LEARNING MADE EASY

Cohesity Special Edition

Next-Gen Data Management

for dummies®
A Wiley Brand

Finding modern solutions

Architecting for cyber resiliency

Protecting your data

Brought to you by

COHESITY

Peter Linkin

About Cohesity

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data — across the data center, edge and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics — reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

Next-Gen Data Management

Cohesity Special Edition

by Peter Linkin

for dummies®
A Wiley Brand

Next-Gen Data Management For Dummies®, Cohesity Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-87093-7 (pbk); ISBN 978-1-119-87094-4 (ebk)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Ryan Williams
Project Manager: Jen Bingham
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Business Development Representative: Matt Cox
Content Refinement Specialist: Mohammed Zafar Ali
Special Help: Lynn Lucas, Chris Wiborg, Brian Paulson, and Karen Logsdon Landwehr

Table of Contents

Introduction

If your organization was a solar system, data would be its sun. A car? Data would be the engine. A human body? Data would be the heart. These examples show how important data has become to today's enterprises. Doesn't it seem logical then that any solutions your company uses to take care of this hugely valuable and powerful business asset would be continuously evolving to take on whatever comes next?

Yet in today's fast-paced, technology-forward world, fundamental innovation surrounding the most widely deployed data management solutions has stood relatively still for nearly 25 years. That time frame predates the iPhone, Y2K solutions, and at least one dot-com boom!

Today, organizations across industries and the world need to take advantage of data to be more competitive. There's really no option B. Yet many can't because most data isn't being put to work while all of it is under attack.

Legacy data management technology has become an enterprise IT nesessity but there's never been much flexibility and choice in it. Vendors introduced tools for individual functions, requiring organizations to put them together like puzzle pieces. That approach led a whole lot of people (both inside and outside of IT) recently to wonder why data management products aren't better at doing the job they're supposed to do — which is simply managing data — and helping extract value from data. That's where next-gen data management comes in.

About This Book

In a few short chapters, this book helps you and your enterprise leaders understand the ins and outs of next-gen data management. You'll read both outlines of the management processes and the business challenges it solves. The book also shows how next-gen data management compares to what's likely rolled out right now in your data centers, public and private clouds, and edge locations. With this information, you and your teams can work smarter today while planning for tomorrow by asking the right questions about current data management tools and evaluating new, next-gen ones.

Foolish Assumptions

In writing this book, we've made some assumptions about you. We assume that:

- You are a business or IT leader interested in data insights and want to get to them as efficiently as possible (which means cutting existing operational complexity and cost).
- You want a better data management strategy.
- You are concerned about ransomware threats.
- You expect hybrid and multicloud to be increasingly important to your IT journey and vision.

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important details. Here's what to expect.

REMEMBER

Key definitions and points follow the Remember icon.

TECHNICAL STUFF

If you're on the IT side, the Technical icons draw your attention to details you won't want to miss.

TIP

Tip icons call out potential time and cost savings opportunities.

WARNING

Beware when you see the Warning icon — these indicate trouble spots.

Beyond the Book

Digital business is continually evolving. So is data management. Even though this book covers a lot, it's a point-in-time reference guide, helping you establish a solid foundation. To go deeper and always get the most up-to-date information about data management, visit `https://cohesity.com/next-gen-data management`.

IN THIS CHAPTER

- Defining data management
- Understanding the current landscape
- Discover who benefits

Chapter 1
The Legacy of Data Management

Data-powered digital transformation has been a top business goal for years. The COVID-19 pandemic accelerated this transformation while introducing new challenges. Companies faced the need to handle always-on digital experiences, hybrid working, virtual learning, pervasive cyberthreats, and changing regulations.

Yet digging just under the surface, businesses aren't benefitting the most from the world's growing data volumes and cloud proliferation. Very few organizations today can harness all their data for insights. Yet a large number of bad actors have figured out how to use enterprise data to their advantage. The data management solutions in use today are a big reason. Data is still the key to business transformation yet today's data management products are neither empowering nor safeguarding digital businesses. They should be. This chapter brings all aspects of data management to light and guides you through the introduction to these concepts.

Don't Go Back in Time

Imagine the capabilities you'd be missing (and security gaps you'd have) if you were still using the same computer you bought in 1999. Yet it's been over two decades since the data management products emerged that most IT teams still use today. Although you might be able to live without every new bell and whistle, legacy data management products haven't progressed in so many ways that they're actually holding your business back. Firstly, legacy data management products are still limited to one function, such as backup or disaster recovery. Secondly, these tools are unable to scale. Thirdly, they're very expensive and require many people to manage them. Fourthly, they provide limited visibility. Fifthly, they lack ways to work with other solutions and emerging technologies such *as artificial intelligence and machine learning* (AI/ML). And that's before diving through their Swiss cheese-sized security vulnerabilities. All of these deficiencies are why next-gen data management exists.

But before we really get into next-gen, you must understand the overall concept of data management. TechTarget defines data management as the process of ingesting, storing, organizing, and managing the data created and collected by an organization. Forward-looking IT leaders would expand this idea to add the way their enterprises make data visible and usable across the company as well as how the organization ensures data is secure and compliant with regulations. These tools encompass the protection of, consolidation of, and secure access to your data. Data management includes:

- Backup and recovery, disaster recovery (DR), archiving, and file and object services
- Development and test provisioning
- Data governance, security, and analytics capabilities

DIY Is Unfit for Digital Business

Digital business moves fast. Employees need the right data at the right time to discover new insights, and it's IT's job to facilitate reliable access to your organization's data with little to no

downtime to keep pace. IT must also keep all that data safe and in compliance with industry and government rules. How do you do that when you're working with a patchwork of products, siloed like Figure 1-1 illustrates, for each data management capability, including backup, file and object services, and data recovery?

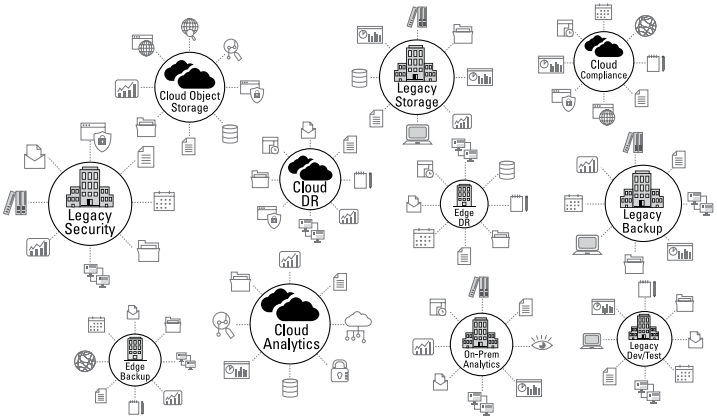

FIGURE 1-1: Silos slow down digital business.

The short answer is you probably don't. Why? Because it's likely you've gingerly assembled a *do-it-yourself* (DIY) environment of siloed data management tools that mostly works today (assuming your team is okay with regular interruptions to their nights and weekends for troubleshooting and restarting systems). And you planned to worry about tomorrow. . . well, tomorrow.

