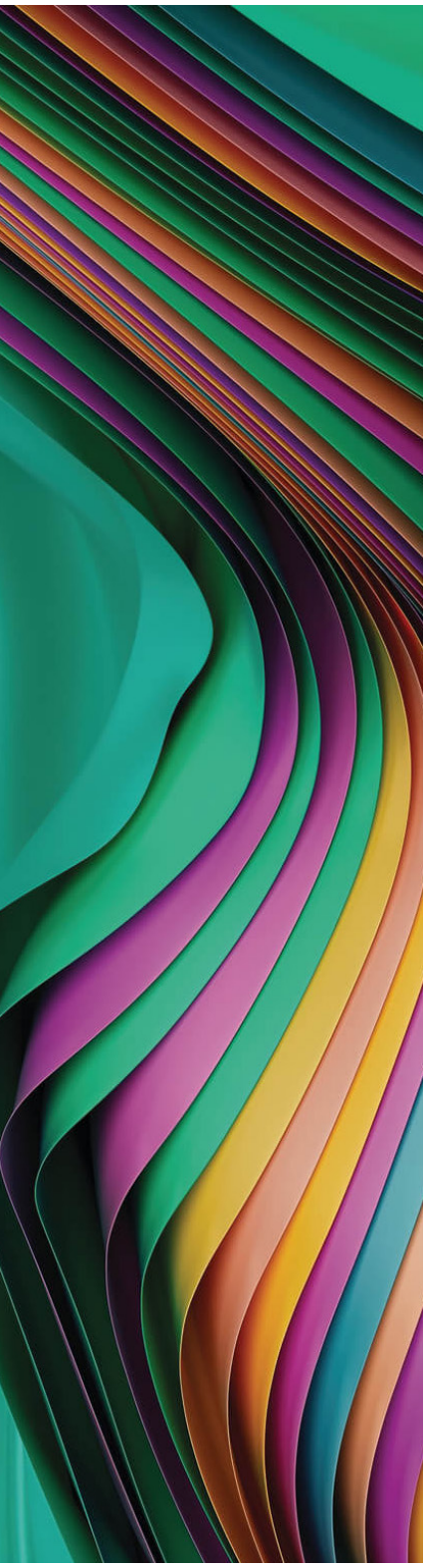
Understanding the necessity of continuous and secure data protection

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

HPE GreenLake

Table of contents



Executive summary

Data represents an enterprise's most valuable asset. Yet, many organizations fall short in their attempts to treat such a valuable asset with the care it deserves. As threats to data grow more serious, modernization and transformation efforts push data in many forms 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 extremely sophisticated hackers.

Existing approaches to data protection are increasingly deficient. Historically, the basic approach was during off-peak hours to copy the data that changed in each company's production environment and store that copy in another, secondary location. This 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 backup software and hardware on-premises or in hybrid cloud environments
- Creating 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—underprovisioning 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 intensifying risk
- Data loss between the last good copy and longer recovery times

What's needed is comprehensive and consistent data protection (a program of controls, processes, and countermeasures) that ensures data integrity and availability are continuously maintained, regardless of location and hosting platform—as well as a robust backup and recovery solution that operates 24x7 to ensure data is backed up in its entirety and ready for immediate recovery to mitigate the potential damages of ransomware and other adversarial attacks.

Introduction

The good news is advanced technologies make continuous and secure data protection a reality. These include backup and disaster recovery as-a-service options and more. The goal is to 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 prevent 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 around the world, we cannot let our guard down for a moment.

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

- **Data protection**—a pervasive, holistic program of controls, processes, and countermeasures that ensures the availability and integrity of data, regardless of where it is located.
- **Continuous data protection (CDP)**—a protection mechanism that allows organizations to continuously capture and track data modifications, automatically saving every version of the data that the user creates locally or at a target repository.
- **Data security**—protects data from threats, malicious actors, or even accidental deletions where it is stored, when it is in movement, and when it is being processed. This should be essential to your data protection strategy.

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 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.

Furthermore, IDC reported that of the respondents who had experienced an attack, 83% also indicated that at least one attack resulted in data corruption. Of greater concern, however, is that 60% also experienced unrecoverable data loss within the past 12 months.

