

WHITE PAPER

Hitachi Vantara and Veeam for Cyber Resilience

Enhancing Cyber Resilience
While Improving Data Management

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

April 2025

This Enterprise Strategy Group White Paper was commissioned by Hitachi Vantara and Veeam
and is distributed under license from TechTarget, Inc.

Contents

Introduction 3

The Cyberthreat Landscape Is Poised to Become More Dangerous to Businesses 3

Effectively Managing Business Risk Is Impossible Without Also Managing Cyber-risk 5

Hitachi Vantara and Veeam Are Simplifying Data and Cyber Resilience 6

Integrated Data Protection and Management With a Flexible, Immutable Cyber Infrastructure 7

Conclusion 8

Introduction

Nearly every facet of modern business relies on maintaining cyber resilience. After all, cyber-risks lead directly to business risks. Any disruption to digital operations costs time, money, and customer trust.

Digital assets are many companies' most valuable resources to begin with, and the risks associated with data loss or data exfiltration can often exceed the cost of an outage itself. Additionally, business growth necessitates scaling the digital infrastructure environment, which often increases the attack surface and attracts additional attacks.

According to research from Enterprise Strategy Group, 89% of organizations ranked ransomware as a top-five threat to their overall viability.¹ Research also showed that cybersecurity is the top technology initiative that organizations considered to have become significantly more important to their futures over the past two years (cited by 59% of respondents), and ransomware preparedness was specifically mentioned by 23% as having become significantly more important.²

With the rise of artificial intelligence (AI), cyberthreats such as ransomware are poised to become even more prevalent and dangerous. Establishing a strong cybersecurity posture is like trying to hit a moving target—threats are continually evolving. Therefore, cyber resilience involves more than having good technology in place; it also requires instituting ongoing practices that include collaboration among multiple technologies, processes, and people.

For IT and data protection professionals specifically, the priority must be to ensure cyber resilience and data recovery. As part of a zero-trust strategy, they need to assume a breach will happen; thus, rapid detection, response, and recovery at scale will all be essential to establish. When it comes to cyber resilience, organizations must be able to reliably, quickly, and confidently recover known-good, clean data and ensure that high-value, sensitive data is being protected across all platforms.

The proven alliance between [Hitachi Vantara](#) and [Veeam](#) can help today's organizations simplify data protection and recovery to strengthen their cyber-resilient posture. The partnership's definition of cyber resilience encompasses intelligent threat governance, protection and portability, detection, and recovery. Such a level of resilience enables organizations to protect their data across platforms so that it is available whenever and wherever it's needed.

The Cyberthreat Landscape Is Poised to Become More Dangerous to Businesses

Enterprise Strategy Group research provided additional context into the rising importance of cyber resilience modernization as attacks become more sophisticated. It appears that defending against and recovering from ransomware attacks has already become a regular part of operating a business today. Consider that 75% of surveyed organizations reported that they have experienced a ransomware attack in the last 12 months, and three-quarters of those attacks were successful.³

¹ Source: Enterprise Strategy Group Research Report, [Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](#), December 2023.

