

Secure Data Throughout Its Lifecycle

Multiple teams secure your organization’s data — but fragmented visibility and siloed processes slow them down and increase risk.

ASK YOURSELF

- Are you confident that all your critical data is protected?
- Are you AI ready on paper — or in practice?
- Is it easy for IT and Security to collaborate on improving response and recovery times?
- Can you respond and recover fast enough if Mythos revelations become our daily reality?

14%

of security and risk management leaders can effectively secure data while enabling its use to achieve business objectives.

— Gartner. 5 Actions to Balance Data Security With Business Enablement. 2025.

THE ANSWER

Veeam is unifying data protection and data security to deliver **Intelligent Resilience Operations (ResOps)** — bringing together the market leader in data resilience and the highest-rated DSPM to secure your data throughout its lifecycle. Whether you’re prioritizing data governance and AI readiness, security operations, or business continuity, you can start that journey with Veeam.

WHAT VEEAM DELIVERS ACROSS YOUR ORGANIZATION

GRC	Data Security	AI Security & Governance	IAM	SecOps	Backup & Recovery
Always audit-ready.	Know where your data lives and how it’s used.	Control what data is accessed and exposed.	Optimize least privilege with access intelligence.	Enrich threat detection.	Recover faster.
	Apply and enforce security policies.	Protect AI systems.	Restore identity trust after an incident.	Accelerate response.	Recover clean.
	Minimize ROT and sprawl.	Reverse AI mishaps.		Bridge gaps between SecOps and IT.	

DataAI Command Platform

PLATFORM

Establish a common operating picture across teams while centralizing command of your data.

Risk lives in the gaps between teams and processes. Establish a shared view into your organization's critical data with the ability to apply data centric security and resilience policies, and accelerate incident response functions. Aligning stakeholders against a common operating picture powered by the Data Command Graph streamlines collaboration and enables context-aware decision-making.



Governance, Risk & Compliance

Maintain visibility into where critical data lives and how it's used — across cloud, SaaS, AI platforms, and backups. Collaborate with Security and IT to define, guide and prove enforcement of security policies.

53%

of security teams lack continuous and up-to-date visibility into sensitive data.²



Data Security

Know what sensitive data you have, where it lives and how it's used. Apply data-centric security policies. Uncover dark data, spillage and ROT to reduce breach risk. Improve DLP performance and accelerate incident response.

90%

have sensitive files exposed to all employees via M365 Copilot.²



AI Security & Governance

Extend visibility and control across your agent estate and implement guardrails grounded in comprehensive data sensitivity and ownership context. Apply dynamically enforced security policies to ensure sensitive information isn't exposed, prevent your AI systems from being compromised, and if your enterprise AI suddenly becomes an insider threat — precisely roll back changes made in error.



QUICK WIN!

Easily find and remove Redundant, Outdated and Trivial data (ROT).

ROT increases your data breach risk and can sabotage AI projects — making it the ideal first step in your journey to data and AI trust.

A Top 5 Wireless Carrier

\$7.8M

ROI realized in the first year



Identity & Access Management

Understand who or what has access and analyze privileges at a granular file and table level using Veeam's unique Data Command Graph. Define privileges and apply dynamically enforced access controls at scale with flexible policies built from hundreds of metadata attributes. Continuously monitor access activity, identify inactive users, and get recommendations for configuring least privilege. In the event of an identity-based threat, easily roll back IAM configurations to a known safe state to help stop threat actor movement.

88%

have stale but enabled "ghost users" — accounts of former employees still active in the system.²



Security Operations

Enrich threat detection and accelerate response and recovery by adding a valuable layer of threat detection telemetry to your EDR, SIEM, SOAR, and more. During an incident, Veeam's unique Data Command Graph and Veeam Intelligence helps IR teams determine blast radius and avoid data breach surprises — providing visibility into which systems contain sensitive and critical data. Veeam can also receive signals from SOAR systems to automate response workflows, flag potentially compromised restore points, and execute restores to minimize MTTR.



Backup, Recovery & Replication

Veeam helps you transform your team into a security and governance asset. Design more sophisticated backup, recovery and replication plans with a clear understanding of data sensitivity and potential business impact by data asset. Enrich threat detection by sending security signal to the SOC, and work in tight coordination with SecOps to accelerate investigation and recovery. Finally, with the most immutable storage options and the greatest portability on the market, you can recover cleanly from any backup store to virtually any production environment.



BACKUP AND RECOVERY TEAMS

The Last Line of Defense

Your backup and recovery team protects every critical data asset in the enterprise. So, they should operate from the same view of sensitivity, identity, access, and risk that Security relies on.

Achieve Intelligent Resilience Operations by enabling context-aware coordination.

28%

fully recovered from a ransomware attack when there was operational loss or encryption.³



Regulatory Alignment

NIST CSF, UK DORA, and the EU AI Act all place recovery firmly within the incident response process. Veeam is purpose-built to help you meet these requirements across every environment.

START WHERE YOU ARE

Achieve Data and AI Trust faster.

Whatever your priority — governance, AI readiness, security operations, or business continuity — the first step is the same: identify the gaps that lead to disruption and adverse outcomes.

→ Take our [Quick Pulse assessment](#) today.

Learn more about Veeam's Data and AI Trust Model.

Whether you're getting ready to deploy AI or strengthening the data foundation behind it, success takes more than tools. Veeam Data and AI Trust Maturity Model starts with real outcomes, then helps you spot gaps, align teams, and prioritize the investments that matter. <https://www.veeam.com/data-ai-trust-maturity-model.html>

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 at www.veeam.com or follow Veeam on LinkedIn [@veeam-software](#) and X [@veeam](#).

Note

¹ Gartner, 5 Actions to Balance Data Security With Business Enablement, 2025.

² Varonis, State of Data Security Report, 2025.

³ Veeam, Data Trust and Resilience Report, 2026.