Connection
we solve IT

TOP ENTERPRISE DISASTER RECOVERY TRENDS AND STRATEGIES

Based on insights from 100+ enterprise IT decision-makers

Hewlett Packard Enterprise

Nearly two-thirds of enterprises have faced ransomware or malware threats in the past year.

Executive Summary

As enterprises increasingly rely on digital operations, the stakes for effective disaster recovery and data protection have never been higher. Despite advancements in technology, many organizations continue to grapple with significant challenges in their disaster recovery strategies. According to a recent survey we conducted in partnership with Foundry of 106 enterprise IT decision-makers, a substantial portion of enterprises exhibit weak security measures or high-risk exposure.

What can enterprises do to improve their security posture? Here's a deeper look at our survey's findings on enterprise disaster recovery trends in the market, their impact on security threats, and how enterprises can best reduce complexity and improve productivity when managing and operating backup infrastructure.

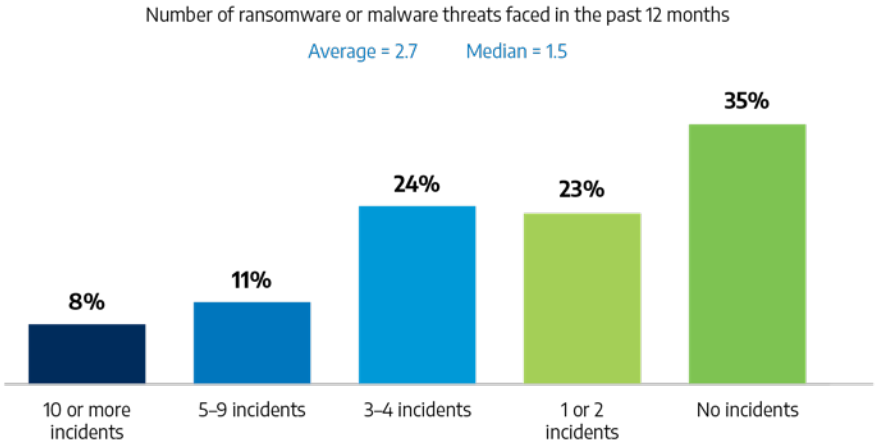
Ransomware and Malware Threats

Nearly two-thirds of enterprises have faced ransomware or malware threats in the past year, with an average of 2.7 incidents per organization. The gap in robust security protocols and the increasing sophistication of ransomware and malware mean that enterprises must continuously evolve their defenses.

The impact of frequent security breaches extends beyond the immediate disruption of operations. When an enterprise experiences repeated attacks, the ripple effect can lead to substantial financial losses. Costs associated with downtime, data recovery, and potential ransom payments add up quickly. Moreover, reputational damage from security breaches can have long-term adverse effects on customer trust and business continuity.

45% of enterprises feel their backup infrastructure is well-aligned with their organizational demand.

Almost two-thirds of enterprises surveyed experienced at least one ransomware or malware threat in the past 12 months, indicating a significant portion of respondents has weak security measures or higher risk exposure.



Misalignment of Backup Infrastructure and Demand

One reason for the gap in robust security protocols could be a misalignment between backup infrastructure and demand. Only 45% of enterprises feel their backup infrastructure is well-aligned with their organizational demand. This misalignment indicates a significant portion of enterprises are struggling to match their backup capabilities with their actual needs.

The primary challenge stemming from this misalignment is the difficulty in appropriately provisioning resources. Organizations that over-provision may find themselves wasting valuable resources and budgets on unnecessary infrastructure. Conversely, under-provisioning can leave companies vulnerable, with insufficient capacity to handle data recovery needs.

The inefficiencies caused by this misalignment have a direct impact on both costs and performance. Over-provisioning leads to higher operational expenses, as organizations spend more on storage and maintenance than necessary. On the other hand, under-provisioning can result in reduced performance during recovery operations, potentially causing prolonged downtime and data loss. These scenarios not only inflate costs but also degrade the overall effectiveness of the backup and disaster recovery strategy.

Complexity of Managing Multiple Point Solutions

Another pain point when managing and operating backup infrastructure is having to manage multiple point solutions and the increased complexity they introduce. According to our survey, enterprises have a median of 3.5 point-solutions for backup and recovery. Over one-fifth (21%) have five or more point-solutions.