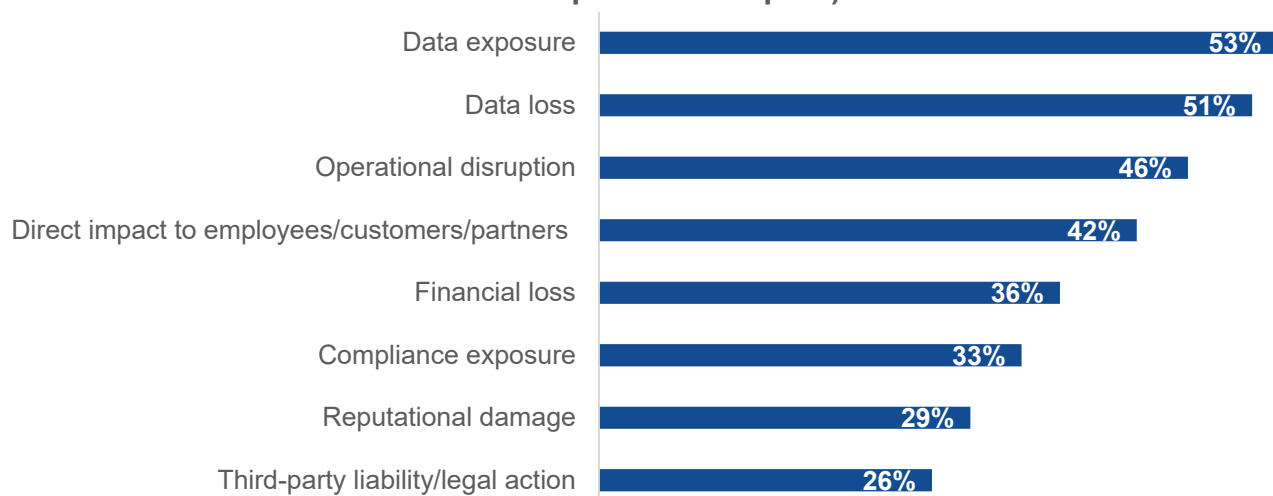
² Source: Enterprise Strategy Group Research Report, [2025 Technology Spending Intentions Survey](#), December 2024.

³ Source: Enterprise Strategy Group Research Report, [Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](#), December 2023.

Figure 1 illustrates the business impacts of a successful ransomware attack. Beyond the operational disruptions and data losses, data exposure was the most common response.⁴

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)



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

The likelihood of data exposure and exfiltration represents the main business risk of a ransomware attack. The combined cost and risk impacts can even exceed the temporary operational disruption. Downtime is extraordinarily expensive, with costs that include lost revenue, lost productivity that affects deadlines, recovery costs, and legal or compliance penalties. Reputational damage to the company can also factor in.⁵ All of that illustrates why rapid recovery is so important.

Data is a valuable commodity to businesses and bad actors alike, with 97% of businesses now storing personally identifiable information (PII) somewhere within their data sets.⁶ The value of that PII data, in particular, will inevitably prompt increases in future attacks.

And, with the advent of generative AI (GenAI), the threat landscape is poised to shift significantly and rapidly, with the frequency and severity of attacks increasing as a result. According to research, 62% of organizations expected their cyber adversaries to gain advantages thanks to continuing GenAI innovation.⁷

Digital business initiatives have become so essential to daily life that governmental regulations such as the European Union's Digital Operational Resilience Act have recently arisen to "force the issue" and ensure that businesses invest appropriately to build resilience against cyberattacks. Of course, new regulations increase the business risk of standing still, while also increasing the complexity involved in simply keeping pace.

The right path forward requires investing in modernization and partnering with experienced players to reduce the cost, time, and risk associated with improving and maintaining a cyber-resilience posture.

⁴ Ibid.

⁵ Source: Damon Garn, "[Avoid the high costs of downtime for small businesses](https://www.techtarget.com/searchdisasterrecovery/feature/Disaster-recovery-for-small-businesses-leaves-no-room-for-excuses)," Techtarget.com, June 2024.

⁶ Source: Enterprise Strategy Group Research Report, [Achieving Cyber and Data Resilience: The Intersection of Data Security Posture](https://www.techtarget.com/searchdisasterrecovery/feature/Disaster-recovery-for-small-businesses-leaves-no-room-for-excuses)

[Management With Data Protection and Governance](https://www.techtarget.com/searchdisasterrecovery/feature/Disaster-recovery-for-small-businesses-leaves-no-room-for-excuses), September 2024.

⁷ Source: Enterprise Strategy Group Complete Survey Results, [Beyond the GenAI Hype: Real-world Investments, Use Cases, and Concerns](https://www.techtarget.com/searchdisasterrecovery/feature/Disaster-recovery-for-small-businesses-leaves-no-room-for-excuses), August 2023.

Effectively Managing Business Risk Is Impossible Without Also Managing Cyber-risk

Cyber-risk equates to business risk, and minimizing that risk requires collaboration among data protection and recovery technologies, malware detection technologies, and other threat detection technologies. Minimizing risk also involves taking into account processes and people spanning the IT, compliance, and cybersecurity teams.