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.[2]

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 from 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 permanently shutting down
- High costs of remediation
- Strict compliance penalties (such as privacy laws)
- Potential loss of competitive advantage in the marketplace

For these reasons alone, thorough data protection needs to be top of mind. This awareness is spreading among IT decision-makers, 51% of whom now view enhancing data security and protection as their #1 priority.[3]

A broader strategy for bigger threats

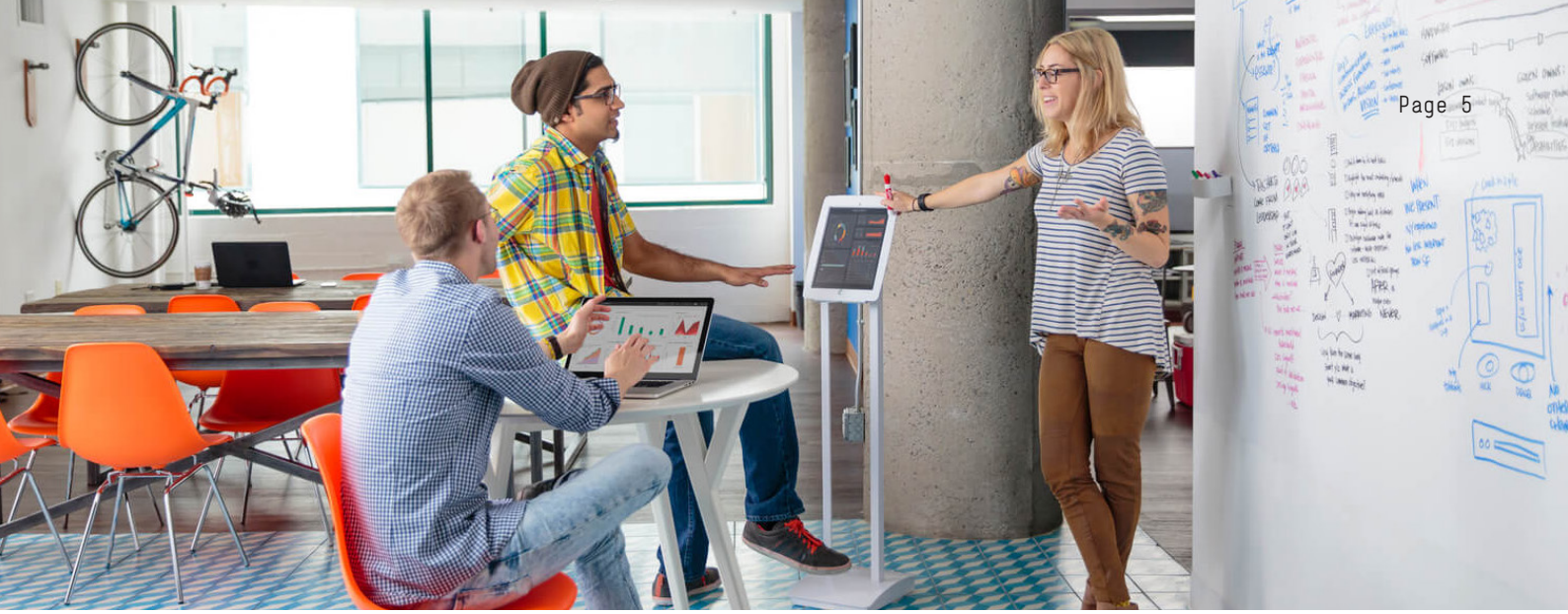
Clearly, a different approach is essential for every organization to efficiently eliminate the growing risk of data loss, mitigate threats from increasingly sophisticated ransomware, and achieve rapid data recovery following a small or large incident. This calls for the adoption of a broad-based, continuous, and secure data protection strategy 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 secure hybrid cloud backups in conjunction with rapid recovery processes to reduce the risk of downtime and improve cyber resiliency in the face of constant and evolving ransomware threats. Conventional data recovery methods are simply too limited and too fragmented.

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

[2] "Using data protection as a service to address modern data threats," IDC technology spotlight sponsored by HPE, November 2021

[3] "The Role of ESG Programs in IT Decision Making," ESG, September 2022



"Most ransomware attacks can be avoided through good cyber-hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed. Our recommendation is that businesses need to be proactive because the decryption keys are not always provided when ransoms are paid and being proactive is often easier and less costly than a reactive approach."

– Raj Samani, CTO for Europe at Intel® Security

How data protection works

Data protection includes data security but it also encompasses data backup, recovery, archiving, disaster recovery, and business continuity. Furthermore, data protection must be continuous and holistic 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 eliminate 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 be grappled with. For example:

- In 2021, it was reported that 91% of industrial organizations were vulnerable to cyberattacks.[4]
- A survey conducted by ESG showed that 47% of organizations surveyed experienced ransomware attacks on at least a monthly basis in 2021 and 73% suffered at least one successful attack.[5]

Also, approximately half of ransomware attack victims describe a breach of sensitive infrastructure configuration data. This level of exposure opens the door to future attacks and complicates the data recovery effort. Based on the statistics mentioned previously, these percentages are not apt to go down anytime soon.

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.

The ideal solution to avoid ransomware casualties is one that continuously backs up and provides granularity to enable the fastest and most effective recovery possible. When backups are protected, recovery from an attack that threatens to delete or modify data should be complete and fast, and at the least, relative to restoring conventional backups. The alternative of paying the ransom and hoping to decrypt all your data is definitely not a road to a quick recovery. A high percentage of organizations do pay the ransom;[6] however, a third of those that paid were still unable to recover all their data.[7]

Don't gamble with the threat of ransomware.