REMEMBER

In the multicloud era where industries and markets are changing at breakneck speed, your team can't afford DIY data management. Instead of providing a leg up, it slows you down and raises your risk profile. DIY tools' constant break-fix cycle burns IT specialists out and prevents you from harnessing data for insights while allowing malware to stay under the radar. In the end, DIY forces you to prioritize keeping your backups going over IT work-life balance and empowering your developers. Next-gen data management doesn't force these kinds of compromises.

Data Is Under Attack

Most technology analysts acknowledge organizations are using multiple public and private clouds while supporting onsite data center and edge infrastructure, creating a hybrid environment. Distributed business operations and uncontrolled cloud expansion, as well as mergers and acquisitions in various industries, create sprawling IT estates full of new data silos.

Now silos may be beneficial for storing food products like grain, but conceptually they're a big problem for digital businesses. By segregating and isolating data, silos make it challenging to unlock all data's value for competitive edge and easier for cybercriminals to hold your data hostage.

WARNING

Ransomware strikes are rising in volume and sophistication. So are ransomware costs. Estimates by Cybersecurity Ventures of global ransomware damage costs — everything from lost business and productivity to rebuilding — put the number above $265 billion by 2031.

But here's a more practical way to think about it. Just over every 10 seconds of every day, an organization like yours is hit with a ransomware attack. A legacy data management product is no match for ransomware criminals.

For the same reason Willie Sutton robbed banks — because that's where the money is — cybercriminals attack legacy enterprise backup. These thieves caught on to enterprises simply rolling back to clean copies to get back to business and are having none of it. Today's more malicious ransom schemes pressure executives to pay up and involve wiping backups clean, or worse, publishing or selling your data on the dark web.

TECHNICAL STUFF

Because existing backup solutions lack immutability (the inability to change data), they hamstring IT teams while allowing thieves to help themselves. So the choice is yours — you can risk losing your data and your reputation or defend your data with next-gen data management.

Complexity Holds IT Back

The title *backup administrator* yields more than half a million LinkedIn search results, making it Exhibit A in the case for how legacy data management continues to limit organizational and employee potential.

How many times have you heard frustrated backup admins say their backups experienced a failure? That backup and recovery times are bleeding into production? That fixing backups takes time away from configuring new systems for analytics or development and testing to help the business? Babysitting infrastructure is common when your organization relies on complex, patched-together data management products.

WARNING

When your organization runs complex, siloed data management capabilities — from backup to DR to analytics — on premises and in the cloud, you end up paying per functional silo in more ways than you may know. These expenses include the following:

- Hardware, software, server, and gateway expenses
- Specialist IT full-time salaries
- Integration expenses for technologies and teams taking care of IT, network, and security operations (ITOps, NetOps, and SecOps)
- Support and maintenance contracts

And those costs don't even include the added gymnastics your team has to do when a backup stops in the middle of the night or over a weekend, with no warning. Think about all the behind-the-scenes scrambling and the actual missing of children's gymnastics competitions and soccer games because only one specialist knows the product interface and how to troubleshoot a particular tool.

Fortunately, you can simplify the complexity that's no longer sustainable for your business or your specialist's professional development.

CLOUD ADDS EVEN MORE COMPLEXITY

After studying the impact of public clouds on data management, Vanson Bourne reported the serious consequences businesses face.

- **More time:** IT teams spend 19 weeks a year managing data and apps infrastructure across public cloud investments.
- **More people**: IT teams need to expand by over a third to glean maximum insights from all the data they store across public clouds.
- **More money:** IT budgets need to increase by nearly half.

Forewarned Is Forearmed

Although most of today's enterprise data is in backups, clouds, and drives, it doesn't have to be dark or dangerous. Your data is only that way because your teams have no canary in the coal mine. Instead they squirreled data away into legacy data management silos with no easy way to automatically search, identify, or access it.

WARNING

Different patterns, unusual access, and atypical actions involving your enterprise data can all be indicators of malicious activity. Yet manual data management makes it highly unlikely that your team can quickly and regularly spot these changes. That lack of insight allows threats to not only penetrate but metastasize in your environment.

Inflexibility Inhibits Innovation

Monopolies are frowned upon for a reason. Customers benefit more from solutions that openly embrace integration with others. Legacy data management is like a monopoly, mostly closed to third parties, by design.

To reiterate, traditional data management tools are meant to run only a single capability, like backup or file services. This

configuration makes existing solutions hard to extend and integrate with modern orchestration and automation tools. These outmoded tools also don't support any way to run external applications such as data analytics, reporting, or compliance functions directly against the global data in them, further limiting their business value.

Current Approach Characteristics

Putting a finer point on it, these characteristics define most current-generation data management tools:

- **Too complex:** DIY management that involves many products from many vendors across an increasingly diverse landscape is unscalable. You deal with an inefficient time sink for already-stretched IT teams. You also deal with higher *total cost of ownership* (TCO) and team burnout as IT struggles to meet operational *service-level agreements* (SLAs).
- **Too risky:** Lots of current-generation tools were designed decades before cloud and sophisticated cyberattack techniques became prevalent. Today, a single ransomware attack can destroy a company's reputation and operation in minutes because isolated components widen the enterprise attack surface and make detecting incoming threats nearly impossible.
- **Too unintelligent:** In addition to being short-sighted on security, earlier-generation tools are slow to automate key operations. Talk to backup admins and you can hear their exhaustion! Manual management is overwhelming IT pros, as are the hundreds of alerts from siloed products that they wade through without knowing which is a catastrophic warning.
- **Too closed off:** The way existing-generation tools are architected also makes them difficult to extend or integrate with other popular software products from orchestration tools to policy creators. Extensible systems take advantage of application programming interfaces (APIs) that closed systems can't. These more open systems also can run external apps such as analytics, reporting, or compliance, directly against the global data for more business value. Older-generation systems can't make this leap.

Legacy data management isn't optimal for doing the important things data management solutions are meant to do:

- Properly protecting data
- Making sure data is available
- Ensuring data compliance with regulations
- Securing data from ransomware
- Making data accessible to developers
- Efficiently storing, searching, and surfacing data for analysis

Isn't it time to rethink the traditional data management approach? Chapter 2 discusses this issue in more detail.

IN THIS CHAPTER

- Understanding foundational elements
- Seeing how simplicity is built in
- Recognizing the value of complete visibility

Chapter 2
Rethinking Data Management Architecture

Just because something has always been done a certain way doesn't necessarily make it the best way. Henry Ford proved it decades ago in transportation. And more recently, Google did it by making the world's consumer data accessible while Steve Jobs' Apple reimagined the phone experience.

What these innovators offered was a radical departure from the norm that included rethinking and redesigning underlying assumptions and architectures. They pursued the goal of simplifying tasks and unlocking new value for both people and businesses. This chapter applies that worldview to data management. Sounds grand, doesn't it? Take a look!

What Hyperscalers Got Right

Upstart, born-in-the-cloud companies taking on traditional brands and industries would still be unheard of if it wasn't for the world's largest cloud providers, including Google, Microsoft, Facebook, Amazon, and Alibaba. By providing apps and services to other organizations at massive scale, these *hyperscalers* jump-started and continue to drive digital transformation around the world.

TECHNICAL STUFF

The secret to the hyperscalers' success lies in their architectural approach, which has three critical components:

- **A distributed file system** enables the platform to keep doing what it does by making physically separate resources shareable across locations.
- **A single logical control plane** enables the management of all data, policies, and more so people can use the platform highly efficiently.
- **The capability to run and expose services atop the platform** delivers new functionality through a collection of applications.

