Advancing government security with Cisco's Security Service Edge

How Cisco's FedRAMP-authorized Security Service Edge with unified IT management gives federal, state, and local agencies a new edge in converged cloud-delivered security.

BY SCOOP NEWS GROUP

As government operations become increasingly digital, there is an accompanying need for efficient deployment and management of user threat defense and application access. Modern, comprehensive and robust cloud-delivered security to protect and enable users everywhere they work has never been more critical. Just as important is partnering with cybersecurity solution partners with extensive experience and versatility working in today's expanded security, networking, and AI ecosystem — who also understand the unique needs of government.

That's why Cisco's FedRAMP-authorized **Security Service Edge (SSE)** is attracting growing attention among federal, state, and local agencies. Cisco SSE offers government agencies a new edge in converged cloud-delivered security — combined with unified IT management. It also offers a measure of trust and assurance coming from Cisco, a global leader in networking, security, AI and IT solutions and a proven partner of the U.S. government for close to 40 years.

THE BIG PICTURE: Traditional security products and practices can no longer keep pace with today's constant barrage of cyberattacks on federal and state agencies.

- **Escalating threats:**
  In fiscal year 2023 alone, federal agencies reported more than 32,200 **information security incidents**, according to the U.S. Government Accountability Office, costing billions of dollars to investigate and repair.
- **The financial impact of security breaches keeps growing:**
  According to the most recent **research** from the Ponemon Institute, the average cost of a data breach in 2024 was $4.88 million per incident, up 10% from 2023.

COMPOUNDING SECURITY RISKS: Adding to the challenge is the relentless evolution of digital solutions and the sprawling distribution of data workloads across the on-premises and multi-cloud environments that users need to access in order to get their work done.

The state of flux gives cyber actors and nation-states new and growing opportunities to exploit networking vulnerabilities:

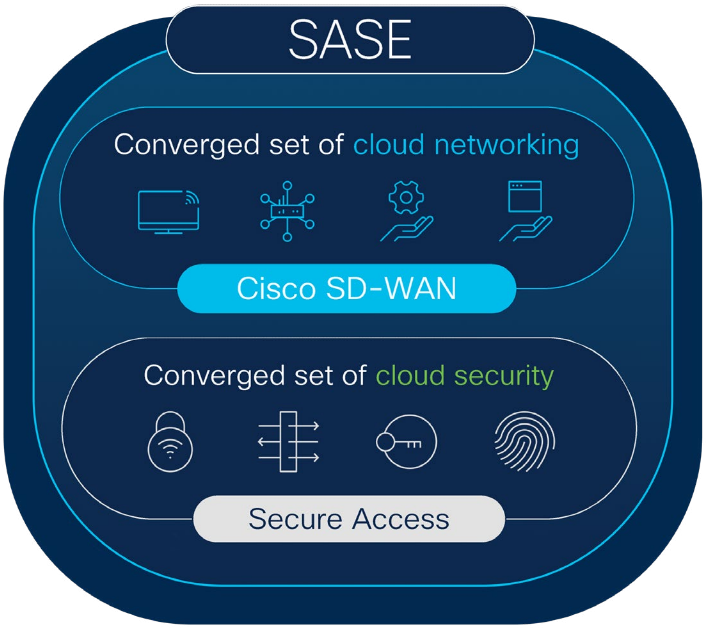
- **Threats continue to grow for Government agencies:**
  According to one measure from Cisco Talos Threat Intelligence Group, the number of **Common Vulnerabilities and Exposures (CVEs)** security teams increased from 29,166 in 2023 to 40,289 in 2024.

- **Your workforce is the #1 attack target:** According to **Cisco Talos 2024 in Review** report, threat actors are opting to compromise networks by simply logging in, with 60% of all attacks being identity-based.
- **Workflows are expanding and changing:** Remote and flexible work models, web-based applications, and software-as-a-service are now features of today's workplace. Data and applications have largely moved beyond the confines of data centers, requiring new, evolving and increasingly complex networking and security architecture that work in both on-premises and remote environments.
- **Diminishing value of one-off security tools:** Traditional security tools operating in agency silos are proving less capable of seeing the big picture. Moreover, they continue to require lots of time and specialized personnel to maintain; they inevitably introduce protection and policy inconsistencies across the infrastructure and add their own security and performance risks to the larger security network. Even the best security tools are failing to keep up with the dynamics of today's government networks.

