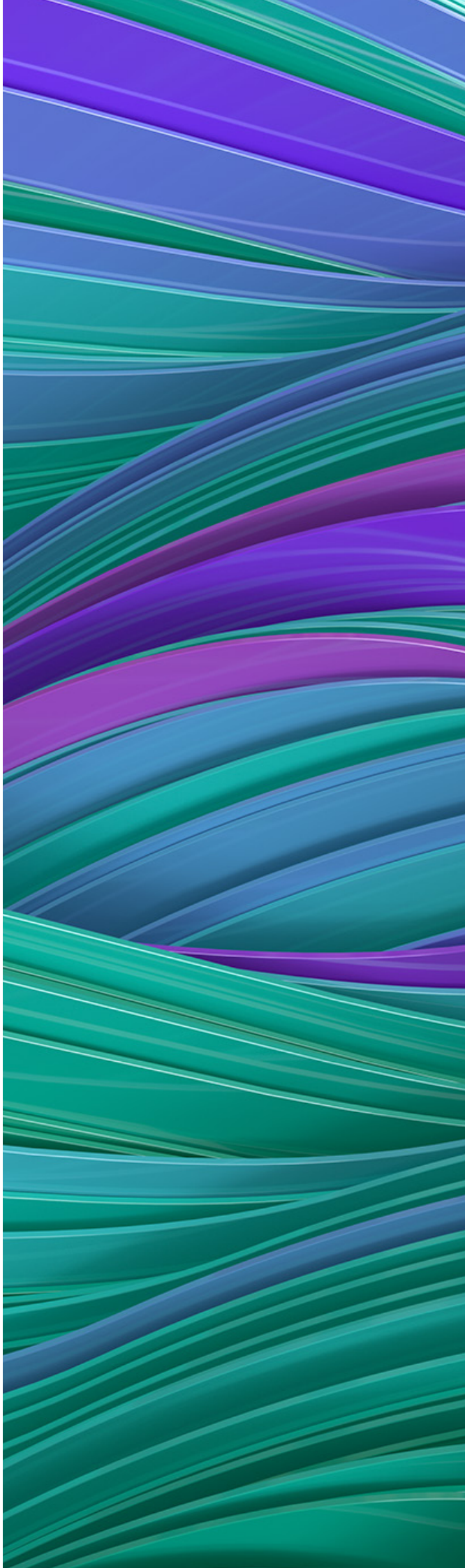
HPE GreenLake

Business white paper

Understanding the breadth and depth of modern data protection

Why getting ahead of modern data threats requires edge-to-cloud data security and protection

Table of contents



Executive summary

Data represents an enterprise's most valuable asset. Yet, many organizations fall short in their attempts to treat data with the care it deserves. As threats grow more serious, modernization and transformation efforts push data into a bewildering array of silos and novel hosting environments — from edge to cloud. This complexity results in data becoming more vulnerable to attack by today's sophisticated hackers.

Existing approaches to data protection are increasingly deficient. Historically, customers' basic approach was to copy the data that changed in each production environment and store that copy in another, secondary location. It was usually done once per day during off-peak hours, typically late at night to avoid impact to infrastructure performance. This periodic approach leaves much to be desired in our changing world where cyber threats abound, posing the following challenges to IT organizations trying to protect, recover, and secure an enormous and ever-growing amount of data:

- Inability to quickly counter cyberattacks such as ransomware and malware
- Complex management and operation, with multiple administration touchpoints and maintenance of data protection software and hardware on-premises or in hybrid cloud environments
- Data silos with fragmented point solutions
- Increased cost, capacity overprovisioning, and underutilization of resources because of ineffective planning for data growth or — in the worst case — under-provisioning resulting in increased risk
- Exploding data growth, demanding recovery service-level agreement (SLA) requirements, and an evolving threat and compliance landscape — all continuing to put pressure on costs and intensify risk
- Data loss between the current moment of recovery and the last good copy of data
- Long, complex recovery times that hinder an ability to get back to business as usual

What's needed is comprehensive and consistent data protection to help ensure that data integrity and availability are continuously maintained, regardless of location and hosting platform. A robust solution that operates 24x7 and keeps data backed up in its entirety, ready for immediate recovery, is key to mitigating the potential damages of ransomware and other adversarial attacks.