Often, the bulk of the cyber-resilience burden falls to backup operations and cybersecurity teams, who must ensure that the business can identify and track high-value, sensitive data such as PII, while also protecting and recovering data, applications, and business operations to a minimally viable status as rapidly as possible.

Cyber resilience success will always amount to hitting a moving target, and it cannot be done with a single investment, vendor, or team. Having the right processes and partners in place is essential. In fact:

- 89% of surveyed organizations agreed that cyber resilience requires an ecosystem of integrated technologies and vendors.⁸
- 75% of organizations agreed that preparing for cyber resilience is going to affect how teams are organized.⁹

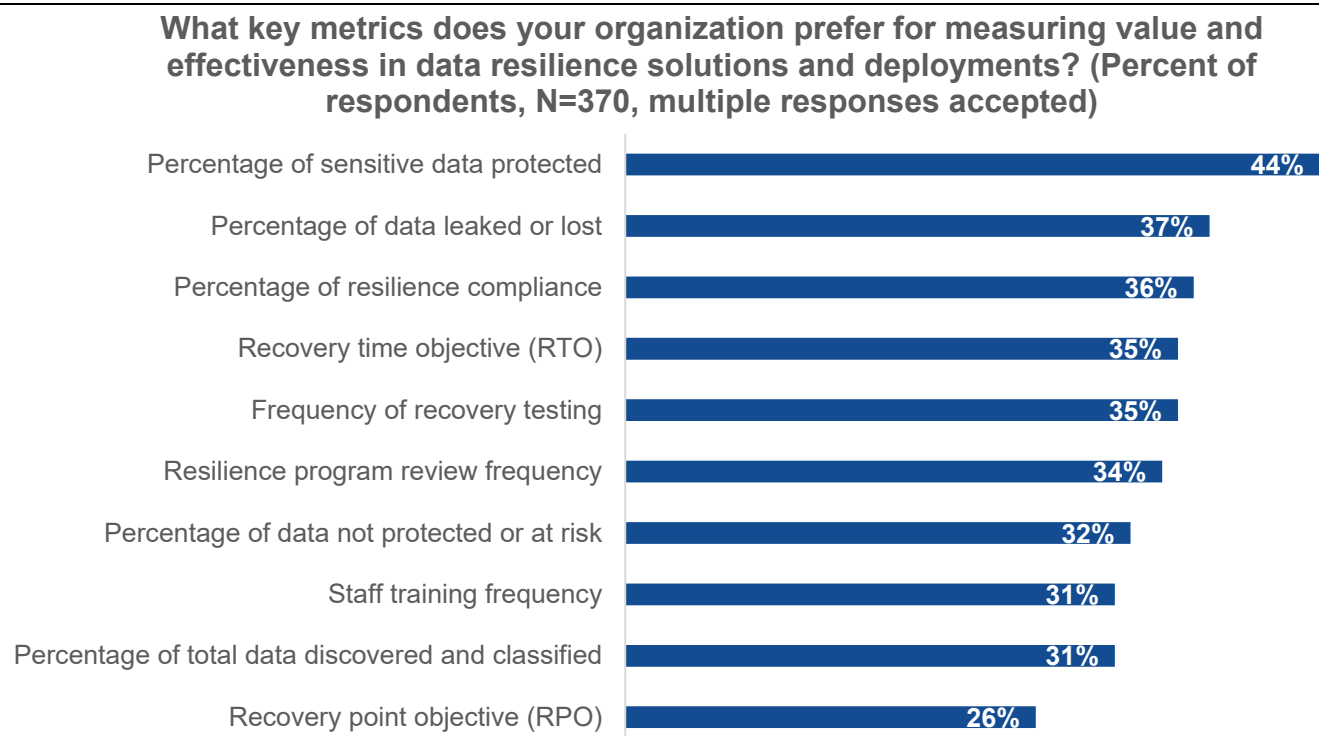
Achieving cyber resilience is practically impossible if an organization can't track and measure its progress. Figure 2 offers insight into how organizations prefer to measure value and effectiveness in cyber resilience-related improvements.¹⁰ Organizations reported that the focus of these improvements is on:

- Understanding and measuring how much sensitive data is under protection.
- Being able to quickly identify when any data is leaked or lost.
- Maintaining compliance.
- Accelerating recovery point objective/recovery time objective (RPO/RTO) at scale.
- Frequent recovery testing, which is a critical element in ensuring that processes in place are sufficient.