Those concepts may be easier to follow with an example. On the way to achieving its goal of harnessing the world's consumer data, Google built a system to catalog all of the publicly available digital information in the world every day, from news stories to company products and more. Google's distributed file system is the heart of the operation. But to manage it, Google also had to invent a control plane that allowed its own engineers to manage all of that data as if it was all in one place. Once those two pieces were ready, Google began to roll out consumer applications like Gmail, Google Drive, Google Classroom, and Google Meet.

REMEMBER

Next-gen data management adapts similar architectural tenets to the specific needs of enterprise data management while adding zero-trust security principles and radical simplicity at scale.

Smartphone-like Simplicity

Today's smartphones put news, maps, a camera, and apps for pretty much anything and everything you want to do at your fingertips. Previously, people could access all of those capabilities in newspapers, GPS systems, cameras, online forums, phone books, and more. Folks just couldn't access them in a single, simple device they could slip into their pockets.

Smartphones, like Skittles or M&Ms, are great on the outside but equally as wonderful on the inside. As a platform, a smartphone runs an *operating system* (OS) like iOS or Android that extends the handset's functionality in new ways that dramatically increase its value. The OS manages all resources as shared, software-defined services, essentially removing the need for separate devices and allowing new apps to be added and used immediately with little or no training. Simple, right?

That simplicity is exactly what enterprise data management needs because it's really not uncommon for your enterprise to use legacy infrastructure that contains 10 to 15 separate components, each with a different *user interface* (UI), and likely an inability to share data with all the other components.

If you want to know more about the unearthed legacy data management challenges, from greater risk and extra management burdens to higher costs and lower agility, turn to Chapter 1.

The Value of a Single Data Estate

Imagine the visibility you'd have with an entire bank of security cameras in one dashboard and you'll understand the value of a single data estate. You can appreciate a fast, easy way to know what's going on everywhere in the environment without having to have a physical presence everywhere. That feature not only provides visibility but gives you the control you need to quickly optimize resources using the single control plane in next-gen data management.

Recent surveys point to somewhere north of 80 percent of companies today operating a hybrid cloud strategy. This approach mixes data center, private cloud, and public cloud workloads. And we see

no sign of that changing anytime soon. So having an easy way to see and manage all of your data, everywhere, will be key to digital business success.

REMEMBER

When you have a truly unified platform for enterprise data, you enjoy these benefits across data centers, edge sites, and public cloud environments:

- Unlimited scale that keeps pace with business and data growth
- Enterprise-grade security that keeps your data safe
- Optimized efficiency that allows everybody to work from a single, authoritative version of the data
- High reliability whether managing yourself or consuming in a *software-as-a-service* (SaaS) model (more on that in Chapter 5)
- Built-in automation that streamlines operations and helps defend your data against ransomware
- Simplified management that permits complete visibility into your data across all locations in just one UI

Now that you've gotten the 50,000-foot view of this new architecture, you can turn to Chapter 3 to get the real substance of what next-gen data management includes and means for your organization.

IN THIS CHAPTER

- Understanding next-gen data management
- Examining the four key pillars
- Recognizing imposters

Chapter 3
Solving Challenges With Next-Gen Data Management

Enterprise leaders share a host of reasons for why they're reluctant to move from the data management paradigm they've known for over two decades. "It costs too much to switch," "It's too disruptive to change," or "There's retraining involved."

What each of these concerns neglects to take into account is that business is always changing and that there's a cost — in hard currency and time — to operating as if it doesn't. There's really no greater example than the COVID-19 pandemic to prove this point. Those organizations with agile technology foundations that were able to surface the data they needed, when it was needed, had a leg up when it came to pivoting and adapting fast.

This chapter shows that the value of next-gen data management is simple: You get maximum agility and efficiency to adapt quickly while reducing risk.

Defining Next-Gen Data Management

Legacy approaches to data management are outdated. They're not only complex and risky, they're unintelligent and closed. That's why you and your organization need a whole new approach to support digital business in the multicloud era.

Next-gen data management delivers simplicity at scale. It provides ransomware protection and adopts principles of Zero Trust security. It also advances AI-powered insights and third-party extensibility to make it even easier for companies to derive value from their data. All-in, the four next-gen data management pillars, shown in Figure 3-1, give you a modern approach to cyber resilience for your hybrid or multicloud environment.

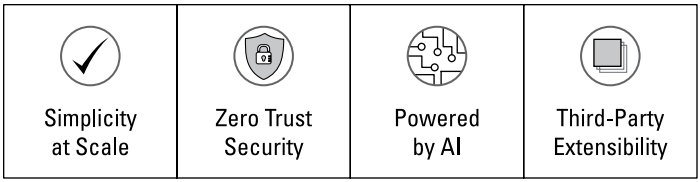

FIGURE 3-1: Next-gen data management delivers cyber resiliency.

Simple and scalable

IT teams spend a lot of effort managing and maintaining data infrastructure. (By one account up to 40 percent of their time.) This obligation limits time that could be used for innovation. Simplicity at scale is the best way to dramatically reduce your IT costs and complexity.

A next-gen data management platform powers multiple data management use cases (backup, archival, disaster recovery, file and object services, and analytics) in one, easy-to-use, scalable platform. This approach gives IT global visibility and consistency through a single user interface for any deployment model while the business enjoys repurposing data for insights.


TIP

Any checklist comparing data management solutions should include a next-gen data management platform that accomplishes the following goals:

- **Consolidates silos:** If the free flow of data is important to business success, silos must go. Next-gen data management lets organizations consolidate previously siloed functions onto a single, scalable software platform that runs multiple use cases at scale, slashing complexity and cost.
- **Supports managing globally:** With just a bit of training and from a single, intuitive user interface, next-gen data management makes the various management functions incredibly simple to operate without needing multiple specialists. This concept surely represents a better value for your IT budget! Complete management also ensures global visibility and control of all distributed data and activity across the hybrid cloud, minimizing admin effort.
- **Provides deployment model choice:** Because a next-gen platform runs natively in data centers as well as in public cloud and edge environments, it can be managed in-house, by a partner, or subscribed to as a managed SaaS service. You get to mix and match solutions to suit your environment and can change your mind (and configuration) over time with no penalty. In all cases, IT teams enjoy the same productive and intuitive experience.
- **Eliminates disruption:** Like many home improvement projects, upgrading legacy backup infrastructure seems easy until you get into the nitty gritty of it. Pretty soon, you're in for forklift upgrade pain. With next-gen data management, executives and IT alike enjoy expansion and software upgrades that take mere minutes and happen transparently while operations stay online. You encounter virtually no downtime.
- **Enables developer self-service:** Developers no longer wait for IT to manually provision datasets for them to test their applications. You can safely access zero-cost clones of production data instantly as needed with self-service tools.

Secure

Need more evidence that your data is under attack? In 2020, 65,000 ransomware attacks reportedly hit the U.S. alone. That's a lot of attacks every hour! Keeping your data safe is key to preserving your brand reputation and running your business smoothly.

