Datasheet

Hitachi Vantara: Ransomware Detection Powered by CyberSense®

From ransomware chaos to predictable clean data recovery — guaranteed[1]

Build ransomware resilience you can count on — 99.99% advanced detection, immutable protection and 2X faster data recovery to keep your business running[2].

Enterprise IT and security leaders face escalating ransomware attacks and mounting operational uncertainty. In 2024, attacks surged by over 70%, frequently breaching traditional defenses and backup environments.

With median ransomware dwell times now under 24 hours, security teams have minimal time to detect and respond. Attackers routinely deploy double and triple extortion — encrypting data, stealing sensitive information and threatening public exposure. This has driven average enterprise attack costs beyond $5 million, including downtime, recovery and regulatory penalties.

In today's threat landscape, it is no longer a matter of if, but when an organization will face a cyberattack.

Reactive defenses are no longer enough. Without a resilient, proactive strategy, organizational risk of data loss, downtime and regulatory exposure rises dramatically. Manual recovery delays restoration and disrupts SLAs, operations and revenue. Advanced detection and rapid recovery are now essential to protect data and ensure business continuity.

Shrink the Ransomware Blast Radius: Detect, Isolate and Recover

Hitachi Vantara delivers a proactive, comprehensive approach to ransomware resilience. We seamlessly integrate our trusted, 100% available hybrid cloud data infrastructure with Index Engines CyberSense AI-driven data integrity validation software. Together, our Ransomware Detection powered by CyberSense solution safeguards against unauthorized changes or deletion using immutable snapshots within block environments[3].

The solution continuously analyzes these snapshots with byte-level content indexing, an AI-powered analytics engine and customizable detection rules. In this way, it detects ransomware-induced or insider-driven corruption with Enterprise Strategy Group (ESG)-validated 99.99% accuracy[4]. By further pinpointing the last known clean data copy, it enables precise, corruption-free data recovery.

Solution Benefits

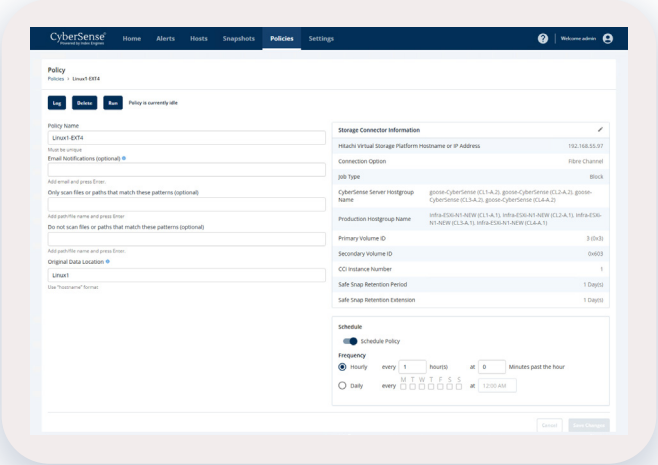
- **Maintain Predictable Continuity**
  Attain 2X or more downtime reduction and meet customer SLAs with rapid, verified clean data restoration — recovering in as little as 30 seconds per snapshot.
- **Minimize Data Loss and Reinfection Risk**
  Reduce data loss and ransomware reinfection by recovering to the nearest recovery point from immutable, AI-validated clean snapshots — not outdated backups.
- **Achieve Compliance-Ready Resilience**
  Simplify NIST Cybersecurity Framework 2.0 standard implementation with cyberattack data protection, detection and recovery assurance from one integrated solution.
- **Future-Proof Against Ransomware**
  Detect ransomware — even zero-day and evolving variants — by analyzing data behavior, not signatures, for 99.99% accurate threat detection without constant updates or patches.
- **Rely on Clean Data Recovery**
  Count on the backing of our Cyber Resilience Guarantee for clean data recovery after a cyberattack — unlike standard SLAs — with incident response and storage credit remediation.