⁸ Source: Enterprise Strategy Group Complete Survey Results, [Data Resilience Emerges: The Collision of Data Discovery, Protection, Security, and Governance](#), September 2024.

⁹ Ibid.

¹⁰ Ibid.

Figure 2. Top Metrics in Use to Track the Effectiveness of Cyber Resilience

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

It is not surprising that the [National Institute of Standards and Technology \(NIST\) 2.0 cybersecurity framework](#) recently added “govern” to the framework’s core tenets (joining “identify, protect, detect, respond, and recover”). The addition of governance to the NIST cybersecurity framework reinforces the importance of managing ongoing processes, testing, and reporting to ensure that the organization is keeping pace with an ever-evolving threat landscape.

Hitachi Vantara and Veeam Are Simplifying Data and Cyber Resilience

The value that Veeam and Hitachi Vantara bring as partners helps organizations modernize their cyber-resilience capabilities to strengthen their cybersecurity posture. Again, no single technology, vendor, or team can deliver complete cyber resilience. A key value point of the Hitachi Vantara/Veeam alliance centers on simplifying and streamlining cyber resilience through seamless integration and speed to enhance the customer experience.

IT organizations face a wealth of digital demands and priorities from the rest of the business, often now tied to increased investments in AI initiatives. More than ever, IT organizations will need to lean on technology provider partners for help with simplification, especially considering that 60% of surveyed IT decision-makers said their IT environments have become more complex in the last two years, with the increasing and evolving cybersecurity landscape the most commonly reported reason why (cited by 42% of organizations).¹¹

Responsibility falls to the vendor community to reduce not only the complexity of their own solutions, but also the complexity associated with integrating multiple technologies. The partnership between Hitachi Vantara and Veeam

¹¹ Source: Enterprise Strategy Group Research Report, [2025 Technology Spending Intentions Survey](#), December 2024.

exemplifies what decision-makers should look for in regard to potential partnerships, as well as exemplifying the benefits that seamless integration combined with simplicity can deliver.

The partnership is designed to deliver the simplicity and integration inherent in a single solution, while offering added functionality via data protection software from Veeam and cyber infrastructure technology from Hitachi Vantara. This is a highly scalable joint solution with cost-efficient yet powerful protection for midsize and large enterprises. Reliability/trust is rooted in Hitachi's customer reputation and 100% data availability guarantee.

However, this alliance is not only about technology, but also about the people and processes that enhance the overall customer experience.

The Hitachi Vantara and Veeam partnership delivers numerous high-level benefits to businesses:

- It is a single, trusted alliance with a track record of cyber resilience and compliance innovations, offering a “one-stop-shop” experience that can provide a complete solution, from the initial tailored assessment to the final deployment.
- Both vendors have deep experience in accelerating deployment and reducing risks related to deployment, which reduces budget impacts and alleviates impacts on internal personnel.
- Hitachi Vantara and Veeam have consolidated the management experience. A single console simplifies data lifecycle control and minimizes the confusion that can otherwise occur during protection and recovery operations.
- Integration is at the backup and snapshot level, offering complete immutability for hardened, comprehensive hybrid infrastructure protection.
- Better RPO: Hitachi high-capacity, efficient storage and Veeam snapshot orchestration enable a shorter RPO at scale.
- The solution offers the flexibility/scalability needed to scale to meet large enterprise requirements, while being efficient, powerful, and cost-effective enough for midsize organizations.

The Hitachi Vantara/Veeam partnership is the foundation behind a solution that can offer tremendous value to organizations looking to deploy an infrastructure and data management solution including threat governance, protection and portability, detection, and recovery.

