BE: READY
RESILIENT

CUSTOMER STORIES

Modernizing IT infrastructure to protect data at scale

How four IT leaders future-proofed their cyber resilience

COHESITY

Introduction

In a 2024 survey commissioned by Cohesity and conducted by Censuswide, 67 percent of those surveyed said their organization had experienced a ransomware attack in the past six months. And while this was just one survey, we know that ransomware is an increasingly dire reality worldwide—and that most companies have put people, processes, and technology in place to secure their information. In fact, Palo Alto Networks found security teams at large enterprises use 130+ separate security solutions on average. However, by implementing these various solutions, many organizations have unintentionally created data silos, which make information difficult to protect.

With so much at stake, enterprises must look for a different approach—one that can reduce silos and scale with their business needs.

True preparedness must also include:

- Increasing visibility across all data environments—because you can't secure data can't see or manage
- Identifying where your data lives and which sources are the most important to protect
- Planning your response and determining strategies to minimize an attack's impact
- Partnering with your security team on cyber resilience initiatives

Cyberattacks will happen, but they don’t have to bring your business to a halt.

Hear from our customers, IT leaders, and practitioners as they share best practices for streamlining data management to scale protection and enable faster recovery.

BECKMAN COULTER

H. I. G.

Ausenco

DEPARTMENT OF FINANCE CALIFORNIA

Why change was needed

Their criteria for choosing a new solution

What improved after switching

Key outcomes

"With Cohesity we have great technology—and also a great partner. Our Cohesity team is invested in making sure we're successful with deployment and support, and that we have the features we need to protect the business today and into the future."

Kevin Chi
IT Systems Engineer
Beckman Coulter Life Sciences

BECKMAN COULTER

Industry
Manufacturing

Region
Americas

Manufacturer manages data across 11 global sites with a single platform

Background

Beckman Coulter produces diagnostic equipment for hospitals, labs, and doctors' offices around the world. Like many leading organizations, they relied on an amalgamation of tools to protect their organization.

Until 2019 they used a variety of backup solutions, including Arcserve, Dell Avamar, Veeam, and Veritas Backup Exec in its largest global offices. This led to complexity.

"Not having a standard backup solution made it complicated to monitor global backups and make sure we were meeting our service level agreements (SLAs)," says Kevin Chi, IT Systems Engineer at Beckman Coulter.

Each office needed an engineering specialist familiar with that location's backup solution, increasing costs.

Industry
Manufacturing

Region
Americas

Why change was needed

The existing solutions didn't protect against ransomware, a growing business risk. And the company wanted to switch to a SaaS model for backups and archiving for smaller locations, part of its "cloud-first" initiative to reduce on-premises infrastructure costs and management overhead.

What improved after switching

Today Beckman Coulter uses Cohesity to back up 330 TB of data in 11 locations in North America (183 TB in Phoenix alone), France, Ireland, and India. With the simple management interface, a central operations team can now manage backups and restores, avoiding the need for engineering specialists in each location.

The company's security posture is stronger now. One reason: With immutable backups from Cohesity, Beckman Coulter can restore clean data in the event of a ransomware attack, avoiding costs and business interruption. In addition, the Cohesity dashboard alerts the operations team to anomalous activity—such as a big change in the number of files from one backup to the next—that could signal a cyberattack. Plus, Beckman Coulter now installs releases containing security enhancements as soon as they're available while updates to backup as a service are handled directly by Cohesity.

Key Outcomes

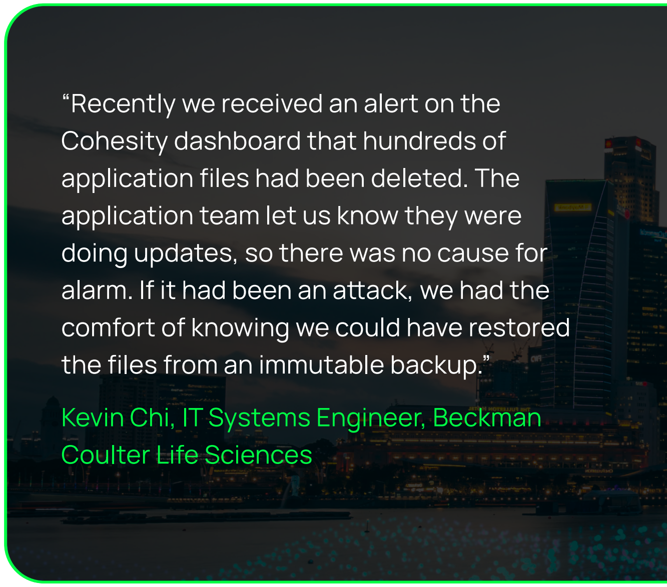
Stronger security and ransomware protection

