SCALITY | storage software

RELIABLE, SECURE, SUSTAINABLE

GUIDE

5 STEPS TO COMPLETE RANSOMWARE PROTECTION

RANSOMWARE REALITY
Modern Data Issues

RANSOMWARE PROTECTION
Rethinking Data Storage

5 STEPS TO PROTECTION
Adapting True Resilience

SCALITY

Introduction: The ransomware reality.

Ransomware protection hasn't kept pace with modern data environments

Ransomware is no longer a niche security threat or an occasional operational disruption. It has become a persistent business risk for organizations of every size, industry, and geography. While attack techniques continue to evolve, what has changed most dramatically is the environment ransomware now targets: highly distributed, data-rich, always-on enterprises that depend on continuous access to information.

Most organizations have responded by investing heavily in security tools. Endpoint protection, identity controls, network segmentation, backup software, and security monitoring platforms are now standard components of modern IT environments. Yet despite these investments, ransomware incidents continue to increase in frequency, impact, and cost.

This disconnect points to a deeper issue. The problem is no longer a lack of tools — it's that traditional approaches to ransomware protection were not designed for today's data realities.

The data landscape has fundamentally changed

Enterprise data environments have grown more complex in ways that directly benefit attackers. Data now spans on-premises infrastructure, private and public clouds, SaaS platforms, and edge locations. It is accessed by users, applications, APIs, and automated services across organizational and geographic boundaries.

At the same time, data volumes continue to grow rapidly. Organizations manage more data, in more formats, with more dependencies than ever before — often under strict availability, compliance, and recovery requirements. In this environment, even a short disruption can have cascading operational and financial consequences.

Ransomware attackers have adapted accordingly. Modern campaigns are designed not just to encrypt data, but to disrupt recovery, exfiltrate sensitive information, and undermine trust in backup and restore processes. Attacks increasingly target shared services, identity systems, and backup environments — the very mechanisms organizations rely on to recover.

Why existing defenses fall short

Most ransomware protection strategies still prioritize prevention above all else. While prevention remains essential, it assumes that attacks can always be stopped at the perimeter or endpoint. In practice, this assumption no longer holds. Phishing, credential theft, supply chain compromises, and zero-day vulnerabilities continue to provide attackers with reliable entry points.

Once inside, attackers exploit the complexity of modern environments. They move laterally, escalate privileges, and quietly prepare for maximum impact. By the time ransomware activity becomes visible, critical systems — including backups — may already be compromised.

The result is a dangerous gap between perceived protection and actual resilience. Organizations believe they are protected because the right tools are in place. But when those tools are stressed by real-world attacks, hidden dependencies and architectural weaknesses are exposed.

From prevention to confidence

This reality does not mean ransomware protection has failed. It means the definition of protection must evolve.

Complete ransomware protection is no longer about stopping every attack. It is about ensuring that when attacks succeed, as some inevitably will, organizations can contain the damage, protect their most critical data, and recover with confidence.

Achieving that outcome requires more than individual security controls. It requires a coordinated, recovery-first approach built around five essential capabilities:

- Knowing which data and systems are most critical to the business
- Limiting how far ransomware can spread after initial compromise
- Ensuring recovery data cannot be altered or destroyed
- Detecting and responding early to preserve recovery options
- Proving, through testing, that recovery works under real attack conditions

What follows will explain why traditional ransomware protection breaks down, and how these five steps help organizations move from theoretical protection to proven resilience.

SCALITY

Why traditional ransomware protection breaks down

The hidden gaps in modern ransomware defenses

Most ransomware incidents don't succeed because organizations ignored security best practices. They succeed because those practices were never designed to operate as a cohesive system under real attack conditions.

Over time, enterprises have built layered security stacks by adding tools to solve specific problems: endpoint threats, identity management, backup and recovery, monitoring, compliance. Each layer works reasonably well in isolation. But ransomware exploits what happens between those layers — the gaps where responsibility, visibility, and control become unclear.

These gaps often remain invisible until an attack is already underway.

Fragmented visibility creates false confidence

Ransomware protection depends on knowing where critical data resides, how it is accessed, and how it can be recovered. In practice, that visibility is fragmented across teams and tools.

Security teams focus on users, endpoints, and network activity. Infrastructure teams focus on systems, storage, and availability. Backup teams focus on recovery workflows and retention policies. Each group has partial insight, but no single view of how ransomware would impact the full data lifecycle.

