HITACHI
Inspire the Next

SOLUTION BRIEF

Protect and Recover from Ransomware with Hitachi Data Protection Suite and Hitachi Content Platform

The headlines are all too common – ransomware attacks are happening more frequently than ever, and the damages are jaw-dropping. One study predicts that global ransomware damages will approach $265 Billion by 2031[1].

Executive Summary

It's no longer a matter of 'if', but 'when' your organization will be impacted by attacks like these, and the damages can be massive. Because of this, CIOs and CISOs everywhere have threat protection and mitigation at the top of their minds – so much so that 86% of surveyed security leaders have ransomware as a budgeted priority for 2022[2].

The numbers are scary, but with the appropriate planning and a robust data protection and management solution in place, the impact of ransomware can be minimized. With a solution that has multiple layers of protection to ensure that data is both secure and recoverable, organizations can reduce the number of attacks that impact their systems while accelerating response and recovery for those that do.

With Hitachi Data Protection Suite (HDPS) software and Hitachi Content Platform (HCP) storage, organizations have a complete solution that can protect against ransomware and assure fast and reliable recovery of data in the event of an attack. From early detection of threats to immutable storage to simplified, fast recovery of data, Hitachi provides an end-to-end solution that's built to ensure data integrity and business continuity.

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) was founded in 1901 and is part of the United States Department of Commerce. According the NIST website, its mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

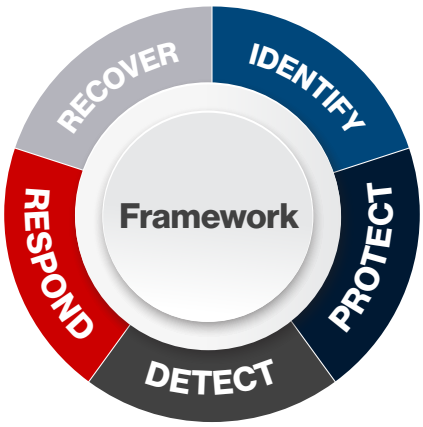

Fig. 1 NIST Cybersecurity Framework Version 1.1

1 Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (cybersecurityventures.com)
2 https://panaseer.com/business-blog/ransomware-statistics-2022/

In 2014, NIST published the initial versions of its Cybersecurity Framework. This framework is meant to "(help) organizations to better understand and improve their management of cybersecurity risk". The latest version of this framework was amended in 2018 and includes 5 key steps to effectively combat a cybersecurity incident (like a ransomware attack).

Those steps are listed here:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence or cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Multilayered Protection from Ransomware with HDPS and HCP

To align with the NIST Cybersecurity Framework, Hitachi has engineered a data protection and management solution that includes multiple layers of safeguards to ensure data is secure and recoverable. The foundation of this solution is Hitachi Data Protection Suite (HDPS), powered by Commvault, providing organizations the most complete data protection with the broadest ecosystem coverage. When combined with Hitachi Content Platform (HCP) object storage, data is secure and protected through its entire journey.

The Hitachi Data Protection solution has multiple layers of security, response, and recoverability to combat ransomware attacks. These layers correspond to the Cybersecurity Framework as shown here:

- **Identify** – HDPS has several features to help identify potential risks, the most notable being **The Security Health Assessment Dashboard**.

