

CYBER VAULT BUYER'S GUIDE

How to approach buying the right
cyber vault solutions for your
cyber resilience strategy

Get started →





CONTENTS

3 Introduction

- 4 Common terminology
-

5 How to approach the buying process

- 6 Step 1—Understand your cyber resilience challenges
 - 8 Step 2—Research and document your requirements
 - 9 Step 3—Establish your cyber vault buying criteria
 - 10 Key buying criteria
-

14 How to buy

- 15 Perform a total cost of ownership (TCO) analysis
 - 16 Using a managed service provider
 - 16 Perform an ROI analysis
-

17 Summary

- 18 Cyber vault buying checklist

Introduction

Cyberattacks have grown to become the greatest single cause of disruption to IT operations, often accounting for more than disaster recovery. From enterprise to midmarket, IT teams face increased pressure to protect business-critical resources within increasingly complex IT environments. Maintaining 24x7, 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 cyber resilience strategy goes beyond traditional cybersecurity and data recovery solutions. As ransomware attackers increasingly target recovery solutions and recovery data, paying a ransom to recover data from a ransomware attack becomes a more attractive option. Cyber resilience plans now include cyber vaults as part of their comprehensive protection strategy, but choosing the type of vault and what data and applications need to be protected by a vault starts with understanding your business's cyber resilience challenges.

When a ransomware attack is successful, 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 brand reputation. Failure to have the right type of protection in place can also put your organization out of compliance and result in fines and other penalties.

The right cyber resilience strategy and the right vault 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 cyber vault solutions, and how these considerations can help you choose the right solutions to mount an effective cyber resilience strategy.

[→ more...](#)

Common terminology

The following are common terms used in cyber resilience, cyber recovery, and 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.
Incident response	The structured process of identifying, managing, and mitigating the effects of cybersecurity incidents to minimize damage, recover operations, and prevent future incidents.
Risk assessment	An assessment of potential threats an organization faces from disruptions like natural disasters, user errors, or cyberattacks.
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.
Cyberattack	A malicious attack by cyber criminals intended to cause disruption, steal valuable data, extort money, or any combination of these.
Ransomware	A cyberattack usually with the intent of disruption through encrypting data and extorting a ransom to get the data unencrypted, sometimes involving extortion for exposing data as well.
Cyber recovery	Recovery from a cyberattack, which incorporates remediation of compromised user accounts, systems, and malware.
Cyber resilience	A combination of measures designed to mitigate damage from and quickly recover from a cyberattack, such as ransomware, that disrupts services and data.
3-2-1-1	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 and one copy made immutable against cyberattacks.
Immutability	Data placed in a read-only state that cannot be modified, even by a system administrator, to protect it from cyberattacks.
Physical air gapping	Physically isolating a data set or clean room environment from the network and internet to make it inaccessible to attackers over any network.
Logical air gapping	Isolating a dataset or network environment that is still potentially available through a network (such as in a cloud environment) but has been logically separated from other networks to make it very difficult for attackers to see or access.
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 hypervigilant 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 cyber resilience challenges

2.

Research and document your requirements

3.

Establish your cyber vault buying criteria

[→ more...](#)

Step 1—Understand your cyber resilience challenges

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



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 cyber recovery from a disruption based on current recovery plans and tools.
- Understand the wider impacts of IT system outages that may affect productivity, customer confidence, and brand reputation. This may include doing a formal risk assessment.

[→ more...](#)

Once you have identified the potential impacts to your IT systems, there are a number of questions that can help you determine what type of cyber vault may be right for you. They can also help you weigh your budget for a cyber vault vs. the financial risks of being underprotected.

- **What is the risk of an attack on my organization?** Studies show that all organizations are vulnerable to attacks across all industries. Both public sector and private sector organizations are targets. While some industries, such as healthcare and financial sectors, are directly targeted more than others because of both valuable data and the impact of downtime, any organization can become a target once a vulnerability is exposed. Your decision to use a cyber vault should take into account the likelihood of an attack.

