NetApp

SECURITY BUILT SMARTER

How security leaders scale AI through cyber resilience

Table of contents

Executive overview

Picture your next board meeting. Your CEO presents the AI roadmap—predictive analytics that will transform the customer experience, automated workflows that will cut costs by millions, and intelligent systems that will outpace every competitor.

You're caught between two impossible scenarios. Say yes too quickly, and you're on the hook when—*not if*—a cyberattack succeeds. Hedge too much, and you're the executive who killed the company's top strategic initiative.

When AI fails, it fails at scale

When training datasets get corrupted, you lose months of model development. When inference pipelines go down, revenue stops in real time. And when attackers poison your data, the damage compounds with every decision your AI makes—and every result it delivers.

86% of security leaders faced an AI-related cyberattack in the past year[1]

80% of organizations have attack paths exposing critical data and systems[2]

2% of companies are fully resilient against these attacks[1]

The shift: To achieve cyber resilience, leading organizations embed security directly at the data layer rather than bolting it on afterward—making protection the foundation of every AI initiative.

AI-ready resilience in action

By strengthening its data foundation, Thor Motor Coach improved efficiency and achieved the resilience to keep operations running—no matter what.

- **30%** infrastructure savings per year[3]
- **45%** monthly reduction in network costs[3]
- **99.999%** system availability[3]
- **Backup time cut** from 76 hours to under 1 hour[3]

"We're a vastly different looking organization than we were before the transformation—faster, more nimble, and cost-effective." [3]

Scott Sibert,
Director of Information Technology,
Thor Motor Coach

Data-layer security that's built-in delivers:

- Real-time threat detection where data lives
- Ransomware-resistant backups
- Recovery in hours, not weeks

While competitors continue cleaning up from breaches, you'll be scaling AI across the organization with confidence. **This is how security leaders become AI leaders.**

1 Your stakes: Why AI-ready data is your most critical business asset

AI-ready data isn't just another IT asset—it's the engine of innovation and value creation. And it's under attack.

As organizations race to scale AI from proof-of-concept to production, they're discovering a dangerous blind spot: traditional security approaches weren't designed to protect the complex, distributed nature of AI data pipelines.

Corrupt the data, cripple the mission

Lost competitive edge	Innovation stalls while your competitors advance
Biased or corrupted models	Flawed business decisions and reputational damage
Regulatory penalties	Audits fail; compliance becomes impossible
Board scrutiny intensifies	Leadership demands answers for failed investments

Corrupting one training dataset can do more damage than locking a thousand servers. Attackers know that enterprises rushing to deploy AI often skip the basics—making data the easiest entry point.

The vulnerability is structural

A single-pane platform spanning all environments—on-premises, private clouds, and public clouds such as AWS, Azure, and Google Cloud—gives AI teams and applications seamless mobility and access to data wherever it resides, without slowing anyone down.

The inflection point

Decouple resources to deliver exactly what AI workloads need, when they need it. Scale storage independently of compute for true cloud-native performance.

84%

of companies report rising attack-surface activity[4]

As you scale AI across hybrid cloud environments and third-party services, your external attack surface grows exponentially. Each new environment, integration, and edge deployment creates potential vulnerabilities that traditional perimeter defenses can't protect.

4. Cybersecurity Insiders, New Report: Attack Surface Challenges Behind 80% of Cybersecurity Breaches

2 Your challenge: Securing the data layer for the AI era

As AI pipelines span clouds and continents, the ability to secure data at its foundation has become the defining advantage of resilient organizations.

Perimeter-based security worked when information stayed behind firewalls, but AI changed the rules. Training datasets, model weights, inference pipelines, and real-time data now move freely across hybrid multicloud environments, well beyond the reach of traditional safeguards.

Where traditional security falls short

Fragmented visibility : Siloed security tools across environments create blind spots where threats hide and spread.

Reactive detection: Alerts come after the damage when threats have already compromised workloads.

Complex recovery: Restoring AI pipelines is slow and disconnected, delaying recovery and disrupting value delivery.

Compliance gaps: When you can't prove continuous protection, audits fail and trust erodes across hybrid environments.

The cost of failure skyrockets quickly

- **$3.32 million**—Average breach cost[1] typically magnified for AI-driven organizations
- **$2 million per hour**—Median cost of high-impact IT outages,[5] a risk that scales rapidly as AI workloads expand across hybrid environments

When protection becomes the problem

The answer isn't more tools—it's a smarter foundation. Integrating security at the data layer closes visibility gaps, eliminates silos, and keeps defenses consistent across every environment.

90%

of companies lack the maturity to counter AI-enabled cyber threats[6]

AI progress accelerates faster than security can adapt. The gap widens every day—and the CISOs who close it first will define the future.

3 Your solution: AI-powered data security that enables cyber resilience

Cyber resilience isn't a feature—it's an outcome. It happens when you engineer protection, detection, and recovery directly into your data layer, where AI workloads live and learn.