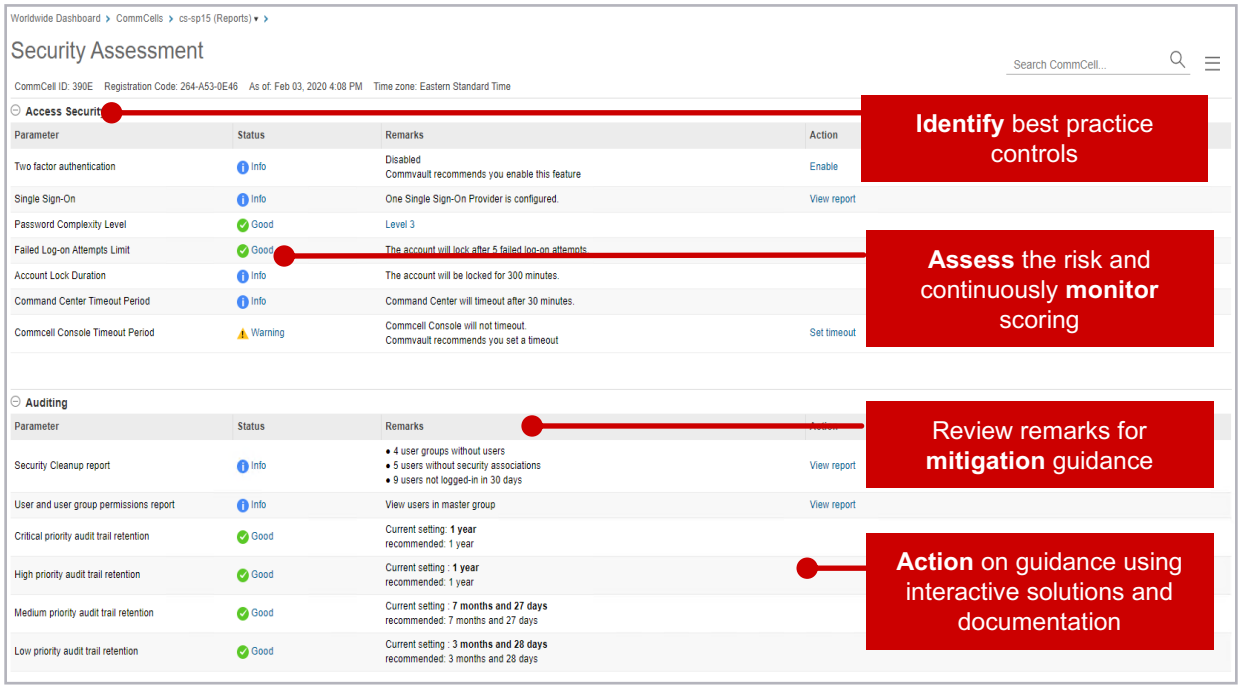

Fig. 2 HDPS Security Assessment Dashboard

This tool helps with the following:

- Identifying and assessing risk
- Mitigating risks with guidance and interactive solutions
- Monitoring for changes and new controls
- Managing risks through a single pane of glass

Beyond this dashboard, HDPS can also take the risk identification a step further with some functionality in their **File Storage Optimization** and **Data Governance** tools, shining light on silos of business-critical data, sensitive data (PII), and passwords. It can also identify cases of data sprawl and orphaned data, as well as access control gaps that leave data exposed to attackers.

- **Protect** – HDPS has several features to protect backup data as well as the backup application and infrastructure itself.

  These include:

  - **Zero trust** – **AAA Security** with advanced **Authentication** (with integrated MFA, certification authentication, CyberArk integration), **Authorization** (role-based security settings, authorization workflows, and FIPS-compliant encryption), and **Accounting** (full audit trail, machine learning events, SYSLOG/SIEM integration).
  - **Hardened infrastructure** – in accordance with CIS and STIG standards to remove all services, protocols, configs, daemons, etc. that are not integral to the operation of the system.
  - **Storage Locks and Air Gapping** – HDPS works in conjunction with the Hitachi Content Platform (HCP) to deliver immutable storage to ensure data is untouched and able to be recovered in the event of an attack. This is covered in greater depth later in the document. **Metallic® Recovery Reserve™ cloud storage** offers and easy, modernized air gap solution for another layer of recoverability.
  - **Data validation** – HDPS continuously validates backup data to ensure it is not compromised or corrupted. HCP provides **geographically dispersed erasure coding** to enable another layer of ensuring data is valid and uncorrupted.
- **Detect** – With HDPS, data is actively monitored at all times utilizing machine learning (ML) to continually improve how threats are uncovered – and all of it can be tracked and viewed from a single dashboard.