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.

[4] "Information security risks at industrial companies," Positive Technologies, September 2021

[5] "The Long Road Ahead to Ransomware Preparedness", ESG, June 2022

[6] "More organizations are paying the ransom. Why?" Help Net Security, April 2022

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

Benefits of continuous and secure data protection

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

A continuous and secure data protection plan works to break down silos of the past to stem the tide of worsening data risk exposure. It also signifies a new, integrated approach to secure data against ransomware by simplifying and automating the backup and recovery operations, thereby, enabling rapid data recovery. Importantly, encrypted backups make your backed-up 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 service

Within the realm of the prevailing subscription-based, as-a-service cloud environment, continuous and secure data protection is another offering to consider. By subscribing to the following cloud services, IT departments relinquish these tasks to a qualified third-party provider with the right tools to get the right results.

- **Data protection as a service (DPaaS)**—is a 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.
- **Backup as a service (BaaS)**—streamlines backup operations with a global protection policy for the consistent protection of all on-premises and cloud-native workloads across 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.

Why should you care?

The quick answer is, there is no end in sight to cybercrime activity. Cyberattacks are predicted to keep rising in the coming years, making the case for a reliable, proven solution even more compelling.

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:[8]

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

Further trends suggest:

- 55% of organizations will have implemented a cloud-centric data protection strategy by 2025.[9]
- 66% struggle to protect complex and dynamically changing attack surfaces.[10]
- 50% complexity and inability to integrate security solutions creates gaps in defenses.[11]

[8] "Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021," Cybercrime Magazine, March 2020

[9] "Using Data Protection as a Service to Address Modern Data Threats," IDC technology spotlight sponsored by HPE, November 2021

[10, 11] "The 2022 Study on Closing the IT Security Gap," Ponemon Institute Research Report sponsored by HPE, January 2022

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

Hewlett Packard Enterprise considers data protection from edge to cloud, building security measures into the very architecture platform. Like all companies, we have been recruiting more staff for our internal security team, while also launching new data protection solutions to help you manage your risk. Our security experts understand it's not a matter of if you will be attacked, but when—or if you already have been infiltrated by hackers.

HPE is rapidly transforming its traditional storage business into a cloud-native data services business and offers solutions for the rapidly growing DPaaS market with HPE GreenLake for data protection. This next-generation data protection of cloud services includes:

- Disaster recovery service with Zerto, a Hewlett Packard Enterprise company
- 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 a growing portfolio of cloud services, HPE offers organizations new ways to innovate with improved agility, manage costs, secure their data from the edge to the cloud, and address sophisticated ransomware attacks plus other cyberattacks. The acquisition of Zerto by HPE has provided data protection to the HPE cloud services portfolio that better helps organizations address cyber threats and ransomware attacks. The continuous data protection (CDP) technology with journal-based recovery helps organizations to recover from an attack in minutes and restores data to the state it was in just seconds before the attack occurred.

With this ability to migrate data and workloads to and from the cloud, backup and data recovery are enabled for on-premises workloads, cloud-native workloads (including containers), and software-as-a-service (SaaS) workloads. Ultimately, this ability to migrate between cloud and on-premises gives you the flexibility to optimize your data recovery solutions.

HPE also stands ready to solve data protection issues in these three key areas:

1. **Comprehensive and consistent data protection**

   HPE provides modern, edge-to-cloud data protection to 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**

   HPE helps to 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 and EC2 Instances.

3. **Protection from ransomware attacks**

   HPE helps 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, in just seconds.

Partner with HPE to secure enterprise data

It's time to break down those old 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. HPE helps you redefine and manage your backup and recovery process effortlessly with the simplicity and flexibility of the cloud experience—and achieve continuous, secure data protection to tackle cyber threats and ransomware attacks head-on. You will get the right blend of disaster recovery, backups, and archives auto-configured and auto-managed for protecting your enterprise data and applications.

Business case—Current state of affairs

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 has to 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 need the flexibility to modernize and continue their digital transformation path without roadblocks stopping them in their tracks or inhibiting innovation to move their business forward.

Continuous and secure 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 SLA at an affordable cost for companies to adopt without hesitation.

Conclusion

So, how are your security posture and status? Have you conducted a data risk assessment of everything in your organization that computes data? It's never too late to create a new data protection strategy (or modernize an existing one) that brings it all together, a resilient strategy you can follow to continuously protect enterprise data dispersed all over the world and recover it as quickly as possible when it is compromised. We're all evolving in our response to these pressing challenges and serious threats, but it can be done as a conscious, collaborative endeavor that scales with your business. The right kind of CDP may very well be the key to business survival in the 21st century.

Learn more

- Reduce your risk of data loss with HPE GreenLake for Disaster Recovery
- Protect data effortlessly with HPE GreenLake for Backup and Recovery

Visit **HPE GreenLake**

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard Enterprise

a50007308ENW, Rev.1