WHITE PAPER

Businesses Modernize Data Protection With Hitachi and Commvault

Bringing Significant Value to Resilience, Simplicity, and Cost of Ownership

By Scott Sinclair, Practice Director
and Monya Keane, Senior Research Analyst
Enterprise Strategy Group

September 2025

Contents

Introduction

Achieving cyber resilience to safeguard vital data assets and maintain business continuity following a cyberattack or other unplanned disruption is an ever-evolving challenge. This urgency intensifies as enterprises manage data protection across increasingly complex, interconnected, and demanding digital environments and is now heightened by:

- A dramatic rise in artificial intelligence (AI)-driven ransomware attacks that make every organization a target, resulting in significant business downtime, loss of customer trust, lasting damage to brand reputation, and substantial financial losses and regulatory penalties.

- Disaster recovery plans that are insufficient to address/recover from ransomware attacks—92% of Enterprise Strategy Group survey respondents said they have experienced attacks explicitly targeting their backups.[1]

- Siloed data environments, outdated infrastructure, and limited IT and security team expertise, which can increase security vulnerabilities and threat vectors for cybercriminals to exploit.

- The explosion of AI across practically every industry, bringing with it the problem of managing and safeguarding the vast amounts of data needed to fuel it.

Questions to Align Cyber Resilience to Business Continuity Plans

Modern data protection requires having comprehensive answers to fundamental questions related to data security and data management, including regulatory compliance, and recovery in accordance with the organization's tolerance of business risk. For example:

- Does the organization know how long it will take to recover the business to a minimum viable state of operations following an incident?

- Does the organization have adequate visibility into the ways that sensitive data is being secured and recovered across the environment? According to Enterprise Strategy Group research, only 26% of organizations are confident in their ability to protect all mission-critical applications and data.[2]

- Could business operations continue if Active Directory, the backbone of identity and access, required a full forest recovery?

- Does it have air-gapped, immutable backup copies of mission-critical data, including Microsoft Active Directory, as a last line of defense against a ransomware attack?

- Does the organization's IT group know if its backup copies are good? In other words, when did they last verify those copies as being malware-free and uncorrupted?

- How is regulation affecting the organization's data resilience posture and processes? And who in the organization is responsible for ensuring that all data protection activities adhere to applicable regulations?

Knowing the answers to those questions is vital. This is all about ensuring that the business can remain operational despite disruptions, keeping in mind that effective data protection requires more than what any one technology can provide.

Keeping pace with the current situation is fueling a need to invest in modernization. Consider that, according to Enterprise Strategy Group research, 72% of organizations expected to increase spending on cybersecurity this year.[3]

---

[1] Source: Enterprise Strategy Group Custom Research commissioned by Commvault, *Preparedness Gap: Why Cyber-recovery Demands a Different Approach From Disaster Recovery*, December 2024.
[2] Ibid.
[3] Source: Enterprise Strategy Group Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

Hitachi Vantara and Commvault, two industry leaders, have demonstrated a 20-year commitment to addressing organizations' data security and resilience challenges. Their integrated solution, Hitachi Data Protection Suite Powered by Commvault (HDPS), helps enterprises modernize their data resilience and recovery capabilities to reduce business risk and improve the availability of operations, while also helping to control complexity and costs.