As a result, organizations frequently overestimate their readiness. They assume that because alerts are firing, backups exist, and policies are defined, recovery is assured. In reality, key dependencies — shared credentials, trust relationships, administrative access paths — often remain undocumented and untested.

Prevention-centric strategies don’t align with attacker behavior

Traditional ransomware strategies emphasize stopping attacks early. While essential, this approach assumes a clean boundary between “secure” and “compromised” states.

Modern attackers do not operate this way. They assume detection will occur eventually and plan accordingly. Initial access is only the first step. What follows is careful reconnaissance, privilege escalation, and preparation designed to delay detection and maximize disruption.

Backup systems, identity services, and administrative tools are no longer secondary targets — they are primary objectives. Once these systems are weakened or compromised, recovery becomes slow, incomplete, or impossible, regardless of how strong perimeter defenses may be.

Recovery plans are rarely tested under real conditions

Many organizations have recovery plans on paper and have successfully restored data during routine failures. But ransomware introduces a fundamentally different scenario: recovery must occur in a hostile environment where systems, credentials, and data integrity cannot be assumed.

In these conditions, recovery processes often fail for reasons that are difficult to anticipate:

- Backups are inaccessible or incomplete
- Restore operations are too slow to meet business requirements
- Clean recovery environments are unavailable
- Dependencies between applications and data are unclear

The result is not just downtime, but uncertainty — uncertainty about what data can be trusted, what systems are safe to bring back online, and how long recovery will truly take.

The cost of incomplete protection

When ransomware protection breaks down, the impact extends far beyond encrypted files. Prolonged outages disrupt operations, erode customer trust, and place intense pressure on leadership to make decisions with incomplete information.

Even organizations that avoid paying ransom often face extended recovery timelines, regulatory scrutiny, and long-term reputational damage. These outcomes are rarely the result of a single failed control. They are the result of architectural weaknesses that only become visible under attack.

Why a different approach is required

Ransomware has exposed a critical truth: protection cannot be measured by the number of security tools deployed. It must be measured by the organization's ability to withstand attack, protect critical data, and recover reliably.

Closing the gap between prevention and recovery requires a shift in focus — from isolated controls to end-to-end resilience. It requires treating ransomware as a data-centric problem that spans security, infrastructure, and operations.

Five steps to complete ransomware protection

From fragmented defenses to resilient recovery

Ransomware protection is often treated as a collection of controls rather than a coordinated capability. Security tools, backup systems, identity platforms, and infrastructure services are deployed and managed independently, each addressing a narrow slice of the problem.

Complete ransomware protection requires a different mindset. Instead of asking whether individual controls are in place, organizations must ask whether their data, systems, and recovery processes are designed to function under attack.

The five steps that follow outline the essential capabilities required to close the gap between prevention and recovery. These steps are not sequential projects or new product categories. They represent foundational principles that must work together to deliver real resilience — regardless of the specific tools already deployed.

Rethinking how storage scales

True scalability requires architectures that are designed to grow without introducing disproportionate risk, cost, or complexity. This means evaluating storage not as a single system, but as a set of interdependent dimensions that must scale together.

The next section introduces a simpler way to think about cloud storage scalability, one that focuses on three essential dimensions: performance, capacity, and operations.

`

Step One

Know what you're protecting

Solves: Lack of visibility into critical data, dependencies, and recovery priorities

1

Ransomware protection begins with understanding what actually matters. In most enterprises, data has grown organically across environments, applications, and teams. Over time, visibility into where critical data lives — and how it is accessed and protected — becomes fragmented.

This lack of clarity creates risk. When organizations cannot clearly identify their most critical datasets, systems, and dependencies, they are forced to respond to ransomware incidents reactively. Recovery decisions are made under pressure, without a clear understanding of business impact or data priority.

Effective ransomware protection requires a clear, shared view of:

- Which data and systems are mission-critical
- Where that data resides across environments
- How it is accessed, shared, and protected
- What recovery outcomes are required to meet business needs

Why visibility breaks down at scale

As environments grow, ownership of data becomes distributed across teams. Security teams focus on access and threats. Infrastructure teams focus on availability and performance. Application owners focus on functionality and user experience. Each perspective is valid — but incomplete on its own.