Fulfillment of most VM restore requests in less than 24 hours

Single dashboard to monitor all on-prem and cloud backups

Criteria for choosing a new solution

- A single solution for all backups, both on-prem and cloud data
- Ransomware protection
- Self-managed and SaaS offerings
- Immutable backups



"Recently we received an alert on the Cohesity dashboard that hundreds of application files had been deleted. The application team let us know they were doing updates, so there was no cause for alarm. If it had been an attack, we had the comfort of knowing we could have restored the files from an immutable backup."

Kevin Chi, IT Systems Engineer, Beckman Coulter Life Sciences

“We don’t need to spend time on the nuts and bolts of backing up in the cloud because Cohesity FortKnox does it for us. **I also recommend FortKnox to the companies we invest in to help them work smarter while strengthening security.** A single product that can do both of those things is a winner.”

Luis Suarez
Chief Information Officer
HIG Capital

H. I. G.
CAPITAL

Industry
Manufacturing

Region
Americas

Investing in the future with stronger ransomware protection

Background

H.I.G. Capital is a leading global alternative assets investment firm. Over time, their legacy cloud backup solution became less reliable.

For more than a decade H.I.G. Capital had been backing up its virtual machines in the cloud, with LiveVault. “Our long-time solution hadn’t kept up with the times,” says Luis Suarez, CIO.

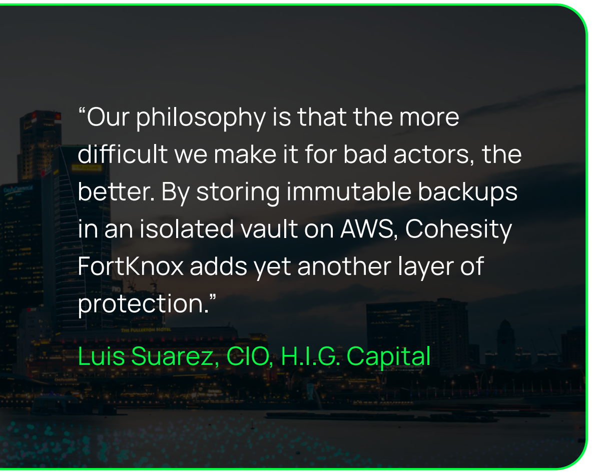
“Resolving periodic hiccups took too long. If a virtual machine failed, our engineering team had to rebuild it from the backed-up data, which took days. And with rising cyber threats, we needed ransomware protection.”

Industry
Finance

Region
Americas

Criteria for choosing a new solution

- Ransomware protection
- Greater efficiency
- Integration with VMware vSphere
- Having an innovative partner



> “Our philosophy is that the more difficult we make it for bad actors, the better. By storing immutable backups in an isolated vault on AWS, Cohesity FortKnox adds yet another layer of protection.”
>
> Luis Suarez, CIO, H.I.G. Capital

Why change was needed

In addition to being less reliable, their legacy solution lacked ransomware protection and a fast way to restore virtual servers. With the number of cyberattacks increasing, they needed a solution that offered greater security.

What improved after switching

H.I.G. Capital started with Cohesity DataProtect, backing up 30 TB of virtual machines and databases in two data centers. A few servers running in branch offices are backed up in the cloud with Cohesity DataProtect delivered as a service. No matter where they’re stored, Cohesity backups can’t be encrypted or deleted as part of a ransomware attack. When Cohesity FortKnox on AWS was introduced a year later, H.I.G Capital adopted it for even stronger security.

Just three months after deployment, H.I.G. Capital saw the value of Cohesity for business continuity firsthand. “When a faulty patch impacted our Citrix servers, with a few clicks, we restored them from a snapshot we knew to be secure,” Suarez said. “The first server was back online in an hour and all of them within a day. Before we had Cohesity, our engineers would have spent two long days rebuilding the servers from scratch, testing them, and checking for security compliance.” Restoring virtual servers with Cohesity is so quick that engineers now do it routinely if they can’t resolve a server issue after 30 minutes of troubleshooting.

