



Reimagining Federal Cybersecurity with Efficiency and Effectiveness at the Core



Between new innovations, government compliance requirements, executive order uncertainties, and constituent demands, federal technology leaders are facing unprecedented challenges as they work through their digital transformation roadmaps.

Underpinning all of these challenges is the need to secure federal systems against increasingly sophisticated cyberattacks. From lone hackers to nation-state operatives, government agencies face constant threats.

To help federal chief information officers (CIOs) and chief information security officers (CISOs) strengthen cybersecurity across their agencies, the White House issued the [Executive Order on Improving the Nation's Cybersecurity](#) (cyber EO) in 2021. The cyber EO directed technology leaders to implement zero trust security across federal networks. Agencies were given guidelines and maturity models to support implementing zero trust security measures from the [Cybersecurity and Infrastructure Security Agency](#), the [General Services Administration](#), the [Department of Defense](#), and the [National Institute of Standards and Technology](#).

In addition to implementing zero trust measures, the cyber EO called for agencies to accelerate movement to secure cloud services.



Technology leaders working to achieve the cyber EO mandates are balancing that work with ongoing and evolving issues, including:



Maintaining legacy systems. According to the [Government Accountability Office](#), the U.S. government spends over \$100 billion annually on information technology, with up to 80% of that used to maintain legacy systems. Legacy systems can create data silos, are hard to secure, and can hinder innovation and productivity.



Balancing cloud-based and on-premises environments. While agencies continue to move apps and workloads to the cloud, most still have on-premises solutions, increasing security and operational complexity.



Supporting remote and hybrid work environments. Although federal employees have been called back into the office, some of the federal workforce will continue to telework or work in the field. A remote and mobile workforce brings security challenges along with issues around network access.



Managing Internet of Things (IoT) devices. Agencies have turned to IoT devices, including smart sensors, to improve operational efficiencies, manage resources, and deploy personnel. These devices are often connected to agency systems and can create security gaps.



Preparing for emerging technology, including artificial intelligence (AI). With the White House announcing a [\\$500 billion investment](#) in AI infrastructure along with issuing an [executive order](#) directing advisors to develop an AI action plan to enhance America's global AI dominance, agencies need to have the systems in place—and secured—to support these emerging technology tools.

Zero Trust

Zero trust is a cybersecurity framework based on a “never trust, always verify” approach to network access. A zero trust architecture takes a layered approach to securing data and networks, including all cloud instances, as well as users and devices. Zero trust security models strengthen access controls and protect sensitive data.

Key elements of zero trust security architecture include:



Identity, credential, and access management (ICAM)



Endpoint protection



Continuous monitoring



Automated detection and response



Microsegmentation



Least-privileged access



Policy enforcement

External Influences That Drive Cybersecurity Technology Choices

Policymakers are putting pressure on CIOs and CISOs to deliver IT solutions that drive rapid, strategic outcomes and meet mission objectives. At the same time, they are integrating zero trust security practices and accelerating the move to secure cloud services to meet federal mandates.

These demands could drive leaders to make quick decisions based on external influences, such as choosing technology that worked for their peers at other agencies or going with a technology brand that they know. They could also choose a solution that solves one issue without taking a holistic view of their overall security needs to meet federal mandates or that overlaps with existing technologies, potentially duplicating costs.

Consequences of Choosing the Wrong Security Technology

When choosing cybersecurity tools based on external influences, it puts the agency at risk. It also undermines the confidence technology leaders should have in their technology choices because they were picked without thorough research and alignment with the agency’s strategy. IT and security leaders also may feel less confident about their ability to guide their agencies to future success in implementing emerging technologies like AI.

A Strategic Approach

To gain the confidence they need in their cybersecurity technology choices and the agency's ability to scale to meet future innovation demands, IT leaders should take a measured approach to selecting technology tools that consider:



Where the agency is on their digital transformation roadmap.



What the agency's cybersecurity needs are based on existing tools and alignment to federal mandates.



What user experience the agency wants to provide their teams and constituents.



What lies ahead on the agency's strategic roadmap.



What mission outcomes the agency wants to achieve in the future.

Here are three things technology leaders should consider when looking for the right cybersecurity tools to achieve zero trust mandates.

1. Balance Legacy Technology with Cloud Migration and Zero Trust Security Practices

Federal CIOs are navigating the challenge of maintaining existing legacy systems while strategically transitioning to modern cloud-based infrastructures to align closely with the intent of federal cybersecurity mandates.

