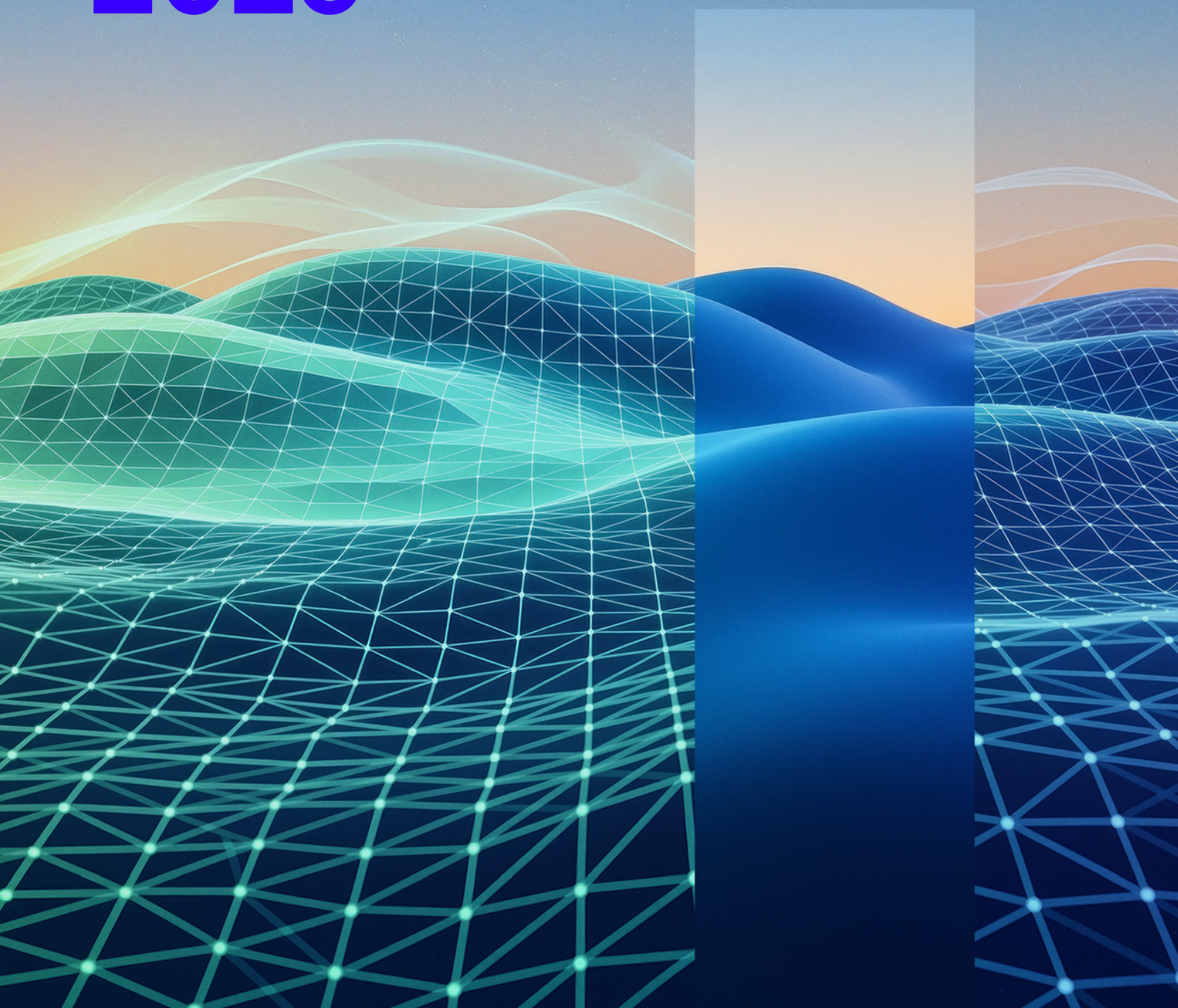
veeam Insights

U.S. Federal Edition

Data Trust and Resilience Report 2026



Executive Summary

Federal agencies today face the same paradox challenging private-sector organizations around the world. Digital transformation, cloud adoption, and artificial intelligence have increased the volume and value of data but have also expanded the attack surface around it. Data now moves across clouds, applications, automated systems, AI models, and agents faster than most agencies can track.

