Hewlett Packard Enterprise

Buyer's guide

The 2025 data protection buyer's guide

How to approach buying the right solutions for your data protection strategy

Get started >

Buyer's guide

Introduction

As the world continues to advance into the digital age, the importance and value of digital services and data are greater than ever before. From enterprise to midmarket, IT teams face increased pressure to protect business-critical resources within increasingly complex IT environments. Maintaining a 24/7, always-on business while protecting and retaining the data it runs on is required not only to compete in a global market, but also to meet regulatory compliance globally.

Creating an effective data protection strategy starts with understanding your business's data protection challenges. Downtime and data loss can result from a variety of causes; from traditional, unintentional natural disasters to manufactured, deliberate disasters. Over the last decade, cyberattacks have become one of the biggest threats to data and IT services. Regardless of the cause, the costs of downtime or data loss can be immense, and disruptions that last for hours, days, or even weeks can cause irreparable harm to customer satisfaction and a business's reputation.

The right data protection strategy and the right solutions to support it can make data and IT services resilient against both downtime and data loss. The purpose of this guide is to help you understand the challenges that may impact your business, the types of available solutions that can provide data protection, and how these considerations can help you choose the right solutions to mount an effective data protection strategy.

Common terminology

The following are common terms used in data protection:

Term	Definition
Business impact analysis (BIA)	An analysis of the impacts caused by IT downtime and data loss across an organization usually in terms of financial cost
Recovery time objective (RTO)	The targeted time between a disruption and when access is restored to data and services
Recovery point objective (RPO)	The targeted point from which data can be recovered after it has been lost in a disruption
Continuous data protection (CDP)	Real time replication of data that combines journaled recovery points and application orchestration for flexible recovery
Disaster recovery (DR)	Rapid recovery from a disruption or disaster that takes systems and data offline
Backup	The periodic copying of data for long-term retention and recovery
Cyber resilience	The ability to quickly recover from a cyberattack such as ransomware that disrupts services and data
Immutability	Data placed in a read-only state that cannot be modified, even by a system administrator, to protect it from cyberattack
3-2-1-1	A data protection strategy that includes three copies of data, in two different medias, with one copy on a remote site for protection against a site-wide disaster, and one copy made immutable against cyberattacks
Air gapping	Isolating a data set or clean room environment from the network and internet to insulate it from outside attackers
Zero Trust	An evolving set of cybersecurity principles that replaces the old "trust but verify" paradigm with "never trust, always verify" to reinforce the need for proactive defense-in-depth and hyper-vigilant processes

How to approach the buying process

Let's begin by breaking down the data protection buying process into three distinct steps.

1

Understand your data protection challenges

2

Research and document your requirements

3

Establish your buying criteria

Sophos reported that **59% of organizations were hit by ransomware attacks** between 2023 and 2024, with **70% of the incidents leading to data encryption**[1].

According to an IDC survey, **94% of victims said attackers targeted their backups.** Of those attacks, **57% of backup compromise attempts were successful**[2].

1 Understand your data protection challenges

We all rely on some data and digital services to do business, and disruptions can affect every organization in every industry. In order to really understand where and how data protection is needed, an analysis of your IT systems and how they may be impacted by a disruption should be carried out.

To perform a business impact analysis:

- Identify all IT workloads, including data and applications.
- Map dependencies between workloads to understand how a disruption to one workload may impact other workloads.
- Rank workloads and their functions to determine which are more critical to your business. This is often done by creating tiers of criticality where tier one is the most critical and each subsequent tier is less critical.
- Determine the impact of both downtime and data loss for each workload or workload tier.
  - –What will it cost to have the workload unavailable for a period of time?
  - –What will it cost to have a data set lost?
- Calculate the cost of recovery from a disruption based on current recovery plans and tools.
- Understand the wider impacts of IT systems outages that may affect productivity, customer confidence, and brand reputation. This may include doing a formal risk assessment.

