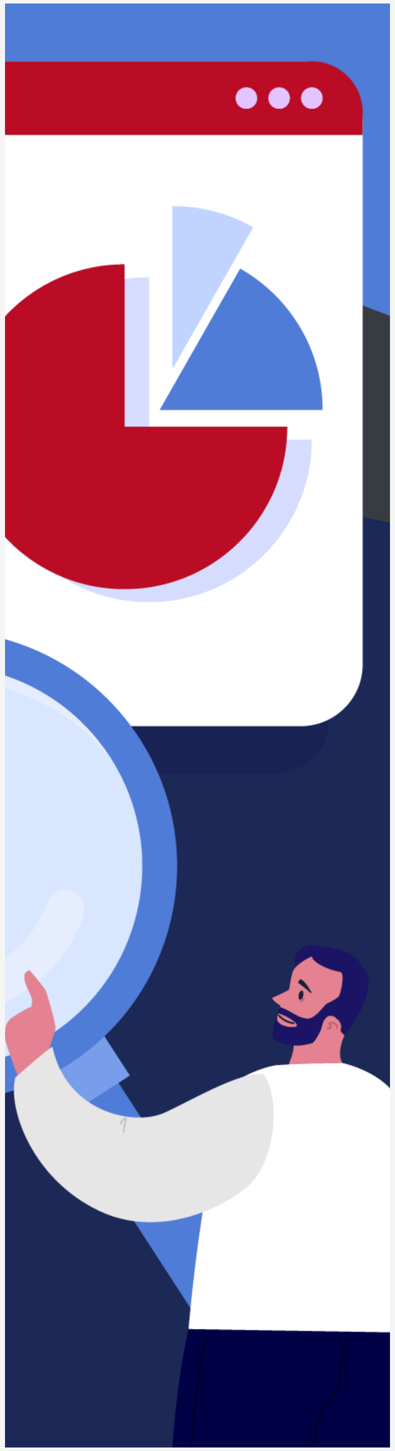
Zertø

a Hewlett Packard
Enterprise company

The 2024 Data Protection Buyers Guide

3 Steps to Smart Data Protection Every IT Leader Must Know



Contents

Select each topic to learn more.

Introduction

As the world continues to move into a new 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
	Recovery time objective (RTO)	The desired time period between a disruption and when access is restored to data and services
	Recovery point objective (RPO)	The desired 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	Recovery from a cyberattack such as ransomware that disrupts services and data
	3-2-1	A data protection strategy that includes three copies of data, on two different media, with one copy on a remote site for protection against a site-wide disaster
	Immutability	Data placed in a read-only state that cannot be modified, even by a system administrator, to protect it from cyberattack
	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

1 Understand Your Data Protection Challenges

We all rely on some amount of data and digital services to do business; thus, disruptions can affect every organization in every industry. Organizations face key challenges like these:

- **How do I maintain an always-on business?** Online or on-premises, whether your business runs 24/7 or only 9-5, 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. 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 options to be effective.

The average ransom payment almost doubled from **$812,380 in 2022 to $1,542,333 in 2023**[1].

[1] "2023 Ransomware Report: Sophos State of Ransomware"

- **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 different 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 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 IT environment.** Document each of your IT systems and their criticality to your business operations to determine what tier of data protection they need. Also document the various platforms, hardware, storage, software, and networking systems that need to support and be supported by your data protection solutions.
- **Document your data protection strategy and plan.** Document your desired RTO and 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 ensure that the solutions you purchase keep you in compliance.

> 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 maximize your data protection strategy, include each of these core solution focus areas:

Disaster Recovery

The ability to recover quickly from a disruption so that your organization can, at a minimum, resume critical operations as soon as possible

Backup

The ability to make copies of data that can be retained for long periods of time for compliance or used to recover less-critical systems after a disruption

Cyber Resilience

The ability to recover as quickly as possible from a cyberattack like ransomware that disrupts critical systems and data

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 (DR). 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 to 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) more for protecting critical, higher-tier business systems.

