# How Government Can Elevate Its Approach to Zero Trust

MARKET TRENDS REPORT

govloop Commvault carahsoft.

# Executive Summary

In today's intricate cyber landscape, a zero-trust architecture (ZTA) security approach is essential for federal agencies. ZTA requires continuous verification and strict access controls because it assumes that all networks and users are potentially comprised. It's essential for protecting sensitive government data, especially as remote work and cloud-based systems dramatically expand the attack surface.

"One of the most integral parts to being able to run any major enterprise network is to weave security in every bit and piece of that fabric at the outset," said Richard Breakiron, Senior Director of Strategic Initiatives for the Americas Public Sector at Commvault, a provider of cloud-based data security.

Unlike traditional perimeter defense, ZTA takes a data-centric approach, minimizing the attack surface and enabling faster threat detection and response, which are paramount to maintaining operational readiness. In an era of increasingly sophisticated cyber threats, zero trust's rigorous verification and access controls are not just best practices. They become the basis for the National Institute of Standards and Technology's Cybersecurity Framework.

In January 2022, a White House memo set Sept. 30, 2024, as the deadline for federal agencies to shift from perimeter-based defenses to ZTA. Nearly all have efforts under way, but most have plans that now target fiscal 2027.

Many have zero-trust basics in place using legacy capabilities, but federal agencies must step up their game and take advantage of AI, automation and other advanced strategies in support of data- and identity-centric security. Agencies need to create a foothold today for the growth into the "dynamic" controls that will secure their zero-trust investments.

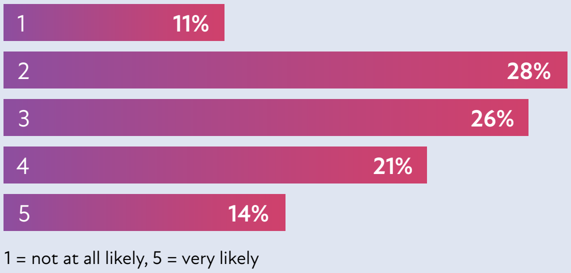
# By The Numbers

## *The Quest for Cyber Resilience*

Nearly all IT leaders say it's likely they will see data loss in the next 12 months because of increasingly sophisticated cyberattacks, according to a recent survey by IDC, a market intelligence firm. A modernized approach to zero trust could help boost their defenses.

**Likelihood of Data Loss in the Next 12 Months due to Increasingly Sophisticated Cyberattacks**

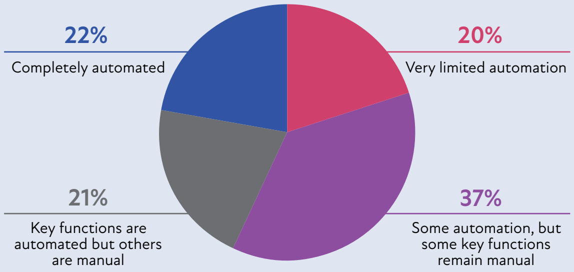
(percentage of respondents)



Although most IT leaders report using automation in cyber detection and reporting, the vast majority still rely heavily on manual processes, the survey found. Automation as part of zero trust could help strengthen defenses.

**Degree of Automation in Cyber-Detection and Reporting**

(percentage of respondents)



## *Funding Hinders Zero Trust*

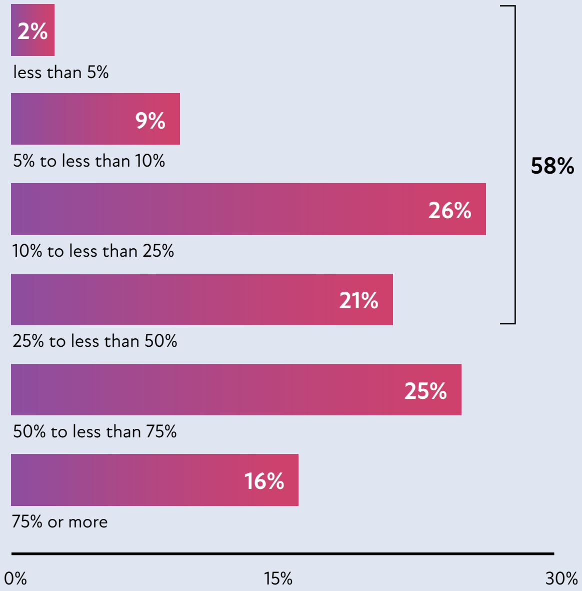
# 75%

of U.S. federal agencies will fail to implement zero-trust security policies through 2026 because of funding and expertise shortfalls, according to a Gartner survey.

