



# Getting ahead of modern data threats

Continuous and secure data protection, edge to cloud

**Get started** >



# Table of contents

<b>Modernize data security and protection for effective defense against cyber threats.....</b>	<b>3</b>
Tackling ransomware and other adversarial data attacks head-on.....	3
<b>All data protection is not created equal.....</b>	<b>4</b>
Delivering a comprehensive, continuous, and holistic approach.....	4
<b>Reduce the risk of data loss from cyberattacks.....</b>	<b>5</b>
Unifying your IT landscape to close the ransomware gap, without adding infrastructure complexity.....	5
<b>Recover quickly following a data breach.....</b>	<b>6</b>
Restoring your data in minutes to a recovery point just seconds before the disruption.....	6
<b>A cloud experience that is simple, strong, and seamless.....</b>	<b>7</b>
Supporting the growth of data and mitigating the proliferation of cyberattacks.....	7
<b>Trusted data protection.....</b>	<b>8</b>
From ransomware safeguards to rapid data recovery, to long-term data retention.....	8
<b>Ready to enhance your data security and protection?.....</b>	<b>9</b>
If not now, when?.....	9
<b>Partner with HPE for continuous data security and protection.....</b>	<b>10</b>



# Modernize data security and protection for effective defense against cyber threats

## Tackling ransomware and other adversarial data attacks head-on

As global threats to data become more serious, modernization and transformation efforts are pushing data in many forms into a bewildering array of silos and novel hosting environments, from edge to cloud. This complexity has made enterprise data even more vulnerable to attack by extremely sophisticated hackers waging technological warfare.

Hewlett Packard Enterprise can help you secure and protect your organization’s data, scaling to cover its exploding growth—wherever or with whomever data resides—for its entire lifecycle. And should a cyberattack or data breach occur, HPE has the right solutions and services to help you meet demanding data recovery service-level agreement (SLA) requirements for uninterrupted computing operations.

For example, as you move toward a more modern data security and protection strategy, HPE can recommend solutions that support a broad, unified, and continual approach to prevent data loss or data compromise due to unwanted intrusions, specifically being held hostage by ransomware or code being modified by malware.

Going a step further, HPE is building security measures into the very architecture platform of systems and offering customers next-generation, cloud-based solutions, including multiple as-a-service options that focus on continuous and secure data protection, backup, and recovery.

**93%**

of organizations surveyed have suffered data-related business disruption and

**68%**

of them experienced more than four events that resulted in business disruption.<sup>1</sup>

### **We cannot let our guard down for a moment**

In a world of prolific cybercrime attempts on all types of industries, utilities, and government installations around the world, we need to keep ahead of these threats.

<sup>1</sup> [“The State of Ransomware and Disaster Preparedness: 2022,” IDC white paper, sponsored by Zerto, a Hewlett Packard Enterprise company, May 2022](#)



# All data protection is not created equal

## Delivering a comprehensive, continuous, and holistic approach

When it comes to protecting your most valuable asset—data—solutions of the past leave a lot to be desired, especially in today's highly distributed operating environment. It will take a continuous and secure data protection plan to break down old silos and stem the tide of worsening data risk exposure in the cloud, in the core, and increasingly at the edge.

### What is data protection?

Data protection includes data security, but it also encompasses data backup, recovery, and archiving, as well as disaster recovery and business continuity. Also, data protection must be continuous and holistic to be successful.

HPE provides a comprehensive portfolio of data security and protection solutions and services that combine the best practices of the following three components:

1. **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.
2. **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.
3. **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.

### A new approach

The result is a new, integrated approach to securing data, starting with the simplification and automation of your backup and recovery operations. Because HPE security experts know it's not a matter of if you might be attacked, but more a matter of when, or perhaps your IT environment has already been infiltrated by hackers.

**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.**



# Reduce the risk of data loss from cyberattacks

## Unifying your IT landscape to close the ransomware gap, without adding infrastructure complexity

Corporate data now resides at countless locations outside the perimeter of the traditional firewall. That means it is exposed to serious vulnerabilities, resulting in an ever-widening security gap. HPE can help you take stock of your existing cybersecurity programs by performing a data risk assessment to identify gaps and then close those gaps.

