



Achieving Efficiency, Resilience Through Zero-Trust Architecture

MARKET TRENDS REPORT



Executive Summary

With cyber peril on the rise and the White House simultaneously pushing for greater efficiency, agencies need a new strategy to navigate requirements and ensure resilience. In federal IT systems, “the inefficiencies have become so great, there is now a pending crisis that has to be resolved,” said Richard Breakiron, senior director of strategic initiatives for the Americas public sector at Commvault, a provider of cloud-based data security.

People, processes and technology must align for effective and efficient security. Yet conventional IT modernization strategies are fragmented: IT teams typically layer on many solutions, requiring multiple support systems and creating logistical failures. Resilience suffers and efficiency breaks down. Federal IT leaders recognize the problem. “Agencies have reported using 15 different technologies, 10 different software platforms. They know it doesn’t make sense,” Breakiron said.

But there’s a potential upside: With the current emphasis on productivity, “federal government has an opportunity to really address all these inefficiencies,” he said.

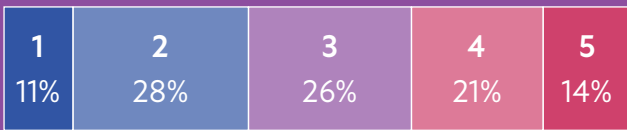
To make systems and data more secure in an increasingly adversarial world, “agencies need a new approach to zero trust,” he said. IT leaders can review their modernization strategies for cybersecurity holistically while focusing on zero trust in particular, shifting from complex and inefficient methods to a more streamlined, process-oriented approach.

Even with fewer people doing the work, “you can still perform miracles if you have the right process in place, along with the right automation and technology,” Breakiron said. A robust zero-trust architecture offers a way forward, integrating automation and technology for improved security while simultaneously driving new efficiencies in process and personnel.

By The Numbers

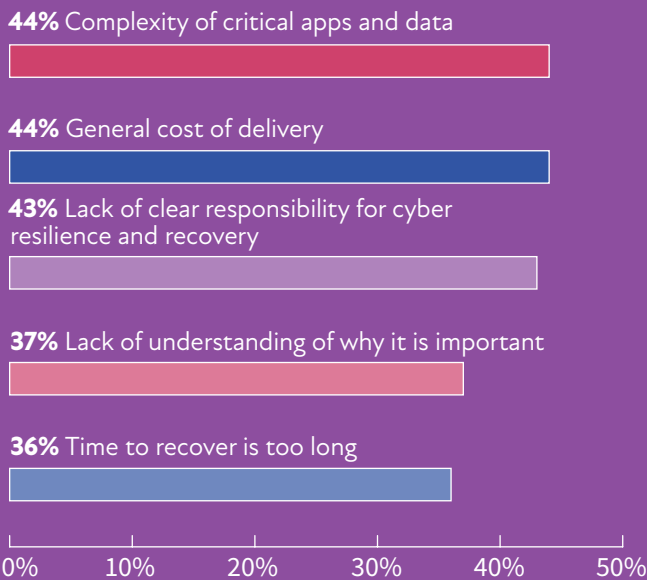
61% of business leaders believe that data loss within the next 12 months due to increasingly sophisticated access is “likely” to “very likely.”

1 = not at all likely, 5 = very likely



Source: [Commvault-sponsored IDC report](#)

What challenges do IT leaders see in delivering on cyber resiliency?



Source: [Commvault “Cyber Recovery Readiness Report”](#)

Organizations are looking to technology to improve their cyber resilience. Among senior leaders ...

52%

believe their organization has the tools and people needed to respond to cyber incidents over the next two to three years.

40%

believe automation in cybersecurity will have the greatest positive impact on their ability to secure the organization.

30%

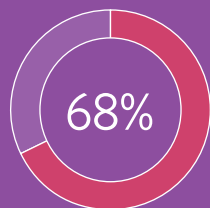
point to advancements in AI as another positive resource for cybersecurity.

Source: [“Seven emerging trends in cyber resilience”](#)

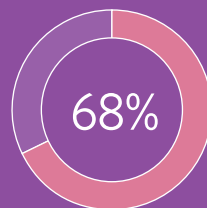
“Cyber-preparedness is a top priority of organizations worldwide, as cyberattack knows no borders and spares no organization.”

