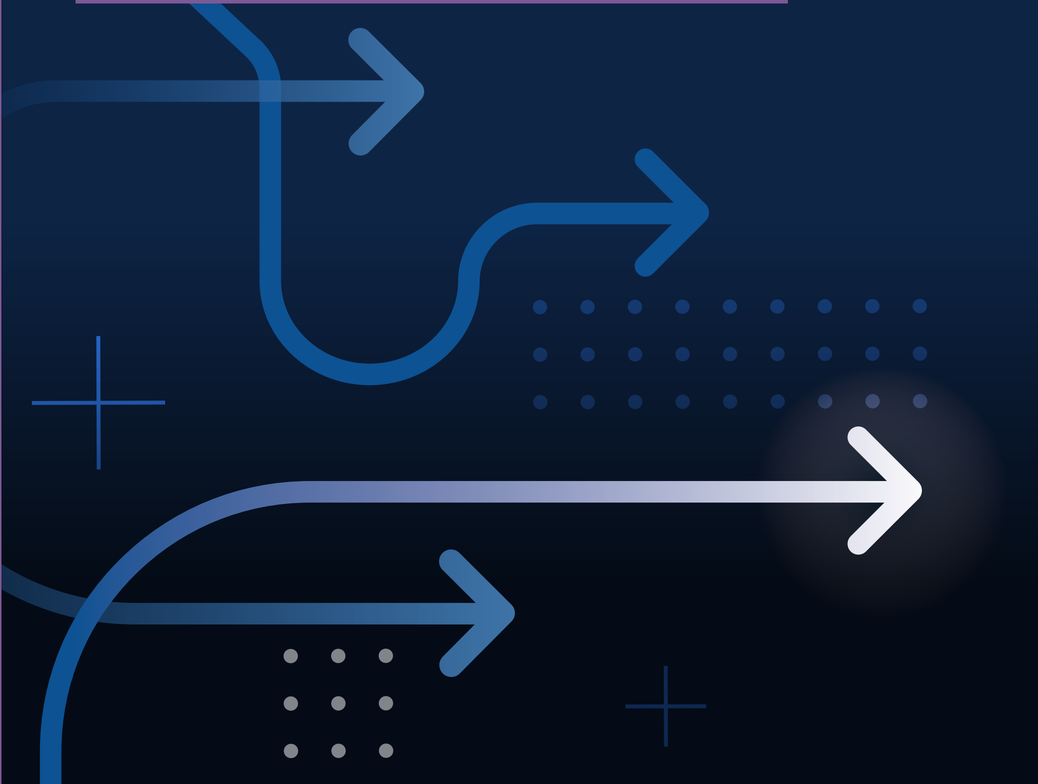
GIGAOM

COMMISSIONED BY:

NetApp

Modern Data Management for a Recoverability-First Strategy

CLOUD, INFRASTRUCTURE & MANAGEMENT



GIGAOM

GigaOm CxO Decision Brief: Modern Data Management for a Recoverability-First Strategy

Solution Overview

NetApp delivers a modern data management platform that embeds ransomware protection directly into storage architecture. By aligning infrastructure capabilities with recovery objectives, the solution helps organizations reduce dwell time, harden the data layer, and enable operational continuity when prevention fails.

Benefits

NetApp's platform strengthens ransomware resilience by integrating detection, protection, and recovery capabilities within the data layer.

- Organizations will benefit from:
- Improved recovery readiness
- Reduced downtime
- Greater alignment between infrastructure and security objectives
- A unified management framework for operational efficiency

Urgency

Ransomware attacks are becoming more targeted, frequent, and operationally disruptive. Regulatory scrutiny and insurance requirements are raising the bar for recoverability, making modern data resilience a strategic imperative for security and infrastructure leaders.

Impact

Adopting NetApp's platform can influence how organizations approach data security, recoverability, and cross-functional coordination. It may require shifts in team collaboration, updates to recovery processes, and broader awareness of infrastructure decisions across security, compliance, and risk functions.

Risk

Delaying modernization increases risk of prolonged downtime, failed recoveries, and non-compliance with regulatory or insurance expectations. Siloed infrastructure and security planning can leave critical gaps in ransomware response, exposing organizations to financial, legal, and reputational harm.

01 Solution Value

This GigaOm CxO Decision Brief commissioned by NetApp.

RANSOMWARE INCLUDES MORE THAN ENDPOINT or perimeter threats—it can, and frequently does, include attacks on data-layer vulnerabilities that have direct implications for business continuity, regulatory compliance, and executive accountability. As attacks increasingly target the data infrastructure supporting critical systems and backup environments, resilience must extend beyond detection and prevention to include effective recovery and platform-level integration. This makes it an interesting and useful conversation for the CISO to be engaged in.