Next-gen data management is built on the principles of least privilege and segregation of duties with granular security. IT grants each person the minimum level of access to all of the organization's data needed to do their job. Critical data processes and functions are spread across IT roles so no one person can compromise the whole business. With next-gen data management, a single platform comes complete with leading security vendor integrations and a holistic approach to threat detection and rapid recovery that keeps data safe and customers confident.

When you evaluate data management solutions, you should be looking for a next-gen data management platform that achieves the following goals:

- **Enables global visibility and control:** A top reason to adopt cloud is agility, which makes it difficult to fathom how bolted-on security makes sense. The hybrid cloud era requires security to be built into the architecture. A hyperscale file system spans from data centers to edge to clouds, enabling consistent control and visibility over all your data no matter where it lives.
- **Features proven, multilevel security:** Those least privileged and segregation of duties concepts covered previously — both for managing your data and administering the platform — are nonnegotiable as bad actors ramp up. You can't feel safe without deep, granular features that add additional security onto the hardened platform, including *multifactor authentication* (MFA*), role-based access control* (RBAC), *secure protocols* (such as NBD-SSL and gRPC), *WORM*, no service backdoor, and more to best safeguard your data.
- **Takes a holistic approach to ransomware:** Cybercriminals are sneaky and they pay attention. These bad actors are aware of traditional backup and restore routines where a company that has been attacked by ransomware rolls back to a system or version of data it believes has not been compromised to combat ransomware. Now, backups are a prime target. Your digital business needs a better way to preempt attacks and quickly recover if attacks get through. Newer tools will include anomaly detection, rapid response

with instant mass restore, automated data recovery and failover, and true immutable snapshots with data isolation via a cloud-based vault.

- **Leverages leading security ecosystem integrations:** Teamwork makes the security dream work. Extra hardened security is easier thanks to extended and operationalized integrations with third-party apps and services. These tools can provide the vulnerability scanning and continuous monitoring with assessments of administrative activity and security postures that's becoming an enterprise security must-have.

Smart

Only 32 percent of data available to enterprises is put to work — the remaining 68 percent goes unleveraged, according to a Rethink Data report. Improving decision making and jumpstarting response starts with AI power.

Think about how digital entertainment and streaming services like Spotify and Netflix build you recommended playlists. Next-gen data management discovers and keeps learning about your organization's data habits and trends, too (and without weird suggestions to try out dry documentaries or nail-biting horror movies). A next-gen data management platform features built-in intelligence that proactively averts potential issues and predicts future trends. This model empowers IT staff to accomplish more, and do it during regular working hours. AI-based integrations should detect cyberthreats without consuming precious resources on production systems.


TIP

Side-by-side comparisons of data management solutions should include a next-gen data management platform for the following reasons.

- **Works smarter, not harder:** Teams using next-gen data management leverage AI insights and ML techniques to lighten the load and prevent problems. Have you heard? Automation rules that you can set to take care of routine tasks and AI-based recommendations are giving IT pros their nights and weekends back.

- **Automates threat visibility:** Organizations can be prepared for when, not if, ransomware scenarios arise by soon using powerful AI-based algorithms that monitor and detect anomalies in their environments in near real time. Coupled with alerting, these capabilities point to signs of potential danger and initiate counter measures — such as recommending a clean backup — for rapid recovery from a ransomware attack.
- **Uses a smart assistant:** AI-enhanced algorithms make it easier to monitor, plan, and optimize operations in today's distributed IT environments. Similar to a parent-child relationship, these algorithms constantly learn and adjust, averting potential issues and providing predictive analytics-based alerts such as providing capacity utilization trends and proactive wellness checks.
- **Adds AI-powered market apps:** With an API-first platform, teams get powerful extensions that add value to enterprise data. AI-enabled apps can run in the same environment as the data, boosting accuracy and speeding time to results.

Ecosystem friendly

Having access to apps that extract value from your data is key to digital business success. But this implementation can be costly. You also need to take time to build all the data management apps from scratch. All of that effort goes into offering new functionality, performing analytics, and ensuring security and compliance. And in some cases, why even consider building, when you can get them faster and cheaper from a marketplace? Third-party extensibility helps your business meet today's unique requirements while future-proofing for tomorrow's by providing APIs for your developers and a single runtime platform for operations.

A next-gen data management platform seamlessly integrates popular third-party and custom-developed apps, including automation and orchestration tools, for deeper data security and simplified compliance. You get all of this along with greater visibility and insights.


TIP

Any evaluation of data management products should include a next-gen data management platform that delivers the following capabilities:

- **Brings apps directly to your data:** Instead of you doing the heavy lifting of moving your data to a separate system to extract insights, a next-gen platform runs apps and services directly against the managed data in the same environment. This considerably streamlines the traditional extract-transform-load (ETL) process and gives you faster results.
- **Allows you to choose which apps to add:** Similar to the way the Apple or Google app stores work, you can easily discover and download apps from a SaaS-based store through the same intuitive UI as all other operations. How much easier could it be to choose apps for everything from analytics and reporting to compliance, security, bare metal recovery, data masking, and more?
- **Empowers developers:** It's hard to overstate how much APIs matter. Next-gen data management is designed from the outset as an API-first environment because doing it this way delivers speed, flexibility, and security. Developers can use a rich set of RESTful APIs and an SDK to easily integrate next-gen functions into their apps and create new capabilities.
- **Supports integration with leading apps:** Your teams can take advantage of preexisting integrations with familiar apps and tools in current environments; for example, automation, orchestration, workflow operations, and configuration management. You get one platform with many choices.

Know What Next-Gen Data Management Isn't

Being armed with knowledge about next-gen data management makes it easier to spot imposters. These pretenders are data management platforms that bill themselves as *modern* but fail to incorporate the four key pillars in a single environment. The pretenders are also vendors promoting two distinct products — one for on-premises and the other for cloud environments — as a platform claiming to deliver a single, integrated experience. Finally, there are the SaaS-only data management products

purporting to be next-gen but only solving a single function and being unable to support the more than 80 percent of businesses predicting they will maintain a hybrid cloud environment well into the future.

REMEMBER

A key tenet of next-gen data management is the capability to take care of on-premises and cloud data sources equally effectively in the same environment.

Benefits of Next-Gen Data Management

Where legacy silos often stick out like sore thumbs, next-gen data management should provide a pervasive, invisible service. When you use this solution for your entire data estate, you evolve your hybrid cloud data strategy:

- Make complex data operations simple by keeping everything in one place and expanding with ease.
- Rapidly detect, protect, and recover from ransomware attacks.
- Improve decisions and act faster with built-in smart capabilities.
- Leverage third-party apps and integrating with industry-leading solutions.

If you're looking for a way to manage data faster and better, next-gen data management can definitely help. Chapter 5 describes next-gen data management platforms.

IN THIS CHAPTER

- Addressing boardroom concerns
- Architecting for cyber resiliency
- Defending against ransomware

Chapter 4
Zeroing In on Security

From pipelines to health systems, food supplies to police departments, high-profile ransomware attacks are making both news and money. *Harvard Business Review* reported the amount companies paid to hackers grew by 300 percent in 2020.

Although paying ransom quickly may be a short-term fix, it's not a long-term solution. Next-gen data management is. It's already proven effective against real-world ransomware attacks, with some organizations paying $0 and keeping their data and reputation intact. This chapter shows how next-gen data management is super helpful in the fight against unintentional human errors and malicious human actions.