Technology executives say recovering from a cyber event is different than traditional outages:

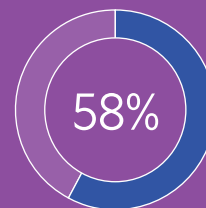
Source: [Commvault report: “Why Cyber-recovery Demands a Different Approach From Disaster Recovery”](#)



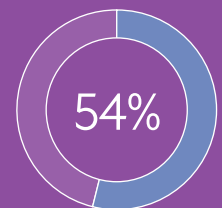
Involves different process/workflows



Involves different technologies/features



Involves different personnel/skill sets



More complex

Improved Security Demands an Architectural Approach

The Challenge: Complex, Rigid Systems

A number of challenges make it difficult for federal agencies to be both efficient and effective in their cyber resilience efforts.

Increasing complexity: The ever-growing complexity of the IT landscape makes agencies more vulnerable to advanced persistent threats, ransomware, insider attacks and other emerging risk vectors.

“With digital transformation, you have computers interconnecting data at a new scale and speed,” Breakiron said. “And there are so many more interconnections. Now the HVAC systems are connected to the internet: If an attacker can’t get to the data center directly, they can bring down the air conditioners that cool that data center via OT.”

Outdated systems: Traditional perimeter-based security is like a moat around the castle. These models are no longer adequate for the current attack landscape. With so many new attack vectors, outdated perimeter-based defenses are insufficient. “With all this data in motion, the ability for bad actors to interrupt that motion goes up exponentially,” Breakiron said.

“With all this incredible interconnectivity, it becomes almost impossible with conventional defenses to even know what path the data is following that needs to be protected,” he said.

Lack of flexibility: A single bridge across the moat is inherently inflexible; it lacks the elasticity needed to address changing circumstances and today’s diverse mission sets. Cyber resilience today demands a dynamic and adaptive security framework that knows where the data is at all times. Defenses need to be dynamic as technology matures and the threat landscape changes.

“Our current digitally transformed world is ever more complex, and without that flexibility, you are not going to be able to secure all of it,” Breakiron said. “The new digital and cloud-connected systems provide vast amounts of data that can be really valuable, but only if we can organize our modernization from an architectural perspective.”

The Solution: A Zero-Trust Architecture Platform

To address complexity and achieve flexibility, government needs a cyber resilience platform defined by zero-trust principles — a zero-trust architecture (ZTA), rather than an inefficient mix of fragmented solutions. Such a platform will ...

Deliver the essentials of zero trust: The current gold standard for cyber resilience, zero trust calls for systems that can verify identity explicitly; that use least-privileged access to restrict the behaviors even of verified users; and that assume a breach is always imminent.

“In a zero-trust architecture, those principles define the new ‘digital transformation,’” Breakiron said, “that will only provide access when absolutely validated, regardless of what system you’re coming from or what your needs are. When it grants access, it gives users only what they need, when they need it. And it will assume a breach, so if something happens that makes you no longer a person of trust, it can eliminate that connection on the fly.”

Offer flexibility to adapt to specific mission sets and deliver “a highly customized, highly focused set of solutions with the flexibility to meet different business and warfighter requirements,” Breakiron said.

Federal agencies may be responsible for health, energy, finance and so on, and each has unique resilience needs. “A platform driven by a zero-trust architecture allows different business-sector verticals to adopt different tactical operational solutions,” he said.

Reduce risk, by taming the complexity of “defense in depth” and going beyond perimeter defense: A platform-based zero-trust architecture consolidates defenses, driving efficiency by pivoting away from fragmented toolsets. It focuses on the user, processes and data in motion, rather than on an increasingly porous perimeter of outdated single drawbridges.

This can help agencies effectively and efficiently as they modernize their IT environments, while addressing new cyber challenges. “This will be essential as agencies look to be ready for the next-generation threats posed by quantum computing and AI,” Breakiron said.

Best Practices in Zero-Trust Architecture

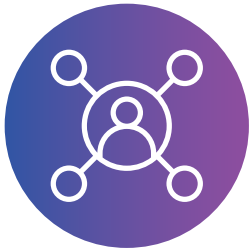
A number of key best practices can help agencies make the most of a zero-trust architecture.



Leverage the Value of an Initial Assessment

As agencies modernize for cyber resilience, it makes sense to start by taking an initial inventory because you can't fix what you can't see. Without understanding the root causes, "you end up treating the symptoms without fixing the underlying problem," Breakiron said.

Agencies can assess their current IT ecosystem using in-house talent, and/or they can enlist a capable cyber-systems provider to compile an overview of the current situation. That assessment will help identify weak points and rank their urgency, while also surfacing areas of inefficiency.



Connect People, Processes and Technology

"A leader of DoD's cyber warriors said recently, 'I start every day with people shooting at me, trying to kill me,'" Breakiron said. Cyber is a pitched battle, and victory (in the form of resilience) demands alignment across people, process and technology.

