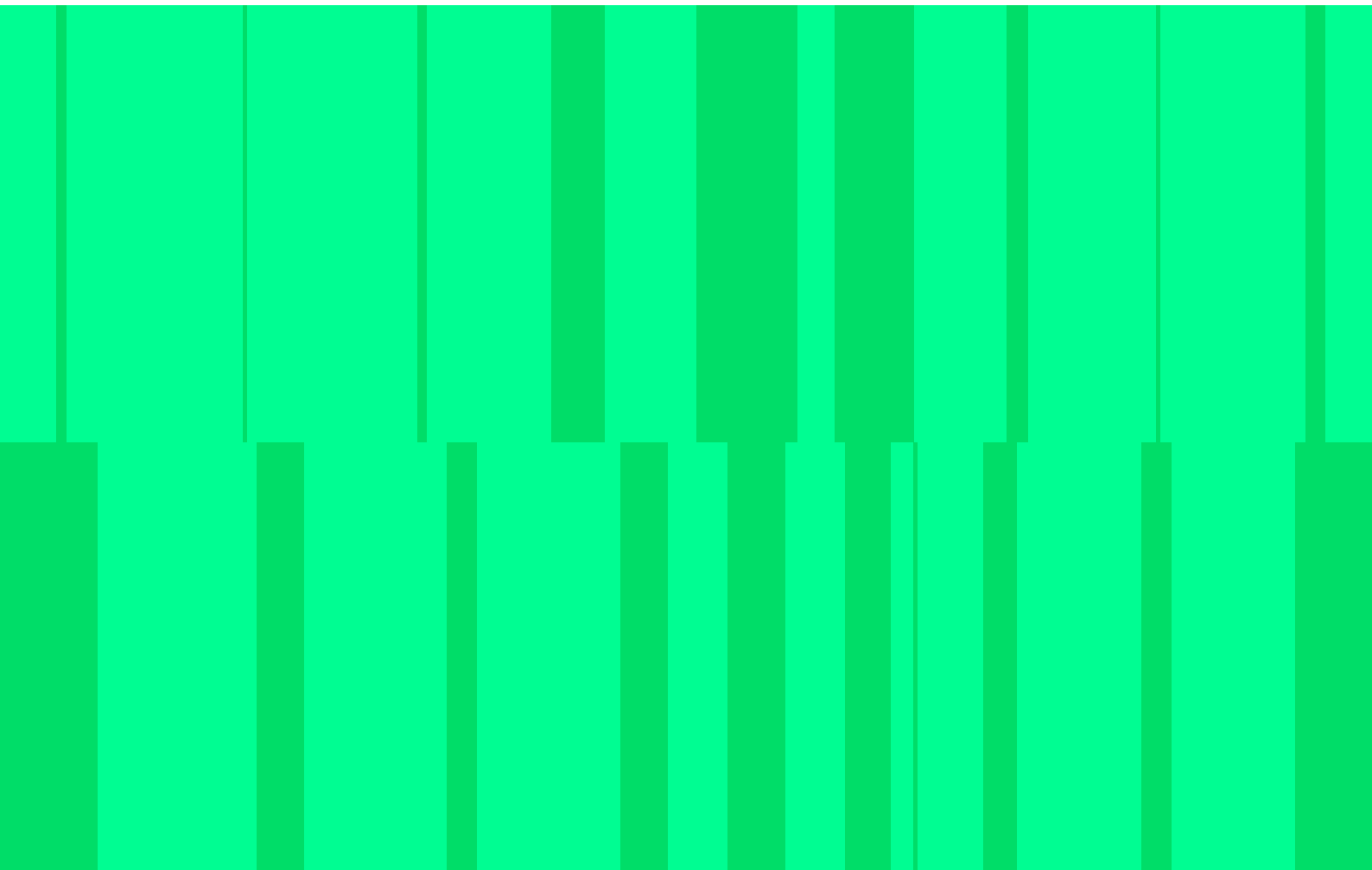
COHESITY

RESILIENCE EVERYWHERE

HOW FOUR ORGANIZATIONS MOVED BEYOND LEGACY FOR MODERN DATA PROTECTION



INTRODUCTION

Across industries, IT teams are rethinking their approach to data protection. The shift isn't just about faster backups or new infrastructure. It's about simplicity, quick and confident recovery, and savings.