Backroom to Boardroom

Data security used to be something InfoSec teams handled quietly in back rooms. With the rise in ransomware attacks, combating cyberthreats is now a board-level concern. For that reason, business and IT leaders alike have a vested interest in building cyber resiliency into infrastructure and operations. Before we dive into the details about how a next-gen data management platform both strengthens a cybersecurity posture and boosts ransomware protection — without requiring IT to do any additional work — it's helpful to define the terms that follow and look at how bad actors are adapting to stay in business. Take a look at the nearby sidebar "Data Security and Cyber Resiliency."

DATA SECURITY AND CYBER RESILIENCY

What is data security? Typically, when teams talk about data security, they're concerned about how best to protect digital assets (for example, documents, files, videos, and more) from unauthorized access, manipulation, and posting or selling of that data inside or outside of your organization. Best practices in data security include safeguarding both physical and digital infrastructure and data with either strict policies and procedures or guidance guardrails. Although very important to your business, data security is a subset of the larger boardroom concern, which is cyber resiliency.

What is cyber resiliency? NIST says cyber resiliency is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Basically, how quickly and efficiently can you bounce back from disaster? Think of this concept as empowering your teams to continually operate at peak efficiency and achieve your business outcomes — competitive advantage and high satisfaction with your brand and reputation — as you face threats head-on. In practice, cyber-resilient organizations have a strategy that accelerates the business while being prepared to respond and recover quickly using modern data security with data resilience, disaster recovery, failover, rollback, governance, and data management technologies.

Dealing with the Increasing Blast Radius of Ransomware

You know digital security is a mainstream business challenge when late-night hosts are pondering the role of crypto-currency in ransoming companies held hostage by cybercriminals as a source of humor and mirth. The increasing blast radius of ransomware is really no laughing matter.

The topic of ransomware continues to garner wide-spread attention because cybercriminals are getting more inventive. Here's what that means to your organization as the number and frequency of attacks and ransom demands grow and the payment countdown clocks begin:

- **Bad:** Early on, ransomware attackers simply went to the production data, encrypted it, and demanded payment for keys to unlock your valuable information. When companies began to counter this vector, bad actors went a criminal step farther.
- **Worse:** Cybercriminals realized it was more effective to go after the insurance policy. So they first destroyed backup data while lying in wait before triggering an assault on production.
- **Worst:** Today, bad actors steal your data (that's known as data exfiltration) and hold it hostage with threats of exposing it online or selling it on the dark web. Can you believe this is now more than 80 percent of new attacks coming in? Scary times!

Figure 4-1 shows the escalating threat to your data. Waiting to be attacked without a plan to recover isn't an effective threat defense strategy. Next-gen data management with sophisticated built-in data-security controls and proactive AI can be.

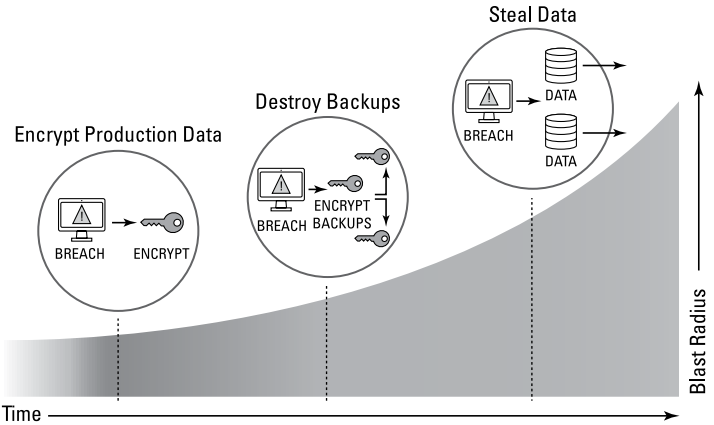

FIGURE 4-1: It just gets worse. . .

Threat Defense Architecture Counters Cybercrime

Data is both your most valuable and your most vulnerable asset. The rise in the number and severity of ransomware attacks makes it not a question of *if* your business will be attacked but

when. To ensure a payout, cybercriminals aren't just attacking a production environment anymore. They're increasingly targeting backup data and infrastructure — effectively hobbling the insurance policy your organization would depend upon if and when disaster strikes. And it's no secret that those ready for the worst case respond both faster and more effectively.

REMEMBER

A Threat Defense Architecture prepares your organization as much as possible to defend your data and improve your cyber resiliency. It's an architecture introduced by Cohesity specifically designed to counter the bad, worse, and worst-case scenarios described in the "Dealing with the Increasing Blast Radius of Ransomware" section.

Bad actors target production and backup data, but modern backup infrastructure as part of the Threat Defense Architecture can assist you in preparing for them. With everything from encryption to immutability to failover and failback, a next-gen data management solution helps defend against intruders and downtime in your environment.

Immutable backups, for example, effectively throw up a wall against ransomware attacks because they can prevent encryption, modification, or deletion — all common tactics cybercriminals use to force a ransom payment. A next-gen data management platform should also provide anomaly detection to alert you to when an attack may have taken place to help you react quickly and rapidly respond. If the worst case happens, you also have a way to rapidly recover data to any place and time.

Continuing on the subject of recovery, the Threat Defense Architecture made real by next-gen data management solution capabilities in Cohesity (we'll get to more of those in Chapter 5) can restore hundreds of *virtual machines* (VMs) in a few minutes versus a few hours, so you can get back to business fast. It also integrates with third-party software that can amplify and add security capabilities such as continuous monitoring, vulnerability scanning, activity assessment, and more.

Security professionals always recommend the *3-2-1 rule of data backup* — three copies of your data in two different locations with one of them isolated. Next-gen data management should offer

a way to accomplish this that doesn't rely on magnetic tapes to get an additional level of protection against ransomware and other disasters. In short, helping to defend your organization against that *worse* scenario. With next-gen data management from Cohesity, for example, you will have tools that let you simply spin up a data vault in isolation in a cloud environment. And the company will manage this for you as part of its cloud-based portfolio of data management services. There, you will still get your platform-based ransomware detection capabilities plus the capability to create a sandbox to run operational drills to validate that you can quickly recover when a real attack takes place.

Finally, stealing data and selling it without permission is getting out of control on the internet. But again, the Threat Defense Architecture prepares you for this *worst* case. By converging data security and data governance, next-gen data management allows you to fight back against nefarious acts and actors intent on making a worst-case negative impact. While data-security professionals are looking for who has access to your sensitive information, your governance pros are looking at where there's sensitive information in your environment. Bring these two goals together with next-gen data management and new tools that can first identify where your sensitive data lives and who has access to it to encourage proper hygiene, and then to monitor suspicious access to your data to identify potential attacks earlier.


TECHNICAL STUFF

This is where AI-powered intelligence and third-party extensibility, both core pillars of next-gen data management, can be very helpful. New tools will provide policy-based pattern and user behavior analysis to identify threats — which can then be sent along to third-party *security information and event management* (SIEM) and *security orchestration, automation, and response* (SOAR) tools for both forensics and to trigger appropriate remediation workflows, improving the interactions between your IT operations and Security operations (ITOps and SecOps) teams.

