Your First 100 Days with Veeam Data Platform

A Leader's Guide to Measurable Resilience

Most organizations assume they're protected, but few have tested it.

In a recent survey, 90% of security leaders said they could recover within their defined targets. However, among ransomware victims, only 28% fully recovered their data (Source: Data Trust and Resilience Report 2026). Confidence is not the same as demonstrated recovery capability, and the gap between the two is where ransomware wins, audits fail, and outages become crises.

90%

of security leaders said they could recover within their defined targets

28%

of ransomware victims fully recovered their data

Because resilience is only real when you can prove it.

This guide takes a strategic view of your Veeam Data Platform deployment. As your team works through the technical deployment milestones, this guide translates them into business outcomes: the risks reduced, the capabilities gained, and the proof you'll have by the end.

Because the decisions about risk tolerance, recovery commitments, and business continuity are yours to make. This guide covers what you're responsible for, and what you'll be able to communicate with confidence to the board, auditors, and insurers by Day 100.

Here's what this guide equips you with:

1. The five outcomes that separate tested resilience from assumed protection
2. What it means for your role: CIO, CISO, or CFO
3. The seven use cases your investment covers, and how activating them drives your ROI
4. The questions worth asking your team to confirm resilience holds after Day 100

From exposure to evidence: the five outcomes that matter

These are the five outcomes your organization commits to when it deploys Veeam Data Platform. Each one represents a step to take you from exposure to evidence, and together they define what a verifiably resilient environment looks like.

01. Deployed

You know exactly what is protected, where it resides, and to what standard. No assumptions, and no gaps discovered under pressure.

02. Protected

Every critical workload is covered by a plan your business continuity strategy can stand behind. Nothing falls through the cracks when it matters most.

03. Hardened

An attacker cannot destroy your ability to recover. Immutable copies exist locally and offsite, giving you a confirmed clean restore point regardless of how an incident unfolds.

04. Verifiably Recoverable

You can prove recovery works, not just claim it. It's tested, documented, and ready to present to your board, your auditors, and your insurer.

05. Operationalized

Resilience does not depend on one person or one heroic effort. It runs on clear ownership, structured reporting, and a defined cadence your team can sustain.

What this means for your role

CIO/CTO

When the board asks whether your organization can recover from a major incident, you have a tested, documented answer. Outage risk is no longer a matter of confidence; it is a matter of record.

CISO

You have a confirmed clean restore point before an incident becomes a crisis, not after. Threat intelligence scanning, immutable copies, and documented test results give you the evidence your insurers, auditors, and legal team require.

CFO

Cyber insurance eligibility, renewal terms, and premium conversations all improve when recoverability is demonstrable rather than assumed. Research shows that organizations with stronger data resilience investments paid a ransom only 33% of the time, compared to 52% among those without. Your investment in Veeam is scoped, predictable, and directly tied to reducing the financial exposure of an unplanned outage.

33%

of the time that organizations with stronger data resilience investments paid a ransom.

52%

of the time that organizations without those investments paid a ransom.

Source: Data Trust and Resilience Report (2026).

The value unlocked

The value Veeam Data Platform delivers extends far beyond a single role or a single incident. From your first 100 days onward, your organization unlocks capabilities that address the real complexity of modern IT environments: Hybrid infrastructure, cloud sprawl, regulatory pressure, and an evolving threat landscape.

These are the seven use cases your investment is built to cover.

Protect and Recover

When an incident strikes, the quality of your response depends entirely on the quality of your preparation. This is the baseline every organization needs, regardless of industry or infrastructure.

1. **Threat detection and response:** Veeam scans backup chains for malware indicators and validates file integrity before restoration, so your organization recovers clean rather than reintroduces a threat. Documented scan results support your incident response process and satisfy insurer requirements.
2. **Disaster recovery to cloud:** When on-premises infrastructure fails, Veeam shifts workloads to cloud targets within your defined recovery objectives. Your team has a tested, executable plan rather than a manual process that can't perform well under pressure.

Control and Comply

Regulatory pressure and data sovereignty requirements are expanding. Your data protection strategy needs to keep pace. If you operate in a regulated industry or are heading into an audit cycle, this is where to focus first.

3. **Governance, risk, and compliance:** Veeam generates the audit-ready reporting your compliance and legal teams need, including recovery test results, coverage inventory, and retention policy confirmation, without requiring manual evidence gathering at audit time.
4. **Sovereignty:** Veeam gives your organization control over where backup data is stored and processed, supporting data residency requirements across jurisdictions without sacrificing recovery capability.

Operate Across Complexity

Modern infrastructure does not live in one place. Your protection strategy shouldn't either. If you're mid-migration or already running multi-cloud or hybrid SaaS, this is where the operational risk concentrates.

5. **Workload mobility across environments:** As workloads move between on-premises, cloud, and edge environments, Veeam moves protection with them. Coverage does not break when your infrastructure changes.
6. **Multi-cloud protection:** Veeam provides consistent protection and recovery capabilities across cloud providers, removing the operational risk of fragmented tools and blind spots between platforms.
7. **Hybrid SaaS:** Critical data held in SaaS applications is protected alongside your infrastructure workloads, thus closing the coverage gap that most organizations discover only after an incident.

These are not future capabilities or optional add-ons. They are what your organization gains as it moves through its deployment and activation, each one reducing a specific category of risk and giving your leadership team confidence when the pressure is on. The question is not whether your organization needs this level of resilience; it's how quickly you can get there.

Day 100 is not the finish line. It's the baseline. Resilience is a practice, not a project.

Veeam provides the Veeam DataAI Command Platform, the proven Data & AI Trust Maturity Model, and the technical expertise needed to guide your team from first deployment to fully demonstrated resilience. We're there to help you every step of the way.

Ensure your team has the First 100 Days technical guide and begin aligning on deployment scope, timeline, and outcomes.

Resilience at this level is not a long-term ambition. With the right deployment plan, it is your organization's near-term reality.

The next move is yours.

Questions worth periodically asking your team

- Is every critical workload covered, and have any protection gaps or failures gone unaddressed?
- When did we last test a full recovery under real conditions, and do we have documented results to show for it?
- If ransomware hit tonight, could we identify a confirmed clean restore point and recover without paying a ransom?
- Can our compliance and legal teams produce audit evidence without manual effort, and does our architecture still meet our current regulatory obligations?
- Who has administrative access to our backup environment, and when did we last review it?

About Veeam Software

Veeam is the Data and AI Trust Company, specializing in helping organizations ensure their data and AI are fully understood, secured, and resilient to enable the acceleration of safe AI at scale. As the market leader in both data resilience and data security posture management, Veeam is built for the convergence of identity, data, security, and AI risk. Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 82% of the Fortune 500. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

Learn more: veeam.com