
The case for a modern data security and management platform

COHESITY

COHESITY

Table of Contents

Executive summary	3
Common beliefs about modern data security and management offerings	4
The cost of not making a switch	6
The benefits of a modern data security and management platform	8
What's next on your journey	10
About Cohesity	11

Executive summary

Today, an organization's most important asset is its data—and your leaders know this. They also know that destructive cyberattacks can happen at any time and cause a significant disruption. They've implemented backup and recovery solutions to mitigate the impact of these risks.

But if you're like many organizations, your current data security and management tools aren't up to the risks posed by modern threats. Many of these solutions only support a specific system, or a unique data source, leading to a fragmented approach to data that increases risk while adding cost and complexity. Today's threats also require an integrated approach where data security and management are seamlessly linked. If you're managing data in multiple systems today, you're increasing your risk and operational costs.

Because of these limitations, many organizations are reevaluating their existing data security and management strategies. After careful research and considering ROI, TCO, and the risk profile of their current data estate, they're moving to modern platforms that offer greater protection, global governance, faster recovery times, and better scalability and extensibility.

So when you decide it's time to take a closer look at a modern solution, the first question you'll ask is, "Where's the best place to start?" That's what we'll focus on here.

If you're trying to understand the business case for a newer tool or are responsible for making a case for one, we'll discuss reasons why people stay with their incumbent tools, the impact of sticking with your current solution, and the added value a unified platform can bring.

"Our long-time solution hadn't kept up with the times. Resolving periodic hiccups took too long. If a virtual machine failed, our engineering team had to rebuild it from the backed-up data, which took days."

- Luis Suarez, Chief Information Officer, H.I.G. Capital

Common beliefs about modern data security and management offerings

As with any change, moving to a modern data security and management solution can be hard, especially if you or your organization have concerns about the transition. Start by considering what criteria are important to you (e.g., compliance, cost, etc.) and use them to weigh your options. You might find that the status quo isn't the best option. Read on to understand why so many organizations are considering a new approach.

Cost

When you move to a new solution, there can be upfront costs for new hardware, software licenses, and personnel training. This investment might be overwhelming, especially when you're used to the expenses of your incumbent tools

Consider this: Maintaining your incumbent point products might actually end up costing you more in the long run. Why? It can be costly to license and maintain. A [survey conducted by Deloitte](#) found that, on average, IT departments allocate over 55% of their tech budget

to maintaining business operations and only 19% to developing innovative solutions. As data grows, it can also become expensive to add storage. What's more, data center space is at a premium for many organizations. Modern appliances can alleviate this pressure.



Security

Many believe a modern solution offers organizations greater control over their sensitive information and more response and recovery capabilities in the event of a cyberattack.

Consider this: Point data management systems are at an increased risk of data leakage and loss due to physical tampering, natural disasters, or outdated protection capabilities, all of which can impact customer relationships and incur high costs. In fact, [IBM reported](#) that the average global cost of a data breach in 2023 was \$4.45 million USD, up 15% over the last three years.



Data Migration

One word: painful. Migrating data can be time-consuming and expensive.

Consider this: Remember why you're considering a modern solution—to reduce your risk and increase your ability to withstand a destructive cyberattack. Data migration can lead to greater efficiency, improved data security, and rich response and recovery features to help you boost your RTO goals. Plus, most modern solutions offer capabilities to make the migration process easier.



Compliance

In highly regulated industries, there may be concerns about whether a new data security platform will meet regulatory requirements. Organizations might prefer to stick with current products that have a proven track record of compliance, rather than taking on the perceived risk of adopting a new platform.

Consider this: Modern solutions are often purpose-built to comply with industry best practices and industry regulations such as GDPR and HIPAA. With some solutions, it can be difficult to restrict access to the data they contain. They also weren't designed with today's threat landscape in mind, so many vendors have cobbled together additional features and capabilities to stay up-to-date, leading to increased complexity and risk.



Adoption

Change can be difficult, especially within large organizations with entrenched cultures and ways of working. There may be resistance to adopting new technologies simply because “that’s not how we’ve always done things” or because learning something new might be difficult.