Ransomware exploits this fragmentation. Without unified visibility, organizations struggle to assess the true blast radius of an attack or determine which systems must be restored first to resume operations.

Establishing recovery-focused visibility

Knowing what you're protecting is not about creating static inventories. It is about aligning data visibility with recovery outcomes. Organizations must move beyond simple asset lists and toward a recovery-aware view of their environment — one that connects data, systems, identities, and dependencies.

Step Two

Reduce the blast radius

Solves: Uncontrolled lateral movement and widespread impact after initial compromise

2

Ransomware rarely causes damage at the point of entry. The most significant harm occurs after attackers gain a foothold and begin moving laterally across systems, identities, and services.

Reducing the blast radius is about limiting how far and how fast ransomware can spread by assuming compromise is possible and designing environments to contain damage.

Why ransomware spreads so effectively

Modern environments are built for connectivity and efficiency. Shared services, centralized identity systems, and broad administrative access simplify operations — but also create powerful pathways for attackers.

Ransomware operators exploit:

- Over-privileged user and service accounts
- Shared credentials across systems
- Flat or loosely segmented environments
- Implicit trust between production and backup systems

Containment requires architectural boundaries

Reducing the blast radius is an architectural discipline. Effective containment requires:

- Limiting administrative privileges
- Separating production from backup environments
- Isolating management planes from data planes
- Enforcing strong authentication for privileged actions

By design, these boundaries prevent a single compromise from cascading across the environment.

Step Three

Make recovery immutable

Solves: Backups and recovery systems that attackers can alter or destroy

3

Ransomware succeeds when organizations lose confidence in recovery. For this reason, modern attackers target backups directly.

If recovery data can be modified, deleted, or encrypted, it cannot be trusted.

Why backups are no longer enough

Many backup systems were designed for operational failures, not adversarial attacks. Common weaknesses include shared credentials, mutable retention policies, and administrative access paths attackers can exploit.

Immutability changes the attacker's equation

Immutable recovery ensures that once data is written, it cannot be altered or deleted for a defined period — regardless of compromise.

Immutability must extend beyond data to include metadata, retention policies, and administrative actions. Partial immutability creates false confidence.

Isolation is as important as immutability

Recovery systems must be isolated so compromise of production does not grant control over recovery. Together, immutability and isolation preserve clean recovery options even under sustained attack.

SCALITY

Step Four

Detect and respond early

Solves: Late detection that turns incidents into outages

4

In ransomware incidents, time is the critical variable. The longer attackers operate undetected, the greater the damage.

Why detection often comes too late

Signal overload, subtle attacker behavior, and delayed prioritization allow attackers to escalate before obvious symptoms appear.

Speed matters more than precision

Early response focuses on containment, not attribution. Effective response includes predefined actions such as:

- Isolating affected systems
- Revoking compromised credentials
- Preserving clean recovery points
- Detection must align with recovery

Alerts that threaten critical data or recovery systems must trigger immediate escalation. Detection is most effective when guided by recovery priorities.

Step Five

Prove recovery works

Solves: False confidence in untested recovery plans

5

Many organizations believe they are prepared because plans exist. But ransomware invalidates common recovery assumptions.

Why recovery assumptions fail

Recovery must occur in environments where access, integrity, and dependencies cannot be assumed.

Testing for ransomware realities

Proving recovery works requires validating the ability to:

- Restore from immutable recovery points
- Rebuild systems in clean environments
- Verify data integrity
- Meet defined recovery objectives

From plans to confidence

Regular testing replaces assumptions with evidence. Confidence comes from knowing recovery works — not hoping it will.

From ransomware protection to true resilience

Together, the five steps outlined here establish a foundation for resilience. They shift organizations from fragmented defenses toward recovery-first design — ensuring systems remain trustworthy even when controls are stressed or bypassed.

This is where Scality makes a real difference. Scality's immutable, ransomware-proof object storage is designed to ensure that backup data cannot be altered, encrypted, or deleted, even if administrative credentials are compromised. By enforcing immutability from the architectural level to the API level, Scality enables unbreakable ransomware protection.

Ready to move from assumed readiness to proven resilience?

Engage with Scality to assess your current recovery architecture, validate immutability protections, and ensure your backup storage can withstand real-world ransomware conditions.

Email us at sales@scality.com or visit us at scality.com

SCALITY