### Multipoint solutions are simply inadequate

Companies cannot afford to maintain the status quo when it comes to data protection across a growing number (tens of thousands) of devices and locations, including the cloud. To meet the challenge of constantly changing data use and locations, HPE helps you unify data security and protection efforts across your IT landscape, providing the same high level of cybersecurity practices at every point. Based on the vulnerability statistics shown at the right, these percentages are unlikely to go down anytime soon.

**Advisory and Professional Services** can provide you with the proven experience and expertise to help you automate your data security and protection journey, so that it scales with your business growth, while not being too complex or costly. For instance, HPE can help you:

- **Streamline operations and minimize risk** with a single management console and global protection policy for consistent orchestration capabilities for your on-premises virtual machines or cloud-native workloads such as Amazon EBS Volumes and EC2 Instances.
- **Defend your business data from the consequences of ransomware** with a fully orchestrated failover and fallback solution that helps in the recovery of infected or compromised applications and data, in just seconds.

**Siloed data; data growth; data sprawling across the core, cloud, and edge; and increasing ransomware and malware threats have contributed to unprecedented complexity and greater risk of data loss for companies worldwide.**

In 2021:

**91%** of industrial organizations were vulnerable to cyberattacks.<sup>2</sup>

**47%** of organizations experienced ransomware attacks on at least a monthly basis.

**73%** of whom suffered at least one successful attack.<sup>3</sup>

<sup>2</sup> [Information security risks at industrial companies](#), Positive Technologies, September 2021

<sup>3</sup> [The Long Road Ahead to Ransomware Preparedness](#), ESG eBook, June 2022



# Recover quickly following a data breach

## Restoring your data in minutes to a recovery point just seconds before the disruption

The virtual state of emergency due to rising cyberattacks calls for avoiding data breaches in the first place and preventing data damage from unauthorized modification. But we also know that no cybersecurity plan can guarantee complete immunity to such pervasive attacks on data integrity.

HPE solutions help you avoid, and rapidly recover from, ransomware and malware data casualties via these specialized services:

- **Disaster recovery service with Zerto, a Hewlett Packard Enterprise company:** Includes CDP technology with journal-based recovery to help your organization recover from an attack in minutes and restore data to the state it was in just seconds before the attack occurred. The CDP technology also allows you to migrate data and workloads to and from the cloud, and backup and recover data for on-premises workloads, cloud-native workloads (including containers), and software-as-a-service (SaaS) workloads.
- **Backup with HPE Backup and Recovery Service** for continuous, encrypted data backup with adequate granularity for fast and effective recovery. When backups are protected this way, recovery from an attack that threatens to delete or modify data should be complete.

HPE experts can help you construct a robust backup and recovery program that operates 24x7 to help ensure data is backed up in its entirety and ready for immediate recovery to mitigate the potential damages of ransomware and other adversarial attacks.

### Key takeaway: Don't gamble with the threat of ransomware

The alternative of paying the ransom and hoping to decrypt all your data is not a road to a quick recovery. A high percentage of organizations do pay the ransom;<sup>4</sup> however, a third of those that paid were still unable to recover all their data.<sup>5</sup>

<sup>4</sup> ["More organizations are paying the ransom. Why?"](#) Help Net Security, April 2022

<sup>5</sup> ["Paying the ransom is not a good recovery strategy,"](#) Help Net Security, May 2022



# A cloud experience that is simple, strong, and seamless

## Supporting the growth of data and mitigating the proliferation of cyberattacks

The implementation of cloud-based continuous and secure data protection offers many undeniable benefits to organizations of any size, particularly as the overwhelming deluge of data grows and cyberattacks escalate. HPE is rapidly transforming its traditional storage business into a cloud-native data services business, built on a stronger, simpler, and more seamless experience to better respond to these challenges.