At the same time, ongoing geopolitical tensions increase pressure on federal security leaders to keep their agencies safe.

Despite that complexity, nearly all agencies believe they're prepared if an attack should happen.

The bottom line: In our survey of 210 U.S. federal security leaders across C-suite and frontline security roles, 95% said they are very or extremely confident they can recover from a cyber incident within their defined recovery time objectives (RTOs, or the maximum acceptable downtime before systems must be restored). That's even higher than the 90% of more than 900 global survey respondents from all industries who expressed high confidence.

Yet actual outcomes tell a more nuanced story.

In the past year, federal agencies reported experiencing cyber incidents resulting in data loss or disruption at much lower rates than U.S. private-sector organizations (16% vs. 41%). When they did experience cyber incidents, their downstream impacts were roughly the same as private organizations.

Federal agencies reported the same rate of successful ransomware attacks as their private-sector counterparts (65%). In this area, they recovered better: 43% of agencies fully recovered their data, compared to 31% of U.S. private-sector organizations. That means 57% of agencies never recovered all their data after a successful ransomware attack.

Together, these outcomes tell a clear story: Confidence alone doesn't guarantee recoverability. Lower incident volume and higher recovery rates may strengthen agencies' sense of security, but those numbers may also mask weaknesses that only become visible when an attack succeeds and cyber threats intensify.

Real resilience requires clear visibility into where data lives and how it's used, enforced controls that reduce exposure in practice, and recovery processes that are proven through testing, not assumed.

> "It's really important to spot problems early on and contain them quickly. Otherwise, they can have a huge impact on connected government systems and operations."
>
> **VP of cybersecurity, defense agency**

AI Risks are Expanding

As federal agencies integrate AI into government operations, the stakes rise further. AI creates new data flows, new attack surfaces, and new governance challenges. Federal agencies report that AI adoption is outpacing their ability to secure data and models at a higher rate than U.S. private-sector organizations, and they express greater concern about shadow IT and unauthorized AI tools (30% vs. 24%).

Our research highlights four capabilities that consistently distinguish agencies with stronger recovery outcomes:

Clear visibility into data and AI risk across the enterprise

Enforced security controls, not policy alone.

Proven recovery capabilities that are tested and validated.

Executive alignment around risk ownership and reporting.

Together, these capabilities form the foundation of modern cyber resilience. Agencies that adopt them are better positioned to withstand cyber incidents and to safely unlock the value of AI and digital innovation. Deploying more data resilience methodologies could help close the gaps that lead to unnecessary risk.

Federal Recovery Confidence vs. Operational Alignment

95%

reported being very or extremely confident in meeting RTOs

73%

said RTOs are fully aligned with business continuity goals

Confidence Is High. Is It Justified?

In our survey, 42% of federal agencies rated their data governance maturity as fully mature and standardized. Nearly half expressed extreme confidence in core capabilities, such as data lineage across cloud and on-premises environments (47%) and immutable backup enforcement (50%).

Federal agencies report fewer cyber incidents than private-sector organizations, but lower incident volume does not necessarily translate into stronger resilience when attacks succeed.

When incidents do occur, the downstream impacts are consistent with global private-sector patterns. Among federal agencies that experienced a cyber incident:

41%

reported customer or constituent service disruption (vs. 42% globally)

41%

experienced extended downtime of critical systems (vs. 38% globally)

29%

noted their insurance fees rose (vs. 30% globally)

Where gaps appear, they can be explained by structural differences. For example, fewer agencies reported revenue impact (29% vs. 41% globally), largely because most agencies don't generate revenue. More reported compliance exposure (35% vs. 27% globally), reflecting mandated compliance requirements.

Ransomware recovery outcomes add an important nuance. Although federal agencies experience successful ransomware attacks at the same rate as U.S. private-sector organizations, their recovery outcomes are somewhat stronger. Still, only 43% fully recovered their data, which means most agencies did not.

Federal agencies express strong confidence in their security capabilities, but incident outcomes suggest that confidence may exceed validated resilience.