Introduction

The good news is advanced technologies make consistent, effective data protection a reality. Modern backup and disaster recovery (DR) solutions can break down data silos and protect data, whether it is at rest or moving from one location to the next, throughout the data lifecycle.

This white paper discusses the importance of adopting a secure data protection strategy with a broad, unified, and continual approach to guard against data loss or compromise due to unwanted intrusions, specifically being held hostage by ransomware or code being modified by malware. In a world of prolific cybercrime attempts on all types of industries, utilities, and government installations, IT organizations must not let their guard down for a moment.

Data protection vs. data security

For this white paper, the difference between data protection and data security is distinguished as follows:

- **Data protection** — A pervasive, holistic program of controls, processes, and countermeasures that helps ensure data availability and integrity, regardless of where it is located.
- **Data security** — Specific processes and protocols that protect data from threats, malicious actors, or even accidental deletions where it is stored, when it is in movement, and when it is being processed.

Explosive data growth, increased risk

Most IT organizations are inundated with more data than ever before and yet they are expected to secure that data using outdated technology, setting themselves up for potential technological disaster. A recent survey by IDC, sponsored by Zerto, a Hewlett Packard Enterprise company, found that 93% of organizations surveyed have suffered data-related business disruption and 68% of them experienced more than four events that resulted in business disruption.[1]

With the prevalence of cyberattacks, the chances of experiencing a data breach have become very high, representing a significant risk to business operations. The same survey determined that respondents had experienced on average 19.3 cyberattacks (of all types) and 2.3 ransomware attacks within the past 12 months. And of the respondents who had experienced an attack, 83% indicated that at least one attack resulted in data corruption. Of greater concern, 60% also experienced unrecoverable data loss within that same 12-month period.

It's no wonder that enhancing data security and protection is a priority for today's IT organizations. Siloed data, data growth, increasing ransomware/malware threats, and data sprawling across the core, cloud, and edge have contributed to unprecedented complexity and greater risk of data loss for companies worldwide.

Consequences of malicious data attacks

This virtual state of emergency calls for a plan to reduce data risk exposure by avoiding data breaches in the first place and preventing data damage due to unauthorized modification. The consequences of malicious attacks on data can result in:

- Reputation damage to companies
- Inability to function in the short or long term or even permanent shutdown
- High costs of remediation
- Strict compliance penalties (such as privacy laws)
- Potential loss of competitive advantage in the marketplace

[1] "State of Ransomware and Disaster Preparedness for 2022," IDC, May 2022

A broader strategy for bigger threats

Clearly, a different approach is essential for every organization to efficiently eliminate the growing risk of data loss, mitigate threats from increasingly sophisticated ransomware, and achieve rapid data recovery following a small or large incident. A broad-based, secure data protection strategy must be adopted, one that spans across the enterprise and beyond to include all corporate outposts (branch offices), remote workers, and partnering entities who are granted access to data while engaged in joint projects and collaboration.

A broader strategy also involves protected hybrid cloud backups in conjunction with rapid recovery processes to reduce the risk of downtime and improve cyber resilience in the face of constant and evolving ransomware threats.

How data protection works

Data protection includes data security, but it also encompasses data backup, recovery, archiving, DR, and business continuity. Furthermore, data protection must be continuous and comprehensive to be successful — simple, strong, and seamless. Therefore, multipoint solutions are simply inadequate. And since the location and use of data constantly change, data protection must keep pace to reduce the risk of data loss, achieve rapid data recovery, scale with automation to protect against evolving threats, and cover data mobility across the entire data lifecycle.