NetApp delivers a data storage infrastructure-integrated approach to ransomware resilience, embedding detection, protection, and recovery directly into its data services. Core capabilities include immutable snapshots, AI-driven anomaly detection, automated response workflows, and rapid recovery capability across on-premises and hybrid environments.

This provides a modern data management solution platform that supports coordinated recovery, aligns with cyber insurance expectations, and can help CISOs fulfill their responsibility to reduce dwell time, avoid or mitigate ransom payments, and contribute to maintaining operational continuity when prevention fails.

Achieving this level of resilience requires coordination across security, infrastructure, and operations teams. While CISOs typically do not direct or own infrastructure decisions or the associated budget, they can play a critical role in influencing and advising on data storage platform choices that align with the organization's recovery, compliance, and cyber-risk requirements. Building resilience in the data layer should be viewed as a shared responsibility—and one that increasingly depends on collaboration between IT and security leadership.

02 Urgency & Risk

AS RANSOMWARE ATTACKS EVOLVE TO BECOME more sophisticated, targeted, frequent, and disruptive, the urgency to modernize organizational resilience strategies evolves in step. Traditional approaches—often siloed across security operations, IT infrastructure, and recovery planning—are increasingly proving inadequate. These disconnected efforts can leave critical gaps between detection, prevention, and recoverability. CISOs and their peers are under increasing pressure—some would suggest an obligation—to be aware of and consider broader, more holistic solutions that reduce recovery time, demonstrate control and management of targeted data-layer risk, and align resilience strategies cross-functionally with regulatory and board-level expectations.

Urgency

The pace and precision of ransomware attacks continue to accelerate. High-impact incidents now include targeted attacks on data backup systems, data storage environments, and data recovery infrastructure. For CISOs, this represents a shift in operational pressure: from simply preventing breaches to ensuring that systems can recover quickly and effectively when defenses are bypassed—as they surely will be in time.

As regulatory expectations increase and cyber insurance policies impose stricter conditions around recovery readiness, ransomware resilience has become a strategic requirement. Any inability to recover cleanly—even if detection is timely—can lead to extended business disruption, loss of trust, and broader organizational risk. Infrastructure modernity, once the domain of IT planning, should now be viewed as inseparable from cyber-risk preparedness.

Risk

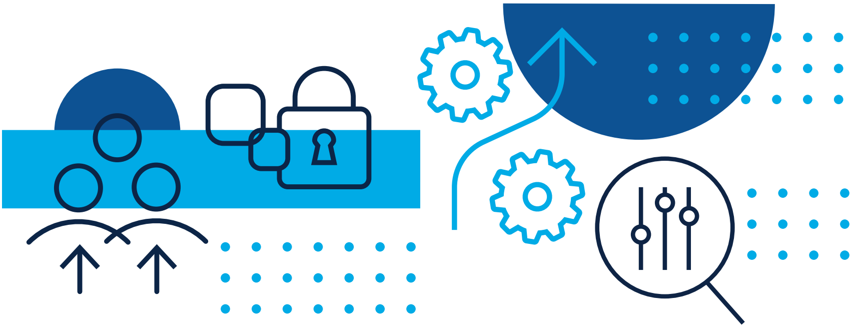
Failing or delaying to modernize ransomware resilience introduces exposure across multiple domains—some operational, others strategic. These risks are often magnified in organizations where data management, security, and recovery processes are fragmented or siloed.

- **Operational risk** - Legacy systems and disconnected teams often lack the automation, immutability, and recovery speed required for modern ransomware response. Downtime extends, recovery windows widen, and business continuity suffers.

02 Urgency & Risk

- **Regulatory and legal risk** - Inability to demonstrate structured, repeatable recovery capability and processes may result in non-compliance penalties and legal exposure—particularly where security responsibilities are not clearly aligned across teams.
- **Reputational risk** - Public breaches and prolonged outages erode customer trust and brand equity, especially when the root cause traces back to uncoordinated recovery practices or outdated infrastructure.
- **Financial risk** - Disruption, ransom payments, recovery efforts, and rising cyber insurance scrutiny can all lead to materially significant financial losses. Lack of investment in recovery modernization may also jeopardize insurability.

These risks underscore the need for a more integrated, cross-functional approach to resilience—one where CISOs, IT leaders, and infrastructure stakeholders share accountability and modernize together.