Recently, Enterprise Strategy Group was provided access to Hitachi Vantara and Commvault customers and field teams to gain greater insight into the drivers behind and benefits of the solution.
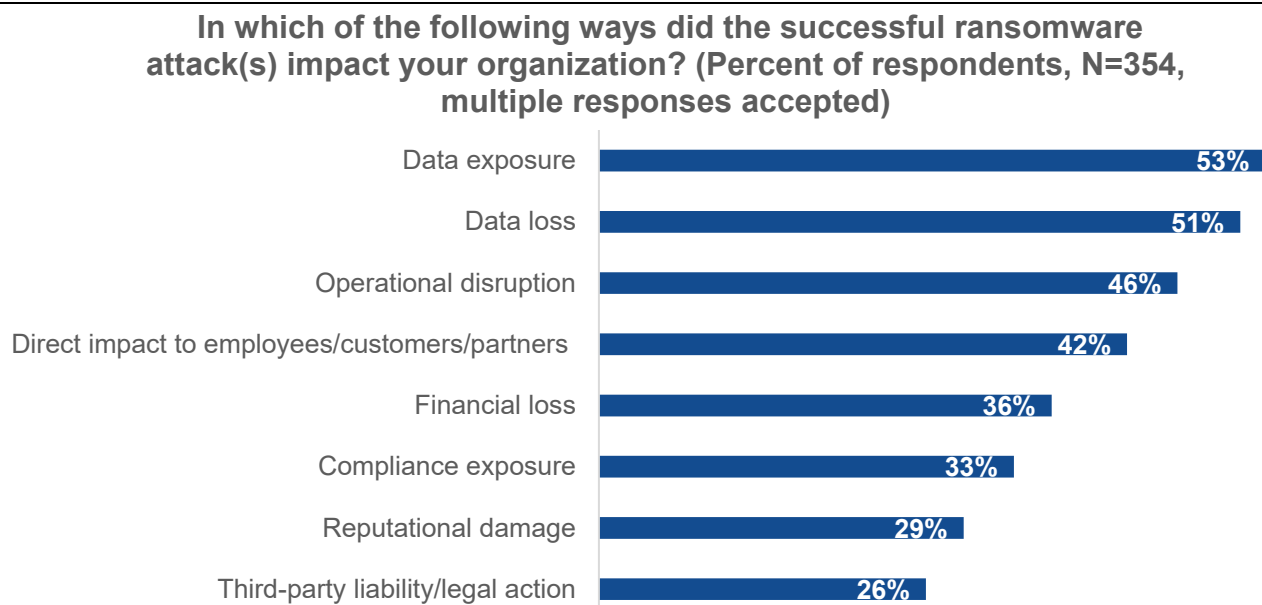
The interviews revealed important insights. Naturally, organizations often do not want to go public about their data protection solutions because of a fear of being targeted by threat actors. But solutions do exist that are protecting organizations successfully; we just don't hear about the cases in which companies are not negatively impacted.

The State of Cyber Resilience

It is worthwhile to examine Enterprise Strategy Group research, which validates the importance of the combined Commvault and Hitachi Vantara solution. Contemporary business depends upon digital operations, and digital threats are a top risk to operations and to the overall survivability of the business. The research showed that 89% of organizations ranked ransomware as a top-five threat to their viability.[4] Defending against ransomware attacks and recovering from them has already become a regular but necessary burden, with 75% of organizations having experienced a ransomware attack in the last 12 months. Of those, 75% were victims of a successful attack.[5]

Figure 1 showcases the business impacts of a successful ransomware attack. Beyond the operational disruption, the data loss, and the compliance exposure, data exposure/exfiltration was the most commonly reported impact.[6]

Figure 1. Impacts of a Successful Ransomware Attack

In which of the following ways did the successful ransomware attack(s) impact your organization? (Percent of respondents, N=354, multiple responses accepted)

Impact	Percent
Data exposure	53%
Data loss	51%
Operational disruption	46%
Direct impact to employees/customers/partners	42%
Financial loss	36%
Compliance exposure	33%
Reputational damage	29%
Third-party liability/legal action	26%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Data exposure and data exfiltration increase the business risk that a ransomware attack presents, and the combined cost and risk impact can exceed the temporary operational disruption in terms of harmfulness. Data is a

---

[4] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.
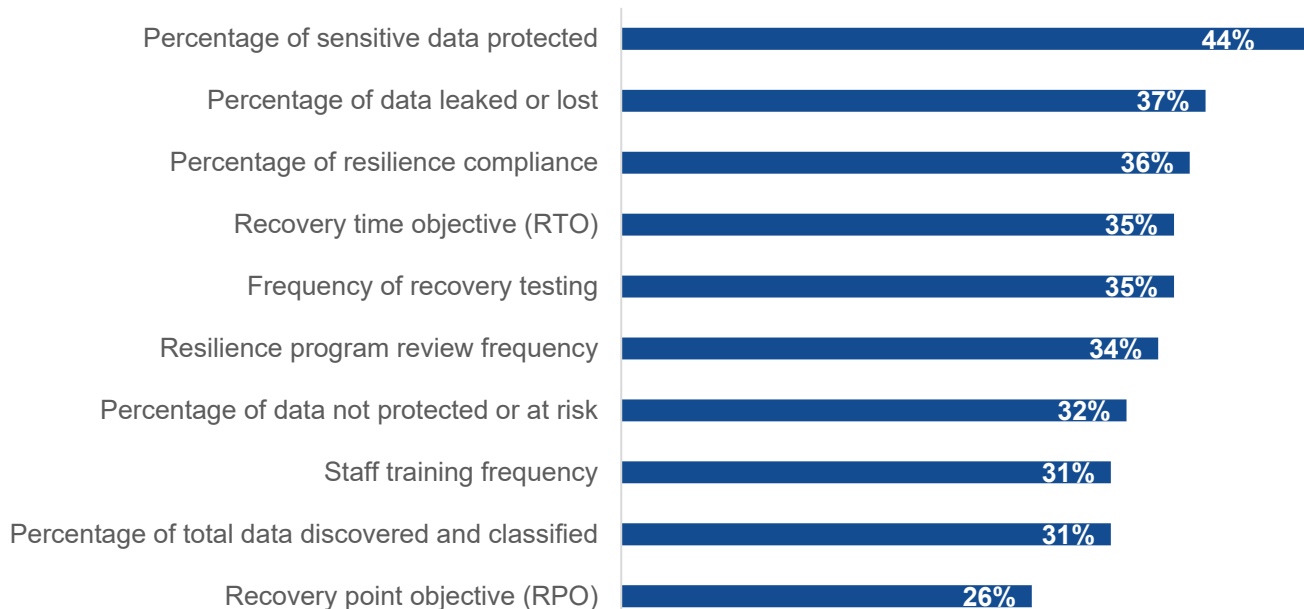[5] Ibid.
[6] Ibid.