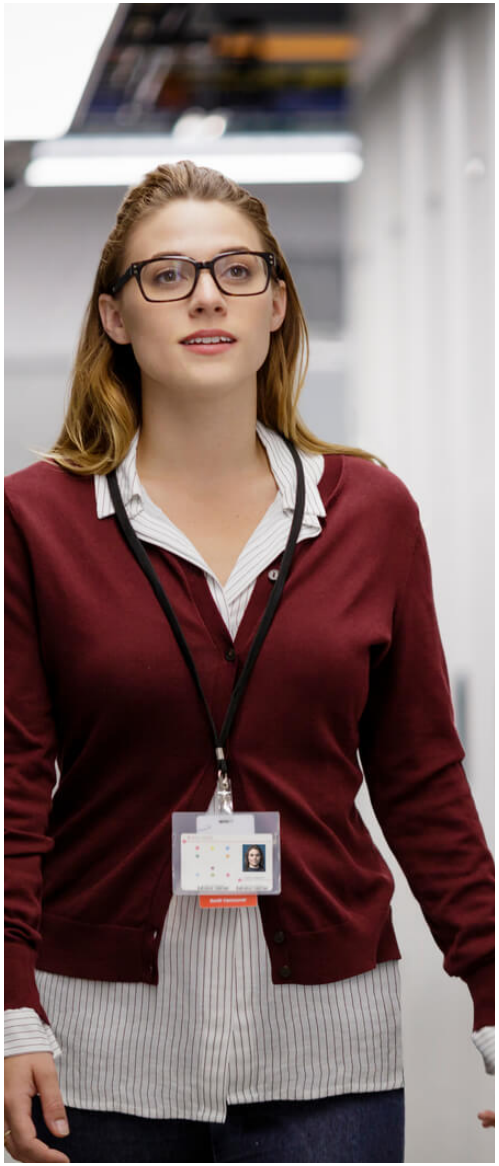
[1] Sophos: The State of Ransomware 2024

[2] IDC white paper–The State of Disaster Recovery and Cyber-Recovery, 2024–2025-Zerto

Once you have identified the potential impacts to your IT systems, there are a number of questions that can help you determine what levels of data protection you need. They can also help you weigh your budget for data protection vs. the financial risks of being under protected. Organizations face data protection challenges like the following:

- **How do I maintain an always-on business?** Online or on-premises, whether your operations are 24/7 or only during the hours you do business, you can't afford an interruption. Loss of sales, productivity, and trust from your customers can seriously impact your business. Failure of applications and computer systems can cripple e-commerce, communications, production lines, or any number of services your customers rely on. Your brand and reputation can be damaged by slow recovery times associated with antiquated data protection solutions.
- **How do I prevent data loss?** Your data is critical to your business, and loss of access to data means a disruption to productivity and sales. It's not if, but rather when, something goes wrong that you need to be able to get your data back online quickly and accurately before it affects your bottom line. Data loss can occur for many reasons, including human error, software corruption, natural disasters, hardware failures, and cyberattacks like ransomware. A few hours of critical data lost during a peak time can be devastating. Only you will know the true value of your data to your business.
- **Can I recover from a cyberattack like ransomware?** Although cybersecurity is crucial to preventing attacks, no amount of prevention is 100% effective. Cyberattacks grow more sophisticated each year and go far beyond simply encrypting data and ransoming the encryption key to the victim. You might not be able to rely on your backups. More and more, ransomware attacks target the recovery solutions themselves, even finding ways to bypass immutable recovery data copies by artificially expiring the immutability timers. Recovery solutions require multiple layers of recovery options to ensure recovery.
- **How can I be compliant with industry regulations and standards?** More government regulations regarding data protection and security are going into effect, and industries are taking it upon themselves to implement stricter standards by which all businesses are expected to operate. Being noncompliant with government regulations can lead to fines and criminal charges that can be very costly, while failure to comply with industry standards may impact your ability to do business and your brand reputation.
- **What complexities in my IT environment make data protection difficult?** IT environments are no longer the monolithic, on-premises data centers they used to be. Now, they typically span across multiple clouds, on-premises data centers, and edge sites while also incorporating cloud-based software as a service (SaaS) applications. Deploying multiple and diverse data protection solutions across different platforms requires more expertise and management interfaces to deal with, not to mention more support numbers to call when an incident occurs.