Consider this: Most newer solutions are built with a modern UI and powerful APIs to automate workflows. Many also deploy their software as a service, meaning your organization doesn't have to worry about purchasing hardware or managing upgrades, and applying security patches.



Currently Happy

Similarly, some might be comfortable sticking with what works for them. Some decision-makers may not fully grasp the capabilities and benefits of modern data security solutions, causing them to miss out on the value of newer offerings.

Consider this: It's easy to be satisfied with your current system. But what happens in the event of a cyberattack? Have you truly assessed your risk, based on your status quo? More and more organizations realize that a modern platform, built with resilience in mind, is the superior option to defend against threats.

The cost of not making a switch

We all know that floods are going to happen and that, at some point, the power will go out. It's likely you're prepared for these well-defined disaster recovery and business continuity scenarios. But what about things that are even more unpredictable, like a cyberattack? When you're hit with an attack, you don't know what went wrong. You need to conduct an investigation and uncover the root cause. Only then can you thoroughly respond and begin your recovery. This new approach likely requires an evolution of your resilience strategy.

After all, it isn't *if* an attack will happen, but *when*. Even if you're satisfied with your current products, the reality is that not all solutions were built to address the needs of today's world. So if you decide to stay with your current provider, consider the impact this decision could have on your business.

Data Silos. Incumbent systems manage many silos of enterprise data, limiting an organization's ability to handle growing data volumes and scale. This can prevent you from responding to a cyberattack, resulting in prolonged downtime and significant operational and legal risk. Silos also cause inefficiencies that drive up operational costs. For example, an [IDC report](#) found the adoption of one modern solution saved organizations over \$720K in staff time per year because they needed 7.2 fewer FTEs to manage their IT infrastructure.

Wider Attack Surface. Today, organizations keep data across multiple environments (e.g., cloud, SaaS, on-premises), which broadens the attack surface and makes security challenging. Each environment may require a different approach to data protection, and there can be inconsistencies in the level of security across these environments.

Outdated Security Strategy. Solutions that weren't built for today's landscape are more susceptible to vulnerabilities, which cybercriminals can exploit to gain unauthorized access to systems, steal sensitive data, or disrupt operations. That's why so many companies pay the ransom. [According to Compliance Week](#), Change Healthcare, a unit within UnitedHealth's Optum, was rumored to pay \$22 million to get their data back after a ransomware attack in early 2024.

System Maintenance. Licensing and maintenance fees can cost organizations [thousands of dollars a year](#), and upgrades can take time away from higher value work that can drive innovation and improve your security posture. Additionally, as newer solutions hit the market, finding the skills needed to operate older systems becomes increasingly difficult and costly.

Employee Productivity. Over the years, companies have added newer products to their tech stack to address specific needs. In fact, IT and InfoSec teams all have dozens of tools operating within a narrow view of the environment. This leads to less productive teams because users have to constantly switch between systems.

Response Times. [Research commissioned by Cohesity](#) found that 79% of respondents were victims of ransomware attacks between June and December 2023 and just 7% were able to recover and restore their business process within 1-3 days. Exacerbating this issue is the fact that most organizations spend a vast majority of their cybersecurity budgets on protection and detection and only a token amount on response and recovery. Thoughtful investments in response and recovery capabilities is imperative to achieving RTOs/RPOs.

The benefits of a modern data security and management platform

We recommend looking for the following attributes when modernizing your backup and recovery efforts.

Simple to Use

A modern data security and management platform should provide a consistent and seamless experience everywhere: across infrastructure (on-prem, across clouds, at the edge) and across workloads. It should also be API-first and support straightforward integration with other IT and InfoSec systems. This way, data can be easily ingested, processed, and analyzed by other systems and tools, instead of creating a complicated web of solutions. By centralizing everything in one location, organizations can eliminate silos and enable IT staff to manage large data estates more efficiently. For example, [a leading insurance provider](#) saved \$2M in backup costs annually and enabled their small team to manage more data with less effort.