Organizations that once depended on traditional systems such as Dell EMC Data Domain and NetWorker are finding that the complexity, maintenance, and limited scalability of those tools no longer align with today's demands. From healthcare to financial services to education, these organizations share a common goal: to simplify operations, strengthen security, and gain confidence in their ability to recover quickly and securely. Whether safeguarding sensitive healthcare data, protecting customer financial records, or maintaining uninterrupted learning, the ability to recover clean data instantly has become nonnegotiable.

The following four customer stories spotlight organizations that modernized their backup and recovery strategies with a single, unified platform. Each achieved measurable gains in speed, efficiency, and security—proof that moving beyond older, siloed systems is not just a technological choice, but a strategic one.

COHESITY
RESILIENCE EVERYWHERE

KASSENÄRZTLICH VEREINIGUNG HESSEN

Product(s)	Region	Use Case	Industry	Environments	
DataProtect SmartFiles	EMEA	• Backup and Recovery • Disaster Recovery • File and Object Services	Healthcare	VMware SQL Oracle	**31%** **faster backups**

KVH STRENGTHENS RANSOMWARE PROTECTION, CUTS BACKUP TIME BY OVER 70%

In healthcare, even a few hours of downtime can disrupt essential services and patient care. Kassenärztliche Vereinigung Hessen (KVH) modernized its data protection to ensure reliability, security, and compliance—all while simplifying IT operations and leaving behind the complexity of traditional systems.

KASSENÄRZTLICH VEREINIGUNG HESSEN

OVERVIEW

In the German state of Hessen, the public healthcare of panel doctors is overseen by Kassenärztliche Vereinigung Hessen (KVH). As data volume grew, KVH needed faster backup and recovery, faster access to files that are used for calculation of doctors' invoices to guarantee correct fee distribution for all the panel doctors, and stronger security—including ransomware protection. The company achieved all three goals with Cohesity's data security and management platform. Today, every piece of data is backed up in three locations, including an immutable vault that attackers can't encrypt. Working with one vendor for backup and recovery, file services, and ransomware protection simplifies IT.

CHALLENGE

The business of healthcare revolves around managing vast quantities of data subject to stringent security, privacy, and compliance requirements. Challenges for KVH include complying with Germany's Patient Data Protection Act and the EU's General Data Protection Regulation (GDPR), retaining doctors' invoices for 10 years, and making sure employees can quickly access invoices, contracts, files, and other data to ensure residents receive needed care and that doctors get paid.

Until 2015, KVH stored data relevant to billing and other file types on Windows File Servers which had their disks on Dell EMC VNX storage, mirrored between data centres. In addition, KVH used Dell EMC NetWorker and Data Domain for backup and restore. "But as data volume grew, performance started to really slow down," says Christian Zinke, Team Lead for IT Infrastructure at KVH. "Backups took seven hours and finding a lost email file or document in the GUI from Dell EMC NetWorker to restore files often took 45 minutes or more—a big problem since we have only one storage administrator." The IT team often had to wait months to find a window to install Windows security patches on the Windows file servers, leaving KVH vulnerable to malware. It was also difficult to extend disk space as all of the file server disks passed 2 TB. With a Master Boot Record (MBR) partition table, partitions are limited to a maximum of 2 TB. Therefore, the limit of scalability was reached.

Concerned about rising attack volume, KVH also wanted ransomware protection. "We needed a set of backups that attackers couldn't delete or alter," Mr. Zinke says. The German government restricts companies in the public sector from processing social data, so the new data management platform had to run on-premises or in colocation facilities.

SOLUTION

Comparing Cohesity to Dell EMC, Mr. Zinke selected the Cohesity data security and management platform. "Cohesity stands out because of its performance, modern architecture, and security protections, including built-in antivirus and immutable backups," he says. "And support is simpler with one vendor for backups, disaster recovery, and ransomware protection."