> **"Public breaches and prolonged outages erode customer trust and brand equity, especially when the root cause traces back to uncoordinated recovery practices or outdated infrastructure."**

03 Benefits

MODERNIZING DATA INFRASTRUCTURE with ransomware resilience in mind brings meaningful benefits that go beyond improved recovery time. It establishes a foundation for business continuity, policy compliance, and greater confidence in response preparedness. For CISOs and their peers, these benefits represent an opportunity to shift from reactive postures to proactive resilience planning.

Key benefits can include:

- **Reduced dwell time and recovery windows** - Automated, immutable data protection can reduce the time between detection, response, and full recovery.
- **Minimized business disruption** - Reliable, infrastructure-integrated recovery processes help prevent prolonged downtime and preserve operational continuity.
- **Improved compliance readiness** - Repeatable, policy-driven recovery capabilities can support internal audits, regulatory mandates, and cyber insurance requirements.
- **Cross-functional coordination** - A unified platform enables security and infrastructure teams to work from shared assumptions, response plans, and recovery metrics.
- **Stronger risk management posture** - Organizations gain clearer insight into where vulnerabilities exist—and how resilient they are to worst-case scenarios.

While technical capabilities underpin these outcomes, the benefits accrue at the business level cross-functionally. They enable CISOs and infrastructure leaders to position recoverability as a core component of enterprise security strategy. For CISOs specifically, these benefits support a stronger organizational role—grounded in resilience, not just detection and prevention. By engaging in platform decisions and advocating for protection-by-design infrastructure, CISOs can contribute directly to recoverability outcomes and broader business continuity assurance.

04 Best Practices

IMPROVING RANSOMWARE RESILIENCE is as much about operational alignment as it is about selecting capable technologies. Modernization for organizations entails treating data-layer resilience as a shared responsibility, bringing together infrastructure, security, and recovery planning in a unified strategy.

Recommendations for best practices include:

Build recovery into platform strategy
Integrate ransomware protection and recoverability into infrastructure decisions—not as afterthoughts, but as first-order design requirements.

Engage cross-functional leadership early
Ensure that security and IT leadership jointly define expectations for recovery time, automation, and risk reporting during platform evaluations.

Adopt immutable and automated protection
Invest in data management solutions with built-in immutability, anomaly detection, and automated response workflows to reduce human error and dwell time.

Test recovery at the organizational level
Go beyond technical drills—practice recovery as a business continuity exercise with security, compliance, and executive teams involved.

Make recoverability a board-visible metric
Align platform capabilities to the language of risk: recovery time, data integrity, and impact mitigation.

For CISOs, these practices offer an opportunity to engage more strategically in platform modernization—not by owning the infrastructure decisions, but by ensuring that recovery readiness is built into how the organization defines security.

05 Organizational Impact

MODERNIZING DATA INFRASTRUCTURE to support ransomware resilience is not simply a technical shift—it brings measurable change to people, process, and investment planning. As organizations adopt protection-by-design principles, they should prepare for the organizational shifts that follow.

People Impact

Cross-functional alignment becomes essential. Teams responsible for infrastructure, security, compliance, and risk must collaborate more closely. While technical skill sets remain critical, and any upskilling or gap mitigation should also be planned for, greater emphasis is typically placed on shared response planning, joint recovery exercises, and leadership-level engagement in resilience metrics. CISOs may need to champion this cultural evolution, even if they do not own the underlying infrastructure.

Process Considerations

Existing recovery processes are often fragmented and outdated, typically designed around perimeter protection rather than data-layer recoverability. Modernization efforts require policy refinement, updated runbooks, and clearly defined escalation paths that span functional teams. Embedding ransomware response within broader business continuity planning becomes a core requirement.

Investment Outlook

While resilience-focused modernization may require new investments in storage data infrastructure, automation, and monitoring, organizations may find that costs are offset by improvements in response readiness, insurance alignment, and avoided downtime. Solutions that consolidate protection, detection, and recovery functions—such as those offered in NetApp's modern data management platform—can simplify architecture and reduce long-term operational overhead.

06 Solution Timeline

IMPLEMENTING A RANSOMWARE-RESILIENT DATA management platform involves more than a software or hardware rollout—it touches processes, policies, and cross-functional practices. Success depends on early alignment between security and infrastructure teams, along with a clear understanding of current-state recovery readiness.

Implementation Considerations

Organizations with fragmented recovery planning or siloed infrastructure and security ownership may require additional time and coordination during rollout. Key steps typically include:

- Assessing existing data protection and recovery capabilities
- Aligning security and infrastructure teams around desired recovery objectives
- Updating policies, response runbooks, and testing plans
- Integrating new platform capabilities with existing operational processes
- The maturity of the organization's current data protection environment, along with its internal alignment, will likely determine the pace of adoption.