Your challenges may vary greatly depending on the type of data and services affected, the size of the organization, and the nature of the industry or business. Only you will truly know the extent of the challenges to your business—and the potential costs if you had to halt operations for hours or days, or if you lost hours' worth or days' worth of data.



2 Research and document your requirements

Once you've outlined your data protection challenges, it's time to establish the requirements for your data protection strategy. Researching and documenting are key to ensuring everyone in your organization is aligned with your goals.

- **Document your data protection strategy and plans.** Based on your business impact analysis, document your desired recovery time objective (RTO) and recovery point objective (RPO) for each tier of workload in your IT environment, whether they are measured in seconds and minutes or hours and days. Document personnel responsible for implementing and managing the data protection plan, including incident response teams. Document not just for implementation purposes but also for ongoing testing of your data protection plans, including testing DR, backups, and cyberattack response.
- **Research and document regulations and industry standards.** Take the time to understand the regulations that govern data protection generally and those specific to your industry, as well as any relevant industry standards that your organization has adopted. Knowing these and having them properly documented will inform your buying decisions and enable the solutions you purchase to keep you compliant.

This step provides you with a clear, thorough map of your data protection needs, which in turn informs your buying choices when you start reviewing your options. With the right information in hand, you can make sure the solution you select is tailored to your needs.

3 Establish your data protection buying criteria

Data protection should cover nearly all workloads and data in your organization at some tier of protection. To make the most of your data protection strategy, include each of these core solution focus areas:

Recovery

Recovery abilities that provide quick recovery times, little data loss, and flexibility to recover granularly from files and VMs to entire sites.

Architecture

Supporting multiple platforms, multiple sites, one-to many topologies, extensibility, and global analytics and reporting.

Cyber resilience

Combining detection, immutability, zero trust principles, and air-gapping, to ensure recovery from cyberattacks that cause disruption and data loss.

Additional solution focus areas may be specific to your industry, but this guide will focus on the buying criteria for these three.

Backup as disaster recovery

Although the terms are often used interchangeably, it's important to understand the distinction between backup and disaster recovery. Backup is retention-optimized, while DR is performance-optimized—and both have a place in data protection.

A backup solution can sometimes meet RPO and RTO requirements for isolated events, but for actual disaster scenarios that affect entire sites, your backup solution's recovery capabilities are inadequate to recover within minutes or even hours. In the context of recovering your business to total production, backups are better suited for long-term data retention rather than 24/7 recovery services. Backups don't address maximum tolerable downtime in any meaningful way.

The two primary and critical use cases for backup in a modern data protection strategy are:

- Long-term retention for archiving and compliance
- Recovery of lower-tier workloads that can afford to have RPOs and RTOs measured in hours or days

All this considered, backup is a crucial part of data protection because neither disaster recovery solutions nor cyber resilience solutions are designed to retain data long-term, and both are designed (and priced) for protecting critical, higher-tier business systems.

Key buying criteria

Choosing a data protection solution—or solutions—is a complicated process that only grows more complicated with larger and more complex IT infrastructures. To simplify the process, this guide includes key buying criteria you should consider in your data protection decision.