AI is likely to widen this gap. As it spreads across daily workflows and is increasingly used by malicious actors, it introduces new risks faster than teams can respond.

AI Adoption Outpaces Risk Visibility

AI is already embedded in federal operations, moving rapidly from experimentation to everyday execution. That momentum creates a new reality: AI risk is no longer limited to model security. It is now a data governance and operational resilience problem. The productivity gains are real, but so are the risks.

AI models often rely on sensitive or proprietary data. Organizations continue to feed information into a growing set of AI tools, creating new data pathways across users, applications, APIs, and third-party services.

This expansion makes data harder to govern and secure. Existing challenges such as data sprawl, inconsistent access controls, and unclear ownership become more difficult to manage. Without clear visibility, teams struggle to enforce policy, detect misuse, and recover cleanly after an incident.

More than half of federal civilian agencies (56%) say AI adoption is outpacing their ability to secure data and models. The same percentage report limited visibility into AI tools used across their agencies. And 45% of both civilian and defense agencies say there's limited executive oversight for AI risk.

Survey response	Federal civilian agencies	Federal defense agencies	U.S. private-sector organizations
AI tool adoption is outpacing our ability to secure data and models	56%	44%	50%
We have limited visibility into all AI tools or models used	56%	37%	45%
We are still assessing risks related to data privacy, model bias, or data leakage	43%	49%	50%
Limited executive oversight or resource allocation for AI risk	45%	45%	30%

Less Communication Results in Less Investment

How frequently agencies communicate cyber risk to leadership shapes how seriously that risk is treated. On this front, federal agencies lag behind the U.S. private sector.

Reporting on Cyber Risk at Least Monthly

Reporting to	Federal agencies	U.S. private-sector organizations
Recovery time objectives (RTOs)	49%	62%
Time to isolate or contain incidents	53%	67%
Percent of recovery processes fully automated / orchestrated	40%	51%

Unlike private-sector organizations, federal agencies often face fewer external pressures, such as competition, revenue expectations, or immediate reputational consequences, which typically accelerate investment decisions.

The slow pace of the federal budgeting cycle, coupled with an uptick in government shutdowns that freeze hiring and spending, may limit the frequency of reporting because of resource constraints.

The downstream effects show up in the risk reduction actions federal organizations take, or don't take:

- **Staffing doesn't grow.** Only 35% of federal agencies added cybersecurity staff, compared to 48% of U.S. private-sector organizations.
- **Controls aren't implemented.** Federal agencies were less likely to deploy encryption, data loss prevention (DLP), and access management (42% vs. 50%).
- **Governance doesn't extend to AI.** Federal agencies were also much less likely to extend data risk governance policies to AI tool use (7% vs. 30%), which is a critical gap as AI adoption accelerates.

The pattern is self-reinforcing. Without regular reporting, leaders underestimate risk and are unaware of potential urgencies, so resources don't flow. Without resources, controls aren't built.

Organizations that report cyber risk to leadership at least on a monthly basis are linked with stronger risk reduction outcomes. This approach should be adopted as a core data risk management practice within federal agencies.

"We realized immutable backups, network segmentation, and incident communication plans are essential for resilient operations during cyberattacks and rapid recovery.."

VP of IT, defense agency

Insurance Outcomes May Mask Resilience Gaps

Federal agencies show comparatively strong outcomes in cyber insurance claims, even though fewer agencies carry cyber or ransomware insurance than U.S. private sector organizations (83% vs. 92%). Among those that do hold coverage, federal agencies are more likely to have claims approved – 64% compared to 49% in the private sector.

Federal agencies also buy more comprehensive policies: 71% have full ransomware coverage, for example, versus 54% of U.S. private-sector organizations. But stronger policies don't prevent breaches or address underlying resilience weaknesses. They offer a potential financial cushion against loss, but that cushion may be temporary.

Insurers increasingly require evidence that controls were in place at the time of an incident, such as multifactor authentication, identity management, and documented incident response plans. When organizations can't demonstrate compliance or modern controls, claims may be denied.

Moreover, only 40% of federal agencies report to insurers monthly. Limited reporting cadence can make it more difficult to clearly document and demonstrate the controls, actions, and decision making in place when an incident occurs.