This is the difference between defending the perimeter and protecting the core—your models, data, and decision pipelines.

How protecting the data layer changes everything

By embedding intelligent, AI-powered security capabilities at the data layer, you transform security from overhead into storage that automatically scales with AI.

Your outcome: Security becomes an enabler, not an impediment. You eliminate the complexity that stalls AI deployments, gaining speed and protection simultaneously.

3 built-in security capabilities that turn risk into resilience

Unified visibility everywhere

End-to-end protection for AI pipelines across on-premises and multicloud environments. Break down silos, preserve integrity, and enforce consistent policies from edge to core to cloud.

Intelligent automation in action

Continuous detection and automated response keep AI workloads running with near-zero disruption. AI-powered ransomware protection stops attacks in real time and cuts operational inefficiency.

Protection that scales with AI

Ransomware detection, automated backup, disaster recovery, and governance unified on a single foundation. Immutable copies and orchestrated recovery prevent tampering, end delays, and keep AI scaling to value.

"Organizations that bake security into their AI-powered transformations will not only survive but thrive, gaining a crucial competitive edge, cementing customer loyalty, and building unshakable resilience."[7]

Accenture

4 Real-world defense: When ransomware targets your AI

Ransomware has entered a new era—attackers target the AI initiatives your CEO has staked her reputation on as the engine of growth. When training data gets corrupted or models get encrypted, the damage extends far beyond downtime.

How will your next attack play out?

3:00 AM: Attackers gain access through a compromised vendor credential.

WITHOUT DATA-LAYER PROTECTION

3:15 AM: Your production AI models and training datasets get encrypted.

3:30 AM: $5M ransom demand received.

- 6 weeks to retrain models from scratch
- $3M+ in lost revenue while AI services are down
- Regulatory scrutiny over the breach
- Board questions about successful AI attackers

WITH DATA-LAYER PROTECTION

3:01: Automated detection flags anomalous behavior in real time.

- Attackers can't encrypt protected backups
- Restore to last known-good state in under 2 hours
- AI services back online before the business day starts

Success in securing AI isn't about luck–it's about strategic evolution. Organizations that embed protection at the data layer strengthen their security posture while eliminating the complexity and cost of managing disparate point solutions across the infrastructure.

Here's how to enable cyber resilience from the start:

Protect

Maintain immutable copies attackers can't touch, even if they succeed at taking over your network. These unchangeable copies protect more than your organization—they protect your career when the board asks if you can recover.

Detect

Identify ransomware behavior in real time at the data layer—before it spreads. Catch attacks at the earliest stage by monitoring anomalies in AI data access.

Recover

Initiate automated restoration in hours—not weeks—so you can act confidently, eliminate manual guesswork, and return quickly to a verified clean state.

Your outcome:

Preserve model integrity, maintain customer trust, and keep AI initiatives on track—even when attacks breach your perimeter.

5 AI compliance: From audit risk to competitive advantage

Compliance isn't just about avoiding fines—it's about earning trust and moving faster than your competitors who are still explaining their last breach to regulators.

When regulators call, you must prove compliance across every environment. That's challenging enough, but add AI and the challenges multiply:

- Proving where your AI training data came from—and that it wasn't compromised
- Demonstrating that automated decisions can be explained and contested
- Keeping data in the right countries as AI trains across multiple clouds
- Documenting the entire AI lifecycle for regulatory audits

Traditional GRC tools run at the application layer, leaving gaps when data moves between environments.

Data-layer governance closes those gaps by carrying controls with the data—keeping compliance even as AI workloads span on-premises systems, multiple clouds, and edge locations.

When compliance gets personal

€1.2 billion in GDPR fines in 2024[8]—and accountability is on the rise.

Recent enforcement actions make one thing clear: accountability doesn't stop with the enterprise; it starts with its leaders.

8. CSO, GDPR fines hit €1.2 billion in 2024 on 8.3% more breach reports, January 24, 2025

Embed compliance into the data layer

Your hybrid cloud platform becomes increasingly valuable as AI complexity grows:

Prove data origins automatically

Track every dataset from source to model with immutable records—so when auditors ask, you have answers ready.

Maintain geographic boundaries

Data stays in required jurisdictions even during disaster recovery. The data layer enforces location requirements automatically.

Generate continuous audit trails

Every data access, transformation, and model update gets logged—no manual work and no gaps during failover.

Adapt to regulations faster

Apply policies once at the data layer, and every workload inherits them—whether it's GDPR, HIPAA, or the next mandate.

Your outcome:

Compliance becomes a competitive accelerator. You can scale AI faster, expand into new and regulated markets, and deploy models sooner without the delays of manual security reviews.

6 Operational resilience: Drive near-zero downtime for AI

When cyberattacks strike, operational continuity is the ultimate measure of resilience. In an AI-driven enterprise, this means keeping intelligent operations running—even in the middle of disruption.