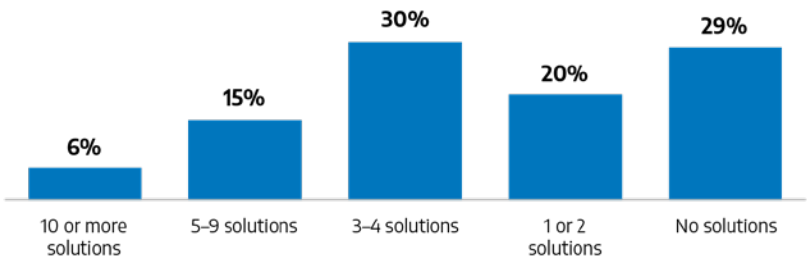
IT teams often struggle with integrating various tools and ensuring they work seamlessly together. This fragmentation not only complicates management but also hinders overall efficiency.

As a result of this complexity, IT teams are forced to spend excessive amounts of time on integration and maintenance tasks. The constant need to troubleshoot and manage these disparate systems can hamper the overall productivity of IT departments, emphasizing the need for more streamlined, comprehensive solutions.

More than one-third (36%) of enterprises report that they do not have a global protection policy.

Number of point-solutions used for backup and recovery

Average = 3 Median = 3.5



Inconsistent Data Protection

More than one-third (36%) of enterprises report that they do not have a global protection policy in place. The absence of consistent data protection policies is particularly problematic in today's complex IT environments, which often include hybrid and multi-cloud setups. Each environment can have different security requirements and protocols, making it challenging to maintain a unified approach to data protection.

Inconsistent policies inevitably lead to security gaps and increased vulnerability to data breaches. Without a comprehensive, overarching policy, organizations are at a higher risk of experiencing data loss or unauthorized access. This inconsistency not only compromises data integrity but also increases the potential for regulatory non-compliance, which can result in hefty fines and legal repercussions.

Recommendations for Addressing Backup and Recovery Challenges

By recognizing these challenges and moving toward comprehensive solutions and consistent protection policies, enterprises can significantly enhance their data security posture and operational efficiency.

Here are five key recommendations to help close security gaps and boost overall productivity and cost efficiency when managing and operating backup infrastructure.

Organizations with a global protection policy report fewer incidents (average 2.3 vs. 3.0).

1. Adopt comprehensive backup and recovery solutions

While less than one-third of enterprises have a comprehensive backup and recovery solution, almost half (43%) of respondents say they prefer the simplicity of an all-in-one solution. And for good reason: a comprehensive backup and recovery solution simplifies management and reduces overhead, allowing IT teams to focus more on core business activities rather than being bogged down by the intricacies of integrating and maintaining numerous systems.

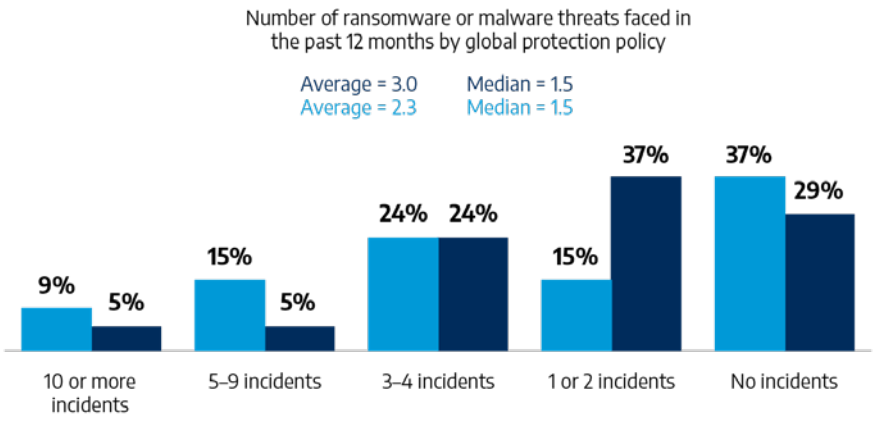
Recommendation: Implement a comprehensive backup and recovery solution to streamline processes and reduce the complexity associated with managing multiple point solutions.

2. Implement global protection policies

Organizations with a global protection policy report fewer incidents (average 2.3 vs. 3.0). Having a consistent and comprehensive protection policy enhances overall security, ensuring that all parts of the organization are equally protected. Moreover, those with a global protection policy feel they are better aligned between provisioning vs. demand and are likely to have fewer single point solutions. In fact, they are more than 5X as likely to have a single consolidated solution as those without a global protection policy.