Recovery

- Recover time objectives
- Recover point objectives
- Flexible recovery options
- Automation/orchestration
- Disaster recovery testing

Architecture

- Platform support
- Hardware/storage support
- Scale-out architecture
- One-to-many architecture
- Extensible architecture
- Software as a service
- Analytics and reporting

Cyber resilience

- Cyberattack detection
- Immutability
- Zero Trust architecture
- Cyber vault

Recovery criteria

Recover time objectives

When your critical business systems go offline, can you afford to wait hours to restore data from a backup or recover across the internet? If not, you probably have a recovery time of minutes as your goal. The fastest way to achieve such an RTO is typically not with a data restore but with a failover to a standby DR site. In this scenario, all your recovery data is already in place, waiting to be recovered as a running workload, and can be booted up within minutes.

Traditional solutions for data protection, like backup or storage replication alone, cannot recover applications and data quickly enough. Disaster recovery fills this gap. And while services may be running in a diminished state while failed over to a remote site, they are still running. Your business can be back up and operational in this state until you fully recover back to your primary production site.

Recover point objectives

When a disruption hits and data is lost, how much data can you afford to lose? With traditional data protection solutions like backups or snapshots, hours of data could be lost since the last good recovery checkpoint. But for your most critical systems and their data, you likely want as close to zero data loss as possible—an RPO measured in seconds.

Backups and snapshots cannot deliver RPOs in seconds. Only real time replication moves data fast enough as it changes to protect data within seconds. However, not all replication solutions are equal. Simply replicating blocks of data in real time does not guarantee data consistency or provide flexible recovery options. To truly ensure recovery, consistent recovery checkpoints must be created. And to ensure an RPO of seconds, those recovery checkpoints must be created every few seconds and recorded in a journal.

Applications can make replication even more challenging when they consist of multiple workloads replicated separately. For applications, replication must be consistent across the workloads that make up an application to ensure recovery to a time-consistent checkpoint across all workloads. Without this, applications can fail to start, and downtime continues until the application can be recovered to a consistent state. The journaled checkpoint created by a replication solution must consider application workload grouping to ensure recovery with an RPO of seconds.

While real time replication and journaled recovery checkpoints every few seconds are ideal, they are not available on every platform. On some infrastructure platforms, periodic, snapshot-based replication may be the only—and therefore best—replication option open to you. With the multitude of cloud infrastructures out there, options will vary, and it's important to understand which are available on the platforms you use.

Flexible recovery options

Disruptions come in all shapes and sizes. In some cases, you may only need to recover a single application, while in others, you may need to recover an entire site or multiple sites. Having the option to recover at a granular level allows for flexible operational recovery—from individual files or folders all the way to failing over entire sites when the disruption warrants it.

Failing over only affected workloads, rather than an entire site, can speed recovery time and make it easier to fail back when needed. Additionally, being able to recover individual files without disrupting other systems can be useful for daily IT operations. The more options you have for recovery, the greater your ability to respond proportionately to a disruption of any size.

Automation/orchestration

Manual steps are one of the most significant factors in slowing down recovery time. Automation and orchestration of recovery dramatically speed up recovery time, particularly when recovering large numbers of workloads. Imagine recovering hundreds of workloads with the multiple manual steps required to recover each workload. That would extend the recovery time to hours rather than minutes.

Automation of recovery steps and orchestration of workload recovery by the dozens or hundreds at a time is key to minimizing recovery time. Automated recovery is especially important for coordinating recovery based on dependencies between applications and federated applications that consist of multiple workloads. Automation and orchestration should be part of the disaster recovery solution to recover quickly and achieve a recovery time of minutes.

Disaster recovery testing

A disaster recovery solution isn't effective if it can't be tested on a regular basis. Traditionally, disaster recovery testing has been difficult enough that many organizations, despite their best intentions, struggled to test their disaster recovery plans even once a year. These tests were often disruptive: the business frequently had to take live systems offline to test recovery properly.

The ability to test without disruption to your business is essential to enabling frequent testing. Whether testing recovery for an individual workload, an application, or an entire site, your solution should allow you to test with confidence and without any disruption to business operations.