Initially, KVH deployed two Cohesity clusters, one in the primary data centre and another in a disaster recovery location. At about the same time, they replaced the Windows file server with Cohesity SmartFiles. "With SmartFiles we can scale up and out as data volume grows," Mr. Zinke says. "And we don't have to schedule a maintenance window for updates because our users can continue accessing files while the update is happening. We now have access to the latest features as soon as they're available."

By 2022 data had grown to over 300 TB, and ransomware had become a bigger threat. KVH asked Cohesity to optimise the existing Cohesity data management solution. The result: today all data and files are stored in three separate locations for optimised security. Cohesity SmartFiles and the primary Cohesity backup cluster are in the main data centre. They replicate to a disaster recovery facility and to a new separate site used expressly for ransomware protection. Like the Cohesity FortKnox cloud service, all backup data is ransomware-protected on all backup clusters. The new separate cluster also stores immutable backups that can't be deleted, encrypted, or modified as an air-gap vault with even higher security and access implementations.

KVH is also using Cohesity to archive data for virtual machines. Storing a VM on a Cohesity cluster is a simple and efficient way to make sure the data is available when needed. Using features like DataLock prevent the data from being deleted or modified, and allow KVH to meet compliance requirements to archive the data for 10 years.

KEY BENEFITS:

- Built-in antivirus file protection with Cohesity Marketplace ClamAV
- 31% faster backups within the VMware environment
- Instant file search and granular recovery through file indexing
- 49.2x storage reduction for greater efficiency

RESULT

Now KVH has a stronger security posture, including ransomware protection. "If we're hit by ransomware, we can quickly restore from the immutable backups in our on-premises data vault," says Mr. Zinke. For added protection, he's getting ready to require administrators to use Cohesity multifactor authentication (MFA) before they can access data, and to use Cohesity's DataLock feature to prevent deletion of data by anyone, under any circumstances, until a specified date. The open-source ClamAV app runs right on SmartFiles, eliminating the need to migrate to, and manage, separate antivirus infrastructure. "Using Cohesity immutable backups and ClamAV significantly lowered our premiums for ransomware insurance," Mr. Zinke says.

Storage efficiency has increased, reducing physical storage costs. KVH now stores more data in less space by taking advantage of Cohesity's data reduction, including cross-volume data deduplication, compression, and optimised storage of small files. "We're seeing 5:1 data reduction ratios and storage reduction of 49.2x, pointing to the efficiency of the Cohesity solution."

When users lose data, an administrator can now find it much faster with Cohesity's ability to index all data stores on the platform. Apps like Spotlight, a Cohesity Marketplace app, can provide even more insight into the data. "Before, our administrator had to scroll through multiple folders to locate a lost file, which often took 45 minutes," says Mr. Zinke. "Now, with Cohesity, the admin simply enters the file name to find it, and can typically start the restore in under five minutes. Users get their file sooner, and if we do three to five restores a week, our administrator saves about three hours." An added benefit is if the administrator discovers that the file is not really lost—just hiding out in a different folder—KVH avoids making an unnecessary duplicate.

VM failures don't interrupt work. With KVH's old backup solution, when a VM failed employees had to pause their work until it was fully restored. No longer. "Cohesity integrates very well with VMware vCenter," Mr. Zinke says. "If a virtual machine fails, users can work on the backup copy, using Cohesity Instant Recovery, as it's migrated back to production. We're now more resilient."

Summing up the value of Cohesity, Mr. Zinke says, "Cohesity is much more than a backup or disaster recovery solution—we also use it as a more modern and scalable alternative to Windows File Services, and for ransomware protection."

> "Cohesity stands out because of its performance, modern architecture, and security protections, including built-in antivirus and immutable backups. And support is simpler with one vendor for backups, disaster recovery, and ransomware protection."

Mr. Christian Zinke
Team Lead for IT Infrastructure
Kassenärztliche Vereinigung Hessen

COHESITY
RESILIENCE EVERYWHERE

First Bank & Trust

Product(s)	Region	Use Case	Industry	Environments	Up to
DataProtect FortKnox SmartFiles	Americas	• Backup and Recovery • Cyber Vault • Ransomware Protection	Financial Services	SQL, VMware Microsoft 365, Physical servers	**98%** **less management time**

FIRST BANK & TRUST INCREASES CYBER RESILIENCE, RESTORES TRANSACTION DATABASES WITH A 5-MINUTE RPO

Like KVH, financial institutions operate in highly regulated environments where data integrity and fast recovery aren't optional. They're foundational. For First Bank & Trust, the challenge was straightforward but critical: protect sensitive customer and banking data around the clock. A lean staff needed cyber resilience and operational simplicity, without adding complexity.

