The case for a modern data security and management platform

COHESITY

COHESITY

Table of Contents

COHESITY

Executive summary

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

But the processes and products used over the last few decades weren't built to meet current and future business needs. Many of these solutions were designed for a specific task, leading to a fragmented approach to data that increases risk while adding cost and complexity. Additionally, modern threats require an integrated approach where data security and management are seamlessly linked. Older tools treat them as separate worlds.

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, 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 legacy providers, the impact of sticking with your current solution, and the added value a newer one 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

COHESITY

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 if you're satisfied with your existing solution.

Consider this: Maintaining a legacy solution 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.

Security

Which is safer: the modern option or your legacy solutions? Many believe the latter offers organizations greater control over their sensitive information and is less susceptible to cyberattacks.

Consider this: Legacy solutions come with their own security vulnerabilities. They're 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.

COHESITY

Data Migration

One word: painful. Migrating data can be time-consuming and expensive and could mean introducing a whole new set of challenges if you move to another solution.

Consider this: Sticking with your current solution could mean missing out on the value a new solution offers. Data migration can lead to greater efficiency, improved data security, and enhanced data quality, and 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 legacy solutions 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 actually quite secure, offering built-in security features, like encryption, access management, and advanced threat protection that help facilitate compliance with regulations, such as GDPR and HIPAA. With legacy 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 UI best practices and are designed to be both user-friendly and easy to adopt. Many also deploy their software as a service, meaning your organization doesn't have to worry about managing the application or handling upgrades and security patching.

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: What will you need to get you through the next 10 years? Will your current solution continue to serve you for another decade or would you want something that incorporates the latest and greatest (e.g., does the solution offer AI-capabilities to inform decision making? Is it cloud-native?)?

COHESITY

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 those situations. But what about things that are even more unpredictable, like a cyberattack? It isn't if it will happen, but when, so having a strategy in place is just as important. Even if you're happy with your current solution, the reality is that legacy solutions weren't built to address the needs of today's world. So before 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 meeting evolving business needs, create performance issues, and decrease productivity. 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. Because legacy solutions weren't built for today's threat landscape, they are more susceptible to known vulnerabilities and exploits, 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, product differentiation, and security initiatives. Additionally, as newer solutions hit the market, finding the skills needed to operate an older system becomes increasingly difficult and costly.

COHESITY

Employee Productivity. Over the years, companies have added newer products to their tech stack to address specific needs. In fact, the average enterprise has over 130 different cybersecurity tools, all operating with a separated view of the data they're protecting. This leads to less productive teams because users have to constantly switch between systems. It also causes staffing issues, as it's harder to find employees who can operate older, complex solutions.

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. One reason: older solutions don't support newer applications or offer the capabilities needed to protect them. Exacerbating this issue is the fact that most organizations spend a vast majority of their cybersecurity budgets on protection and detection and only a fraction on response and recovery. However, as this data suggests, attacks are going to happen no matter what, so investing in both equally will be imperative to achieving RTOs/RPOs.

[2] https://www.cohesity.com/press/cohesity-research-reveals-most-companies-pay-millions-in-ransoms-breaking-their-do-not-pay-policies/

COHESITY

The benefits of a modern data security and management platform

At this point, we've looked at the problems associated with older technology and discussed what a modern solution is not. We haven't, however, discussed an alternative or what to look for when modernizing your backup and recovery efforts. In general, we recommend looking for the following attributes.

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 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 legacy 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

COHESITY

Reliably Secure

A modern platform is based on Zero Trust principles, including role-based access controls (RBAC), MFA, immutability, and data encryption at rest/in transit. This ensures sensitive data is secured and protected from unauthorized access and cyberattacks. It also supports the identification of sensitive data, vaulting of data, detection of attacks, and bundle cyber incident response capabilities. Lastly, 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.

Data Driven

Every modern data management platform should support a range of data analytics and visualization tools, such as SQL-based analytics, machine learning, and natural language processing (NLP), so organizations can extract insights and value from their data. It should also offer AI capabilities, which aren't offered by every vendor, but can empower organizations to gather insights more quickly.

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

COHESITY

What's next on your journey

Moving to a modern data security and management solution may seem daunting, especially when your legacy solution has proven reliable over the years. 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.

COHESITY

About Cohesity

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data—across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises.

COHESITY

www.cohesity.com

2000052-001-EN 7-2024