## *Zero Trust Could Go Further*

Another Gartner survey found that zero trust still has room to grow. Respondents said that although 63% of organizations have implemented a zero-trust strategy, the solution often covers less than half of the IT environment.

**Percentage of Environment to Cover With Zero-Trust**



> ***"Zero-trust architectures can limit the scope of cyberattacks.... [T]his includes such things as multifactor two-factor authentication (MFA) to sign in and two-person authentication to change backup, retention, and immutability policies."***

- IDC

# How to Put Zero Trust on New Footing

## The Challenge: Factors that Hinder Zero Trust

Several hurdles can obstruct agency efforts to make the most of zero trust.

- **Complexity:** Many federal agencies operate on outdated infrastructures, but fully transitioning to a more dynamic one is challenging. For agencies to truly embrace zero trust's "never trust, always verify" position, they need technological (infrastructure and software) and cultural (mindset and skills) shifts.

  Complex internal processes, such as budgeting resources, acquisition and implementation, all add complications. The federal government's bureaucratic standard doesn't always provide the incentives needed to look for efficiencies, Commvault's Breakiron said.

- **Money:** IT teams often lack the budget they need to implement changes that would allow for more robust use of ZTA. Too often, "there's no program and no funding line for modernization programs of the scale of zero-trust architecture," Breakiron said.

  Securing that funding requires time and effort: Government agencies usually need a two-year ramp to get congressional approval to build a budgetary pipeline that supports major programs such as modernization to support ZTA.

- **Scale:** Zero trust will impact people, processes and technologies across the board. "This is an enterprisewide architecture," Breakiron said. When people try to access government systems, "you're going to stop them at that virtual front door and do a complete inspection of their credentials and their device's credentials — a radical change to the current standard."

  That needs to happen smoothly and on a massive scale. "In the case of the Army, for example, that's 1.4 million people, many with multiple devices," he said. Policy and practice must align to realize zero trust's full benefits without interrupting mission-critical work.

## The Solution: Modern, Automated Tools

Several trends are shaping the future of zero trust, and agencies can begin to embrace a range of modern tools and approaches now to gain the maximum-security advantage.

- **AI and Machine Learning Integration:** By integrating AI and advanced analytics into zero-trust frameworks, agencies can enhance threat detection and response capabilities. The technologies can identify anomalous behavior with light-speed response times, providing an essential proactive layer of security.

  AI and machine learning (ML) "can take what has often been written down in documents and make these documents dynamic," Breakiron said. By empowering automation that supports zero-trust protocols, the technology takes the pressure off thinly stretched security teams and leads to more effective outcomes.

- **Zero-Trust Segmentation:** This trend involves dividing networks into smaller, isolated segments to limit the potential spread of threats. Consider massive ocean vessels: Decks that are below the waterline typically have "a series of rooms that can be sealed off in the event of running aground, allowing the ship to remain afloat," Breakiron said. "ZTA allows for a similar approach."

  By applying granular access controls at the microsegment level, agencies can significantly reduce the attack surface and contain breaches more effectively.

- **Identity-centric Security:** Fundamental to effective ZTA use is a shift in emphasis toward identity — both of individuals and endpoint devices — when a request to enter the network comes in.

  The aim is "to create a momentary isolation, so the individual identity and status of endpoint devices can be fully verified," Breakiron said. "This comprehensive check with only a momentary delay is another new critical parameter." Although many government entities now use identity-based access control, solutions are often slow and not comprehensive, but "now new technology allows this to move much faster," he added.

# Best Practices in Zero Trust

As agencies look toward more robust zero-trust implementations, some best practices can help your agency be successful.

## Do the necessary planning:

Zero trust must deliver the right level of access to the right people in the right context, while also enforcing "least privilege" — eliminating excess or outdated access rights. That means going beyond mere compliance checklists to implementing zero trust in a way that protects critical data while ensuring necessary access to support the mission.

To strike that balance, IT leaders should be diligent in charting their course and learn from others' planning experiences. "It's very hard to get the planning right," Breakiron said. "When you read about major IT projects failing, it's because they just didn't put enough time up front in the planning."

As government IT teams look to implement modernized tools that support zero trust, "you've got to translate that into your organization and align your organization against this new architecture," he said.