Data vulnerability — Closing the ransomware gap

As corporate data now resides at countless locations outside the perimeter of the traditional firewall, it is exposed to serious vulnerabilities, resulting in an ever-widening security gap to grapple with. For example:

- A 2022 survey revealed that 94% of attackers target backup repositories, and 72% of the attempts are at least partially successful.[2]
- In that same survey, 52% of respondents report a disconnect in the interactions between cyber and business continuity/disaster recovery strategies in their organizations, noting that improvement is required.
- In 2023, it was reported that 43% of cyberattacks target small businesses, of which 60% of victims go out of business within six months.[3]

This level of exposure opens the door to future attacks and complicates the data recovery effort.

Zero-day malware is also becoming more common, so antivirus software does not necessarily protect against these evolving threats. Backing up your data is crucial, but the key to effectively recovering from ransomware lies with granularity. Traditional backup methods don't provide this granularity, putting most organizations with infrequent backups at increased risk if their systems become infected. They may even lose days' worth of data, which could be disastrous and costly to the organization.

[2] "Paying the ransom is not a good recovery strategy," Help Net Security, May 2022

[3] "30 Surprising Small Business Cyber Security Statistics," Fundera, 2023

An ideal solution to avoid ransomware casualties is one that uses continuous data protection (CDP) with always-on replication and granular journaling to enable the fastest and most effective recovery possible. CDP enables rapid recovery after an attack without losing untenable amounts of data. The alternative of paying the ransom and hoping to decrypt all your data is not a quick or reliable road to recovery. A high percentage of organizations choose to pay the ransom with mixed results — according to the 2022 survey, a third of those that paid[4] were still unable to recover all their data.

No industry is safe from hackers and cybersecurity threats, making it important for all companies to take stock of their existing cybersecurity programs by performing a data risk assessment to identify gaps and then take action to close those gaps.

Cybersecurity trends and challenges

Forecasters predict that cybercriminals are not letting up. Quite the contrary, they are driving up IT organizational challenges in the process. According to Cybersecurity Ventures:[5]

- Ransomware will cost the world economy $265 billion per annum by 2031.
- Cybercrime will grow 15% year-over-year for the next three years.
- Cybercrime will reach $10.5 trillion by 2025.
- An expected 3.5 million cyber-roles will be open by the end of 2023.

Further trends suggest:

- Only 55% of organizations will have implemented a cloud-centric data protection strategy by 2025.[6]
- 51% struggle to protect complex and dynamically changing attack surfaces.[7]
- 50% struggle with complexity and inability to integrate security solutions, creating gaps in defenses.[8]

Benefits of modern data protection

The implementation of modern data protection offers many undeniable benefits to organizations of any size, particularly as the overwhelming deluge of data grows and fragmentation makes it difficult to effectively protect data in the cloud, core, and increasingly at the edge.

Modernizing data protection can help break down silos of the past to stem the tide of worsening data risk exposure. A new, integrated approach can secure data against ransomware by simplifying and automating backup, replication, and recovery operations, thereby enabling rapid data recovery. Importantly, encrypted data copies make your protected data inaccessible to cyberattacks, even ransomware. Additional benefits include long-term data retention, data mobility, immutable backups, and the regular testing of data resilience.

Data protection as a services

Within the realm of the prevailing subscription-based, as-a-service cloud environment, modern data protection across the hybrid cloud is another offering to consider.

[4] "Paying the ransom is not a good recovery strategy," Help Net Security, May 2022

[5] "2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics," Cybercrime Magazine, May 2023

[6] "State of Ransomware and Disaster Preparedness for 2022," IDC, May 2022

[7, 8] "The 2022 Study on Closing the IT Security Gap," Ponemon Institute Research Report sponsored by HPE, January 2022

- **Data protection as a service (DPaaS)** — Cloud-based or web-delivered software as a service, which enables organizations to protect their data and applications by securing their network and providing recovery options.
- **Disaster recovery as a service (DRaaS)** — Moves an organization's computer processing to its cloud infrastructure in the event of a disaster.
- **SaaS-based backup** — Streamlines backup operations with a global protection policy for the consistent protection of on-premises and cloud-native workloads across the hybrid cloud.