What's Driving Increased Cybersecurity Budgets?

Federal investment trends are also shaped by policy and regulatory drivers. Executive Order 14306, released in June 2025, requires federal agencies to take several steps in "defending our digital infrastructure, securing the services and capabilities most vital to the digital domain, and building our capability to address key threats."[1]

[1] SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144. The White House. June 6, 2025.

Subsequent independent analysis indicates that both civilian and defense agencies are ramping up cybersecurity spending to enhance operational readiness, secure infrastructure, and manage AI risks. For example, the Department of Agriculture has prioritized expanded deployment of Security Information and Event Management (SIEM) and Endpoint Detection and Response.[2]

[2] Quarterly Market Assessment | Q4 2025. Technology Area: Cybersecurity. GovExec Intelligence.

From Investment to Operational Resilience

Federal policy and budget trends reflect a growing focus on cybersecurity investment. Veeam's global Data Trust & Resilience Report 2026 adds an important related finding: organizations with increased budgets are more likely to adopt resilience-focused technologies that improve recovery outcomes.

Top Priorities for Improving Data Resilience, All Respondents

Priority	Organizations with increased budget	Organizations without increased budget
Immutable storage	38%	11%
Automated backup	42%	33%
Integrated cyber resilience and business continuity planning	16%	9%

Strengthening Federal Data Resilience

The survey findings point to several clear opportunities to strengthen federal data resilience. The following actions are consistently associated with stronger recovery outcomes and reduced operational risk.

1) Establish clear visibility into data and AI risk.

Visibility is the foundation of resilience. But as AI tools proliferate across government operations, maintaining visibility into data flows, AI model usage, and emerging risk becomes more difficult.

Federal agencies recognize this challenge and are prioritizing AI security and governance. However, gaps remain in three areas that directly affect visibility: integrating AI security into the broader cybersecurity strategy, training employees on acceptable use, and implementing formal risk management frameworks.

Top Priorities for AI Security or Governance for the Next 12 Months

Priority	Federal agencies	U.S. private-sector organizations	Gap
Integrate AI security into broader cybersecurity strategy	25%	35%	10%
Develop employee training on acceptable-use policies for AI tools	17%	25%	8%
Implement or formalize an AI risk management framework	27%	31%	4%

2) Deploy enforceable security controls.

Policies set expectations. Controls enforce them. As AI-enabled tools become embedded in mission-critical and operational workflows, federal agencies require governance that translates policy into enforceable day-to-day controls. These controls include encryption, data loss prevention, access management, and third-party risk oversight.

Across many agencies, responsibility for AI-related risk remains distributed or unclear. Questions around ownership, such as which teams define acceptable use and how policy decisions are operationalized, can result in inconsistent guardrails and slower response times during incidents, ultimately slowing recovery under pressure.

Survey results underscore where federal agencies trail U.S. private-sector organizations in risk-informed actions taken over the past year. The largest gap, extending data risk governance policies to AI tool usage (7% vs. 30%), suggests that while agencies recognize emerging AI risks, governance frameworks have not yet been consistently translated into enforceable controls.

Actions Taken by Leadership in the Past Year Based on Cyber Risk Reporting

Action	Federal agencies	U.S. private-sector organizations	Gap
Created data risk governance policies extending to AI tool usage	7%	30%	23%
Improved third-party risk management	31%	40%	9%
Enhanced data security controls, such as encryption, DLP, and access management	42%	50%	8%
Implemented more frequent or advanced cyber risk reporting, including CRQ	38%	44%	6%
Engaged with a managed service provider	20%	26%	6%

Clear, enforceable policies and controls, supported by defined ownership structures, are foundational to managing data and AI risk. They enable agencies to adopt new AI tools while ensuring cybersecurity protections extend to their use.

"We have strengthened backup strategies, implemented immutable storage, improved monitoring tools, enhanced employee training, and conducted frequent recovery testing exercises."

VP of IT, defense agency

3) Build proven recovery and response capabilities.

Resilience isn't defined by having a plan, but by executing it effectively. Effective recovery depends on capabilities that are tested, validated, and supported by automation that enables response at the speed of modern threats.