First Bank & Trust

OVERVIEW

A community-focused bank, First Bank & Trust wanted better protection for sensitive customer and bank data, stronger cyber resilience, and lower management overhead for a lean staff. The bank found its answer in Cohesity.

In the event of an attack or system failure, any IT admin can recover a clean copy of data from one of three immutable Cohesity backups, including one copy in Cohesity FortKnox, a cyber vault. A unified interface for on-premises and cloud data sources reduced weekly management time from 10-12 hours to about 10 minutes.

CHALLENGE

When it comes to data security, First Bank & Trust doesn't stop with regulatory compliance. "A higher concern is customer trust," says Luke Schwingler, Director of Technology. "We take cyber resilience very seriously because our customers expect banking services to be available 24/7 on our bankeasy.com website and app. Staying ahead of threats instead of constantly putting out fires gives us more time to improve the IT environment and customer experience."

First Bank & Trust previously backed up databases and virtual machines with a Dell EMC solution. When Schwingler took the helm in 2022, his first priority was stronger data protection and security. "Every business needs to be thinking about ransomware, and with the old solution I couldn't confidently state that we had immutable backups," he says. Another priority was simplifying backup management: Troubleshooting the old solution's frequent failures consumed more than 25% of an IT admin's work week. Rather than continue investing in the existing system, the bank decided to switch to a modern data-protection platform.

SOLUTION

At his previous employer, Schwingler had solved the same operational challenges by switching to Cohesity Data Cloud. "When I first saw the Cohesity solution, I had a light-bulb moment," he says. "Viewing the status of all on-prem and cloud workload backups in a single report significantly reduces management overhead." Cohesity also provides leading security protections, including immutability, role-based access controls, multifactor authentication, and a feature to block any alterations to backup data, by anyone, until a specified expiration date.

To protect and secure data, the bank maintains three immutable Cohesity copies: two in on-prem clusters that replicate to each other plus an air-gapped copy in Cohesity FortKnox on AWS. Should a disaster or cyber attack strike, the IT team can restore data from any of the three copies. "Other vendors require separate management consoles for backing up on-prem and cloud data, which is no better than having separate vendors," Schwingler says. "With Cohesity, we can centrally manage all data—virtual machines, file shares, Microsoft 365 data—from a single pane of glass. Knowing we can protect any future on-prem or cloud workloads without buying a new solution is even better."

Schwingler and his staff regularly attend Cohesity webinars. "I like to work with forward-thinking vendors that I can learn from," he says. "Our Cohesity account team understands that data protection is a piece of our overall cybersecurity strategy, and I meet with them regularly to hear their latest insights and industry trends."

KEY BENEFITS:

- Up to 98% less management time: 10-12 hours saved weekly
- Increased cyber resilience
- Stronger data security
- Consistent customer experience resulting from reduced network traffic

RESULT

Weekly time spent managing backups has dropped from 10-12 hours to about 10 minutes, freeing up time for staff to work on a backlog of IT projects to improve the customer experience or add automation. "With Cohesity we no longer need to assign someone to troubleshoot backups," says Schwingler. "We just take a look at an automatically generated report to see if a backup didn't complete. That's rare, and when it does happen, the Cohesity report tells us why. When I give presentations to IT professionals, I ask if they have somebody who is focused on backups. If the answer is yes, I tell them they need Cohesity."

Non-disruptive, one-click upgrades save more time. "With Cohesity we can upgrade whenever it's convenient, even during business hours," says Schwingler. "Our admins are happy they don't have to perform upgrades over the weekend."

Resilience increased because applications or data lost to an attack or disaster can be recovered quickly from any of the three immutable Cohesity backups, including one in the cloud-based cyber vault. And if a production database fails or is attacked—an especially severe risk for financial institutions—First Bank & Trust can restore a clean copy of the database to its state no more than five minutes before the outage. The solution, Schwingler explains, is writing transaction logs to Cohesity SmartFiles every five minutes, replaying them to the most recent backup. "Cohesity provides a simple solution to restore a database with a 5-minute RPO [recovery point objective] that doesn't require deep database skills or high-availability technologies," he says.