Recommendation: Establish and enforce global protection policies across all environments, including on-premises, hybrid, and multi-cloud setups, to reduce the frequency of incidents and enhance your organization's resilience against data breaches.

Organizations with a global protection policy not only experience fewer incidents, but also have a higher percentage of reporting no incidents compared to those without it.



Connection
we solve IT

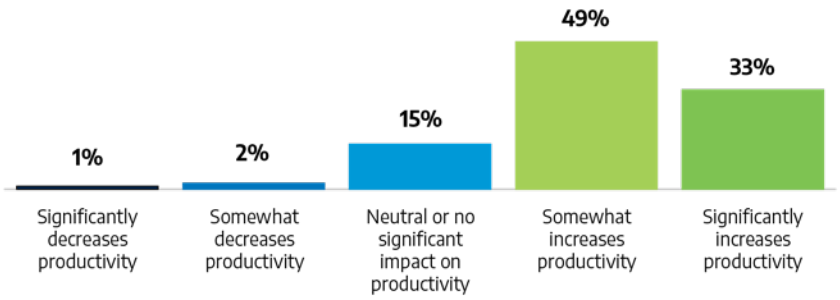
3. Leverage hybrid cloud backup for improved productivity

For 82% of respondents, managing and operating backup infrastructure across the hybrid cloud somewhat (49%) to significantly (33%) increases productivity. This is because hybrid solutions combine the best aspects of on-premises and cloud environments, offering greater flexibility and scalability that allow organizations to adapt quickly to changing needs and demands.

Recommendation: Use hybrid cloud backup solutions to optimize IT infrastructure to ensure that resources are used efficiently and that the IT infrastructure can grow in line with business requirements.

For 82% of respondents, managing and operating backup infrastructure across the hybrid cloud somewhat (49%) to significantly (33%) increases productivity.

Impact of managing and operating backup infrastructure across the hybrid cloud

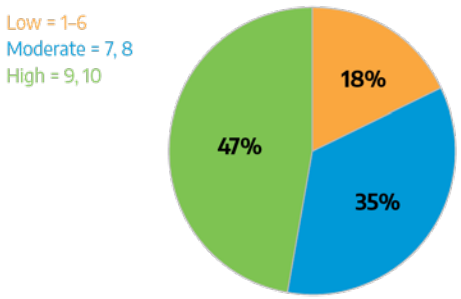


4. Focus on cost and storage efficiency

Almost half (47%) of enterprises rate saving backup storage capacity and reducing costs as highly important. By focusing on cost and storage efficiency, organizations can significantly reduce their overall expenses and maximize resource utilization. Efficient storage management not only lowers costs but also improves the return on investment (ROI) for backup solutions, making them more economically sustainable in the long term.

Recommendation: Prioritize backup solutions that offer efficient storage management and cost-reduction features. Technologies like data deduplication and compression can play a crucial role here.

Saving backup storage and capacity and reducing the overall cost of protecting data



Connection
we solve IT

Hewlett Packard Enterprise

5. Ensure scalability and flexibility

For 85% of respondents, scalable solutions without upfront costs are highly (41%) or moderately (44%) important. Scalable and flexible backup solutions provide the necessary agility to adjust resources as needed, avoiding unnecessary expenditures and ensuring optimal performance. This adaptability is crucial in managing costs effectively while maintaining high levels of data protection and operational efficiency.

Recommendation: Choose backup solutions that allow for on-demand scalability. This means selecting systems that can expand or contract based on the organization's current needs without requiring significant upfront investments.

Turn to Your Trusted Partners

Building a backup and recovery strategy is complex—that's why we're here to help. Turn to the Connection experts for help in selecting the right HP GreenLake Server solutions and Connection services to ensure your organization is protected—no matter what.

Connection we solve IT

Contact your Connection Account Team to learn more about creating a backup and recovery strategy that works for your organization.

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/BackupRecovery

Methodology and Demographics

The research and associated charts in this report are from an online survey sponsored by Connection and conducted by Foundry from May 9–23, 2024. This study was designed to understand the enterprise disaster recovery strategy trends in the market and their impact on security threats. A total of 106 IT-decision makers at companies with 500 or more employees globally with an enterprise disaster recovery strategy (or strategies) in place that were neither fully on-premises or fully in the cloud were surveyed. All respondents held a manager or above level role in IT.