A key mechanism for validating recovery readiness is the consistent tracking of recovery metrics. Federal agencies do track recovery metrics. However, when compared with private-sector benchmarks, the data indicates clear opportunities to improve recovery speed and outcome consistency.

For example, 59% of federal agencies track RTOs, 55% track restore and recovery testing, and 51% track mean time to recover. However, only 17% track their percentage of fully automated or orchestrated recovery processes, compared to 28% of U.S. private-sector organizations, highlighting an opportunity to reduce manual workloads and accelerate response times.

Adoption of AI enhanced cybersecurity tools for automated detection and response remains lower among federal agencies than in the private sector. These tools represent a practical governance aligned opportunity to strengthen recovery and response capabilities, particularly in budget constrained environments where efficiency and scale are critical.

AI-driven Tools for Cybersecurity, Already in Use or Planned

AI-driven Tool	Federal agencies	U.S. private-sector organizations	Gap
Automated threat detection and remediation	38%	64%	26%
Malware or anomaly detection	40%	64%	24%
Phishing detection and email security automation	38%	61%	23%
Incident response and investigation	32%	53%	21%

AI-driven Tools for IT Operations or Business Continuity, Already in Use or Planned

AI-driven Tool	Federal agencies	U.S. private-sector organizations	Gap
AI-driven capacity planning for resource allocation	41%	71%	30%
Infrastructure performance optimization and anomaly detection	38%	62%	24%
Automated system maintenance and patch management	31%	55%	24%
Service desk or IT support automation	50%	66%	16%

By reducing response times and accelerating threat isolation, AI-enhanced tools directly improve recovery performance and overall resilience.

"The biggest lesson our organization learned from our recent ransomware experience is that less automation has the ability to increase human errors."

Senior VP of cybersecurity, civilian agency

4) Strengthen executive alignment around risk ownership and reporting.

Cyber resilience isn't a security department problem. It's an organization-wide challenge. Agencies that bring IT, security, risk, legal, and mission leaders together are better positioned to align policy with operations and respond effectively when incidents occur.

Today, 34% of federal agencies have cross-functional committees that review or approve data and security policies, compared to 47% in U.S. private-sector organizations.

Broader involvement creates shared ownership. When more leaders have visibility into risk, decisions happen faster and resources flow to the right places. Regular risk reporting gives leaders greater insight into emerging cyber challenges. When paired with strong governance, it supports better informed decisions on investment, staffing, and policy.

Among federal agencies that increased their cybersecurity budgets, 67% report cyber risk to the board monthly or more frequently, compared to 49% of agencies with flat or decreased budgets. A similar pattern appears at the executive level (55% vs. 44%). Consistent, decision ready reporting enables leaders to better align risk oversight with mission priorities and resource allocation.

Conclusion: Moving From Confidence to Capability

The Data Trust and Resilience Report 2026 survey results reveal a distinct federal agency profile.

Federal agencies express higher confidence in recovery capabilities than private-sector organizations, and their recovery performance suggests this is, in part, justified. Agencies experience fewer cyber incidents overall, achieve higher insurance claim approval rates, and recover more completely when ransomware incidents succeed in encrypting data.

At the same time, these strengths can mask governance and operational challenges that may constrain agencies' ability to respond and recover as cyber threats grow in frequency and complexity.

Federal AI governance is less cross-functional, cybersecurity budget growth is less common, and AI adoption continues to outpace security implementation. Agencies also report greater concern around shadow IT and unauthorized AI tools. As AI accelerates change across data, identities, and workflows, the ability to validate recovery readiness becomes even more critical.

The path forward is clear. More frequent risk reporting, broader cross-functional engagement, stronger AI governance, and targeted investment in automation for detection and response are consistently associated with stronger recovery outcomes. These practices are becoming standard in the private sector, and they represent the next phase of maturity for federal agencies – one that moves from generalized confidence to a more secure, recovery-ready standard.

Veeam stands ready to help federal agencies protect and recover from an array of modern data security threats. Please reach out to us here, or visit www.veeam.com to learn how to move from protecting data to unlocking its full potential.