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

- **Are my current backups or recovery data vulnerable to compromise?** Most data used for recovery resides on primary or secondary storage systems within the data center. Cybercriminals do not want organizations to recover data and intentionally try to disrupt the ability of organizations to recover from their stored recovery data by compromising that data and the recovery systems. Cyber vaults exist to protect recovery data using immutability, air-gapping, and other security principles specifically to prevent compromised recovery.

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 "The State of Ransomware 2024," Sophos, 2024.

² "The State of Disaster Recovery and Cyber-Recovery, 2024-2025," IDC, 2024.

- **How quickly could I detect a ransomware attack in progress encrypting data?** Speed matters in an attack both for the attacker and the victim. Once an attacker begins encrypting data, the sooner it can be detected, the sooner the victim can react and start isolating networks and data so that the blast radius of the attack is reduced. Unfortunately, many forms of encryption detection are based on analyzing backups only periodically, meaning the attack may have already encrypted data for hours before it is detected.
- **How long would it take me to isolate an environment to recover into?** One of the biggest barriers to recovery in a cyberattack is that the computing environment is already known to be compromised, so it is not advised to start recovering applications and data back into the compromised environment. Instead, an isolated environment that the attackers cannot reach is needed to begin recovery. Without having this in place already, the time it takes to build such an environment must be part of the recovery equation.
- **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 cyber resilience 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, cyber resilience, and cyber recovery 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.

→ more . . .