In a nutshell, the Threat Defense Architecture and a next-gen data management offering illustrated in Figure 4-2 offers you a simple way to monitor your business and help you stay secure.

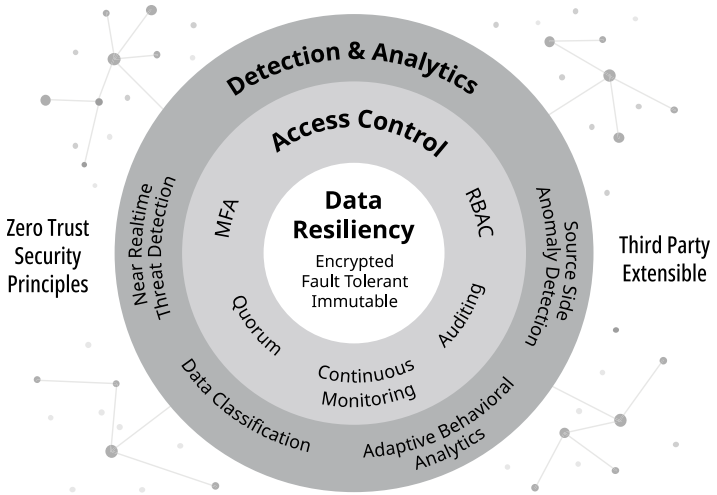

FIGURE 4-2: A quick overview of the Threat Defense Architecture.

Bring It All Together

Everything about next-gen data management centers on the same four pillars. The Threat Defense Architecture fleshed out in the Cohesity portfolio does, too. As a reminder, that's these:

- Simplicity at scale
- Zero Trust security principles
- AI powered insights
- Third-party extensibility

So let's get into Chapter 5 and dive deeper into what it means to bring next-gen data management into your organization.

IN THIS CHAPTER

- Breaking down silos
- Modernizing with purpose
- Discovering business benefits

Chapter 5
Welcome Next-Gen Data Management to Your Business

In everyday language, the word *disruptive* has a negative connotation, being unruly or undisciplined. In technology speak, disruptive is a positive. It may be a buzzword, but it represents innovative and trailblazing concepts that are always necessary. Next-gen data management is disruptive in the good, technology way. This chapter makes the proper introductions and gets your business moving the right way. It also introduces you to the Cohesity next-gen data management offerings.

Evaluating the Latest Platform

Like hyperscalers and smartphone innovators, modern tech companies are on a mission to radically simplify something that has been too complicated for far too long: data management. The goal is to use modern, cloud-scale engineering principles to solve an old problem in a brand-new way. The goodness this approach brings to organizations is not only breaking down data silos but securing and simplifying data management to unlock its limitless value.

INNOVATIVE ARCHITECTURAL APPROACH

The Cohesity solution takes the architectural approach used by the hyperscalers and adapts it to the specific needs of managing enterprise data. Three major parts support all the next-gen data management tenets. You get a software-defined multicloud platform, based on a web-scale distributed file system, that consolidates data across data centers, edge locations, and clouds. You also receive a single, logical control panel that lets you manage all aspects of a distributed deployment from a single, easy-to-use, graphical *user interface* (UI). Finally, you can run apps and expose services on top of the platform to provide new capabilities and extend the value of the managed data from within the same environment.

Consider the architectural principles used by the hyperscaler vendors (see the nearby sidebar **"Innovative Architectural Approach"** and Chapter 2). These concepts, used to manage exabytes of the world's consumer data, could be applied to the parallel challenge of managing enterprise data.

Innovative multicloud data platforms can consolidate all data, applications, and functions into a single logical software environment, effectively eliminating the silos, together with their associated complexity, inefficiency, cost, and risk. Today, that reimagined approach represents a market-leading next-gen data management platform with considerable innovations.

- Simplicity at scale
- Zero Trust security principles
- Powered by AI insights
- Third-party extensibility

Enterprises using this type of system can deploy a range of modern data management services and applications, including backup and recovery, data recovery, file and object services, development and test provisioning, data security and governance, and analytics. You can implement these features anywhere across your hybrid or multicloud environment, all while managing everything from a single, easy-to-navigate UI. Figure 5-1 gives you a high-level view of how all this works in the Cohesity world of products.

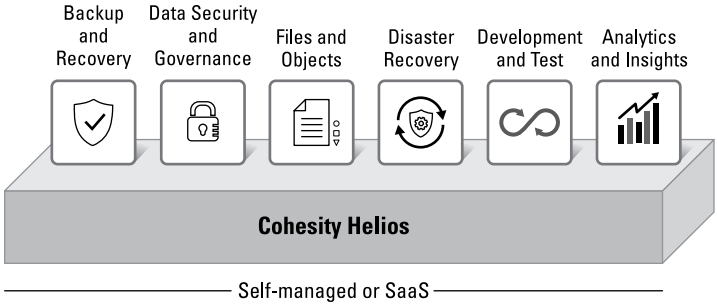

FIGURE 5-1: Take a look at this example Cohesity platform.

Inside the Cohesity Helios platform, Cohesity SpanFS brings together data from different systems across lots of different places by surfacing industry-standard, communication sharing pathways — specifically NFS, SMB, and S3 protocols — across many computing environments on a single platform. You can also take frequent read-only snapshots of your organization's data and store them efficiently, with little impact on how much space you're using. The original snapshot stays immutable, which means it can't be accidentally deleted.

Like certain soda companies or fast-food establishments, next-gen data management's secret recipe appeals to a lot of people. This approach makes it harder for enterprises to justify uniquely supporting and replacing a host of different legacy data management tools when one solution can not only do it all, but do it all better!

Next-gen data management means you'll have no need for your IT team to cobble together point products that were initially optimized for widely conflicting system demands. It's an all-in-one platform, for example, with backup; file and object services; agile dev and test; and more. You can even use it to handle a combination of data sources in public clouds, data centers, and edge locations. You want a solution that uses a single platform that solves all of these challenges while scaling to the moon with no performance compromise and the bulletproof reliability and availability organizations can bank on (especially if you happen to be working for a bank — we've noticed people take money seriously). Finally, make sure that solution takes care of the previously mentioned IT team by including features around instant restore, global dedupe and search, and unlimited zero-cost snapshots and clones. Those folks deserve a break, too.

Simplicity at scale

The optimal design of your solution should bring together a whole bunch of separate data management functions into a single platform. The platform needs to handle the next-gen data management pillar capabilities described in Chapter 3 to make operations easier and eliminate the generation of copy data that can account for up to 60 percent of total storage costs. You'll also want a metaphorical flashlight to get visibility into the previously *dark* data you've always had to worry about (even though you didn't really know where it was).

A COMPLETE PORTFOLIO IN ONE PLATFORM

The unified Cohesity platform approach provides a path to building and executing a successful data strategy. Often, enterprises begin by protecting all of their data and progress to consolidating all of their data and then putting all of their data to work. Your modern data protection solution handles backup and recovery for a wide range of data sources and environments across on-premises, cloud, and edge environments for maximum scale, performance, and efficiency.

The consolidation of files and objects from disparate sources, such as corporate file shares, cold buckets, videos, archives, and other unstructured data, combine with data-reduction technologies to more efficiently manage the data your organization keeps. Automated failover and failback orchestration for mission-critical workloads keep your business operating continuously. Agile development and testing represent your best approach to empowering your developers by providing high-quality test data to build better software, faster for competitive advantage.