The switch to Cohesity Data Cloud also eased demands on the bank's network, avoiding network congestion that can affect the customer experience. With the old solution, First Bank & Trust ran a full backup every Saturday night, when network utilization would spike from 18% to 80%. "Now backups have zero impact on other workloads because Cohesity only backs up data that's changed," Schwingler says. "Avoiding network congestion allows our app and website to perform consistently whether a customer wants to move money Tuesday at 9:00 a.m. or Sunday at 3:00 a.m. Full recovery is faster because we can restore from the most recent snapshot instead of waiting to apply an incremental backup to the last full backup."

Looking to the future, First Bank & Trust expects to use Cohesity's APIs to act on new opportunities. "In the age of AI, it's hard to know how our operations will change in three months," says Schwingler. One plan is to have application upgrades automatically trigger a Cohesity snapshot of the application environment, an insurance policy if the upgrade fails.

"IT doesn't drive revenue," says Schwingler. "But IT can definitely help our revenue-generating departments avoid disruption. I've implemented Cohesity at two companies now, and Cohesity experts have helped educate me so I can make confident decisions about security and resilience."

> "Other vendors require separate management consoles for backing up on-prem and cloud data, which is no better than having separate vendors. With Cohesity, we can centrally manage all data—virtual machines, file shares, Microsoft 365 data—from a single pane of glass. Knowing we can protect any future on-prem or cloud workloads without buying a new solution is even better."
>
> **Luke Schwingler**
> **Director of Technology**
> **First Bank & Trust**

COHESITY
RESILIENCE EVERYWHERE

Product(s)	Region	Use Case	Industry	Data Sources	
DataProtect FortKnox	Americas	• Backup and Recovery • Disaster Recovery • Data Isolation • Recovery as a Service	Higher Education	Ellucian Banner File Shares Oracle Databases VMware vSphere	**91%** **Faster backups**

PEARL RIVER COMMUNITY COLLEGE FORTIFIES SECURITY WITH A VIRTUAL 'AIR-GAPPED' DATA VAULT – IN COHESITY FORTKNOX

The need for cyber resilience extends across every sector. Just as financial institutions like First Bank & Trust must protect customer data without interruption, higher education institutions face their own high-stakes demands: safeguarding student records, meeting compliance requirements, and keeping operations running even under threat. Pearl River Community College did just that by adding isolated, immutable protection in the cloud to ensure uninterrupted learning and compliance.

PEARL RIVER COMMUNITY COLLEGE

OVERVIEW

Colleges have become popular targets for identity theft and ransomware attacks. To protect student information and keep operations running smoothly during disasters, Pearl River Community College (PRCC) wanted a virtual air-gapped backup copy isolated from its network. The answer: Cohesity. Now the college has two immutable backup copies: on campus and on Cohesity FortKnox, a Cohesity-managed cloud vault hosted in AWS. A unified management interface features multifactor Authentication (MFA) and a quorum feature that requires a minimum of two people to approve changes. Backups complete in a fraction of the time. And the IT team has peace of mind knowing they can quickly restore backup data and virtual machines from FortKnox in the event of a cyberattack or disaster affecting backups at both data centers.

CHALLENGE

With 5,500 students, PRCC is the fourth-largest of Mississippi's 15 community colleges. The IT team backs up 15 TB of critical data, including student databases, virtual machines, file shares, the Ellucian Banner ERP system, and the document management system. "We've digitized records from the college's earliest days, and it's critical for learning and administration to make sure a clean copy of data is available—even if our building is taken out by a tornado or we're hit by a cyberattack," says Matt Logan, CIO. "Secure backups are the only means of recovery from attacks."

Until recently, PRCC kept one backup on campus and replicated it to a disaster recovery facility around 50 miles away, using Dell EMC Data Domain and Veeam. But an uptick in cyberattacks on colleges, including one that hit PRCC, prompted IT leaders to add another backup in a third location isolated from the college network.