Architecture criteria

Platform support

Having multiple computing platforms, like VMware®, Hyper-V, Amazon EC2, or Azure VMs, can complicate finding a solution. Many data protection solutions only support a single hypervisor or a single cloud infrastructure as a service (IaaS) platform. Depending on your IT environment, it is possible to use more than one solution, which may be necessary, but this complicates your overall data protection strategy. Having multiple vendors, with multiple sets of expertise required and multiple support numbers to call, makes every part of the data protection plan more complex.

Finding a single vendor to support all your platforms can significantly simplify the buying process, as well as your need for support, licensing, and training. Consider the possibility that you may add another platform to your IT environment in the future and whether your solution of choice also supports that platform. Carefully evaluate which solution or solutions best help you meet your RTO and RPO goals across all your platforms.

Hardware/storage support

Some data protection solutions are software-only, while others include their own hardware, and in either case, they may have specific types of hardware or storage they do or do not support. Solutions that support only specific hardware or storage can lock you into purchasing more of that hardware and storage in the future.

A hardware-agnostic and storage-agnostic solution, typically one that is software only, can support a diverse hardware environment and give you more choices for vendor hardware when adding to your environment in the future. Once again, you want to consider what solutions best meet your needs while helping you meet broader data protection goals across your IT environment.

Scale-out architecture

The need for data and digital services continues to grow. IT environments are expanding to meet this need, and likewise, data protection solutions must be able to scale out while minimizing disruption. Every solution can scale out by simply adding more components, but as you add more components, the solution can become too complex to manage and support. Supporting thousands of workloads with an agent-based solution means thousands of agents to install and manage. With a hardware-based appliance solution, you may end up with dozens of hardware appliances to manage.

Any solution can be demoed while easily protecting only a handful of workloads. It is important to research whether a particular solution, when used in larger-scale environments and at scale, is still able to meet desired recovery times and recovery points. Solutions that can operate without agents and with the ability to seamlessly deploy and manage scale-out resources can make scaling out effortless and efficient.

One-to-many architecture

As the 3-2-1-1 rule shows, multiple copies provide greater information security, and that applies in DR without question. You need multiple copies of data to ensure timely recovery because disasters may impact more than your primary operations. The ability of a solution to recover within your RPO and RTO requirements can be compromised when you only have a single recovery copy of the data available and that copy is compromised. Consider a solution that can simultaneously protect data to two different recovery targets. These copies of recovery data may be local and remote, on-premises or in the cloud—whatever best provides the protection and recovery options you need to safeguard your data.

Extensible architecture

Extensible options like APIs in data protection solutions can give you the ability to integrate with and leverage unified management solutions. These integrations can help pull data into unified management views alongside other systems like cybersecurity for greater visibility into potential threats and provide access for unified control and external automation.

Solutions that use an API-first architecture typically expose all controls, including lock-down security measures, for integration with third-party tools and services. The flexibility of an extensible architecture provides more options for management and monitoring throughout your organization.

Software as a service

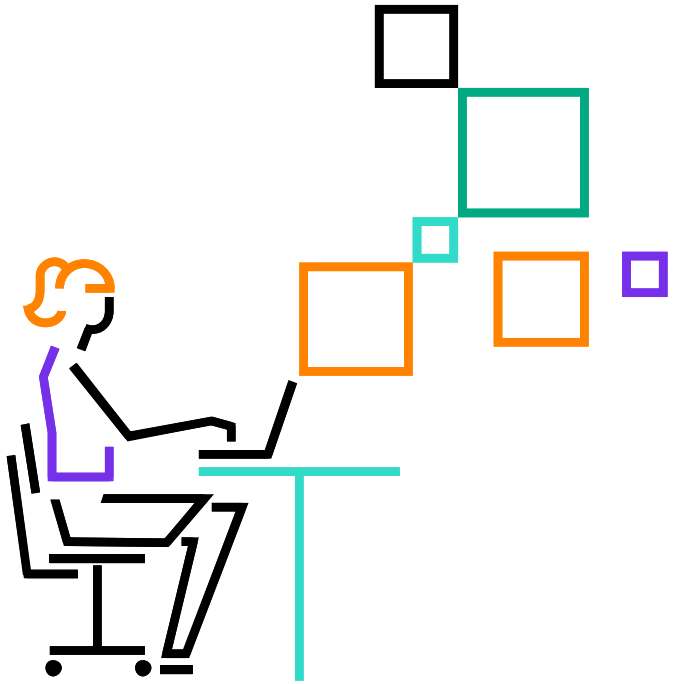
It's important to understand that moving to cloud-based applications like Microsoft 365 still requires you to back up data. In a shared responsibility model, the customer is responsible for protecting and backing up their data—SaaS providers do not automatically back it up. SaaS backup and recovery solutions create additional copies of SaaS application backups and store them in separate, secure locations. Some can also create partial backups or snapshots for additional protection and convenience.