With forensic snapshot identification and Red Hat Ansible-driven recovery automation, data can be restored in as little as 30 seconds per snapshot[2] — minimizing downtime and business disruption.

One Solution: Rapid Ransomware Resilience

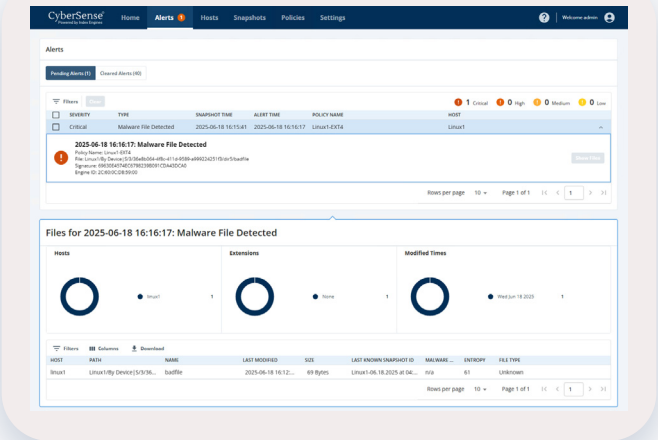
Ransomware Protection

Ensure data is always available and recoverable. Employ native production data immutability and orchestration, automating snapshot creation, mounting and scanning on a custom schedule or manual trigger to secure data against unauthorized changes or deletion.



Ransomware Detection

Snapshots are continuously analyzed using full-content indexing. The process leverages over 200 behavioral indicators of ransomware corruption, combined with AI-driven analytics trained on tens of millions of datasets and more than 7,000 real ransomware variants.

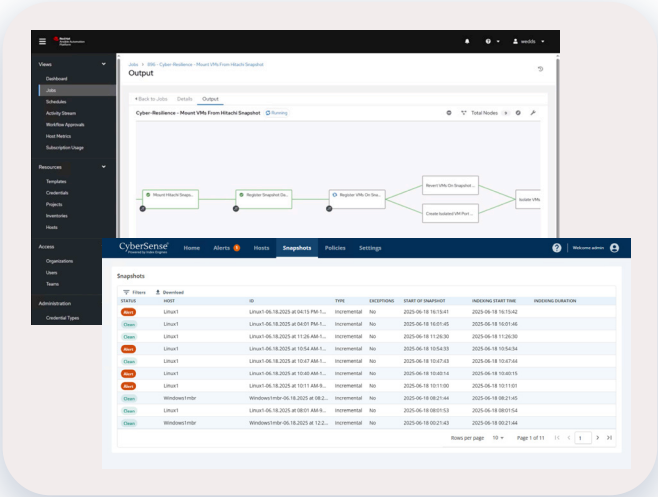


This integrated approach detects ransomware-induced or insider-driven data corruption with 99.99% accuracy, identifying modified, added, deleted or encrypted files.

Snapshot scans generate alerts based on metadata and content changes, using customizable thresholds delivered through the Ransomware Detection powered by CyberSense UI, email notifications and integrated security information and event management (SIEM) or security orchestration, automation and response (SOAR) platforms.

Ransomware Recovery

When corruption is detected, the last known clean snapshot is identified for recovery complete with forensic analysis of the corrupted files. You can initiate surgical restoration using the Hitachi hybrid cloud data platform administration or automate the process with Ansible playbooks. Data recovery completes in as little as 30 seconds per snapshot for most environments, minimizing downtime and ensuring operational consistency.