"If we can't restore data from our local backup or the disaster recovery facility, we need a virtual air-gapped copy in the cloud as a fallback," says Kevin Lomax, Director of Technical Services. The IT team also wanted stronger access controls, including MFA and a requirement that at least two people approve critical actions. Ease of use was essential because just one system administrator manages backups as well as servers.

SOLUTION

PRCC found its answer in Cohesity. Today the college backs up data in two locations: on Cisco UCS servers on campus, and on Cohesity FortKnox, a Cohesity-managed vault in AWS Cloud. The IT team chose Cohesity over Rubrik and Dell Cyber Recovery. "Cohesity FortKnox is the only fully baked virtual air-gapped cyber vaulting solution we've seen," says Logan. "The other vaulting solution was a bunch of piecemeal features bolted together and lacked the comprehensive security measures that are built into FortKnox."

Cohesity's ease of use also set it apart. "Our system admin literally jumped up and down seeing she could manage on-prem and cloud backups from a single interface," Lomax says. "Adding FortKnox as a backup target was as simple as a few clicks in our protection policy. And Cohesity is 'set and forget'—though we restore 25% of the environment each quarter as a smart practice."

For tighter access controls, PRCC set up Cohesity to require two people—a quorum—to modify a backup. "Cohesity FortKnox is like a safe deposit box for backups," says Lomax. "Two people need to enter their login credentials and approve any changes or recoveries. We replaced our existing data management solution with Cohesity even though more than a year remained on the maintenance and support contract. Cohesity's stronger security protections are so valuable to the college that we couldn't justify waiting. That's confidence."

KEY BENEFITS:

- 91% faster backups – 1 TB/hour
- 94% faster full file share restores – Backing up ¼ of the environment now takes 7 minutes, down from 120 minutes with Veeam
- Better visibility of security threats with Cisco SecureX integration
- Improved business continuity: virtual machines can run on backup servers

RESULT

Switching to Cohesity strengthened security, made the college more cyber resilient, and simplified IT operations. "Even if both of our network-connected backups are unavailable, we rest easy knowing we can restore a clean copy from Cohesity FortKnox," Logan says. And when a potential ransomware attack does strike, the IT team discovers it sooner because Cohesity integrates with Cisco SecureX.

"There's no way we could investigate all the malicious hits on our network happening every hour, and any potential data compromise," says Logan. "The integration between Cohesity and Cisco SecureX makes security operations much simpler. If Cohesity spots anomalies from one backup to the next, it automatically sends a ransomware alert to Cisco SecureX, which opens a security ticket just like it does for other threats. With all security alerts in one place we're now faster at detecting, investigating, and responding to attacks," says Lomax.

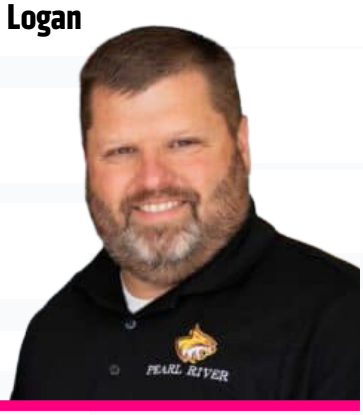
The Cohesity solution even helped the college get cybersecurity insurance. "With Cohesity, we can answer 'yes' to new requirements for cybersecurity insurance – yes, we have immutable backups, keep a copy in the cloud, use MFA, and require multiple administrators to approve changes to backups," Logan says. "Without those capabilities our insurance premiums would be much higher, if we could get insurance at all."

Backups and restores are also faster with Cohesity running on Cisco UCS. The time to make a full backup of 15 TB dropped from seven days to 15 hours. Time to recover 25% of the environment from the Cohesity clusters dropped from 120 minutes with Veeam to seven minutes. "Faster backups give us more flexibility for when we schedule other tasks and processes," Lomax notes.

Finally, the Cohesity solution helps learning and administration continue even when virtual machines fail. "If the building hosting the virtual server farm is damaged or loses power, we can nearly instantly restore all virtual machines at once, running them right from Cohesity," Lomax says. "By helping us keep student information secure and not let disasters interrupt learning, Cohesity is an investment in student satisfaction."

