BE: READY RESILIENT

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

COHESITY

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.

ENDOR

croix-rouge française

EASTERN COMPANY SAE

infrafürth

Why change was needed

Criteria for choosing a new solution

What improved after switching

Key outcomes

ENDOR

" "

"If you just look one year into the future, the time that you spend on the initial deployment, on meetings, and on support cases will be very small compared with the time you would have spent maintaining an older infrastructure— and you'll be no closer to growing. I'm fully confident in the way we work now. If you want to create a scalable platform for growth, then **Cohesity is the obvious partner.**"

David Thor Kristjansson
Co-Founder and Manager of Sales
Endor

ENDOR

Industry	Region
Service Provider	EMEA

Eliminating legacy infrastructure silos with a modern backup and recovery solution

Background

Endor provides strategic consulting and IT services, and like other fast-growing organizations, its IT infrastructure no longer met its business needs.

Towards the end of 2020, Endor faced a significant technology challenge. Chief Technology Officer Magnus Franklin says his company relied on a complex array of partners and licenses to help serve its clients. The IT environment involved many moving parts and interfaces across its backup software and disk devices. Even worse, Endor's legacy Veeam backup, HPE 3PAR storage and HPE Apollo server environment, were running out of support.

This legacy infrastructure required a huge amount of maintenance. Staff would endure sleepless nights as they worried about potential network downtime or new backups choking Endor's existing storage arrays.

ENDOR

Industry	Region
Service Provider	EMEA

Why change was needed

The antiquated nature of the environment required investment in its data management infrastructure. Franklin and his colleagues believed that investing in modern technologies would create a simpler IT setup that would be easier to manage.

"We took a step back, looked at everything, and we thought, 'What can we do that would make sense in five years?' And that was really an easy decision on our behalf. We are planning to grow a lot in our domestic market in the coming years."

What improved after switching

In February 2021, Endor made the move to Cohesity DataProtect, a radically simple backup and recovery solution that allows the company to eliminate legacy infrastructure silos by consolidating its data services.

"It was incredibly easy. We had already worked extensively with Cohesity, so I expected an incredibly simplified process compared to our legacy infrastructure. The actual setup was just so streamlined—it arrived, we racked it, plugged it in, and we started backing up data on the same day it was delivered to us."

Using Cohesity has had a huge impact on human resources. Rather than having to relying on three in-house staff members to actively manage Endor's legacy IT environment, these resources are freed up to work on strategic projects and the team can focus on acquiring new business. Additionally, major restores that once took as many as 26 hours can now take just 10 seconds.

Franklin explains how Endor recently onboarded a new major Icelandic customer, Vodafone Iceland. By working with Endor and its Cohesity platform, Vodafone Iceland increased the number of VMs it could back up fivefold, thanks to Cohesity's superior deduplication and compression compared with the previous Veeam solution.

Key Outcomes

Data recovery times reduced by over 99%

Data center footprint reduced by 80% for significant cost savings

Return on investment anticipated within 24 months

Storage reduction of over 55x

Criteria for choosing a new solution

- Scalable backup and recovery
- Easy to use
- Greater operational efficiency

"This was something that wasn't even possible in our old infrastructure. We simply didn't have the capacity to offer the number of services and solutions that we can now,"

David Thor Kristjansson, Co-Founder and Manager of Sales, Endor

"**Cohesity helps ensure that data and IT services are available or made available.** In doing so, it helps ensure that applications and services to the public that would become inoperative in less than a second in the event of an outage are maintained, which could avoid very serious situations for people whose health, and in some cases survival, depends on the ability of the Red Cross to function fully."

Yves Couturier
National Head of the French Red Cross Production Department
The French Red Cross

Industry	**Region**
Other	EMEA

Better data management and protection can help improve lives

Background

The French Red Cross has more than 66,000 volunteers and 16,000 employees, gathered around 35 professions—all dedicated to helping people from birth to end of life.

The organization manages more than 120 TB of data, including the personal data of beneficiaries (shared medical records, home care data, nursing services, and meal delivery), as well as its operational management data (emergency doctors and ambulance drivers) and administrative data (payroll, ERP, and business intelligence). In 2019, under the guidance of Yves Couturier, head of information system production, and with the help of Cohesity, the French Red Cross undertook a process of modernizing its systems and storage to improve its data management.

croix-rouge française

Industry	Region
Other	EMEA

Criteria for choosing a new solution

- Simple data management
- Automated backup and recovery
- Cloud-based
- Predictable costs
- Extendable functionality via APIs

"Our ultimate goal is to manage our operations as much as possible via the cloud, and the flexibility of the Cohesity architecture and data security allow us to protect ourselves all the more serenely in the continuation of this collaboration"

Olivier Geremy, Head of Security Architecture Strategy (SAS), The French Red Cross

Why change was needed

"When we embarked on the modernization of our information system, we had two imperatives regarding the management of data backup: that it be as flexible, automated and reliable as possible; and that cost be predictable in a context of increasing data volume," said Yves Couturier, National Head of the French Red Cross Production Department.

What improved after switching

The Red Cross initially adopted Cohesity DataProtect, in a project piloted and implemented by its longstanding IT partner, Skill Partner.

The migration took approximately two weeks, during which the data was encrypted and transferred securely for disaster recovery purposes. The handling was done quickly.