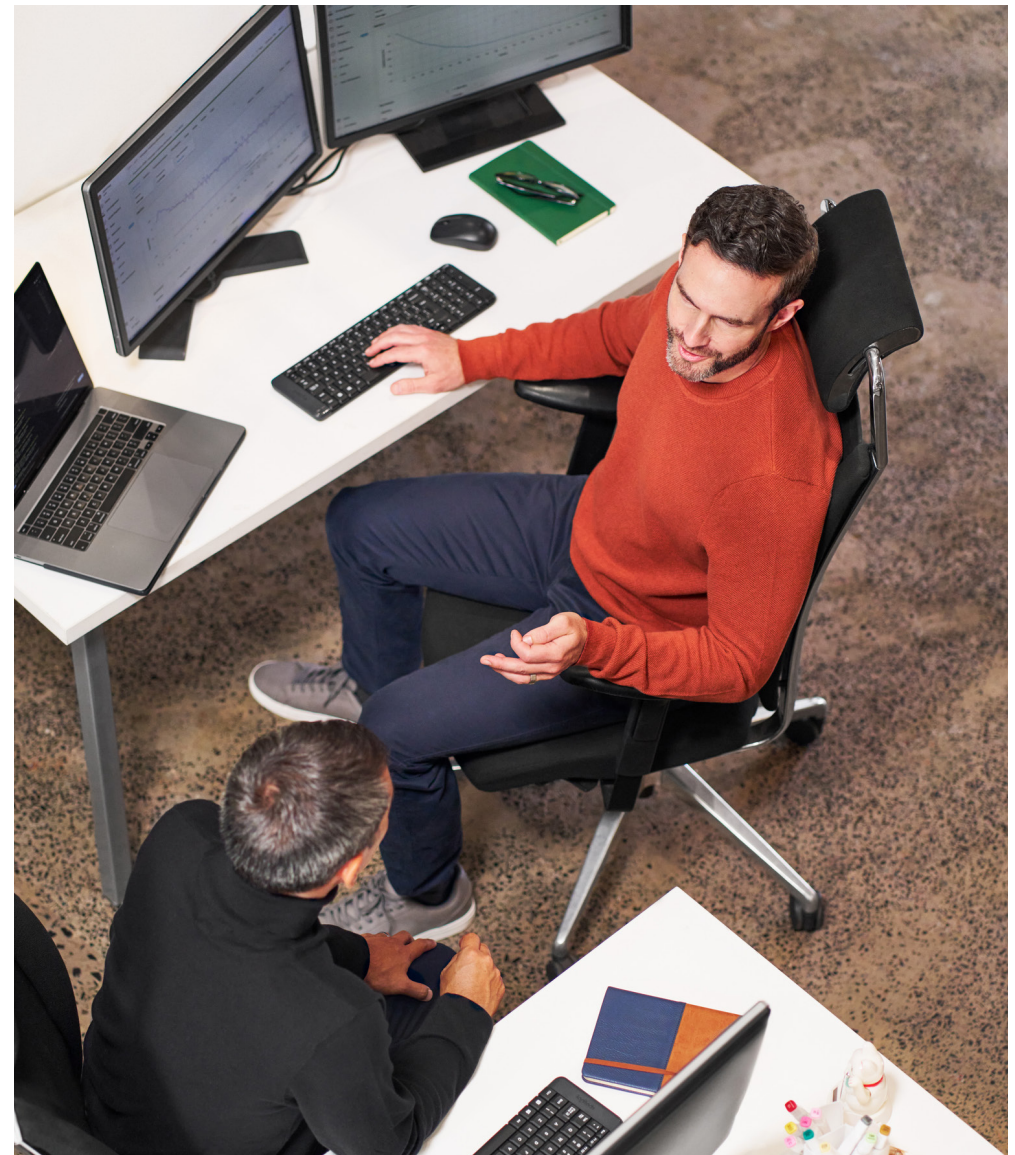


Step 2—Research and document your requirements

Once you've outlined your cyber resilience 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 cyber resilience strategy and in an incident response plan.** Based on your business impact analysis, 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 cyber resilience plan, including incident response teams. Document not just for implementation purposes but also for ongoing testing of your cyber resilience plans, including testing detection, remediation, and recovery.
- **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 compliant.

This step provides you with a clear, thorough map of your data protection needs, which in turn informs you of 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.



[→ more...](#)



Step 3—Establish your cyber vault buying criteria

Cyber resilience should cover nearly all workloads and data in your organization at some tier of protection. To maximize your cyber resilience strategy, you have to decide which tiers a cyber vault works best for and what type of cyber vault might be appropriate. There are two primary types of cyber vaults to consider:

- 1. Cloud vault**—A cloud vault is a logically air-gapped vault residing in a public or hosted cloud environment, offering isolation from production networks to store recovery data in an immutable state.
- 2. Physical vault**—A physical vault is a physically air-gapped hardware and software vault, typically on-premises (but can be hosted by a managed service provider), that requires someone to be physically present to manage.

The criteria you establish as being most needed for your organization will help inform you of which of these vault types best suits your needs. It may be that you choose a physical vault for some of your workload tiers and a cloud vault or even no vault for other tiers of workloads.



[→ more...](#)

Key buying criteria

Choosing a cyber vault 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 cyber vault buying decision.



Physical air gapping

The ultimate level of protection from cyberattacks is data that is not accessible on the network to a user of any kind. If data is on a network, someone with access to that network could access the data with the right compromised credentials, regardless of how well obfuscated it is. Physical air gapping means someone must physically have access to the data where it resides, for example, in the data center. This is usually done on-premises but could also exist with a data center managed by a service provider. Either way, someone would have to be physically on-site to access and manage the data. This protects recovery data from attackers, making it available in the event of an attack.

Logical air gapping

Unlike physical air gapping, logical air gapping isolates data that does exist on the network, most commonly through microsegmentation. Microsegmentation is a security method of managing network access between workloads. Organizations use microsegmentation to reduce the attack surface, improve breach containment, and strengthen regulatory compliance. While not as completely effective as physical air gapping, logical air gapping can be effective where attackers only have compromised, limited-privileged accounts.

Immutability

Beyond air gapping, the stored data in a vault is protected even from accidental deletion or compromise by making that data immutable. Immutability is the state in which the data cannot be deleted or modified for a specified period of time. This, by definition, requires that the data remain in a static state, as with a traditional backup, so more effective types of data protection where data is being written in real time to a recovery copy cannot use immutability until a copy of the data is made static, as with a snapshot. Regardless of how data is protected in real time or periodically, static and immutable copies of the data are used in a vault to protect against any potential data loss.