"With Cohesity, we can answer 'yes' to new requirements for cybersecurity insurance – yes, we have immutable backups, keep a copy in the cloud, use MFA, and require multiple administrators to approve changes to backups. Without those capabilities our insurance premiums would be much higher, if we could get insurance at all."

Matt Logan
CIO



COHESITY
RESILIENCE EVERYWHERE

Product(s)	Region	Use Case	Industry	Environments	
DataProtect FortKnox	Americas	• Backup and Recovery • Dev/Test • Ransomware Recovery	Education	VMware SQL	**90%** faster dev/test patch testing

ATLANTA SCHOOL DISTRICT SELECTS COHESITY FOR RANSOMWARE RESILIENCY AND REDUCED TCO

Cyber resilience isn't limited to colleges and universities. For K–12 districts like Clayton County Public Schools, ensuring the safety of student data and continuity of instruction requires the same level of protection—and the same simplicity in managing it.

OVERVIEW

Clayton County Public Schools (CCPS) is located just south of Atlanta, Georgia, and serves more than 52,000 students from kindergarten through twelfth grade. The district has 66 school campus locations, including sites for alternative education, STEM and STEAM programs, and psychological education centers. A challenging curriculum is offered at every level, and students can also participate in exploratory courses and extracurricular activities.

The IT team and primary data center are located in Jonesboro, with a disaster recovery site at a separate school location. With an annual budget of more than $744M, CCPS is dedicated to developing programs to foster the best place to learn.

CHALLENGE

Over the last several years, CCPS has witnessed a dramatic change in technology, including the move to virtualized environments and the increased threat of ransomware. At the time, the IT team relied on solutions from Dell EMC and Data Domain. The legacy environment was not able to back up and restore virtual machines (VMs), and as most of its entire server environment was running VMware, a new solution was needed.

Routine backups took exorbitant amounts of time, often more than 12 hours and even then, the IT team did not have a clear sense of how long backups were taking because the process was tedious and cumbersome.

In the last year, CCPS needed to meet mandates for cybersecurity insurance compliance. While the district has a separate disaster recovery (DR) location, it was required to have an offsite copy of data isolated from the primary environment to qualify for cybersecurity insurance.

SOLUTION

CCPS was on the verge of deploying a Veeam solution when the IT team learned about Cohesity, and then decided to do a Proof of Concept before making a final decision. The ability to manage their entire backup and unstructured data environment from a single, secure multicloud data platform, along with the significant cost savings it offered, drove CCPS to move forward with Cohesity. CCPS also recently implemented Cohesity FortKnox, a SaaS data isolation and recovery solution hosted on AWS that provides an immutable copy of data in a Cohesity-managed cloud vault to provide an added layer of security against ransomware and other cybersecurity threats.

"We are confident we made a good choice in selecting Cohesity for our enterprise data management across our entire school district," said Kurt Pritchett, Sr. Network Engineer. "Like many enterprise environments, Clayton County Public Schools has seen tremendous changes in IT in the last five years and we needed a single, secure solution for our virtualized infrastructure. Cohesity has not only enabled significant cost and time savings, it has set us up to optimize our future data management and meet cyber resiliency requirements."

The school district deployed two Cohesity nodes, including one at its disaster recovery location several miles away. Reducing cost was a primary concern for CCPS. EMC licensing costs alone were more than the total cost of the Cohesity solution. The school district also made a policy decision to only store 30 days of backups to reduce the amount of data needed to recover. If the policy were to change down the road, Cohesity's native integration with the leading cloud providers would provide a seamless route for archival storage.

CCPS is backing up its entire virtualized infrastructure and its SQL database environment. The district is also using Cohesity for dev/test to test patches for VMware, OS upgrades, and other updates.

RESULT

Like many organizations, security is top of mind at the school district. With Cohesity FortKnox, CCPS not only meets requirements for cybersecurity insurance, it also ensures an additional layer of protection against ransomware. CCPS has had minor incidents of malware, but the threat was mitigated quickly with Cohesity that helped restore data quickly and fix vulnerabilities that led to the attack. "We incurred no financial impact or ransom, and we are confident that with Cohesity we are well-positioned to recover confidently and combat any future attacks," said Pritchett.