Key Buying Criteria

To maximize your data protection strategy, include each of these core solution focus areas.

Backup

- Secure backups
- Backup frequency
- Backup storage efficiency
- SaaS backup

Disaster Recovery

- RTO/RTO
- Platform, hardware and storage support
- Scale-out, one-to-many, and extensible architecture
- Automation & orchestration
- Analytics, reporting, and DR testing

Cyber Resilience

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

*Select each of the focus areas to learn more and select **Key Buying Criteria** in the sidebar menu to return to this page.*

Backup

Secure backups

As copies of entire workloads, backups can be attractive targets for unauthorized intrusions or cyberattacks like ransomware for deletion. Your ability to protect these backups with built-in encryption, configurable immutability, and dual authorization is a crucial factor in keeping your backups safe throughout their lifecycle.

Backup frequency

How often backups can be performed is a key consideration, particularly for those tier-two workloads using backup as their primary recovery solution. Although daily backups may be adequate for many tier-two workloads, some may deserve a more frequent backup schedule, possibly as often as every four hours. The ability to perform backups on custom, workload-specific schedules provides a high degree of flexibility in creating a data protection strategy.

Backup storage efficiency

Backups and the retention of backups over the long term can consume a lot of storage. Although backups can often be safely stored on lower-tier storage for cost efficiency, reducing the storage footprint of your backups using built-in compression and deduplication can dramatically reduce the cost of storage over time. This is especially important as the amount of data collected and stored in IT systems continues to rapidly increase.

Backup

Software as a service (SaaS) backup

Moving to cloud-based applications like Microsoft 365 still requires you to back up data. SaaS providers do not automatically back up data created on their platform. 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.

Disaster Recovery

RPO/RTO

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.

Disaster Recovery

When your critical business systems go offline, can you afford to wait hours to restore data from a backup 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. 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.

Platform, hardware, and storage support

Having multiple computing platforms, like VMware, Hyper-V, Amazon EC2, or Azure VMs, can complicate finding a solution that supports them all. Many data protection solutions only support a single hypervisor or a single cloud infrastructure as a service (IaaS) platform. 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. 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.

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. 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. Carefully evaluate which solution or solutions best help you meet your RTO and RPO goals across all your platforms.

Disaster Recovery

Scale-out, one-to many, and extensible architecture

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. 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.

As the 3-2-1 rule shows, multiple copies provide greater information security. You need multiple copies of data to ensure timely recovery because disasters may impact more than your primary operations. 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.

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. Extensible architecture provides more options for monitoring throughout your organization.

Disaster Recovery

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.

Analytics, reporting, and DR testing

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.

No disaster recovery solution is 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.