Leaving the job of securing enterprise data to experts in the field is a smart, cost-effective solution to protect your most valuable asset, data.

The right services, with the right technologies and the right experts

Hewlett Packard Enterprise and Zerto offer data protection solutions from edge to cloud, to help you manage your risk. Our security experts understand it's not a matter of if you will be attacked or infiltrated by hackers, but when.

HPE and Zerto offer new ways to innovate with improved agility, manage costs, secure data and address sophisticated ransomware attacks plus other cyberattacks. Flexible cloud-native data services and next-generation data protection solutions include:

- Ransomware resilience, disaster recovery and multi-cloud mobility services with Zerto
- SaaS-based backup with HPE GreenLake for Backup and Recovery

Together, they provide the flexibility to modernize data protection. The innovations span from rapid recovery to ransomware protection and long-term data retention, along with immutability for on-premises and the public cloud with operational simplicity. They help further accelerate HPE's overall transition to a cloud services company with the intent of giving you greater choice and freedom for your business and IT strategy, with an open platform that delivers a seamless cloud experience, regardless of location.

With the ability to migrate data and workloads to and from the cloud, backup and data recovery are enabled for on-premises, cloud-native, and SaaS workloads, giving you the flexibility to optimize your solutions.

HPE and Zerto stand ready to solve data protection issues in these three key areas:

1. **Comprehensive and consistent data protection**

   Modern, edge-to-cloud data protection help ensure continuous availability via simple, fast recovery from disruptions, globally consistent operations, and seamless app and data mobility across multiple clouds.

2. **Efficient backup and recovery**

   Streamline operations and minimize risk with a single management console and global protection policy for consistent orchestration capabilities for all your on-premises virtual machines or cloud-native workloads, such as Amazon EBS volumes, EKS clusters, and EC2 or RDS instances.

3. **Protection from ransomware attacks**

   HPE and Zerto help organizations defend their businesses from the consequences of ransomware, with a fully orchestrated failover and failback solution that helps in the recovery of infected or compromised applications and data. Downtime can be limited to minutes and data loss to mere seconds.

Partner with HPE and Zerto to modernize data protection

It's time to break down data silos and secure your organization's data against ransomware, recover from any disruption, and protect virtual machine workloads across on-premises, hybrid cloud, and multicloud environments. Our experts help you redefine and manage your backup and recovery process effortlessly with the simplicity and flexibility of the cloud experience — and achieve modern data protection to tackle cyber threats and ransomware attacks head-on. You will get the right blend of DR, backups, and archives auto-configured and auto-managed for protecting enterprise data and applications.

No enterprise is exempt from managing day-to-day adversarial data threats and, as research has shown, this will persist well into the future. Companies cannot afford to maintain the status quo when it comes to data protection across the growing tens of thousands of devices and locations, including the cloud.

In a highly distributed operating environment, a broader approach to protecting data must look at where it is stored, where it is consumed, and who owns it. Stronger, more integrated measures are necessary to win this technology war being waged on an escalating scale. Organizations also need the flexibility to modernize and continue along their digital transformation path without roadblocks stopping them in their tracks or inhibiting innovation to move their business forward.

Modern data protection — from ransomware safeguards to rapid data recovery and long-term data retention — is required either on-premises or in the public cloud. And it must be provided with operational simplicity and efficiency, meeting every service-level agreement (SLA) at an affordable cost for companies to adopt without hesitation.

Conclusion

It's never too late to create a resilient data protection strategy to continuously protect enterprise data dispersed all over the world and recover it as quickly as possible when compromised. The right kind of modern data protection may very well be the key to business survival in the 21st century.

Learn more at

Protect all your data. All the time. Zerto, a Hewlett Packard Enterprise company

Protect data effortlessly with HPE GreenLake for Backup and Recovery

Visit **HPE GreenLake**

Chat now (sales)

Hewlett Packard Enterprise

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50009795ENW, Rev. 1