### Main benefits

With continuous and secure data protection from HPE, you have the flexibility to modernize and continue your digital transformation path, without roadblocks stopping you or inhibiting innovation to move your business forward. To this end, HPE delivers these benefits:

- Comprehensive and consistent enterprise data protection for all your locations around the world, from edge to cloud
- Encrypted backups that make your backed-up data inaccessible to cyberattack, even ransomware, increasingly at the edge
- Rapid backup and recovery, restoring your data to its original state in a matter of minutes
- Operational simplicity and efficiency, leveraging automation to meet your disaster recovery SLAs at an affordable cost
- Support of long-term data retention, data mobility, immutable backups, and the regular testing of data resilience
- Optimized cybersecurity awareness, cloud security, data protection, risk assessment, threat identification, and more
- Ability for your organization to compete and survive in the face of 21st-century cybercrime threats

Entrusting the job of protecting your enterprise data to HPE experts is a smart, cost-effective solution to protect your most valuable asset, your data.

## The right tools get the right results

By subscribing to the following next-generation cloud-based data security and protection services, your IT department can relinquish day-to-day, security-related tasks to HPE:

- **Data protection as a service (DPaaS)**—Is a cloud-based or web-delivered SaaS helping you protect your organization's data and applications by securing your network and providing recovery options
- **Disaster recovery as a service (DRaaS)**— Moves your organization's computer processing to your cloud infrastructure in case of a disaster
- **Backup as a service (BaaS)**—Streamlines your backup operations with a global protection policy for consistent protection of all on-premises and cloud-native workloads across the hybrid cloud



# Trusted data protection

## From ransomware safeguards to rapid data recovery, to long-term data retention

Offering capabilities across the security spectrum, HPE has a portfolio of [Enterprise Security and Digital Protection Services](#) designed to help you reach your data protection goals across the enterprise. These capabilities are meant to reinforce and enhance (rather than replace) your current data security and protection program. Together, we can integrate new solutions into your existing strategy—including ransomware safeguards, rapid data recovery, and long-term data retention—to help ensure data integrity and availability are continuously maintained, regardless of the location and hosting platform.

[HPE GreenLake for Data Protection solutions](#) help you modernize your organization's data protection and security. Take ransomware head-on, while protecting data with rapid disaster recovery and backup—across edge to cloud.

[HPE GreenLake for Backup and Recovery](#) modernizes the backup and recovery of your SLAs with backup, ransomware protection, and disaster recovery. Protecting your data has historically entailed complex management tasks, overprovisioned hardware, and fragmented solutions with a slow recovery from disruptions. Enhance your data protection with cloud backup, on-premises backup, and disaster recovery that scale with your needs, can be managed for you, and are consumption-based.

[HPE GreenLake for Disaster Recovery](#) can also help you reduce your risk of data loss in a disaster, without adding infrastructure complexity. Protect your virtual machine (VM) workloads from ransomware attacks, natural disasters, and outages with the ability to restore in minutes to a recovery point just seconds before the disruption. You get the HPE expertise and experience for managing protection across multi-site deployments.

### **Continuous data protection is the key to business survival**

Ransomware attacks can impede your business. The new HPE continuous data protection solution offers quick recovery from significant data losses.



# Ready to enhance your data security and protection?

## If not now, when?

While such programs may already be in place, they lack consistency and continuity across the full IT estate—consisting of all assets and locations. Now is the time to enhance data security and protection, as modern cybercriminal techniques are clever enough to find any gaps. Thankfully, HPE can deliver proven approaches for closing those gaps. We can help you:

Identify where ransomware and other data gaps exist

Build a more comprehensive, continuous data security and protection strategy

Remove roadblocks to achieving digital transformation projects

Reduce overall risk exposure to unwanted data intrusions, data loss, and operational disruptions

Backup and recover data using efficient and cost-effective solutions



# Partner with HPE for continuous data security and protection

HPE offers organizations 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 that continue to evolve.

## Learn more at

[HPE GreenLake for Data Protection solutions](#)

[HPE GreenLake for Backup and Recovery](#)

[HPE GreenLake for Disaster Recovery](#)



Make the right purchase decision.  
Contact our presales specialists.



Chat now (sales)



Call now



Get updates

Visit [HPE GreenLake](#)



  
**Hewlett Packard  
Enterprise**

© Copyright 2022 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.

a50007342ENW, Rev. 1