Detection

If an attacker goes undetected when initially infiltrating a network, either through a vulnerability or a compromised account, then the attack may not be detected until after data encryption begins. While it is important to try to detect intrusions when they occur, it is equally important to detect an attack in progress as quickly as possible. The longer an attack goes on, the more data can be encrypted. Detecting an attack in progress early allows incidence response teams to react quickly, isolating data and reducing the blast radius of an attack.

Many detection solutions are based on analyzing backups against previous backups to detect encryption. This can leave undesirable gaps in detection, measured in hours. Early detection within seconds or minutes of encryption helps to reduce the severity of the attack and speed up both recovery and remediation.

[→ more...](#)



Isolated recovery infrastructure

When you have been attacked, you know you have been compromised, but you likely do not yet know how or to what degree. Discovering compromised accounts, vulnerabilities, and malware is part of the remediation process. Until you can remediate the compromise in your networks, it is unwise to recover data and applications back to those networks where they can be attacked again.

Having an isolated recovery infrastructure that you know is not compromised is an important step in early recovery. Early recovery is not only important to perform remediation of recovered data but also in getting critical systems back online for business and operational functions. That isolated environment may not be where the data will ultimately be fully recovered, but it is, at the very least, an early staging area for verifying recovery of your data and application and preparing to recover back into full production.

RTO

When your critical business systems get hit by ransomware, can you afford to wait days or even weeks to recover? If not, you probably have a recovery time of hours or even minutes as your goal. Recovery time is crucial for reducing the impact of a disruption from a ransomware attack in terms of direct and indirect financial costs. Many factors, like how quickly you can detect an attack, how quickly you can have an isolated environment available, and how quickly you can begin remediation efforts, are key to how quickly you can recover.

RPO

When a ransomware attack strikes and data is encrypted, how much data can you afford to lose? Even paying a ransom does not guarantee you will recover all your data. 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 minutes or even seconds.

Because of the way cyber vaults use immutability and static copies of data, their RPOs are often measured in minutes and hours rather than seconds. This is a trade-off in having the data both air gapped and immutable in the vault for

protection from attackers. But a vault is not needed for every recovery scenario, so combining a vault with a real-time continuous data protection solution gives you the benefit of RPOs of seconds for some recovery scenarios, even from ransomware, and RPOs of minutes or hours in scenarios where recovering from a vault is necessary.

Scale-out architecture

Your critical data and application workloads may range from dozens to hundreds or even thousands. One key criteria for any data protection or cyber recovery solution is scale. It is not just a matter of storage and computing but also the ability to achieve desired RTOs and RPOs as the number of workloads and data scale up. Cyber vault solutions are no different, and you need a solution that can scale, whether it is a physical or cloud vault.

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 large-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.

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.

[→ more...](#)



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 successes 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 through recovery points. The larger your IT environment, the more valuable environment-wide analytics can be in monitoring the state of your data protection.