Consider a complete backup solution for your on-premises, cloud, and SaaS application data—or use separate backup tools for each. Either way, ensure that your SaaS data is backed up along with the rest of your on-premises and cloud data workloads.

Analytics and reporting

It's important to be able to easily see whether your data protection solution meets your requirements, both for compliance and peace of mind. Viewing data protection analytics and reporting on them can be essential for informing stakeholders or government compliance agencies of success or problems.

Monitoring the health and effectiveness of your data protection solutions with analytics helps identify potential problems and allows you to better plan recovery based on DR testing results and trends in how quickly data is protected via recovery points. The larger your IT environment, the more valuable environment-wide analytics can be in monitoring the state of your data protection.



Cyber resilience criteria

Cyberattack detection

Cybersecurity solutions are designed to detect intrusions, but what if an intrusion has avoided detection by cybersecurity and an attack is already underway against your data and applications? A data protection solution that can detect when an attack has begun can help your incident response team act more quickly to isolate and remediate the attack, shortening your recovery time.

Backups can be scanned for potential malware or encrypted data that indicate an attack has begun, but that can take hours to detect. Being able to view data changes in real time—as with real time replication in a disaster recovery solution—can help alert you within seconds of an attack beginning, giving your incident response team the fastest warning. Combining this detection with other metrics measured by cybersecurity systems, such as network activity, can help those teams quickly identify the starting point and blast radius of an attack.

Immutability

Backup and recovery data of every type, including replicated data for disaster recovery, is vulnerable to cyberattacks, particularly if the attackers gain administrative privileges to the recovery solution. The ability to make immutable copies of recovery data is critical to ensuring data can be recovered if the recovery solution is compromised.

Although having to recover from an immutable copy of data is typically slower and not ideal, it is still preferable to paying a ransom to an attacker and encouraging more attacks. Immutability is one of the simplest ways to heighten data protection against ransomware.

Zero Trust architecture

As attackers increasingly target recovery solutions, the security of your recovery solution is essential in preventing attackers from compromising your ability to recover. Recovery solutions should be configurable, with options based on Zero Trust architecture principles, including least privileged access, role-based access controls, secure appliances, and routine security updates.

Although no security precautions can be 100% effective, the ability to deter attackers with security measures can mitigate both the severity and frequency of attacks. Any recovery solution that resides within production systems is vulnerable to some level of intrusion, but with the right security, the surface area of intrusion into the solution can be minimized.

Cyber vault

Cyberattacks like ransomware can lead to a doomsday scenario where all sites and systems are compromised or encrypted. A cyber vault can provide protection even in these doomsday scenarios, with data protected in an isolated, air-gapped environment where it is immutable and can only be managed locally by someone directly in the data center. Unfortunately, not all vaults are truly isolated or air gapped. Some are cloud-based, where the vault's management plane is exposed to potential hacking.