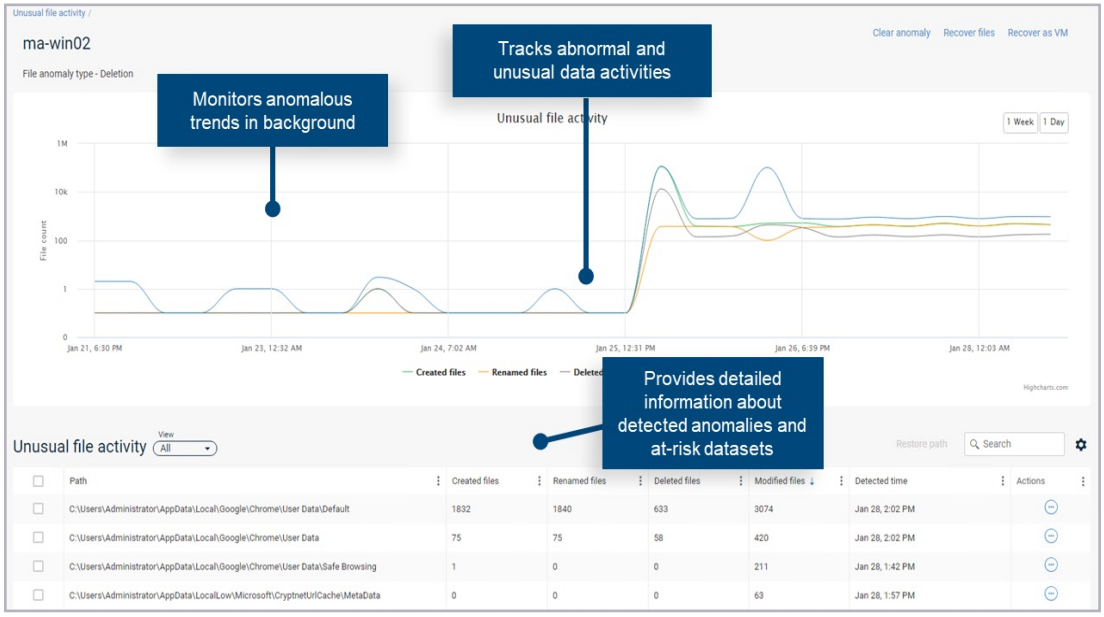

Fig. 3 HDPS Threat Monitoring Dashboard

This threat monitoring includes:

- **Active Monitoring** – anomaly detection, looking for changes or suspicious operations. Also monitors for bad malware extensions.
- **Backup Monitoring** – monitors anomalous change rates and activity between backup jobs
- **Honeypotting** – security mechanisms are put in place to mimic common attack vectors and attract potential attackers. When that 'honeypot' has its data changed, HDPS alerts that there is an active attack under way and begins remediation steps.
- **Event Monitoring** – monitors the HDPS infrastructure for login failures or other job-based anomalies that could indicate a threat in action.

- **Respond** – response time is critical when ransomware attacks occur, and HDPS ensures that you can quickly remediate those threats so you can safely move onto the recovery phase.

  This response includes:

  - **Removing Threats from Backups** – search backup data for infected files and remove them prior to system restores to avoid reinfection
  - **Validate Backups for Recovery** – as covered previously, HDPS backup data is continuously validated using CRC to ensure any data being restored is uncorrupted.
  - **Orchestration with Workflows and APIs** – using REST APIs, HDPS can integrate into existing SIEM and SOAR platforms (e.g. Splunk or ServiceNow) to manage and orchestrate actions and events centrally.
- **Recover** – Recovery with HDPS is as simple, fast, and flexible as possible with an array of features and options to ensure affected organizations get back online as soon as possible.

  These include:

  - **Recovery of Encrypted Files, Servers, or VMs** – recover via automated workflows with flexibility in where files are brought back online. Restore files in place, to a secondary location, or even to a new cloud instance to get online quickly if your primary site is still at risk.
  - **Built-in High Availability and Live Replication** – HDPS offers fully automated, orchestrated Disaster Recovery (DR) options to meet the most stringent RTO requirements.
  - **Granular File Search/Restore/Download/Delete** – HDPS enables a wide variety of options to ensure you can quickly locate important or affected files and remediate appropriately.

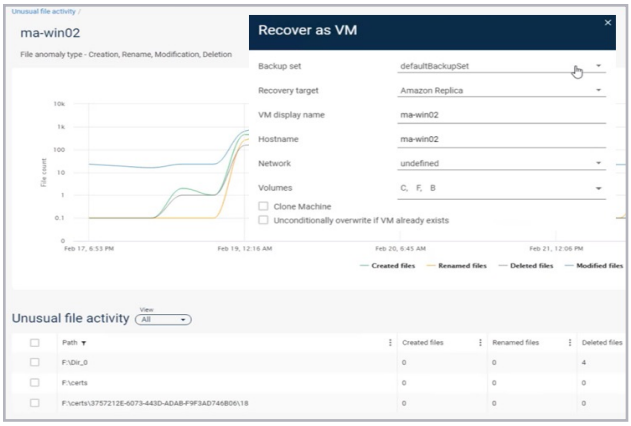

Fig. 4 HDPS VM Recovery Options

Immutable, Object Locked Backup Copies with HCP

As discussed in previous sections, it is imperative for any solution protecting against ransomware to have a trusted method to ensure the validity of their backup data. The most robust solutions have several different copies of data, including one or more copies in an immutable data store or air gapped location.

With Hitachi Content Platform (HCP), there is native capability to store data as **immutable**, undeletable, and write once, read many" **(WORM)**. These compliance features are built into the storage platform, making them easily configurable across different sets of files.