Key Outcomes

Faster restoration of virtual servers

Stronger ransomware protection

Less time spent on backup and maintenance

“We do everything we can to prevent cyberattacks, but **having the ability to restore clean M365 data** from Cohesity’s immutable backup copies means we have a solid fallback.”

Kalpesh Bhathella
Director of Operational Services
Ausenco

Ausenco

Industry
Other

Region
Americas

Saving time and money with simplified data management

Background

With their engineering and consulting services business growing, Ausenco's previous backup solution no longer met the company's security needs.

The company backs up 100 TB of critical M365 data for its more than 3,000 employees. "Microsoft provides some data protection built-in, but not enough for our business," says Kalpesh Bhathella, director of Operational Services. "We retain some SharePoint and OneDrive files indefinitely, and can't afford to lose them to cyberattacks."

Until 2022, Ausenco's IT team backed up M365 data with Veeam software, using infrastructure as a service (IaaS) from Amazon Web Services (AWS). But managing the infrastructure and software was brutal, consuming 50% of one IT administrator's time. Another shortcoming: Taking immutable backup copies, a must-have to recover from cyberattacks, would require more infrastructure and more management time.

Ausenco

Industry
Other

Region
Americas

Why change was needed

“Security is top of mind for us,” Bhathella says. “Prospective customers always ask about it, and lately they also want to know if we have cyber insurance. We needed immutable copies, but without more management burden.”

What improved after switching

“The savings from not having to pay monthly fees for cloud infrastructure fully paid for Cohesity DataProtect delivered as a service,” says Bhathella. “On top of that, we’re saving the 20 hours a week we used to spend tuning and managing our backup software and cloud infrastructure.” The team member who used to devote 50% of their time managing backups can now spend that time on higher-value digital transformational work. And together with Ausenco’s other cybersecurity measures, immutable backups helped the company qualify for favorable rates on its cyber insurance policy.

For the first time, Ausenco is offering a 4-hour SLA for M365 email or file recovery—a big hit with the company’s busy engineering, consulting, and operations teams. “With our old backup solution, restoring a lost Exchange, SharePoint, or OneDrive file could take weeks because our IT admin had to comb through hundreds of backups just to find it,” Bhathella says. “Cohesity’s search engine is like the Google of backups. We just enter a filename or phrase, and a list pops up. The file we’re looking for is often right on top.”

Key Outcomes

Immutable copies—a requirement for cyber insurance

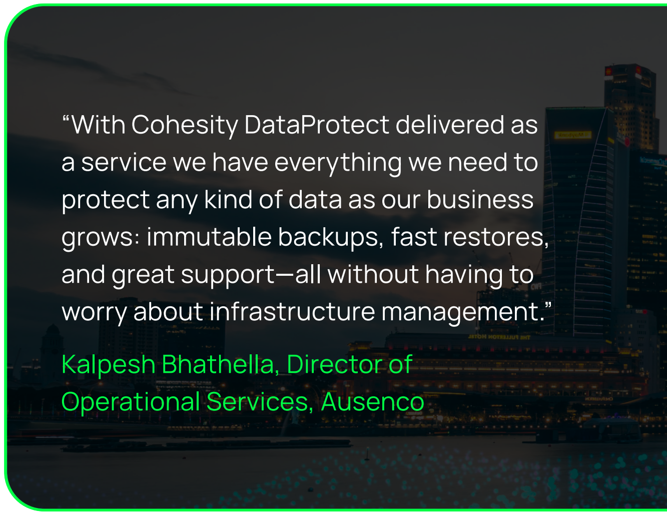
Up to 99% faster restoration of M365 email and file restores

20 hours/week management time saved

$0 additional expense

Criteria for choosing a new solution

- Scalable
- Easy to use
- Protection for M365
- Immutable backups



> “With Cohesity DataProtect delivered as a service we have everything we need to protect any kind of data as our business grows: immutable backups, fast restores, and great support—all without having to worry about infrastructure management.”
>
> Kalpesh Bhathella, Director of Operational Services, Ausenco

> “Maintaining our old on-prem data protection solution took more than 24 hours a month. By providing backup as a service, Cohesity has freed up time to work on other projects that support our mission.”

Chris Dove
Enterprise Architect
California Department of Finance

Industry
Public Sector

Region
Americas

Restoring data within 12 hours of a cyberattack

Background

The California Department of Finance's mission is to serve as the Governor's chief fiscal policy advisor and to promote long-term economic sustainability and responsible resource allocation.