Data security and governance will provide multilayered data protection, powered by AI insights. Combine those features with new robust data classification and governance capabilities to help prevent, detect, and analyze cyberthreats, particularly ransomware.

Finally, the data intelligence and analytics you build or get from a third-party marketplace enable you to report on-demand or on schedule to uncover new insights from your data and power competitive advantage.

You can easily manage a next-gen platform no matter how big your digital environment gets. You see and control your data in whatever locations you have — on-premises, in public clouds, or at the edge — from a single UI. That feature makes it a whole lot easier to keep up with your business and data growth.

Zero Trust security principles

Like the hard shell of an egg protects the soft center, consider how next-gen security capabilities will safeguard the data at the center of your business and keep your reputation intact. Security is built into the heart of the multilayered platform that reduces your attack surface. Bad actors and code have a much harder time getting through without your organization knowing about them.

TECHNICAL STUFF

For example, consider implementing an immutable file system that protects your backups. Why does immutability matter? Immutable data can't be tampered with, modified, or accidentally removed. This trait is super important for protecting the authenticity of data, particularly massive amounts of data such as audio and video files. Immutability also protects images for certain fields, such as law enforcement and healthcare, that require additional regulatory compliance. These days, organizations of all kinds are embracing immutability to avoid paying ransom while securing critical information, enforcing retention policies and streamlining compliance.

But vendors can't just talk the talk. Solutions have to walk the walk when it comes to granular built-in data safeguards. If Elizabeth Barrett Browning asked, "How Do I Love Thee?" information and security (InfoSec) pros might count the capabilities in Table 5-1 among the ways.

Finally, the right platform includes a new, innovative Threat Defense Architecture (covered in Chapter 4). This framework brings together the security capabilities plus ecosystem of security industry leaders to enhance and extend cyber resiliency even more.

TABLE 5-1 Built-in Data Security Safeguards

Capability	Advantage
Immutable snapshot	Produces gold copies of backup data that can never be altered
AI/ML	Powers proactive threat remediation and response
DataLock	Creates a write-once, read-many (WORM) lock on the backup snapshots
Encryption	Conceals data in code at-rest and in-flight
Role-based access control (RBAC)	Gives only authorized users data and operational access
Strict access controls	Gives admin and view options flexibility to assign based on job profiles
Multifactor authentication (MFA)	Requires both "something you have" and "something you know" before access is granted
No back door	Requires support account enablement by authorized customer users only
Secure SSH access	Creates a secure access path to tunnel across an unsecured network
Data isolation	Provides virtual air-gap protection, keeping data safe from external and internal threats
Failover and failback	Enables automated failover and orchestrated failback to the point and location of your choosing
Leading security integrations	Supports third-party security information and event management (SIEM) as well as security orchestration, automation, and response (SOAR) tools

AI-powered insights

Remember all those next-gen data management AI-powered insights requirements highlighted in Chapter 3? Leading platforms regularly monitor your backup data and will use machine learning and vulnerability scanning to give you visibility into anomalies — those suspicious behaviors that just don't seem right and often pop up before an attack. Detecting these atypical patterns can dramatically speed up detection and accelerate recovery time.

SHIFTING LEFT

It's never a good time for cybercriminals to let themselves in or internal staff to make an innocent error. But the architecture for Threat Defense and the Cohesity portfolio can help take your security incidents from crippling to manageable. By "shifting left" — as the tech industry is doing in moving testing earlier in the software development process to find and fix errors sooner — Cohesity is keeping up with the latest good-for-IT processes in helping teams improve ransomware threat detection.

There's an old saying that when you know more, you do better. AI technology helps you understand more about what's happening and avoid mistakes while giving you what you need to make better decisions in a shorter amount of time. These tools bypass the by-hand work that IT teams used to have to do with automated, proactive alerts and system health checks. Scanning capabilities are like drive-by looks across systems to make sure nothing is amiss while its recommendations for remediating issues save you time and can boost performance.

Third-party extensibility

It would be nearly impossible for one tech company — even one with a whole lot of engineers and product lines — to deliver every product and service a company needed and wanted to operate its digital business. Today, ecosystems and APIs take on the job of building bridges and pathways inside, between, and across applications and environments.

The right platform exposes a rich set of APIs and services that let developers use the exact same APIs and services for business benefit that in-house engineers use to build the product. The reimagined architecture makes sure these applications can run in the same environment as the managed data rather than requiring a separate system to be set up, really accelerating time to value compared to traditional methods.

Look for your platform choice to include a self-service marketplace for teams to consume them. We include some popular ready-to-use apps and extensions examples here:

- Data protection, including vulnerability and virus scanning
- Cyber resiliency, including eDiscovery, compliance, and data-masking security features
- Analytics and insights, including reporting, automation, and orchestration

These extensions expand structured and unstructured data value across many types of use cases.

Flexibility and Choice

The next-gen data management platform offers a high degree of choice and flexibility and that extends to deployment options, too. This software can be installed on-premises, at edge locations, or in multiple public clouds as a native solution. You or your IT team can manage it directly, or you can turn it over to a service provider. You should even be able to implement it as a service.

In all cases, IT teams use a simple UI to manage all data, workloads, apps, and policies globally with the same intuitive experience. This feature dramatically simplifies administration effort and allows your organization to match the solution to your exact environment as needed.

Organizations that rely on platforms like this are already experiencing significant business value and these benefits:

- Lower *total cost of ownership* (TCO) from simplified management and consolidation of silos
- Greater resiliency to disruption from cyber risk, including rapid recovery from ransomware attacks
- The capability to search globally for sensitive or regulated data
- Greater agility from unlimited scale and native multicloud support
- Capability to easily extract value from data through applications that can run in the same on-prem environment

This design is based on hyperscaler principles, a full range of enterprise-proven solutions, and a dramatically simplified

operational model with flexible deployment options. In short, this platform is setting a new standard for next-gen data management that's hard to beat.

What about DMaaS?

If you remember those Garanimals mix-and-match patterns and colors of clothes that let you dress how you want and made sure you looked great, you can appreciate next-gen data management. It might not include the animals, but it lets you mix-and-match, too. You can add *as-a-service* (aaS) and cloud-based capabilities to your on-prem environment or vice versa. Keep changing it up to meet your business needs, and pay only as you grow.

Data management-as-a-service (DMaaS) is for organizations seeking easy access to multiple data management capabilities as a comprehensive, integrated set of offerings in a *software-as-a-service* (SaaS) model. DMaaS is yet another aspect of an emphasis on flexibility and choice in how and where you want your data sources to reside. It's another simple way to protect, connect, and unlock value in data spanning those hybrid, on-premises, and public cloud IT environments.


TIP

If you want to know more, check out *Data Management as a Service For Dummies,* Cohesity Special Edition (Wiley) at `https://www.cohesity.com/forms/ebook/data management-as-a-service-for-dummies`.

Stair-Stepping to Benefits

For many organizations, getting into next-gen data management may seem intimidating. Yet just like the piece of fitness equipment that helps simulate walking up the stairs, with every investment there's a correlation to overall results improvement. For example, many organizations start by rethinking data ingest. They figure out how best to protect their valuable data from inevitable ransomware attacks while reducing costs. They then reimagine data services and streamline provisioning to gain efficiencies and insights. That's all before considering how to extract even greater insights and value by adding apps.