HCP for Cloud Scale has all of the compliance and immutability features as other HCP storage, but also has the capability to apply **S3 Object Locking** technology. Object Lock provides another layer of protection at the bucket-level, applied across all objects within that bucket. With immutable storage and S3 Object Lock, Hitachi Content Platform for Cloud Scale provides massively scalable, secure, performant storage with the necessary compliance and retention capabilities that enable enterprise-grade ransomware protection.

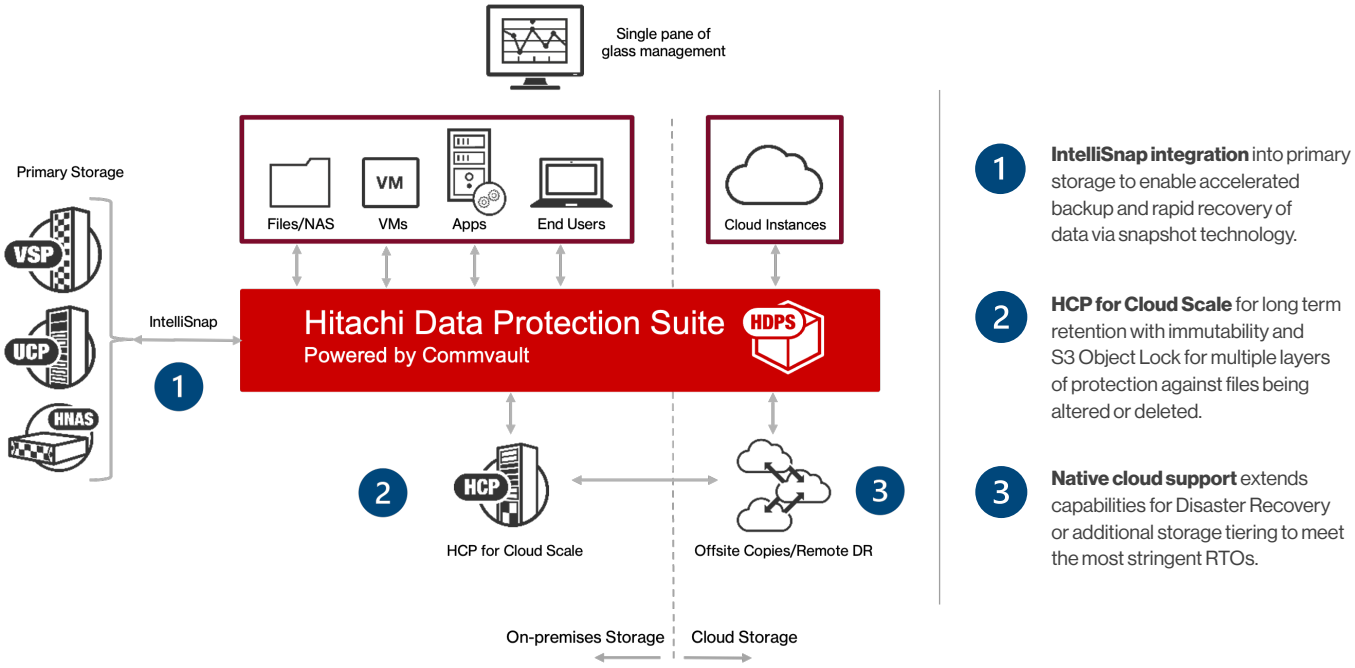

Fig. 5 Complete Ransomware Protection with HDPS and HCP

Summary

As ransomware threats continue to evolve and grow, CIOs and CISOs are making it a priority to mitigate these threats to avoid massive ransom payments, major data loss, or both. Cybersecurity threats are a substantial threat to business continuity, and there is no one proven method to preventing these attacks altogether. As such, NIST recommends a multilayered approach to protect organizations from these threats and ensuring recoverability when data is impacted.

To meet NIST standards, Hitachi Vantara has engineered a complete data protection solution that consists of many different layers of defense, including advanced identification and detection of threats, secure, immutable storage to protect against attackers, and native capabilities to respond and recover data quickly and easily. By combining the industry leading data protection capabilities of HDPS, powered by Commvault, with the massively scalable, industry leading object storage of HCP for Cloud Scale, organizations are ready for the threats of today and whatever might come tomorrow.

Learn more at: https://www.hitachivantara.com/en-us/partners/commvault.html

ABOUT HITACHI VANTARA

Hitachi Vantara, a wholly-owned subsidiary of Hitachi Ltd., delivers the intelligent data platforms, infrastructure systems, and digital expertise that supports more than 80% of the fortune 100. To learn how Hitachi Vantara turns businesses from data-rich to data-driven through agile digital processes, products, and experiences, visit hitachivantara.com.

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-CBE-SB-Protect-Recover-from-Ransomware-HDPS-HCP-14Mar23-A