Typical Timeline Elements

While timelines vary by environment, ransomware resilience initiatives typically unfold in stages:

- **Discovery and assessment** - Understanding current infrastructure, exposure points, and recovery capabilities
- **Design and policy alignment** - Defining recovery objectives and embedding them into platform and process design
- **Implementation and testing** - Platform configuration, integration, and validation through simulated recovery exercises
- **Operationalization** - Transitioning to ongoing monitoring, automated detection, and readiness reporting

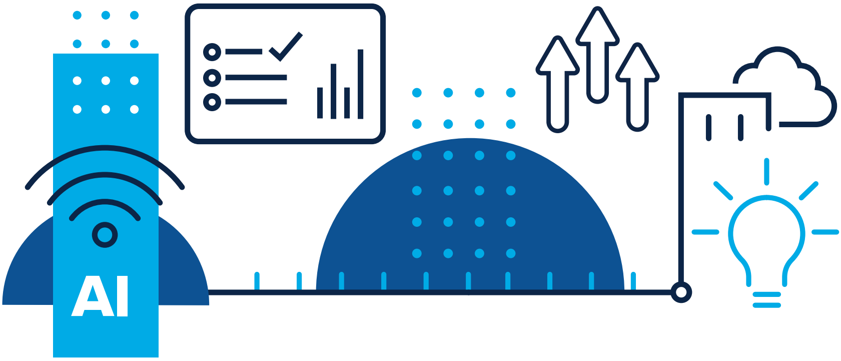
In general, organizations with modern infrastructure and aligned teams may find implementation relatively straightforward. In others, where responsibilities and recovery planning are less formal, effort levels may trend toward moderate to complex.

07 Future Considerations

AS RANSOMWARE TECHNIQUES EVOLVE and recovery expectations rise (as we anticipate them to do), data platforms will need to do more than just protect—they must anticipate. Emerging features such as AI-driven pattern recognition, intelligent response automation, and continuous posture scoring may quickly become standard components of resilient architectures.

NetApp has continued to invest in such capabilities, embedding security and recoverability features directly into its modern data management platform. These include anomaly detection, workload-aware snapshot policies, and integration with compliance and incident response frameworks.

For CISOs, ongoing platform evolution should matter. Infrastructure choices made today should account for how recovery and protection capabilities will adapt over time. A platform that demonstrates sustained investment in protection-by-design capabilities is more likely to remain aligned with future threat conditions, policy requirements, and recovery expectations.



> “Emerging features such as AI-driven pattern recognition, intelligent response automation, and continuous posture scoring may quickly become standard components of resilient architectures.”

08 Analyst's Take

RANSOMWARE RESILIENCE IS INCREASINGLY inseparable from modern data management. It requires a shift in architecture, process, and culture—one that security and infrastructure leaders should shape together. Yet too often, decisions around data platforms and recovery capabilities are treated as operational concerns, disconnected from border security planning.

For CISOs, this could be a missed opportunity. While they may not own the infrastructure roadmap or budget, they can and should consider how best to influence how recoverability, automation, and risk readiness are defined and measured. Doing so strengthens their role in enterprise resilience, positioning them as strategic contributors to operational continuity, and hardens the organization's resilience capabilities and culture.

Platforms like NetApp's—built with protection-by-design principles and an ongoing commitment to embedded resilience—can help close any gaps that may exist. By enabling security and infrastructure teams to plan, test, and recover together, they offer not just recovery tools, but the foundation for a more unified resilience strategy.

Organizations that recognize and support this shift will be better positioned to reduce risk, respond faster, and lead with resilience—not just react to threats.

Report Methodology | NetApp®

THIS GIGAOM CXO DECISION BRIEF ANALYZES a specific technology and related solution to provide executive decision-makers with the information they need to drive successful IT strategies that align with the business. The report is focused on large impact zones that are often overlooked in technical research, yielding enhanced insight and mitigating risk. We work closely with vendors to identify the value and benefits of specific solutions, and to lay out best practices that enable organizations to drive a successful decision process.

About the Authors

HOWARD HOLTON IS AN ANALYST AT GIGAOM. He has worked in IT for three decades, the last half in executive leadership, as a CIO and CTO. He has been an engineer, an architect, and a leader in telecom, health care, automotive, retail, legal, and technology.

Howard is also a technologist at heart; passionate about how data science and new technologies can be used to accelerate time-to-market and better serve the customer, now and in the future. Howard has been a trusted advisor and agent of change to a number of organizations, bringing vision and successful execution to internal and external customers alike.

DARREL KENT IS AN INDUSTRY VETERAN with several decades of experience bridging technology and business disciplines with designed-for-purpose enablement of people and process to drive desired business outcomes. He's an expert in Cloud, Infrastructure, Data Management and Governance, Sales and Marketing, Product Management and Technical Leadership.