Recovery testing

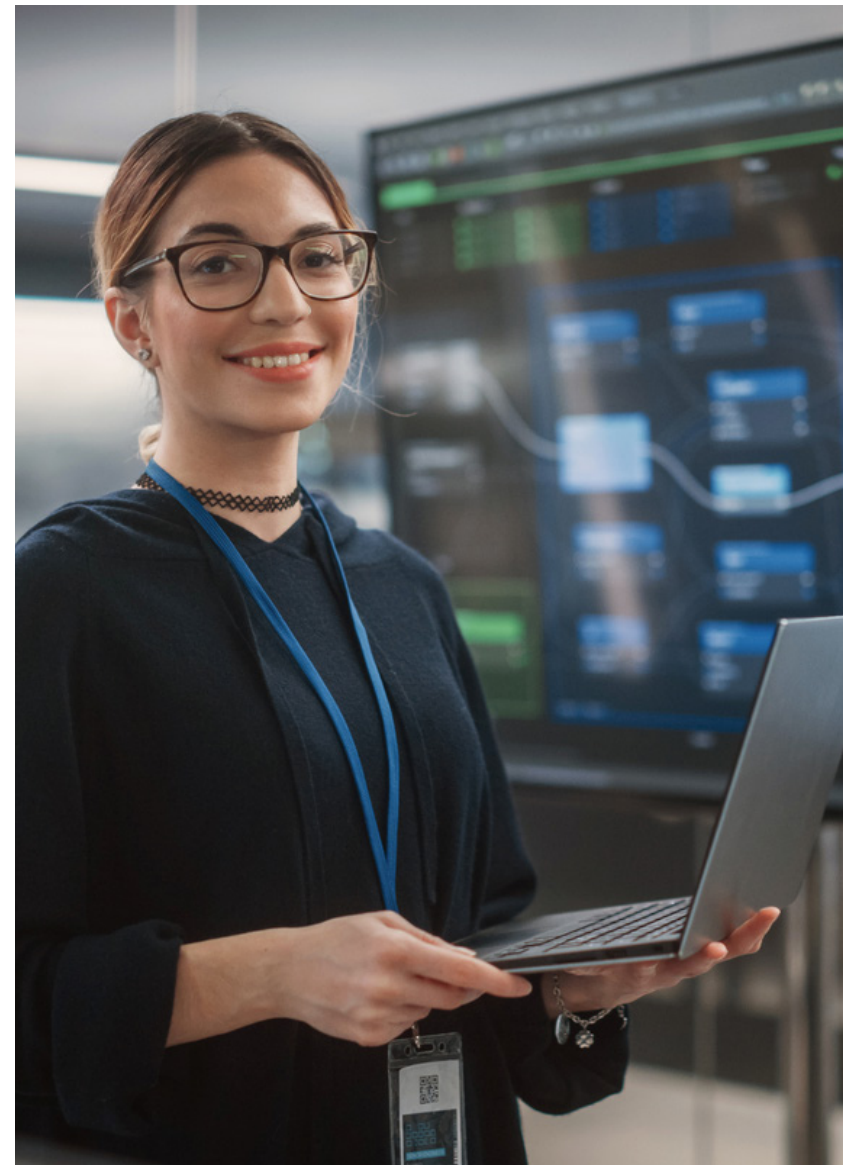
Like any data protection solution, a cyber vault solution needs the ability to test recovery regularly. Traditionally, recovery testing has been difficult enough that many organizations, despite their best intentions, struggled to test their recovery plans even once a year. These tests were often disruptive: 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. Frequent testing helps keep recovery plans up to date, identifies any issues due to infrastructure changes, and helps incident response teams stay fresh on understanding the recovery procedures.

Extensible architecture

Extensible options like APIs in a cyber vault solution can give you the ability to integrate with and leverage other solutions for detection and recovery. These integrations can help pull together cybersecurity solutions for more extensive detection, incorporate scans for malware, and speed remediation after an attack.

Solutions that use API-first architecture typically expose all controls, including lockdown security measures, for integration with third-party tools and services. The flexibility of extensible architecture provides more options for managing and monitoring protection both outside and inside the vault.



[→ more...](#)



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.



Backup as cyber recovery

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

A backup solution can sometimes meet RPO and RTO requirements for smaller, isolated events, but for cyberattack scenarios that affect entire sites, your backup solution's recovery capabilities are inadequate to recover within minutes, hours, or likely even days. In the context of recovering your business to total production, backups are better suited to long-term data retention rather than 24x7 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:

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

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 complementary:

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 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

