



How Cloud-Native Security Supports Federal Government Modernization

MARKET TRENDS REPORT



Executive Summary

The federal government has embraced the cloud to modernize capabilities and drive efficiency. That creates new opportunities, and new challenges. While the Federal Cloud Computing Strategy's "cloud smart" approach urges government to focus on security and privacy, security delivered from the cloud remains a sticking point for many agencies.

Legacy approaches to security aren't keeping pace with efforts to modernize infrastructure. Most agencies have cobbled together an assortment of defenses, including secure web gateways, firewalls and cloud access security brokers (CASBs). Each of these tools has a role to play, but many IT teams find it difficult to manage a heterogenous mix of solutions in the emerging IT environment where workers and applications are everywhere.

This leads to potential gaps at a time when bad actors increasingly view government systems and data as high-value targets.

"Cloud requires a new security framework," said Christina Hausman, Product Marketing Manager for Security at Cisco Systems. "When applications are no longer exclusively in a data center, and employees no longer gain access strictly from the office, agencies need to adopt a different approach."

"Cloud requires a new security framework. When applications are no longer exclusively in a data center, and employees no longer gain access strictly from the office, agencies need to adopt a different approach."

- Christina Hausman, Product Marketing Manager for Security at Cisco Systems

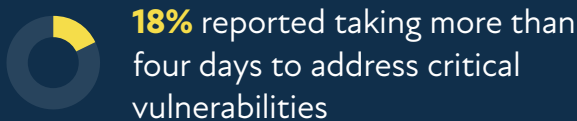
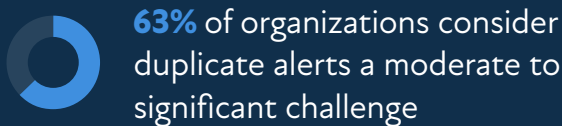
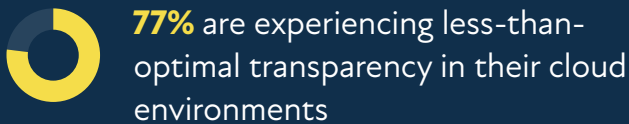
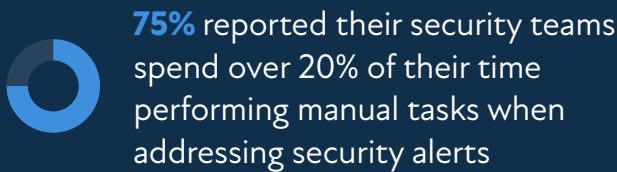
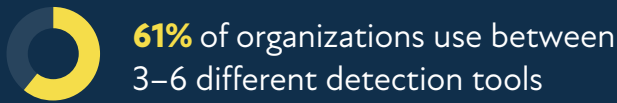
To elevate the protection of mission-critical systems and sensitive data, agencies can look to a cloud-native cybersecurity platform. Rather than extending on-premises security approaches into the cloud, they need a solution purpose-built to safeguard applications and data in this new environment: tools designed specifically to run in the cloud.

Delivered as-a-service, such a solution cuts through the present complexity, helping ensure agencies can meet their compliance obligations. And a platform that brings together networking and security in a single service can help ensure cyber resilience in support of an increasingly hybrid government workforce, a key goal for many agencies.

By the Numbers

Common Cloud Security Challenges

A *Cloud Security Alliance* survey of more than 2,000 IT and security professionals found:

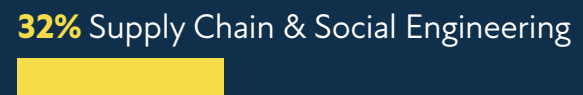


Foreign actors “have targeted governmental, think tank, healthcare, and energy targets for intelligence gain. It has now observed Russian (SVR) actors expanding their targeting to include ... government financial departments, and military organizations.”

– *Report from the Cybersecurity and Infrastructure Security Agency (CISA) on foreign actors adapting tactics for initial cloud access*

Types of Attacks Experienced by Organizations

From the *2024 Cisco Cybersecurity Readiness Index*



32,000+

security incidents were reported by federal agencies in FY21, according to [GAO](#)

93% of corporate and government networks today can be penetrated by [cyber criminals](#)


30% espionage | 68% financial

motivation among bad actors targeting public administration; spying nation-states seeking information or for financial gain


Legacy Security Can't Stop Modern Threats

Challenge: The Stakes Are Getting Higher


With their applications modernized to be delivered from the cloud, agencies face a few significant challenges around security. Legacy approaches may struggle to address ...