To ensure data is recoverable, it must be physically air gapped and isolated from network access. Like a tape that can be physically air gapped by removing it and storing it in a secure area, a vault must be accessible only to management in person in the data center. The advantage of a vault over tape is that the vault contains an isolated storage and high-performance computing environment in which the data can be restored quickly and safely for forensics.

Bringing data and applications online into a purpose-built clean room environment can dramatically speed up the recovery process—from months to days. With tape or other isolated data backups alone, the recovery process just to move the data can take weeks. In a fully compromised scenario, a vault can enable your incident response teams to accelerate recovery—which avoids paying a ransom and saves time and costs on the recovery process.

How to buy

Assess the data protection solutions available in the market and determine whether they meet the criteria you have defined. There are multiple ways to approach this, each of them complimentary:

Research

Perform research on a particular solution, using your own experts—independent of communication with the solution vendor. Use third parties to validate research.

- Analyst reports can evaluate solutions specifically or speak to preferred solution types for relevant use cases.
- Customer reviews and references can offer insights into customer success and challenges with solutions.

Connect with solution vendors

Validate your own research directly with the vendor and have the vendor provide insights into your specific use case.

- Solution architects can help design a solution specific to your organization's needs and criteria.
- Demonstrations can provide insights into management capabilities and functionality.

Evaluate the solution

Have your own experts and stakeholders try the solution to understand optimizations and potential challenges. Evaluations can be performed in a variety of ways:

- On-demand testing labs are often available in virtualized or cloud environments to evaluate the solution in a closed environment.
- Evaluation licensing can allow testing directly within your own infrastructure environment.
- Proof of concept (PoC) can be used to evaluate certain use cases relevant to your business.

In addition to considering the capabilities of various solutions as buying criteria, one must also consider the costs, licensing, and service models available for the solutions.

Perform a total cost of ownership (TCO) analysis

The total cost of a data protection solution can include the licensing cost of the solution, supporting infrastructure/hardware costs, implementation costs, maintenance costs, and other soft costs for monitoring and managing the solution.

Consider the three types of license models commonly offered in data protection solutions:

Perpetual licenses	Subscription-based licenses	Consumption-based licenses
Buy the solution as a capital expense up front with ongoing support and maintenance fees.	Pay to use the solution for a specified period of time in which the cost can be spread out over the course of the subscription period as an operational expense.	Also referred to as "pay-as-you-go,"* but priced based specifically on how many workloads or TBs of data are protected, so that the cost can scale up or down based on consumption/usage.

Determine what additional infrastructure or hardware may be needed to support the solution, which may include additional networking, storage, and compute resources as well as data center and cooling costs. Don't forget to include the cost of implementation, whether performed in-house or using professional services. Add ongoing costs for managing and monitoring the solution and executing recovery testing.

As complex as this can seem, the takeaway here is to explore multiple pricing and licensing options to see which best matches your budget and the way your organization prefers to consume IT resources (i.e., as a capital expense or an operational expense).

* May be subject to minimums or reserve capacity may apply"

DIY vs. managed service provider (MSP)

If the TCO of purchasing, implementing, and managing data protection yourself is not to your liking, you might consider an MSP to deliver and operate the service on your behalf. One key advantage of using a managed solution is that you potentially get to use best-of-breed solutions for each part of your environment without having to learn, configure, and manage multiple products or services. The MSP can configure a solution that specifically meets your needs and satisfies your data protection strategy.

There are three dominant models for the data protection services that MSPs provide:

Data protection to an MSP-hosted cloud	Data protection from the MSP-hosted cloud	Data protection and production hosted within the MSP cloud
Your production environment is on-premises, while the protected recovery data is stored off-site in an MSP-hosted cloud for recovery. This is ideal if you do not already have an off-site location for data protection and have no desire to create one yourself.	Your production workloads and data are hosted by the MSP, and your on-premises site is used to store your recovery data. This gives you full access and control over your recovery data if the MSP experiences a disruption.	The MSP hosts your production workloads and data on a cloud site and hosts your recovery data on a separate cloud site. This is ideal if you lack the expertise or desire to manage any of the infrastructure yourself.