January 10 holds special significance for the California state government, as that's the day the governor submits a budget to the legislature. The vote is held on June 15, and the weeks before both dates see a flurry of activity for the Department of Finance. "If data goes AWOL in the busy weeks leading up to those deadlines, the budgeting process grinds to a halt," says Chris Dove, enterprise architect for the State of California Department of Finance.

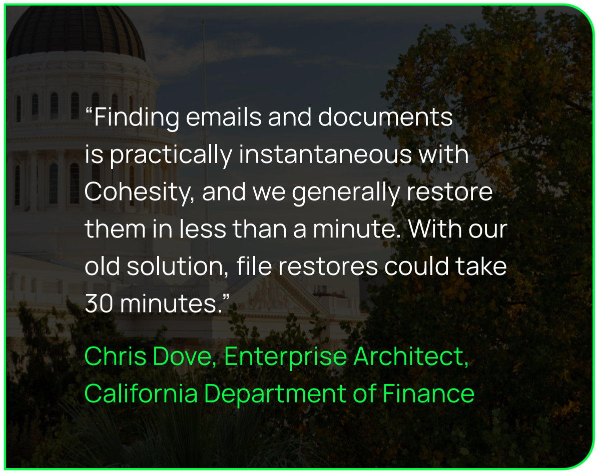
This is one reason why the Department's IT team needs secure backup and recovery of M365 data—Exchange, OneDrive, and Teams—for its nearly 500-person workforce. "M365 doesn't have SLAs for data restores," Dove says. "Your only backup is your recycle bin. So if the recycle bin gets corrupted or you need a deleted file past the retention period, you're out of luck."

Industry
Public Sector

Region
Americas

Criteria for choosing a new solution

- M365 protection
- Robust security capabilities
- Fast recovery times
- Backups stored in the cloud



> “Finding emails and documents is practically instantaneous with Cohesity, and we generally restore them in less than a minute. With our old solution, file restores could take 30 minutes.”
>
> Chris Dove, Enterprise Architect, California Department of Finance

Why change was needed

Until 2020, the Department backed up M365 data on-prem, using the server vendor’s proprietary software. But backups and restores required multiple interfaces, finding lost files took too long, and software maintenance consumed several days a month. “We spent more time on software updates than on backups,” Dove says. “We knew we’d move backups to the cloud at some point.” That point arrived sooner than expected when the Covid pandemic sent staff home to work.

What improved after switching

The Department started by using Cohesity to back up M365 data in Microsoft Azure. At first, they continued using their legacy software to back up virtual servers on-prem. All was well until December 2022, when the Department was hit with a ransomware attack—in the middle of a budget cycle. “I woke up to an early-morning call from my system analyst, who was alarmed about unusual activity on the network,” Dove remembers. “We took what action we could, but soon our laptops were encrypted and mountains of ransom notices started spewing out of every network-connected printer. I’ll never forget having to call our CIO to say, ‘We’ve been ransomed.’”

In the frantic hours that followed, a bright spot: “After the ransomware attack we restored all 2.5 TB of M365 data—protected by Cohesity DataProtect on Azure—in 12 hours,” Dove says. “We paid no ransom.”

The Department also ultimately recovered its virtual servers, which had been backed up on-prem with another solution. But restoring that data took a herculean, 72-hour effort.

Today, with the ransomware attack in the rearview mirror, the IT team has peace of mind. They know they can recover data quickly when the next security event happens.

Key Outcomes

12 hours for automated restore of M365 data

24+ hours/month reclaimed by eliminating software maintenance

97% faster file restores: < 1 minute

68.7% savings in TCO

Final thoughts

As our most recent survey report shows, organizations have a significant opportunity to strengthen their cyber resilience capabilities to protect against today's threats. In fact, only 2% of those surveyed said they could recover their data and restore business processes within 24 hours if a cyberattack occurred.

But the customer experiences in this eBook tell a different, better story. And your reality can be like theirs. By taking a new approach and implementing a modern backup and recovery solution, it **is** possible to future-proof your cyber resilience.

To learn more about the solutions these leaders implemented and try them out for yourself, visit our Cohesity Product Demo hub.

Download the full survey to learn more

COHESITY

Ready to strengthen your cyber resilience?

Get to know our AI-powered
data security at cohesity.com