 **Increasing complexity of cyberattacks:** With a growing range of attack tools in their arsenal and increasingly sophisticated technical capabilities, cyber criminals today can penetrate 93% of commercial and government networks, [Forbes reports](#).

That's especially problematic for government. From personally identifiable information to financial mechanisms, government is home to a wide range of high-value data stores. "All of that makes government a target of choice today," Hausman said, and the fragmented nature of legacy security approaches gives bad actors a window of opportunity.

 **Growing nation-state threats:** Cyber today is a weapon in adversarial nation-state conflicts, with state-sponsored bad actors playing a growing role.

"This isn't like an attacker trying to steal credit cards in a retail environment," Hausman said. "State-sponsored activity certainly is targeting critical personal information like credit cards and health care information. But they're going further, looking to disrupt critical services and critical infrastructure."

 **Regulatory compliance requirements:** As agencies look to counter these threats, they need to do so within a well-established framework, in compliance with a range of specific government regulations and guidelines.


There's the need to leverage CISA's Protective Domain Name System (DNS), intended to shield federal users online from reaching known or suspected malicious destinations. Agencies need to comply with the Office of Management and Budget Memo M-22-09, which describes cyber standards in support of a zero-trust architecture, as well as a variety of other mandates.

All this requires a deliberate and thoughtful approach. "Agencies need to adhere to the mandates, but also make sure that those mandates don't hinder their ability to focus on their mission and purpose," Hausman said.


Solution: A Cloud-Delivered Approach

A single, integrated, cloud-delivered security service offers multiple levels and layers of security protection. With a software-as-a-service (SaaS)-based solution, Hausman said, "you can deploy security protections right away, and then customize and layer on additional capabilities based on how your needs evolve."


Such an approach delivers several key benefits:

 **Overcoming complexity:** Rather than having to manage multiple solutions across its on-premises and cloud infrastructures, an agency can leverage such a platform to gain both consistency and simplicity in its cyber efforts.

A cloud-based security solution will integrate cyber with networking, delivering the domain-layer security that is crucial to ensuring safe connectivity. It will offer a secure internet gateway to protect the network against unwanted software or malware that users may encounter on the web. And it will be informed by current threat intelligence automatically.

 **Empowering hybrid workers:** With legacy tools, people accessing cloud applications from offsite "may not have a robust level of security protection," Hausman said. "Critical information contained in that cloud application may be subject to theft or compromise."

A cloud-native security platform "protects users no matter where they're located," she said. "The user is secure, whether they're connecting into the cloud applications or just accessing the internet as part of their job."

 **Enabling compliance:** A platform authorized through the Federal Risk and Authorization Management Program (FedRAMP) will inherently meet many of the key mandates around cybersecurity, making it easier for agencies to ensure they are in compliance. "Agencies who purchase a cloud-delivered security service that is FedRAMP-Authorized already know that it has met a particular level of security protection," Hausman said. As new mandates emerge, the SaaS nature of the platform ensures they will be able to keep pace.

Key Capabilities for Cloud-Native Security

A cloud-native approach to security brings to the table several key capabilities that are critical to ensuring success across today's increasingly complex IT landscape.



Domain Name System-layer security:

Security that addresses DNS is a critical part of any agency's overall security posture. A vital element of internet infrastructure, DNS translates domain names into their associated IP addresses. By ensuring its security, a cloud-based platform can block malicious domains, IP addresses and cloud applications before a connection can be made.

"CISA takes this seriously," Hausman said. "They released their protective DNS mandate, which says that all government employees must use a protective DNS resolver service to access cloud applications."

As an integral part of a security platform, DNS protection addresses this need. "If a user attempts to establish a browser connection to a malicious site, the DNS security blocks that connection before the browser session is even established," Hausman said.



Secure internet gateway:

Also known as a security service edge, a secure internet gateway is a single cloud service that contains multiple layers of security protection. That's important, because threats come in all shapes and forms.

"You need additional capabilities, which in a secure internet gateway will include things like visibility into the dark web, threat detection in all web-based transactions and application visibility and control over web applications," Hausman said.

On top of this, a cloud-native solution will deliver a CASB, a capability that allows an agency to control which users have access to what applications and can prevent the running of particular applications in the environment.

In addition, deep packet inspection protects against indicators of compromise, and built-in data loss prevention helps stop critical information from being exposed or exfiltrated in the cloud.



