards, operational resilience and compliance without overwhelming complexity. This unique approach helps our customers mitigate rampant data growth and sprawl, cyber threats, downtime costs and regulatory oversight.

Rapid Response to Cyberattacks

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 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

Contain the Impact of a Potential Cybersecurity Incident

No matter how thorough your cybersecurity protocols are, there’s always a chance an attacker will manage to find a way to get in. That’s why it’s critical to have a plan to detect and respond to incidents as quickly and effectively as possible.

The Respond function supports the ability to contain the impact of a potential cybersecurity incident. The response plan includes communications regarding the incident, analysis of its impact and steps to contain and mitigate it. This function also involves improving incident response plans and strategies based on lessons learned and forensic analysis following an event.

Effective response strategies require a coordinated effort across different organizational levels. They incorporate communication plans and an analysis of the incident and activities to prevent expansion or recurrence. Response strategies are also intertwined with recovery processes, aiming for a swift return to normal operations.

Ransomware – Managed Security Services

- **Managed EDR (Endpoint Detection and Response) Service:** Offers a managed EDR service to continually monitor and respond to cyber threats at the endpoint. Our service is tailored to look for abnormal behaviors that are associated with malware and ransomware.
- **Managed NDR (Network Detection and Response) Service:** Similar to our managed EDR service, we also offer a managed NDR service which continually monitors and responds to cyber threats at the cloud, SaaS, data center and enterprise infrastructure levels in real time.
- **Cyber Resilience & Incident Response:** This service can be utilized during an active ransomware attack, can be offered as a standalone to have in the event an attack occurs. We identify, contain, investigate and eradicate the attack, and work with the client to restore their services.
- **24/7 Managed Security Service:** This is our flagship service offering which allows us to proactively monitor the client’s environment (note we are environmental agnostic) for indicators of compromise or attack.
- **Compromise Assessment:** This service offer seeks to assess the client’s environment to determine if any compromise (malware/ransomware) has occurred and for which they are not aware.
- **Malware Resiliency:** This service offer measures the client’s ability to continue their operations despite a malware event. The goal of this service is to harden the environment in regards of cybersecurity.
- **Security Awareness Training:** This can be offered in a “stand and deliver” format to specific cohorts within the organization, tailored in a format that is impactful for them.
- **Phish Testing:** Tailored phishing campaigns can be developed and implemented to test the security awareness of the employees.

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

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