Figure 5-2 shows how a company's IT team looking to make a small change with Cohesity's next-gen data management can wind up with transformational improvements across the business.

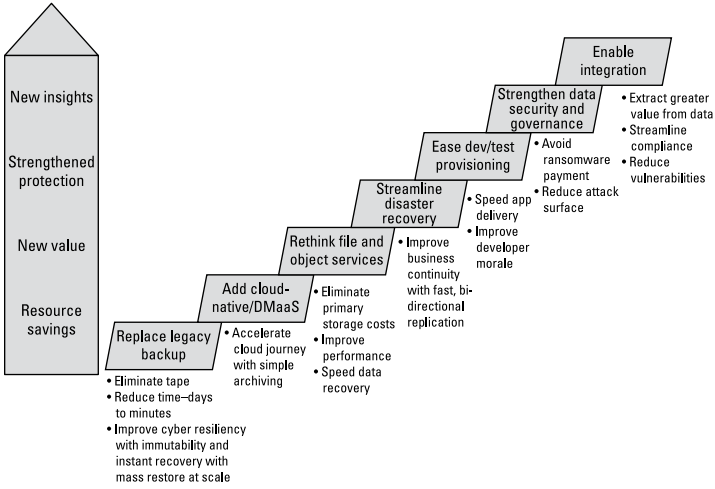

FIGURE 5-2: Climb the stairs to a better platform!

At the end of the day, this type of platform does two important things well: disrupting the long-established legacy data management industry *and* ushering in an era when data becomes a valued business asset rather than a risky and costly management headache.

To read all about how companies are using similar solutions to gain business advantage, move on to Chapter 6.

Chapter 6
Ten Industries Seeing Next-Gen Data Management Rewards

It's all well and good to have a basic understanding of what next-gen data management is (and isn't). It's another thing to discover it's already being used with exceptional results. Here are ten ways real-world organizations are using next-gen data management today.

Healthcare

After its IT environment was attacked by ransomware, a western U.S.-based health provider needed to rapidly recover data at scale — without paying the ransom. Not only did the company lose no money and rapidly recover its data, but it strengthened its overall security posture.

Financial Services

A global bank reviewed its entire data management strategy. Leaders hoped to reduce data silos and efficiently and securely manage large volumes of unstructured data. Their implementation included a dedicated infrastructure for sensitive data that met regulations, including SEC Rule 17a-4, CFTC, FINRA, and GDPR. This cost-effective solution had a comparable cost to low-tier cloud archiving. As part of the solution, the bank migrated nearly one billion files from tape. It also created an integrated NAS ecosystem with antivirus, file audit, and enterprise search capabilities across all file metadata and file content.

Government

Increasing data silos made operations and customer self-service for a U.S. federal government agency challenging. This solution lowered total cost of ownership by 50 percent and saved staff 30 hours per week by simplifying management. It also eliminated over-purchasing and long procurement cycles while implementing continuous customer service. The agency automated upgrades with no SLA impact and gained peace of mind. Finally, staff cut policy management time by a third.

Services Provider

Managing customer cloud environments and offering new services according to specific business requirements was becoming increasingly difficult for this service provider. The next-gen implementation reduced its total cost of ownership and helped it offer an expanded range of cloud services. The company now has seamless integration with leading public clouds. Finally, it implemented a simple and intuitive platform to manage multiple petabytes of data.

Pharmaceuticals

Facing a costly forklift upgrade of existing backup licensing and support across worldwide data centers, an international life sciences company sought simpler data management with seamless cloud integration. The company ended up with a 50 percent reduction in data management costs through cloud enablement. It restored data five times faster than before and improved efficiencies and IT productivity. Finally, the improved risk mitigation gave team members valuable peace of mind.

Education

Running a patchwork of point products was costly and inefficient for a K-12 school district. Its implementation eliminated four costly legacy backup solutions and vendor management. Leadership realized a five- to six-hour reduction in file restore times. Total cost of ownership took a 10 to 15 percent dip, and its strengthened security posture gave the school district valuable peace of mind as well.

Technology

The combination of ever-growing storage hardware and an existing backup solution had become overly complex and inefficient for a technology company to manage. Worse, its reality showed no signs of new data growth and sources slowing. The next-gen platform implementation reduced backup times by 98 percent. Any future expansion includes a scalable solution for data recovery and dev/test needs. The company also realized ease-of-management improvements for increased efficiency and automated processes. Finally, it saved up to 240 hours per month in SQL instance backup times. Everybody could stand to get that much time back!

Entertainment and Media

A digital studio dealt with massive projects including petabytes of data that IT regularly had to back up and archive to tape. This process led to growing storage costs and archival challenges. Imagine backing your phone up to an old cassette, then multiply both the scale and the frustration. This company's new implementation lowered data management total cost of ownership by 20 percent and realized a twofold reduction in storage data. Its 75 percent lower data volume reduced costs, and it gained 3 hours a week in IT productivity. Project backups that used to last months now take mere hours.

Hospitality

Managing multiple legacy IT products across numerous worldwide locations had this company's IT team looking to gain efficiencies. It specified high-quality data replication and agile dev/test capabilities between data center locations. The company's implementation handled all of this, including a 40 percent capacity reduction. The platform included rapid backup and restore capabilities, shaving necessary time from days to minutes. Finally, staff could quickly replicate backups for zero-cost dev/test.

Legal

A variety of legacy infrastructure solutions at a firm with six locations was becoming cost-prohibitive and difficult to manage, especially when it came to data recovery. Its next-gen implementation consolidated three platforms to a single interface for complete data management. The firm reduced Microsoft Exchange backup times by 99 percent and achieved data reduction rates of more than 150 times. All of this added up to significant capital and operational expense savings, which we're sure all the partners loved.

COHESITY

Next-Gen Data Management

AI Powered. Cyber Resilient.

Modern Challenges Need Modern Solutions

As your data grows, it becomes more complex to manage. With rapidly increasing ransomware threats, your data—and your business—is more vulnerable than ever.

At Cohesity, we believe that technology should work harder and smarter for you, whether it's reducing complexity, keeping your business secure, or delivering more value. We relentlessly innovate to build next-gen data management solutions that help you stay ahead of modern day challenges.

- Simplicity at Scale
- Zero Trust Security
- Powered by AI Insights
- 3rd Party Extensibility

Cohesity.com/next-gen-data-management

Discover next-gen data management

This book helps you understand the ins and outs of next-gen data management. You'll read both outlines of the management processes and the business challenges it solves. The book also shows how next-gen data management compares to what's likely rolled out right now in your data centers, public and private clouds, and edge locations. With this information, you and your teams can work smarter today while planning for tomorrow by asking the right questions about current data management tools and evaluating new, next-gen ones.

Inside...

- Defining data management
- Examining the four key pillars
- Looking at next-gen use cases
- Defending against ransomware
- Recognizing the value of complete visibility
- Seeing how simplicity is built in

COHESITY

Peter Linkin is a 30-plus year veteran of high-tech who has been writing and creating content around data management and associated industry trends for the last decade. He is currently responsible for strategic messaging and content at Cohesity.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119--87093-7
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.