Integrated Data Protection and Management With a Flexible, Immutable Cyber Infrastructure

The software component of the solution, the Veeam Data Platform, provides many capabilities, including:

- Data protection suited for today's diverse modern application environments, providing backup, recovery, portability, security, and intelligence that spans cloud, edge, data center, and SaaS apps (including support for Kubernetes and container-based applications).
- Malware and ransomware detection during and post backup.
- Automated, low-impact testing to efficiently manage complex recovery plans, enhance resilience, and prove compliance with dynamic test reports.

The infrastructure components come from Hitachi Vantara's enterprise hybrid cloud cyber storage technology:

- Hitachi VSP One, which is a multi-protocol (block, file, and object) hybrid cloud data platform that can be deployed on premises or within public cloud environments backed by a 100% data availability guarantee and 5-star rating for ransomware protection.

- VSP One Object offers high-performance, immutable object storage. It comes with compliance capabilities including S3 object lock to preserve data for regulatory retention periods or legal hold purposes.
- It is scalable and reliable, with intelligent data services (i.e., multiple data protection options and synchronous/asynchronous replication).

Not surprisingly, this combined solution provides plenty of real-world benefits, including:

- **Simplified cyber resilience and compliance.** Hitachi Vantara and Veeam offer data management for compliance-related use cases. As organizations endeavor to mature their cyber-resilience capabilities, these features are absolutely critical to better understand, track, and monitor sensitive data.
- **Rapid recovery at scale.** Veeam and Hitachi Vantara claim to offer near-zero RTO and shorter RPO disaster recovery as well as ransomware recovery for VM and bare-metal environments. This is backed by Hitachi lab testing showing recovery up to 1,500 virtual machines in 70 minutes.
- **Consolidated protection, regardless of the application environment.** The combined solution can protect diverse modern application environments that span cloud, edge, data center, and SaaS apps, including support for Kubernetes and container-based applications.
- **Native storage complete immutability.** Veeam Data Platform applies immutability to the data stores that its software leverages as backup copies. And when used with VSP One Object, the backup data gets an added level of immutability—the platform offers inherent immutability in how the storage stores object data. That added level of immutability helps organizations remain confident that their known-good data will stay good.
- **Accelerated data backup and recovery with Veeam’s storage snapshot orchestration.** Organizations can restore data via Veeam Explorer for Storage Snapshots, and they can access granular recovery from enterprise applications such as Oracle, SQL Server, SharePoint, and Exchange.
- **A 100% data availability guarantee.** Hitachi Vantara’s enterprise storage technology comes with a 100% availability guarantee from the company. This guarantee, combined with Hitachi Vantara’s experience in enterprise storage, adds further confidence that recovery data will stay protected.
- **Flexibility.** The solution offers power and scalability for large enterprises, while being efficient and cost-effective for midsize organizations. Examples of its flexibility include a choice of:
 - Backup source (file, object).
 - Backup target (block, file, object).
 - Backup storage provider.
 - Object and file storage.
 - Deployment model.

This solution also provides minimum-impact data movement and replication, a policy-driven data lifecycle for retention/portability, and scalability to move to new storage environments.

Conclusion

When it comes to reducing business risk, achieving a mature cyber-resilience posture offers advantages versus continuing to follow a traditional protection strategy.

But beyond reducing risk, maintaining resilience while improving data management capabilities can provide advantages in terms of staying compliant with regulations, with compliance becoming more and more intertwined with resilience. This approach can even bolster GenAI and other internal initiatives on the horizon.

To keep pace in today’s cyber-vulnerable, cost-conscious world, streamlining cyber resilience is essential to maintaining cost-effectiveness. That means organizations require more from their vendor community. This alliance

between Hitachi Vantara and Veeam makes a lot of sense, and it is an excellent example of what organizations should require.

Find more information here: <https://www.hitachivantara.com/en-us/solutions/data-protection-cyber-resiliency>.



©2025 TechTarget, Inc. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

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