## Find the right partners:

Robust zero-trust implementation will include a range of specialized tools and approaches. It may encompass MFA, network segmentation, software-defined perimeter solutions, and AI and ML capabilities.

But few federal agencies will have in house the wide range of technical capabilities needed to make the most of zero trust. Breakiron's advice: "Don't go it alone."

"Learn from early adopters. Go find people in industry. Go find partners that have been working [on] similar issues in industry for many years," he said. "Bring them in to consult. You can say, 'Here is what I understand about the architecture, here is what we're looking at that we don't understand.'"

The right partner can help an IT team build its plan and pursue the most critical capabilities, then put them together in a way to truly deliver on ZTA's promise.

## Look for small wins:

When looking to elevate zero trust, it makes sense to start with a limited use case. "Find a small gap — something that takes an easy fix — and do that," Breakiron said.

Look for areas where solid security processes already exist and where added automation will raise these to meet ZTA requirements.

"If you can fix something quickly, then go ahead and implement that piece," Breakiron said. "Build some confidence that the rest of this architectural layout will work and then keep moving down that path."

# Case Study: Intelligence Agency Focuses on Data Pillar

In a zero-trust framework, you must know what data you have to know what to keep and what you access controls to apply. In one recent case, Commvault helped a major intelligence agency modernize across this key pillar of cybersecurity.

**The challenge:** In a fully realized approach to zero trust, it's crucial "to be able to do data identification, data segregation and overall records management," Breakiron said. The agency needs a way to ensure it has a firm grip on its data stores as it looks to optimize zero trust.

**The solution:** The agency found a team of internal process owners, reached out to their existing contractor team and found experts at Commvault who were willing to understand their current state and uncover where needed information was already readily available. For example, email already contains metatags that say when and where it was created, plus subject information that can be easily cross-indexed — "little bits and pieces of data that are already captured well," Breakiron said. With that foundation, the team has integrated Commvault technology to not only help with immediate modernization needs, but also build the underpinnings needed for long-term modernization efforts.

In addition to helping inform zero-trust access controls, those existing metatags can support records retention policies and data restoration strategies. Commvault solutions bring those capabilities to life. "Commvault has made it a fundamental to its architecture for 25 years," he said.

**The outcomes:** The agency has begun to realize that by adding Commvault, they can leverage their on-hand data within the context of the ZTA data pillar. Agency leaders created the synchronization among people, process and technology to move forward.

## HOW COMMVAULT HELPS

Commvault software's integrated capabilities already align and meet the ZTA capabilities that empower business continuity and mission-readiness in government agencies, enabling them to protect their data and manage it comprehensively. By integrating automated rules and processes, agencies reduce the human effort around ZTA implementation, while delivering more consistent security outcomes.

"We understand how people use data today," Breakiron said. "Data is the lifeblood of every organization in today's digital world. Agencies cannot do anything unless they can rapidly and securely provide the right data to the right place and [make it] virtually accessible at any time." Commvault's data protection offering, which has a Federal Risk and Authorization Management Program High certification, "that protects your data with a fully air-gapped solution."

With tools for MFA, segmentation and AI-supported automation, Commvault helps agencies make the most of their ZTA, keeping data secure while also making it readily available to those who need it.

***Learn more:*** ***commvault.com/solutions-overview***

# Conclusion

Although most federal agencies have begun putting ZTA basics in place, they can and should be doing more to implement it as soon as possible. By taking advantage of modernized tools and approaches, they can maximize the return on their modernization investments to meet ZTA requirements, elevating security to successfully prepare for heightened cyber threats.

An intentional shift to a data- and identity-centric mindset will help with effective use of ZTA. Solutions based on AI and ML bring needed levels of automation, easing the burden on security teams while simultaneously driving improved security outcomes. Micro-segmentation ZTA strategies can help agencies limit the impacts of cyber events and provide granular controls that zero trust requires to be fully effective.

Federal agencies that tailor their modernization efforts within ZTA as rapidly as possible will position themselves to not only stay ahead of ever-evolving cyber threats, but they will also fundamentally control their data ecosystem to the highest levels of effective and efficient operational readiness.

## ABOUT COMMVAULT

Commvault is the gold standard in cyber resilience, helping more than 100,000 organizations to uncover, take action, and rapidly recover from cyber attacks—keeping data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere with advanced automation—at the lowest TCO.

Learn more: commvault.com/use-cases/government.

## ABOUT CARAHSOFT

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

## ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop