

Media Contact:

Christie Deane
703-883-9000 ext. 103
cdeane@meritalk.com

New Research Reveals Federal IT Leaders Struggle to Balance Data Access With Zero Trust Requirements

Just 6 Percent Say Their Agencies Have Mastered Data Strategy, Despite Rising Threats and Investments

ALEXANDRIA, Va. – June 25, 2025 – Security dominates the Federal data agenda, but agencies are struggling to balance protection with performance, according to a [new study](#) from [MeriTalk](#), government IT's top digital platform, and [NetApp](#), the intelligent data infrastructure company. While Federal IT leaders say security is the single most important component of their data strategy, only 60 percent rate their approach as highly effective. Seventy-seven percent still lack proper visibility into where their most sensitive data resides, and 83 percent say they struggle to balance data access with zero trust requirements. Artificial intelligence (AI) and innovation are gaining momentum as the cornerstones of future data strategies, but they aren't yet fully integrated, with just 43 percent having deployed AI-driven or automated security solutions.

As agencies are evolving their data tools and frameworks, security still falls short. Eighty percent say their agency's data security strategies are not evolving fast enough to keep up with today's threats. In just the past month, 40 percent faced delays in detecting data security threats or anomalies. Additionally, only 6 percent of IT leaders say their agencies are highly effective across all four pillars of data strategy: security, access, innovation, and efficiency.

Legacy Systems and Vendor Sprawl Challenge Federal IT Security

Federal IT leaders aren't just battling cyber threats, they're battling structural inefficiencies that slow progress and sap confidence. Reliance on outdated or legacy systems is the biggest barrier to better security (45%). And while Federal agencies have moved aggressively into cloud environments – with most saying their security posture is better for it – the shift hasn't been seamless.

Adapting legacy architectures and security models for cloud and OPEX-based environments has required rethinking governance, automation, and recovery strategies from the ground up. IT leaders identified the shift from traditional appliances to cloud-based security services as the top

change made to adapt to cloud and OPEX models (64%). While trusted partners play an essential role in Federal data strategies, the sheer number of systems, tools, and providers is creating complexity that can jeopardize policy consistency and operational management. Seventy-five percent say the number of disparate data systems and storage vendors makes data access difficult. On average, agencies use seven or more vendors.

Habits of Highly Effective Agencies

Agencies that rate themselves as highly effective in three or more pillars of data strategy (innovation, security, access, and efficiency) are consistently more likely to report investing in training, vendor management, and automation. Sixty-five percent of highly effective agencies have increased security training and awareness, compared to just 40 percent of other agencies. They're also significantly more likely than others to have reduced their number of data storage vendors (49% to 32%) and to have adopted managed services for threat monitoring (54% to 38%). Additionally, 76 percent of highly effective agencies plan to deploy AI-driven monitoring and anomaly detection in the next three years, versus 51 percent of others.

“Federal agencies are under immense pressure to modernize while safeguarding mission-critical data,” said Matt Lawson, Director, Solutions Engineering, NetApp. “This research underscores the need for a more integrated approach to data security – one that breaks down silos, embraces automation, and builds resilience into every layer of infrastructure. As AI and cloud adoption accelerate, aligning strategy with operational maturity will be essential to stay ahead of evolving threats.”

When reimagining data security and infrastructure strategies, the report recommends Federal agencies:

- Move from security silos to a more integrated data strategy
- Streamline vendor ecosystems to strengthen governance and control
- Accelerate AI adoption with a focus on operational maturity
- Strengthen resilience in contested and high-threat environments



The *Modern Data Defense* report is based on a survey of 100 Federal IT decision-makers in April 2025. The resulting research has a margin of error of $\pm 9.78\%$ at a 95% confidence level. To view the full findings, [download the report](#).

About MeriTalk

The voice of tomorrow's government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. Our award-winning editorial team and world-class events and research staff produce unmatched news, analysis, and insight. The goal: a more efficient, responsive, and citizen-centric government. MeriTalk connects with an audience of 160,000 Federal community contacts. For more information, visit <https://www.meritalk.com/> or follow us on Twitter/X, @MeriTalk. MeriTalk is a [300Brand](#) organization.

About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data, operational and workload services to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our operational and workload services provide continuous optimization of performance and efficiency for infrastructure and workloads through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. Learn more at www.netapp.com or follow us on [X](#), [LinkedIn](#), [Facebook](#), and [Instagram](#).

###