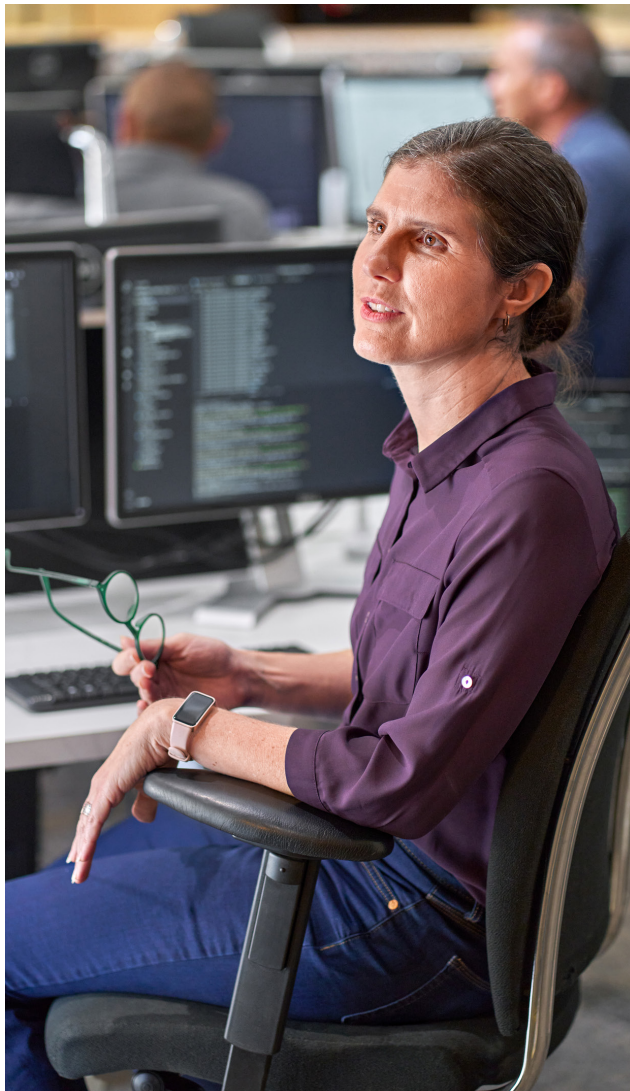
Have your experts and stakeholders try the solution to understand optimizations and potential challenges. Evaluations can be performed in a variety of ways:

- 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.

[→ more . . .](#)





Perform a total cost of ownership (TCO) analysis

The total cost of a cyber vault 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:

1. Perpetual licenses

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

2. Subscription-based licenses

Pay to use the solution for a specified period of time, in which the cost can be spread over the course of the subscription period as an operational expense.

3. Consumption-based licenses

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 running 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 (that is, as a capital expense or an operational expense).

[→ more...](#)