Built to Scale

Modern data platforms must be highly scalable to handle the large volumes of data generated by modern applications and devices—and to handle growing volumes of data and users. This allows for seamless expansion of capacity and performance as enterprise requirements evolve. The platform should also be able to handle data from a wide range of sources (VMs, enterprise databases, NAS, SaaS, cloud data sources), including structured and unstructured data.

Before and After: Hyatt's Story

For Hyatt, a global hospitality leader, managing multiple IT products worldwide became unsustainable, especially as data grew up to 20% at some of their locations. To gain efficiencies, its IT team moved to a modern solution that would ensure high-quality data replication and agile dev/test capabilities between its data center locations.

As a result, Hyatt reduced the time for data replication from days to minutes and saw a 40% reduction in capacity.

[Read the case study](#)

World-Class Security Built-in, Not Bolted On

A modern platform is based on Zero Trust principles, including role-based access controls (RBAC), MFA, immutability, and data encryption at rest and in transit. This ensures sensitive data is secured and protected from unauthorized access and cyberattacks. Ideally, your chosen solution can integrate with other [incumbent and emerging security tools](#) to strengthen your organization's security posture.

Fast to Recover

In the event of a cyberattack or unplanned disruption, a modern platform provides rapid, predictable recovery of mission critical databases. Organizations are able to do this with incremental backups and snapshots, which are stored in a separate location where they can't be altered. This is especially important for compliance purposes. A modern platform will also provide instant recovery and granular restore options so organizations can quickly recover specific files, databases, or applications without restoring entire backups. Using these capabilities, [Fortune 500 companies](#) have reduced their recovery time by up to 10x.

Before and After: Pearl River Community College

Over the last few years, colleges have become popular targets for identity theft and ransomware attacks. To protect student information and keep operations running smoothly during disasters, Pearl River Community College moved to a modern data security and management solution that offered access controls, including MFA, immutable backups, quorum, and cyber vaulting capabilities.

"Without those capabilities our insurance premiums would be much higher, if we could get insurance at all," said their CIO, Matt Logan.

[Read the case study](#)

What's next on your journey

Moving to a modern data security and management solution may seem daunting, but with the number of attacks increasing and the changing nature of cyber events, the status quo is no longer sufficient. That's why leading enterprises are preparing for the future by protecting their data with modern security and management solutions.

We recommend these next steps:

1. Determine what you want to accomplish by moving to a new solution.

- Set goals for RTOs and RPOs, storage, operation costs, etc.

2. Outline the use cases you'd want to support and what features are important.

3. Assess the ROI and TCO of a modern data platform for your incumbent solution. Key points of comparison should be:

- Data protection efficiency
- Operational efficiency
- Risk and compliance

4. Develop a business case. To win over key

stakeholders, make sure to:

- Demonstrate how the new technology aligns with the company's strategic objectives
- Clearly define the issues that the modern solution will address
- Explain the new technology and how it works
- Consider the cost and criteria of cyber insurance
- Quantify the benefits, such as cost savings, productivity gains, and enhanced capabilities (i.e., ROI)
- Outline the next steps for deploying the solution, addressing potential risks and how you'll mitigate them

Once you've gotten buy-in on a solution and you're ready to select a vendor, you'll want to assess your data, where it lives, and what dependencies your team has. You'll also need to think through data governance processes to maintain long-term hygiene.



About Cohesity

Cohesity is the leader in AI-powered data security. Over 12,000 enterprise customers, including over 85 of the Fortune 100 and nearly 70% of the Global 500, rely on Cohesity to strengthen their resilience while providing Gen AI insights into their vast amounts of data. Formed from the combination of Cohesity with Veritas' enterprise data protection business,

the company's solutions secure and protect data on-premises, in the cloud, and at the edge. Backed by NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud, and others, Cohesity is headquartered in Santa Clara, CA, with offices around the globe. To learn more, follow Cohesity on LinkedIn, X, and Facebook.

COHESITY

www.cohesity.com

© 2025 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and © is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

2000052-002-EN 1-2024