Legacy systems often lack the necessary flexibility to seamlessly integrate advanced security measures. Therefore, agency IT and security leaders must:

- Assess and align legacy systems with zero trust frameworks and cloud security capabilities.
- Implement phased migration strategies to modernize effectively while maintaining operational continuity.

To achieve cybersecurity goals, agencies require a true single platform designed from the ground up with efficiency, effectiveness, and mission readiness at its core.

The ideal platform will inherently facilitate an incremental yet continuous improvement in zero trust maturity. By leveraging a unified approach, federal agencies can significantly reduce complexity, eliminate redundancies, and streamline their operations.

A single, comprehensive platform eliminates dependency on public cloud infrastructure, providing agencies clear visibility into performance, eliminating hidden costs, and substantially reducing resources required for platform management. This allows agencies to concentrate more resources and attention on mission-critical activities rather than on routine maintenance.

**By selecting a unified platform,
federal agencies can:**



Consolidate and simplify their technology stacks, minimizing software licensing and maintenance expenditures.



Optimize operational efficiency through centralized security policies, controls, and integrated automation capabilities.



Lower administrative overhead via automated compliance reporting, streamlined policy enforcement, and proactive system updates.



Ensure scalability and adaptability to evolving federal mandates and emerging cybersecurity threats.

Furthermore, federal IT and security leaders should prioritize platform selections that transparently align with compliance requirements and relevant governmental frameworks, including the [Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model \(CISA ZTMM\)](#) and the [Department of Defense Zero Trust Capability Execution Roadmap](#).

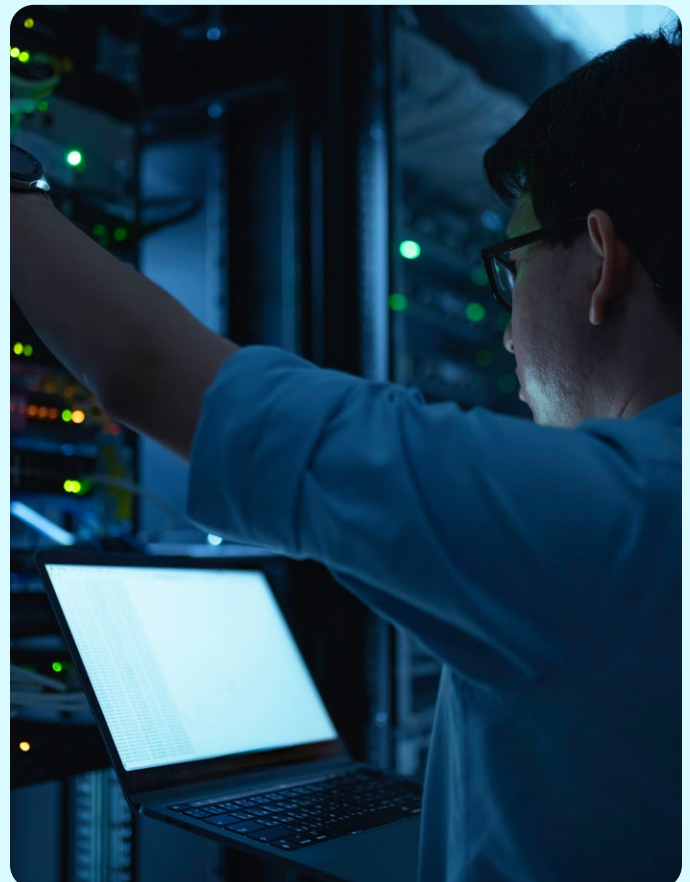
Only through transparency can agency technology leaders ensure that security tools and platforms support federal government mandates and initiatives while identifying and eliminating overlaps to achieve cost-avoidance goals.

By embracing this intent-driven, unified platform strategy, agencies can confidently address both current and future cybersecurity mandates, leveraging a FedRAMP High cloud environment. This type of unified platform delivers exceptional performance, complete visibility, and zero trust-based security and data protection for agency resources, irrespective of user location.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Defense (DoD) have issued zero trust frameworks to guide agencies on implementing all the elements of a zero trust architecture.

The DoD's Zero Trust Capability Execution Roadmap aims to achieve target-level zero trust by 2027 and advanced-level zero trust by 2032 across the DoD's enterprise.

CISA's Zero Trust Maturity Model 2.0 is being used by civilian agencies across the federal landscape.





2. Look for a Platform That Supports Integrations

There currently isn't one tool or platform that can achieve full zero trust security across an agency's enterprise. While many vendors claim to have platforms or solutions that solve all security challenges, they often are just okay at many things while never truly excelling at the key elements of zero trust, leading to gaps in functionality. These gaps can be discovered by attackers, making an agency vulnerable.

A more effective approach is to adopt a platform that supports the seamless integration of multiple key technologies, ensuring agencies can align with zero trust principles while maximizing security effectiveness and cost efficiency. By integrating best-in-class solutions, agencies can create a more resilient cybersecurity framework, leveraging technologies that excel in their respective areas, including:

- **Identity, Credential, and Access Management (ICAM):** Ensures the right individuals have the appropriate access to technology and data resources, reducing insider threats and unauthorized access. ICAM is critical during federal agency extended probation periods and potential restructuring.
- **Endpoint Detection and Response (EDR):** Protects endpoints and cloud workloads by detecting and preventing threats, minimizing the risk of breaches, and enabling rapid incident response by correlating endpoint signals with cloud security policies.
- **Automated Threat Detection and Response:** Detects, investigates, and mitigates threats in real time across the agency's digital ecosystem by enabling teams to automate incident response and threat intelligence sharing.
- **Secure Access and Network Visibility:** Monitors and controls user access to networks and data, ensuring compliance with zero trust principles. Integrations with Netskope's Secure Access Service Edge (SASE) help agencies enforce least-privileged access while securing sensitive government workloads.

By leveraging an open, integrated platform, federal agencies can:

-  Enhance interoperability between security tools without the need for constant rip-and-replace cycles.
-  Unify security policies across on-premises, hybrid, and cloud environments, ensuring consistency in enforcement.
-  Reduce operational complexity by automating threat detection, response, and compliance reporting.
-  Maximize ROI by extending the life cycle and effectiveness of existing security investments.

Taking an open platform approach allows agencies to bridge the gap between legacy and modern security technologies, enabling a scalable, future-ready zero trust architecture without unnecessary disruptions or excessive costs.

Secure Access Service Edge (SASE)

A secure access service edge (SASE) is an architecture first described by [Gartner](#) that applies zero trust security standards to protect data wherever it moves.

SASE converges multiple security technologies for web, cloud, data, and threat protection along with cloud-edge networking capabilities into a scalable, elastic platform that protects users, data, and applications everywhere. It doesn't matter how many cloud instances, on-premises environments, or remotely connected devices an agency has—the SASE architecture provides protection and visibility across the enterprise.

A SASE platform allows agencies to get the flexibility they need to add zero trust technology tools over time as legacy technology migrates to the cloud. They also optimize the end user experience.

3. Create a Technology Strategy That Prepares for the Future

While we can't know what technology innovations will happen in the future, prioritizing zero trust principles within IT infrastructures that allow for integrations ensures agencies are well-positioned to adapt to future advancements and challenges.

When systems are secure in a way that can adapt and scale, leaders can have the confidence to bring on new innovations and adopt new use cases, including integrating AI into their workflows.

Potential use cases include:

- **Improving security by understanding the size and scope of cloud-based apps.** Research has found that employees of large enterprises can access more than 2,400 apps. Many of these apps are cloud-based SaaS applications. 97% are adopted by teams or individual users without the oversight of the IT team. With a platform approach that integrates zero trust security principles, apps can be found, rated, and monitored to reduce risk.
- **Blocking suspicious or risky activity.** If a user attempts to open a risky application or transfer sensitive data to a personal instance of a company-approved application, AI tools can help coach the user in real time and guide them to safer options and better choices.
- **Securing access to internal apps.** federal agencies have many internally developed apps, which also need to be locked down

with zero trust security. This ensures that users are accessing only what they need and not unnecessarily moving laterally through the agency's network.

- **Stopping unapproved data movement.** The right platform tools can help IT and security leaders understand how their agency collects, transmits, stores, and shares data across applications. With that knowledge, they can strengthen security by stopping unapproved data movement.

By prioritizing zero trust through a platform approach, IT and security leaders will be at the forefront of innovation in their agency, blending technology management with security leadership to guide the enterprise in unlocking new value and staying competitive in the future operational landscape.

Netskope partners with federal agencies to build a more secured government.

Digital transformation and the implementation of holistic, zero trust security across government networks takes time and resources. Netskope offers FedRAMP High authorized SASE solutions designed to help agencies achieve zero trust security across disparate environments seamlessly.

With Netskope, IT and security leaders can gain confidence in their cybersecurity technology while driving value, meeting constituent needs and mission goals, and improving federal operations—all while keeping networks and data secure. They will be well-positioned to adopt new technology and will be prepared for any dynamic changes the future may bring.

+ Visit www.netskope.com/federal to learn more about Netskope's security solutions for government.