Using an MSP completely removes day-to-day operations from your organization. It does not remove the responsibility; that is still yours. This is essentially a complete outsourcing of data protection to a third party. You don't have to worry about the design, its capacity, whether it is running or not running, or whether someone is closely watching it because you are employing the service provider's expertise.

Perform an ROI analysis

Justifying the cost of data protection can often be as simple as showing the cost of downtime and data loss without the ability to recover easily or quickly. Hours or days of downtime and/or data loss can add up fast, as can the cost of bringing in outside recovery services when a disruption occurs. If you have performed a business impact analysis, then the ROI analysis can easily incorporate the projected costs of downtime and data loss and compare that to the cost of data protection. The cost-benefit of being able to recover within minutes and experience only seconds of data loss can often demonstrate the value of a data protection solution with just a single incident. Many organizations have prioritized data protection after suffering from such a disruption.

Summary

The data and the digital services we rely on daily are constantly under threat from disruption, whether from natural disasters, accidents, or malicious attacks. Organizations like yours face many challenges in developing a data protection strategy to mitigate such disruptions. Your organization is unique, and only you fully understand the particular challenges your strategy must overcome.

There are many data protection solutions available to incorporate into your data protection strategy, and sorting them requires careful consideration of your requirements. Considering the criteria outlined in this guide—like RTO, RPO, scalability, testing, and more—can help inform your buying decisions and enable you to choose the best solutions for your data protection needs.

This guide ends with a checklist to help you keep track of the buying criteria we outlined in the previous section as well as the steps you need to take to get ready to start the buying process. The goal is to help you choose the best data protection solution for your organization's needs and to prepare you to handle any disruptions you may encounter. You can find more information about specific data protection solutions in the following resources.

Additional resources

White paper: Modernize data protection across hybrid cloud

Infographic: Cyber resilience and cyber vaults

Video: Continuous and secure data protection from edge to the cloud

Products: Data Protection products | HPE

Learn More

Data protection buying checklist

Approaching the buying process

Step 1	**Identify your challenges by performing a business impact analysis**	Downtime disrupting business operations
		Data loss causing disruptions and lost productivity
		Unprepared to recover quickly from a cyberattack
		Difficulty achieving compliance
		IT complexity making implementation and management difficult
Step 2	**Research, planning, and documenting**	Document your data protection strategy and plans
		Research and document regulations and industry standards

Data protection buying checklist

Approaching the buying process

Step 3	**Establish your data protection buying criteria**	Does the solution offer RTOs of minutes?
		Does the solution offer RPOs of seconds?
		Does the solution support your critical infrastructure platforms, including cloud?
		Does the solution have a scale-out architecture?
		Does the solution support your hardware and storage?
		Does the solution support multiple on-premises and cloud platforms?
		Does the solution feature automation and orchestration?
		Does the solution support a one-to-many architecture?
		Does the solution feature nondisruptive DR testing?
		Does the solution have flexible recovery options?
		Is the solution available as a managed service (DRaaS)?
		Does the solution feature detection for ransomware attacks?
		Is the detection real time or based on scanning backups?
		Does the solution provide immutability options for recovery data?
		Is the recovery solution protected by a zero-trust architecture?
		Does the solution offer a truly isolated vault for protection?

Data protection buying checklist

Approaching the buying process

How to buy	Research the solution capabilities.
	Research analyst reports.
	Research customer reviews/references.
	Work with a vendor solution architect.
	Evaluate the solution with testing or PoC.
	Perform a TCO analysis.
	Will the solution be implemented internally?
	Will an MSP be employed?
	Perform an ROI analysis.

Learn more at

HPE.com/Zerto

Visit **HPE.com**

Chat now (sales)

Hewlett Packard Enterprise

a00150054enw