For thirty-seven years, he served as a technical leader at Hitachi, driving their Technical Sales department and providing Data Infrastructure Solutions. He's been an IT advisory board member at Regis University, a board advisor at the University of Colorado, and is a founding member of the Colorado Institute of Technology.

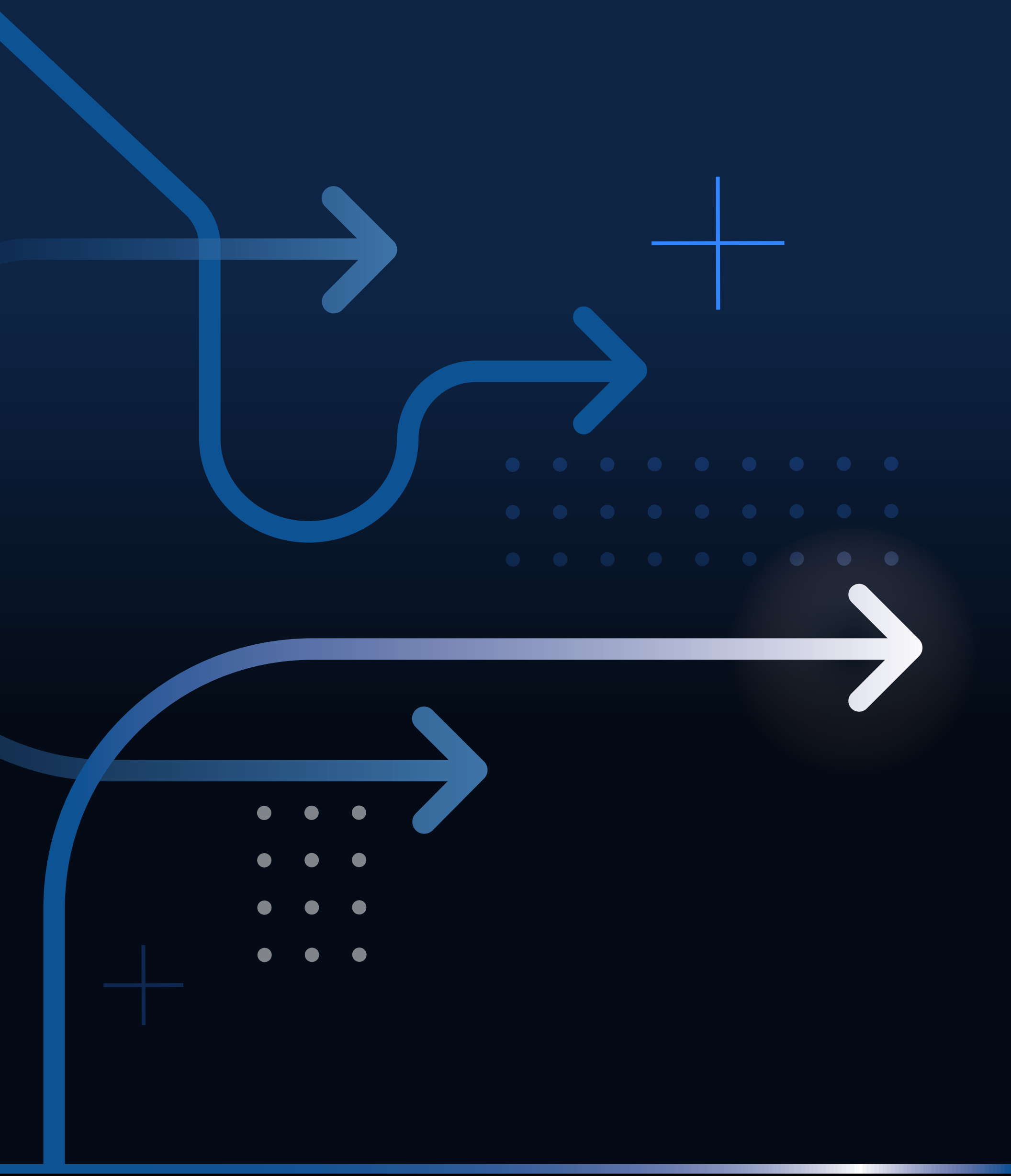
GIGAOM

About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.



GIGAOM

GigaOm democratizes access to strategic, engineering-led technology research. We enable businesses to innovate at the speed of the market by helping them to grasp new technologies, upskill teams, and anticipate opportunities and challenges. The GigaOm platform changes the game, by unlocking deep technical insight and making it accessible to all.