Threat intelligence:

Bad actors are constantly evolving new threats, and agencies need timely insight there. "Your security tool is only as good as the threat intelligence that feeds into it, and the security environment is continuously changing and evolving," Hausman said.

The right solution enables agencies to keep pace with those changes. Cisco Umbrella, for example, is informed by the Cisco Talos threat intelligence and research group. Informed by timely intelligence, "security protections are continuously being updated to protect against the latest nation-state-sponsored activity and attacks," she said.

Having breadth and depth in threat intelligence is critical in the face of an ever-evolving cyber threat landscape.

Common Federal Government Use Cases

The government IT environment presents several urgent uses cases for a cloud-native security platform.

Hybrid workforce

Many people increased their work-from-home strategies during the pandemic, and there's little sign of the practice waning. Federal IT teams today are tasked with securing this hybrid workforce.

In this environment, a cloud-native approach “ensures security, no matter where they are connecting from,” Hausman said. “You’re securing those users as they are accessing applications in the cloud, and also protecting the critical data contained there.”



Cloud applications

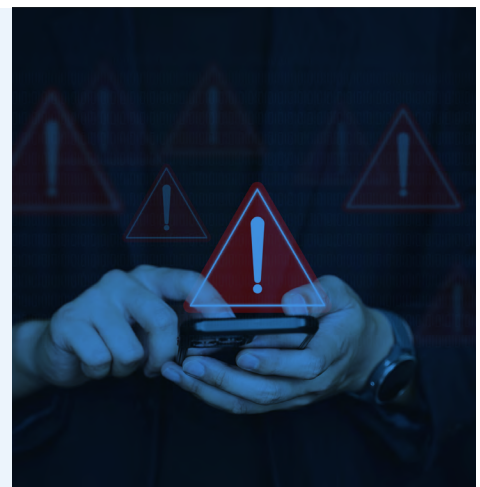
Agencies are working hard to migrate their applications to the cloud, and they need a streamlined and robust way to ensure security as users interact with those applications. Cloud-native security answers that call.

“The right solution will deliver DNS protections and secure web gateway capabilities, along with CASB functionality to control which users can access particular applications and the data contained in them,” Hausman said. The tools protect against outside attack and help ensure that “only users who should have access to that application are allowed that access.”

Containing the sprawl

Unauthorized online applications present a security risk. Malware can find a way in, and data can potentially leak out, especially via tools leveraging generative artificial intelligence (AI).

With a strong cloud-native solution, “you can prevent that from happening,” either by blocking access to entire applications, or by implementing controls. In Cisco Umbrella for Government, for example, “we have controls for over 70 different generative AI applications. We can control what information is added to them, who uses them, how they are used.”



How Cisco and Presidio Federal Can Help

The commercial version of Cisco Umbrella is a proven solution, with over 30,000 customers. It integrates a number of different security technologies within a single cloud-based SaaS service, including CISA Protective DNS integration, cloud-delivered firewall, CASB, secure web gateway and data loss prevention.

A FedRAMP Moderate Authorized solution, Cisco Umbrella for Government, brings these tools to government agencies, protecting the hybrid workforce and cloud-based applications. Agencies can manage all those capabilities from a single console, customizing them to meet specific mission needs. They can deploy DNS security in just a few hours, then layer on additional security as needed.

A mid-tier integrator exclusively focused on federal government, Presidio Federal can help agencies access these powerful tools. An outcome-focused trusted adviser and longtime Cisco partner, Presidio Federal boasts a credentialed, cleared team with decades of experience and deep expertise addressing the unique challenges of government agencies.

Learn more at presidiofederal.com/partners/cisco.

ABOUT



Presidio Federal, a wholly owned subsidiary of Presidio, is a mid-tier integrator that is exclusively focused on federal government. We work with large prime contractors as well as small businesses to become a sort of “easy button” for our federal customers.

We are proud to be an outcome focused, trusted advisor with a credentialed team that has experience and understanding with the legacy systems and unique challenges of government agencies. We have an extensive partner ecosystem, including many of the best-of breed OEMs in the business like Cisco, but we layer in an unbiased, broad perspective that is driven by mission and a long-term, accountable relationship.

For more information, please visit www.presidiofederal.com.



Cisco is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals.

To learn more, visit: www.cisco.com/government.



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.com | [@govloop](https://twitter.com/govloop)



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

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

www.govloop.com
@GovLoop