valuable asset to businesses and bad actors alike, especially considering that 97% of businesses store personally identifiable information (PII) within their data sets.[7]

The risk of having that PII exposed has prompted increased regulatory requirements related to the handling and protection of data. Those new regulations make "standing still" even riskier, as well as making the effort to keep pace with future requirements more complicated.

When organizations measure the effectiveness of their resilience solutions, the ability to locate and protect sensitive data while adhering to regulatory requirements is among their main concerns (see Figure 2).[8]

Figure 2. Top Metrics Used to Track the Effectiveness of Data Resilience

What key metrics does your organization prefer for measuring value and effectiveness in data resilience solutions and deployments? (Percent of respondents, N=370, multiple responses accepted)

Metric	Percent
Percentage of sensitive data protected	44%
Percentage of data leaked or lost	37%
Percentage of resilience compliance	36%
Recovery time objective (RTO)	35%
Frequency of recovery testing	35%
Resilience program review frequency	34%
Percentage of data not protected or at risk	32%
Staff training frequency	31%
Percentage of total data discovered and classified	31%
Recovery point objective (RPO)	26%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The right path forward is to invest in modernization and establish partnerships with the right experienced vendors that can help to reduce the cost, time, and risk associated with improving a cyber-resilience posture. Specifically, businesses need to:

- Streamline and simplify with a trusted partner to reduce risk and optimize efficiency.
- Accelerate and scale their ability to protect, back up, and store data.
- Accelerate their ability to restore their business to a viable state of operation.
- Ensure that their data is protected, secured, and compliant.

---

[7] Source: Enterprise Strategy Group Research Report, *Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance,* September 2024.
[8] Ibid.

Hitachi Data Protection Suite Powered by Commvault Strengthens Data Protection and Cyber Resilience

The explosion of data being collected and generated by organizations increases the importance of having robust capabilities to efficiently protect data at massive scale and then rapidly restore it if an incident occurs. Commvault is a leader in cyber-resilience technology, and Hitachi Vantara is a leader in enterprise storage. Their partnership in developing Hitachi Data Protection Suite Powered by Commvault is more than an OEM reseller agreement; it provides deep engineering integrations and services collaboration to provide a comprehensive approach to cyber resilience and business continuity.

For organizations, HDPS offers multiple technical advantages:

- **Immutable, indelible data copies** to enable clean recoveries with Commvault Air Gap Protect on Azure, AWS, Google, and OCI.

- **Secure and rapid recovery for Active Directory** in hybrid cloud environments, from granular object-level restores to forest-level recovery so organizations can quickly re-establish identity services after outages or cyberattacks while maintaining security and compliance.

- **HDPS IntelliSnap** allows organizations to create and protect snapshots and immutable snapshots on Hitachi storage arrays to meet demanding RPOs for mission-critical Tier 0 and Tier 1 workloads in the event of a cyberattack.

- **Early threat warning, anomaly detection, and continuous scanning** of backups with Commvault Threat Wise and Threat Scan, in addition to role-based access controls to secure sensitive data with Commvault Risk Analysis.

- **The ability to live-mount replicas** in place to enable operations to continue during recovery.

- **A disaggregated architecture** that supports data mobility across hybrid cloud environments.

- **AI-assisted automation and insight** to speed response and simplify cyber-resilience-related operations.