Stay Ahead of Ransomware Evolution

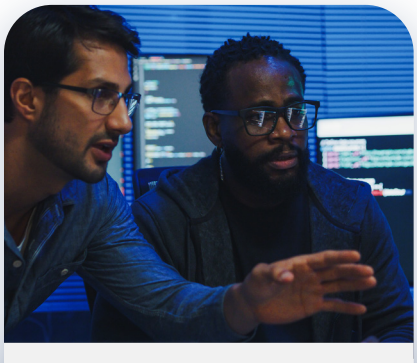
Even with advanced prevention tools, ransomware attacks remain inevitable. Ransomware Detection powered by CyberSense accurately detects attacks pre-execution by analyzing how data changes — distinguishing malicious behavior from normal user activity.

Unlike traditional tools reliant on signatures or patch cycles, this joint solution detects both slow-moving and zero-day threats through AI-driven behavioral analysis. Ransomware constantly evolves, but its impact on data is predictable. Ransomware Detection powered by CyberSense uses probabilistic models to detect corruption with 99.99% accuracy.

By learning from each scan and focusing on behavior, not signatures, this solution eliminates the need for constant updates — making it a future-proof detection solution.

AI-Powered, Automated Data Integrity Validation

- AI-driven anomaly detection: ransomware, mass deletion, encryption and tampering
- 99.99% accurate, real-time ransomware data corruption detection and isolation
- Nearest clean snapshot data recovery point identification
- Fully policy-driven scheduling, retention, thresholds and alerting



Unified Management and Support

- Simplified UI: snapshot orchestration, dashboards, alerts and recovery
- Single source for 24/7/365 support
- Ansible automation playbook support
- Syslog integration with leading SIEM and SOAR platforms

Trusted, Proven Hybrid Cloud Data Infrastructure

- 100% data availability guaranteed
- Cyber resilience clean data recovery guarantee[1]
- Scalable across on-premises and cloud environments
- 5-star ransomware protection rating — GigaOm[5]

Ransomware Clean Data Recovery — Guaranteed

Ransomware Detection powered by CyberSense is more than advanced data integrity validation — it is your gateway to guaranteed clean data recovery after a ransomware attack. As part of the optional Cyber Resilience Guarantee from Hitachi Vantara, it gives IT and security teams the confidence that recovery is not just possible — it's assured. By combining AI-driven ransomware corruption detection, immutable infrastructure and rapid, snapshot-based recovery at scale, the solution delivers predictable, corruption-free restoration in seconds—minimizing downtime, data loss and reinfection risk.

The Cyber Resilience Guarantee is available to organizations who meet these requirements: run Hitachi Vantara Virtual Storage Platform One Block (VSP One Block) midrange or high-end data infrastructure, possess an active Ransomware Detection powered by CyberSense subscription and have successfully completed the Ransomware Detection Installation and Validation Service.

If clean data cannot be recovered after an attack, Hitachi Vantara provides up to 40 hours of expert-led incident response or up to 100% storage purchase credit — ensuring your business remains resilient, no matter what.

99.99%

ESG-validated ransomware data corruption detection accuracy. Gain confidence with near-elimination of false positives and negatives that put productivity, data integrity and uptime at risk.

2024 Enterprise Strategy Group

Achieve Resilience, Achieve Peace of Mind

Ready to get started? Contact a Hitachi cybersecurity expert.

Connect Now →

[1]Subject to Hitachi Vantara's terms and conditions; please contact your Hitachi Vantara Representative for details. Cyber Resilience Guarantee coverage from Hitachi Vantara requires an active Ransomware Detection powered by CyberSense subscription, qualifying VSP One Block midrange or high-end storage array, and Ransomware Detection Installation and Validation Service.

[2]Hitachi lab tests show that Hitachi Thin Image Advanced Safe Snap snapshots are recoverable in under 30 seconds per snapshot for snapshots taken of 16TiB or fewer volumes stored on VSP One Block.

[3]The Ransomware Detection powered by CyberSense solution is supported for VSP One Block midrange and high-end storage arrays.

[4]Enterprise Strategy Group: Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption Report

[5]2024 GigaOm Radar Report for Primary Storage Report

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

Hitachi Vantara

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-DS-Ransomware-Detection-5June25-A