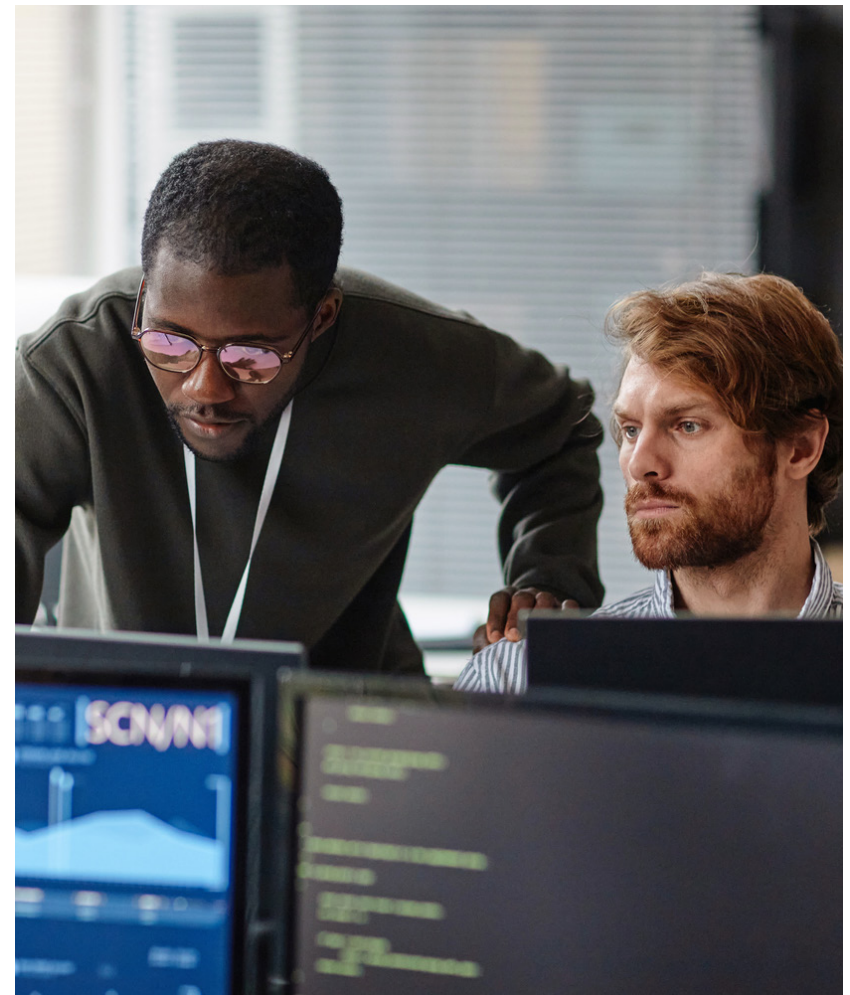
Using a managed service provider

Whether choosing to deploy a physical or cloud vault, a managed service provider (MSP) can add value to your cyber vault solution. An MSP can provide a separate security infrastructure from your environment, adding another barrier to an attack on your network reaching the MSP environment and your protected recovery data. An MSP can also offer add-on services for cybersecurity and protection, cyber resilience expertise, and day-to-day management of the solution.

When an attack happens, the MSP can also act as part of the incident response, taking actions to further isolate and protect data if necessary. For a cloud vault, an MSP can give you a more personalized cyber vault experience. With a physical vault, you should weigh the security risks of having the vault located on-premises in your own data center vs. within the hosted environment of the MSP. As with choosing the right recovery tools and infrastructure, choosing an MSP requires weighing the pros and cons of benefits vs. risk and cost.

Perform an ROI analysis

Justifying the cost of a cyber vault 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 a cyber vault solution. 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 a cyber vault after suffering from a ransomware attack.



Summary

Additional resources

Infographic: [Cyber resilience and cyber vaults](#)

Video: [What is a Cyber Vault?](#)

Solution brief: [HPE Cyber Resilience Vault](#)

Solution overview: [HPE Cyber Resilience Vault](#)

The data and the digital services we rely on daily are constantly under threat from cyberattacks. Organizations like yours face many challenges in developing a cyber resilience strategy to mitigate such disruptions. Your organization is unique, and only you fully understand the challenges your strategy must overcome.

There are many cyber recovery and cyber vault solutions available to incorporate into your cyber resilience strategy, and choosing one requires careful consideration of your requirements. Considering the criteria outlined in this guide—air gapping, detection, RTO, RPO, scalability, testing, and more—can help inform your buying decisions and enable you to choose the best solutions for your cyber resilience needs.

This guide ends with a checklist to help you keep track of the buying criteria we outlined in the previous section and the steps you need to take to get ready to start the buying process. The goal is to help you choose the best cyber vault solution for your organization's needs and to prepare you to handle any ransomware attacks that target you. You can find more information about specific cyber vault solutions in the listed resources.



→ more...



Cyber vault buying checklist

Approaching the buying process

Step 1—Identify your challenges

Perform a business impact analysis

Determine the likelihood of a cyberattack like ransomware

Gauge the difficulty of detecting an attack and responding quickly

Measure downtime disrupting business operations

Estimate data loss causing disruptions and lost productivity

Examine vulnerability of backups and recovery data to attacks

Determine the difficulty of achieving compliance

Analyze IT complexity, making implementation and management difficult

Step 2—Research, planning, and documenting

Document your cyber resilience strategy and plans

Research and document regulations and industry standards

[→ more...](#)



Approaching the buying process

Step 3—Establish your data protection buying criteria

Does the vault solution use physical or logical air gapping?

Does the vault make recovery data immutable?

Does the solution feature detection for ransomware attacks?

Is the detection real-time or based on scanning backups?

Does the vault feature an isolated recovery environment?

Does the solution offer RTOs of minutes within the vault?

Does the solution offer acceptable RPOs?

Does the solution have a scale-out architecture?

Does the solution feature automation and orchestration?

Does the solution feature nondisruptive recovery testing?

Does the solution have flexible recovery options?

Is the solution available as a managed service (DRaaS)?

Is the solution built on zero trust principles?

[→ more...](#)



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

[Visit HPE.com](#)

Learn more at
[HPE Cyber Resilience Vault](#)

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties 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.

a00151132ENW

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