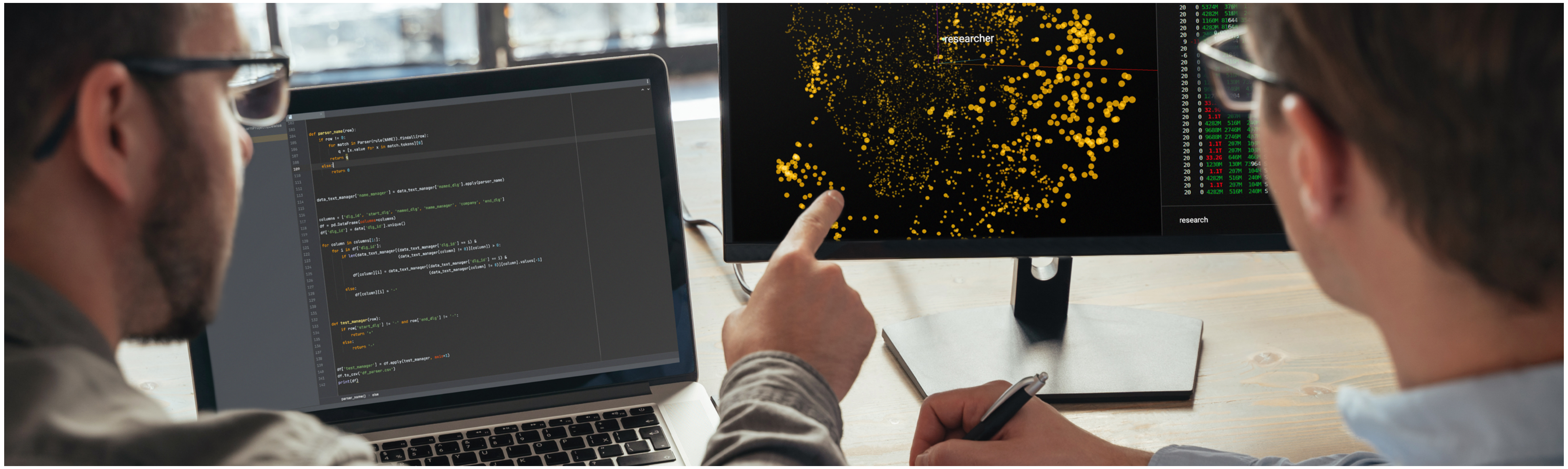
The ability to test without disruption to your business is essential to enabling frequent testing. Whether testing recovery for an individual workload, an application, or an entire site, your solution should allow you to test with confidence and without any disruption to business operations.

Cyber Resilience

Cyberattack detection

Cyber security 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.



Cyber Resilience

Immutability

Backup and recovery data of every type, including replicated data for disaster recovery, is vulnerable to cyberattack, 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 Resilience

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 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 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.

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 complementary:

Making the Purchasing Decision

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, buyers 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

Buy the solution as a capital expense up front with ongoing support and maintenance fees.

Subscription-based licenses

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.

Consumption-based licenses

Referred to as "pay-as-you-go," these are priced based specifically on how many workloads or TBs of data are protected, so 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 in ongoing costs for managing and monitoring the solution and executing recovery testing.

The takeaway 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).

Choose DIY or Managed Service Provider (MSP)

If the TCO of purchasing, implementing, and managing data protection yourself (DIY) is not to your liking, you might consider a managed service provider (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

Your production environment is on premises, while the protected recovery data is stored offsite in an MSP-hosted cloud for recovery. This is ideal if you do not already have an offsite location for data protection and have no desire to create one yourself.

Data protection from the MSP-hosted cloud

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.

Data protection and production hosted within the MSP cloud

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.

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. 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.

Additional Resources

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.

White Paper: Modern Data Protection: What Is It and Why Should You Care?—Zerto

Guide: Key Considerations for a Disaster Recovery Strategy

White Paper: Recovery Is the Cornerstone of Ransomware Resilience—Zerto

White Paper: Understanding the Necessity of Continuous and Secure Data Protection (hpe.com)

Learn More

Your Data Protection Buying Checklist

Data Protection Buying Checklist		
Approaching the Buying Process		
Step 1 Identify Your Challenges	□	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 IT environment
	□	Document your data protection strategy and plans
	□	Research and document regulations and industry standards

Your Data Protection Buying Checklist

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 feature automation and orchestration?
	□	Does the solution support one-to-many architecture?
	□	Does the solution feature non disruptive DR testing?
	□	Does the solution have flexible recovery options?
	□	Is the solution available as a managed service (DRaaS)?
	□	Does the solution provide secure backup formats?
	□	Does the backup frequency meet your RPO requirements?
	□	Does the solution have storage efficiency features like compression and deduplication?
	□	Can your solution back up to the cloud?
	□	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?

Your Data Protection Buying Checklist

Zerto
a Hewlett Packard
Enterprise company

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
	□	Determine if the solution will be implemented internally
	□	Find out if an MSP be employed
	□	Perform an ROI analysis