Organizations are often struggling to identify skilled staff resources with cybersecurity and data isolation expertise. With SaaSbased solutions like FortKnox, CCPS can ensure continuity for IT management. "Honestly, it doesn't get any easier than this. SaaS solutions are what every K-12 needs when you are hard-pressed to find the right talent pool. It was easy and fast to deploy and has simplified our entire environment. With FortKnox, we were able to vault all our data to the cloud in a couple of hours without having to deal with the overhead of managing cloud storage buckets

KEY BENEFITS:

- Secured critical data against ransomware and other cybersecurity threats
- Met cybersecurity insurance requirements for data isolation
- Gained the ability to use Cohesity for dev/test for operational efficiency, including over 90% faster patch testing
- Achieved time and cost savings by moving away from legacy environment
- Obtained the ability to easily and quickly recover data, with tremendous time savings for enterprise backup and recovery
- Improved backup times for VMs by 98%

ourselves," adds Pritchett.

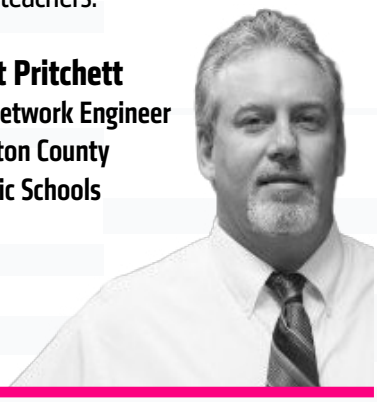
Additionally, the Cohesity solution enabled the IT team to search and recover data directly from Cohesity, without the need to recover whole volumes. Many times an employee would lose a file on a mapped drive and the IT team would only have the name of the file. Without being able to know which server the file resided on, CCPS would have to recover many backups at once, costing the IT team time and resources.

CCPS realized greater efficiency with Cohesity for time savings and business continuity, including reduced RPO and RTO. Backup times for VMs went from five hours to only several minutes, and full backups are completed in less than a day with Cohesity.

Now when the IT team needs to test a patch for VMware tools, they can use Cohesity to clone a VM into an isolated test environment. The district can test and apply new patches before applying them into a production environment. When the IT team upgraded the Windows OS for its servers, they were able to test ahead of time to ensure application compatibility, determine how long the upgrade was going to take in production, and better plan for school staff and resource disruption. With the previous solution, this process took more than an entire day but now with Cohesity, the team conducts many of these operations in under 30 minutes.

"Cohesity support has been instrumental to ensure a smooth deployment. They have been tremendously responsive in providing the IT team what it needed quickly. Cohesity's performance monitoring features also give the district insight into its infrastructure and gained the ability to spread backup jobs over a broader time range for optimal performance," said Pritchett.

"Like many enterprise environments, we at Clayton County Public Schools were looking to update our 3-2-1 backup strategy to protect our data from increasingly sophisticated ransomware attacks. The simplicity and convenience of the Cohesity FortKnox SaaS solution were just what we needed to achieve this, while reducing operational complexity and meeting demanding SLAs. With FortKnox, we now have an isolated, immutable copy of our critical data in the cloud without having to manage an offsite data vault ourselves, saving us a lot of time and budget that can be utilized to better serve our students and teachers."



Kurt Pritchett
Sr. Network Engineer
Clayton County Public Schools

CONCLUSION

Across these four stories, a common pattern emerges. Organizations moving away from older, siloed systems aren't just replacing infrastructure—they're modernizing how they protect, manage, and recover their data. Whether supporting patient care, securing customer financial data, or maintaining uninterrupted learning, each organization gained a simpler, more resilient, and more efficient approach to data protection.

Strengthening data security and ensuring fast, clean recovery is no longer optional. It's foundational. By consolidating protection, streamlining operations, and introducing modern safeguards like immutability and isolated recovery, these organizations are better prepared for today's risks and tomorrow's demands. They've built a foundation that gives IT teams confidence that their data—and their mission—are protected.

Simplify and accelerate backup and recovery of enterprise workloads across on-premises, cloud, and SaaS, with a modern, unified platform for cyber resilience.

Learn more about Cohesity DataProtect

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

6100032-002 EN 6-2026