For Couturier and his team, "The simplicity of the interface was vital. Our small team can't afford to waste time on backup or worry about whether backup operations have been completed. We needed a solution that could give us a very clear picture of real time data to make the right decisions."
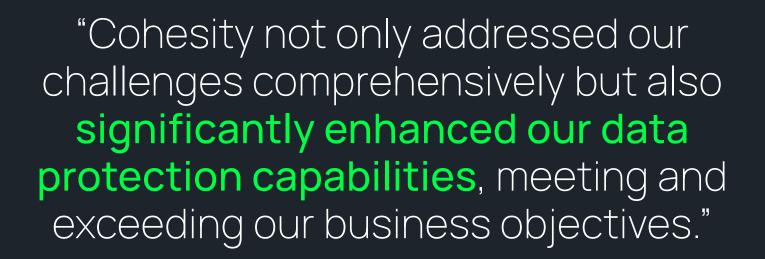
Key Outcomes

The backup operation has a 100% success rate, and the system is self-contained 95% of the time

Reduced backup times mean the team can focus on other, higher value projects

All flows and data transmitted from applications are encrypted, stored, protected, and instantly accessible when needed

"Cohesity not only addressed our challenges comprehensively but also **significantly enhanced our data protection capabilities**, meeting and exceeding our business objectives."

Hossam El-Morshedy
General Manager of Infrastructure and Cloud Computing
Eastern Company

Eastern Company modernizes data protection strategy to strengthen security

Background

Founded in Egypt more than a century ago, Eastern Company produces a varied collection of tobacco products. With over 13,000 employees spread across seven locations, Eastern Company is determined to scale its 32 brands sustainably.

As ransomware attacks became more frequent worldwide, Eastern Company decided to take extra steps to safeguard its data. "Previously, we relied on traditional data protection," explains Hossam El-Morshedy, general manager of Infrastructure and Cloud Computing at Eastern Company. "But ransomware is something that we cannot avoid. It will happen sooner or later. We need to be ready with an environment that has clean data, enabling a fast recovery."

Industry	**Region**
Manufacturing	EMEA

Why change was needed

In addition to improving cyber resilience, Eastern Company wanted a more flexible solution. "We needed the flexibility to move data between on-premises and cloud environments and the ability to switch services from Azure," continues El-Morshedy.

What improved after switching

After a successful implementation, Eastern Company gained much-needed security and flexibility—and the assurance it can recover quickly if a ransomware attack does happen. Eastern Company can also more easily manage its critical security environment.

"Previously, when dealing with databases, three different teams would need to collaborate. Aligning these resources was challenging and time consuming. Now, we only need one resource for data security and management, and it's fully automated. All we need to do is monitor the system," notes El-Morshedy. Previously, Eastern Company also used separate tools to manage data on virtual machines. Contacting application providers was also sometimes necessary to restore running services. "With Cohesity, the process is streamlined. Data recovery is simplified, requiring just a few clicks and creating efficiency and time savings for our team," adds El-Morshedy. But the proof is in the numbers.

Key Outcomes

92% faster backup time

88% faster recovery time

1-2 hour Recovery Point Objective (RPO)

94% less time spent on data management

Criteria for choosing a new solution

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

"We significantly improved our Service Level Agreements (SLAs). Backup time was reduced from 24 hours to just two. Recovery time to Azure, which used to take seven to eight hours, was slashed to one hour. Additionally, we achieved an impressive Recovery Point Objective (RPO) of one to two hours."

Hossam El-Morshedy, General Manager of Infrastructure and Cloud Computing, Eastern Company

" "

In the past, setting up backups with our previous providers was a cumbersome process involving multiple installations, configurations, and reconfigurations whenever our infrastructure changed. **Now it takes 92% less time**, requiring only half an hour. The time and resource savings across the board have been remarkable.

Martin Hofmann
Head of Information Technology
Infra Fürth

infra fürth

Industry
Public Sector

Region
EMEA

Energy provider ensures business continuity with reinvigorated security

Background

For the more than 131,000 residents of Fürth, Germany, Infra Fürth is the primary provider of all essential needs—electricity, natural gas, water, and district heating. With a mission to make the region a hospitable living environment for future generations, Infra Fürth prizes innovation and passion.

Infra Fürth relies on mountains of data to function efficiently. "In a modern utility company, data is not just crucial; it's indispensable. It's what enables us to control our business services, deploy solutions effortlessly, and make informed decisions about every aspect of our operations," explains Martin Hofmann, head of Information Technology at Infra Fürth. "From identifying which components need immediate maintenance to forecasting future demands and managing power storage, every critical task hinges on data."

For Infra Fürth, data security is paramount, and backups are the last and most important line of defense. Struggling with two disparate backup structures, the company started looking for a more flexible, centralized approach.

infra fürth

Industry
Public Sector

Region
EMEA

Criteria for choosing a new solution

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

"Losing data has a huge impact on us. But now we're better prepared and shielded in the case of big outages. We are able to plan our resources better, and we can test restores and make them quicker and more efficient."

Martin Hofmann, Head of Information

Why change was needed

"We needed a single point of management—i.e. a unified platform to oversee our databases—as well as ransomware protection," shares Hofmann. "We wanted to ensure we were protecting all of our data and to make our backup systems simpler and more flexible."

What improved after switching

The company was immediately drawn to Cohesity because of its simplicity, single point of management, ransomware protection capabilities, and immutable backups—the last of which ensures that backups are encrypted and protected against tampering. With Cohesity SmartFiles, Infra Fürth consolidated data from its 400 virtual machines and 10 physical servers on a single platform, using intelligent data management and active threat defense. The company also started protecting custom applications and servers. "We backed up critical infrastructure data," explains Hofmann. "We dedicated a small team of data center administrators to Cohesity and they've been very impressed by its capabilities."

Key Outcomes

Stronger security and disaster recovery

€125,000 yearly cost savings

92% time saved on data management

Faster and more efficient data recovery

COHESITY

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 report to learn more ⬇

COHESITY

Ready to strengthen your cyber resilience?

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

6100025-001 EN 9-2024