- **The ability to establish an on-premises, isolated recovery environment** (Hitachi Data Fortress) or to spin up an on-demand, isolated environment in Azure or AWS with Commvault Cloud Cleanroom. Recovery enables testing of recovery flows, validation of clean copies, and forensic analyses.

Similarly, HDPS offers organizations valuable real-world, business-level benefits:

- **Reduced risk and business downtime:** With comprehensive capabilities to secure, defend, and orchestrate rapid recoveries, organizations are enabled to prepare for, withstand, and rapidly recover from unplanned disruptions and cyberattacks.

- **Enable cyber resilience strategies:** Supporting incident recovery and minimum viability business strategies following a cyberattack or unplanned disruption, including complex, dynamic applications such as Active Directory.

- **Simplified management:** Unified data resilience operations and storage management across on-premises, edge, and cloud with the ease of the HDPS single pane of glass interface. This eliminates multiple tools for data protection, reduces the administrative burden, streamlines vendor management, and enhances organizations' agility in meeting new requirements.

- **Support compliance obligations:** HDPS offers data management and compliance solutions that are designed to meet industry standards and that enable a business to centralize data management operations, identify and secure sensitive data, and comply with evolving regulatory compliance requirements. This includes providing automated audit and reporting capabilities.

Case Study: Optimizing Mission-critical Resilience and TCO for a Transportation Infrastructure Firm

Enterprise Strategy Group spoke with an IT infrastructure team leader at a public enterprise responsible for railroad infrastructure, focusing on the enterprise's experience with the HDPS solution. This organization had been experiencing a challenge following the decision by its previous data protection partner to raise costs to a price point that exceeded what the budget could support. The organization needed to keep the trains running safely while lowering its total cost of ownership.

"We had a financial conflict with [our previous partner]," the team leader said. "As a public enterprise, it was impossible for us to support the brutal price increase that [this partner] was envisioning." Instead, the organization reached out to Hitachi Vantara, its data center infrastructure provider, explained that it couldn't absorb the price increase, and said that it needed another solution.

Demanding Requirements for Speed and Petabyte Scale

This is an organization managing a massive data environment comprising approximately 18 petabytes, and it must back up thousands of virtual machines. It is also under extreme pressure to adhere to numerous, highly stringent rules and regulations.

When sizing the requirements for a new data protection solution, it was working under certain constraints. As a public company, it is mandated to retain backups for 35 days. The organization takes one full backup every week, and several incremental ones over the course of those seven days. According to the infrastructure team leader, "We have to manage a global capacity of data that is already pretty big, and we have to manage our backup window from 5:00 pm to when business is back, which is around 7:30 am."

Uninterrupted Operations and Data Security in Mission-critical Infrastructure

Those backups need to be pristine and available to this mission-critical environment because lives are at stake. The environment supports a system that permits the organization to see, every second, where each train is situated— and to stop them if they're on a collision course. "That system cannot break, and it cannot be stopped," the team leader said. "If it were, all trains on every track would stop. Imagine a situation where all trains stop, and it takes two or three hours to get back on schedule. That is not possible."

Several aspects of the HDPS solution stood out to this organization. One core consideration was that it had to be able to handle massive scale while ensuring that the organization could continue to meet its backup and time-to-recovery objectives. The team leader said, "We had to find a solution capable of supporting a lot of data while offering a manageable restoration time. I'm pretty happy about the Hitachi Vantara and Commvault solution. It's working well, and we have very good, responsive support. Now we are working on a new contract to ensure their presence in our data centers."

Business Continuity Relies on Fast Recovery

Another consideration for this organization related to business continuity was the solution's highly effective snapshotting capability. "The snapshotting capability is really interesting in regard to its ability to back up a really big environment of data pretty fast," the team leader said. "If we are facing a long restoration time, then we have to be working with a solution that permits us to continue business while we are restoring."

Virtualization for Seamless Maintenance

The organization saw value tied to the ability to run applications in the backup environment. "That feature was especially interesting: You can mount an existing backup, present it as a VM, and start it while you are restoring the backup," the team leader said. That is an efficient way to restore databases that, in this organization, can be up to

2PB, which can take time to restore. The ability to virtualize a physical environment that was backed up and then be able to put it back into production while undergoing a maintenance operation proved to be extremely interesting. As the team leader explained, "Let's say I need to swap my CPUs in a bunch of machines. I can take backups of those physical machines, mount them as VMs, start them, and point users to that virtual environment."