Why continuity matters:

Attacks target availability, not just data
End-to-end protection for AI pipeline across on-premises and multicloud environments.
Break down silos, preserve integrity, and enforce consistent policies from edge to core to cloud.

AI pipelines amplify disruption
Continuous detection and automated response keep AI workloads running with near-zero disruption.
AI-powered ransomware protection stops attacks in real time and cuts inefficiency.

Enterprise-wide resilience requires proof
Demonstrate to boards and customers that your AI initiatives can scale securely and reliably, even during attacks.

Traditional continuity plans assume you can fail over to a backup system. But with AI, you need the exact training data, trained models, and configurations that were in production. To achieve this, you must have data-layer continuity.

Resilience without disruption: Modern continuity for AI at scale

Continuous AI operations
When ransomware strikes your training environment, all production models keep running on protected replicas. Your customers never see disruption.

Instant failover
If attackers compromise a model registry, automated systems detect the anomaly and fail over to the last verified-clean version. Recovery happens in minutes.

Protected real-time intelligence
Maintain continuous access to accurate data and analytics. AI results stay reliable under pressure.

Your outcome
Protect both trust and your balance sheet. With near-instant recovery, you'll safeguard revenue, maintain continuous AI operations, and transform resilience into your strategic edge.

Beyond traditional security: What AI demands

Traditional data security	AI-powered, data-layer cyber resilience
Back up entire applications	✓ Protect data and models at the source
Manual recovery procedures	✓ Automated decision and failover
Hours to days to restore	✓ Minutes to hours to restore
Risk of inconsistency	✓ Guaranteed integrity
Separate tools for disaster recovery	✓ Unified protection

7 From defense to AI dominance: Fortifying resilience at the data layer

The organizations that win with AI won't be the ones with the most data scientists or the biggest budgets. They'll be the ones who solve the cyber resilience equation first.

That means rethinking how you build your security foundation—not as an afterthought scattered across dozens of point solutions, but as a unified approach anchored at the data layer, where protection, detection, and recovery begin.

5 strategic advantages that strengthen cyber resilience

SPEED
Detect threats in real-time and recover in hours, not weeks—while competitors are still assessing damage.

SIMPLICITY
Unify ransomware protection, backup, disaster recovery, and governance in one foundation. Fewer tools mean fewer gaps.

SCALABILITY
Maintain protection as AI workloads span clouds and other environments. Security grows with your ambition.

ALIGNMENT
Bridge security and storage teams with a shared foundation that accelerates response, detection, and recovery.

ASSURANCE
Prove compliance to boards, regulators, and customers—and build trust that turns security into an advantage.

Make your next move

Security leaders can keep patching tools that slow or even stall AI deployment—or they can design resilience into the data layer to scale AI value with confidence.

It's time to make data security the foundation of your legacy and your company's future in AI.

SUMMARY

Ready to unlock AI value through cyber resilience?

Be the kind of security leader who transforms resilience into acceleration—fueling AI success at scale. With built-in data security and protection across every environment, your impact can go further, faster.

It's not whether you embed security at the data layer—it's whether you act early enough for resilience to hold when the next attack hits.

Take the next step:

Assess your AI resilience →

Identify your critical data security gaps in minutes.

Explore cyber resilience strategies →

Uncover resources for building data-layer security.

Secure AI at the data layer—where it matters most

AI success depends on one critical foundation: data you can trust and protect. The NetApp data platform embeds cyber resilience directly into your data infrastructure—unifying ransomware protection, backup, disaster recovery, and governance at the source.

With real-time threat detection, immutable data protection, and rapid recovery built into the foundation, you don't just defend AI—you accelerate it with confidence. Intelligence built in, not bolted on.

Discover the topics in this series

- Data infrastructure modernization →
- Cloud →
- Cyber resilience
- Artificial intelligence →

About NetApp

For more than three decades, NetApp has helped the world's leading organizations navigate change—from the rise of enterprise storage to the intelligent era defined by data and AI. Today, NetApp is the Intelligent Data Infrastructure company, helping customers turn data into a catalyst for innovation, resilience, and growth.

At the heart of that infrastructure is the NetApp data platform—the unified, enterprise-grade, intelligent foundation that connects, protects, and activates data across every cloud, workload, and environment. Built on the proven power of NetApp ONTAP, our leading data management software and OS, and enhanced by automation through the AI Data Engine and AFX, it delivers observability, resilience, and intelligence at scale.

Disaggregated by design, the NetApp data platform separates storage, services, and control so enterprises can modernize faster, scale efficiently, and innovate without lock-in. As the only enterprise storage platform natively embedded in the world's largest clouds, it gives organizations the freedom to run any workload anywhere with consistent performance, governance, and protection.

With NetApp, data is always ready—ready to defend against threats, ready to power AI, and ready to drive the next breakthrough. That's why the world's most forward-thinking enterprises trust NetApp to turn intelligence into advantage.

Learn more at www.netapp.com or follow us on X, LinkedIn, Facebook, and Instagram.

NetApp