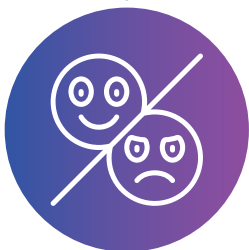
"In your e-assessment, you might find a major problem is with people: Maybe they use the word 'password' as a password and recognize that process and/or technology can fix that," he said. "It's all interconnected."



Take a Risk-based Approach to Resilience

Granting access to systems always entails a certain degree of risk. "Resilience is not about risk elimination, it's about risk management," Breakiron said.

"Resilience is a sliding scale based on what you are trying to protect. It's never a one-size-fits-all," he said. "That initial assessment should include a risk evaluation. If you're trying to protect nuclear access codes, that criticality demands stringent controls. If you're trying to set up golfing tee times at Fort Belvoir, that is a totally different risk category."



Ensure Zero Trust Doesn't Impede the User Experience

Resilience will falter if you embrace solutions that are too burdensome for the end user. "If you make entry into the system too hard, you're going to motivate people to find a back door: You're going to motivate bad behavior," Breakiron said. "The user interface has got to be the simplest, most intuitive part."

When you introduce ZTA, "you have got to get people involved. Sit down with a testing group of people and say 'Do you want to remember a really difficult password, or would you rather have the hard token and an eight-digit number?' A platform will have multiple ways to manage this," he said.

Use Cases in Zero-Trust Architecture

Multiple government agencies have successfully tapped a ZTA platform approach to improve their cyber resilience.

- **The Department of Defense** has taken a highly coordinated approach as it leverages ZTA to enhance cybersecurity. “They long ago implemented the use of the common access card, or CAC, that went across all services,” Breakiron said. “It is no longer Navy blue, Army green, Marine brown. You get one card, and it’s white. According to some intel analysts, it has reduced cyberattacks by 40 percent.”
- **The IRS** tapped ZTA to support strong identity verification and access controls in a mission area that requires allowing dynamic access by individual taxpayers, while also meeting some of the most restrictive security protocols to interface with the banking and finance industry. “ZTA supports appropriate access, enabling users to prove identity beyond a doubt, while limiting their access to only their own financial information,” Breakiron said.
- **The Department of Health and Human Services** is looking to leverage a ZTA platform to gain immediate enterprise efficiencies while supporting multiple stakeholders and diverse mission sets. “They need to provide a capability to a health care provider at the point of incident. They need to get managers access to information about performance. They need to meet these dozens of characteristics across network, identity management, data management and so on,” Breakiron said. “With zero-trust architecture as a platform, they get one solution that enables all these different business processes. It gives them the needed security, and that in turn makes all those business processes so much more efficient.”

HOW COMMVAULT HELPS

Commvault has worked with industry leaders like Microsoft and AWS, as well as with government and Fortune 100s to deliver data protection products built on core software, now offered also as an SaaS product.

“Commvault’s DevSecOps engineering team supports a single base code. As we acquire new capabilities and bring to bear new technologies, they are folded seamlessly into a single solution — no duct tape required,” Breakiron said.

Commvault ZTA delivers a secure rapid cleanroom for minimizing enterprise-level risk in cyber recovery. “Its hybrid cloud and on-premises unified platform offers a command center with an intuitive user interface, allowing consolidation of tools, optimization of processes and personal technical skills, with industry-leading lowest total cost of ownership,” he said.

The platform’s cloud-native Workload Protection, Recovery, Rebuild provide compliance and clarity across all data workloads, at speed and scale. Fully integrated data and cyber assessment tools, along with audit and alert features, ensure agencies keep current with ever-evolving policy and regulatory changes.

Learn more: commvault.com/solutions-overview

Conclusion

With cyber risk on the rise — from criminal gangs to nation state actors to disgruntled ex-employees — the stakes have never been higher in government. At the same time, there’s a laser-focus on efficiency in the federal space right now, and that creates an intriguing dynamic and a window of opportunity.

Fragmented legacy systems embody inefficiency: Too many tools to manage, too much human labor spent on care and feeding. These systems are proving ineffective, too. The castle-and-moat approach doesn’t work in an era of highly interconnected data and systems.

With a platform delivering a zero-trust architecture, it’s possible to align people, process, and technology. This approach tames complexity and delivers needed flexibility based on the key principles of zero trust, including explicit identity verification and least-privilege access.



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.

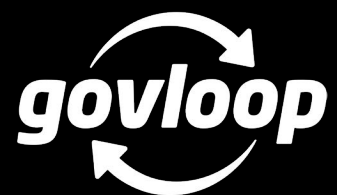
Learn more: commvault.com/use-cases/government.



ABOUT 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.



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

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

www.govloop.com
@GovLoop