Case Study: Trusted Data Protection for a Federal Banking Institution

Enterprise Strategy Group was also able to speak with a member of the Hitachi Vantara field team regarding a federal banking customer. The federal bank's previous solution was not meeting its needs, prompting it to look for data protection alternatives. It already had a longstanding relationship with Hitachi Vantara, which helped accelerate initial conversions and the project.

For this bank, what mattered most was having a trusted partner. The reputation of the partner was even more important than the specifics of the individual solution. This is an important consideration. Cybersecurity and data resilience represent evolving targets. Maintaining resilience requires continued innovation from the partner, beyond just a point solution. "Reliability was very important," the field team member said. "The decision-makers at the bank preferred the Hitachi Vantara brand, especially Hitachi Vantara's 100% data availability guarantee."

This organization was able to achieve several benefits following implementation. For example, it was able to simplify both its data protection portfolio and its support experience in general, thus reducing the burden on its internal personnel. "The bank is very pleased to have one consolidated solution to manage its infrastructure, backup, and security," the field team member reported.

The bank has experienced high levels of resilience post deployment. According to the field team member, it has experienced "no data breaches, and no data losses. Other institutions have been hit with ransomware attacks, but this bank has never had a ransomware issue, never had data loss, and always has business continuity."

Case Study: Consolidating Resilience and Compliance at a Multi-campus University

A member of the Hitachi Vantara field team also spoke with Enterprise Strategy Group regarding a university customer. This university spans 24 campuses. Each one was using its own data protection solution and had its own specific compliance requirements. The university needed to scale and consolidate its approach to data protection and management. Essentially, it had to simplify and reduce its costs, all while not sacrificing capability.

The overarching goals were to:

- Reduce the complexity of data protection operations on administrators.
- Ensure that each campus could continue to follow the same protection policy subsets it needed.
- Be able to support the specific compliance requirements of individual campuses.

In other words, the university was looking for consolidated, multi-site protection that enabled it to specify protection and compliance capabilities by individual campus.

The field team member said, "What also mattered was that we could provide a compliance package in that consolidated approach to make sure compliance requirements were met." Notably, Commvault offers comprehensive tagging and self-service capabilities with role-based access control and granular control over how data is recovered or deleted to meet GDPR requirements, along with retention and archiving to make it easier for organizations such as this university to manage compliance requirements.

"We see a lot of these multi-site protection scenarios," the field team member said. "Other providers approach it on a one-by-one basis. We approach it at a higher level, and we then ensure that each site is able to meet its specific data-related requirements."

The university also appreciated having the ability to leverage HDPS running on Hitachi Vantara object storage to simplify management of the data protection environment. Specifically, it is able to monitor protection-related processes and hardware with a combined dashboard that includes alerts and reporting capabilities.

Case Study: Predictable Protection for Financial Services

As part of this project, Enterprise Strategy Group spoke with a member of the Hitachi Vantara field team regarding a financial services customer. This customer approached Hitachi Vantara, seeking a predictable data protection solution that would minimize downtime. That was an important factor because the financial services firm had a high cost of downtime, estimated to be between $250,000 to $400,000 per hour.

The organization sought to maximize the number of predictable recovery points in time without costs escalating. It had a target recovery time of four hours, according to its service-level agreement. The field team member reported that the Hitachi Vantara storage and HDPS solution "was able to get that recovery window down to one hour with no extra cost."

For this financial services industry customer, the solution was able to better protect incremental changes to the data set, enabling IntelliSnap hardware-accelerated snapshots to be captured during the day "rather than all the data copy efforts having to take place in the off hours," the field team member said.

According to Hitachi Vantara, the solution, once deployed, was able to provide "near-instant protection and near-instant recovery."

Conclusion

While many technologies aim to protect enterprise data, Hitachi Vantara stands out with a long-standing track record of delivering trusted storage solutions to thousands of organizations worldwide, including those with strict data integrity and availability requirements.

HDPS powered by Commvault is tightly integrated with Hitachi storage systems. As Commvault's premier OEM partner, Hitachi brings 20 years of co-engineering expertise, supporting over 1,300 joint customers, securing more than one exabyte of data, and holding 1,500 patents. Together, they offer a powerful, proven foundation for cyber resilience, scalability, and data mobility.

HDPS enables IT teams to optimize backup and recovery performance and streamline operations. With unified visibility, verified clean recovery, and air-gapped, immutable copies of critical data, Hitachi and Commvault deliver a trusted solution for organizations with complex workloads, strict compliance needs, and zero tolerance for downtime. Beyond protection, they enable enterprise cyber resilience that evolves with new requirements, helping organizations reduce risk while maximizing ROI from their data protection investments.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com