MOVING FORWARD: While federal and state agencies have significantly improved their zero-trust security posture over the past three years, experts agree that implementing an integrated security platform that provides holistic visibility, and control remains essential to safeguarding government data systems from rising attacks.

- **Agencies are increasingly moving** to Security Service Edge (SSE) platforms to secure their applications and data. SSE embodies the convergence and consolidation of multiple security technologies into a modern, cloud-delivered network security architecture that secures access from users to applications and resources across numerous use cases and environments.

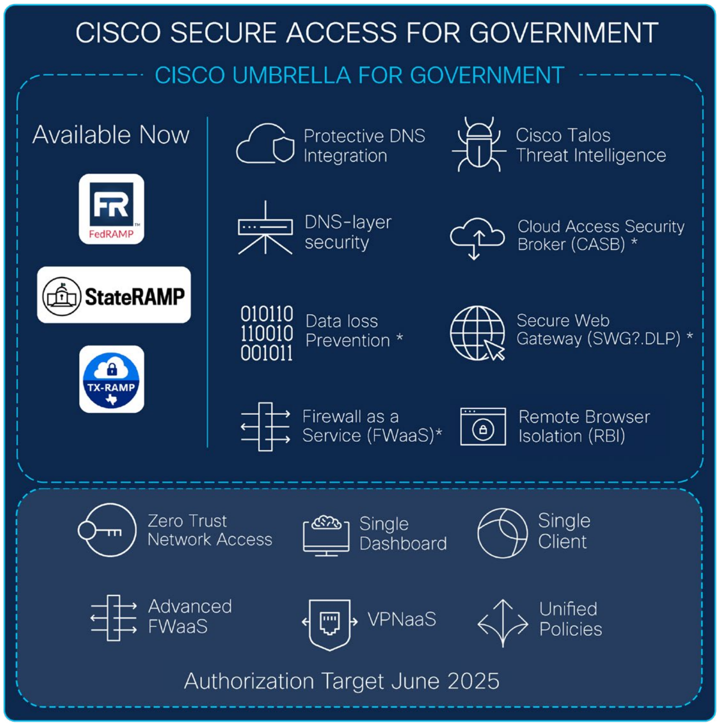
- **Combined with SD-WAN** (software-defined wide area network) capabilities, the SSE technology stack delivers **Secure Access Service Edge (SASE)**, which **Gartner predicts** will continue growing as a preferred technology solution at an annual average rate of more than 30% through 2027.


SASE
Converged set of cloud networking
Cisco SD-WAN
Converged set of cloud security
Secure Access

SELECTING THE IDEAL SSE: Because IT security leaders typically struggle with managing a vast and diverse patchwork of security products and systems, most look for a single SSE/SASE vendor solution to simplify the management of a wide range of security capabilities.

- That's borne out in a March 2024 **IDC survey**, which found that **84.7% of SSE/SASE buyers** prefer or strongly prefer a single vendor solution for all SSE/SASE solution components. Cisco provides a FedRAMP-authorized single-vendor SASE solution to meet government requirements.

- **Cisco SSE solutions attracting growing attention** in the federal and state government are **Cisco Umbrella for Government** and **Cisco Secure Access**.


CISCO SECURE ACCESS FOR GOVERNMENT
CISCO UMBRELLA FOR GOVERNMENT
Available Now
FedRAMP
StateRAMP
TX-RAMP
Protective DNS Integration
Cisco Talos Threat Intelligence
DNS-layer security
Cloud Access Security Broker (CASB) *
010110 110010 001011
Data loss Prevention *
Secure Web Gateway (SWG?.DLP) *
Firewall as a Service (FWaaS)*
Remote Browser Isolation (RBI)
Zero Trust Network Access
Single Dashboard
Single Client
Advanced FWaaS
VPNaaS
Unified Policies
Authorization Target June 2025

CISCO SSE SOLUTIONS FOR GOVERNMENT are built on Cisco's commercial SSE and zero trust network access (ZTNA) solutions, used by over 30,000 customers and recognized as a **leader in its category** by Miercom, a third-party security testing and certification facility.

- **Cisco Umbrella for Government** is a FedRAMP-moderate and StateRAMP-authorized platform designed to securely enable government cloud transformation and protect hybrid/ remote workers.
- In mid 2025, it is expected that Cisco will deliver options for government customers to upgrade to **Cisco Secure Access for Government** (FedRAMP authorization in process). This solution combines both Secure Internet Access and Secure Private Access, including a novel approach that **unifies modern ZTNA and VPNaaS** in one solution, enabling protection for all applications (not just some), over any port or protocol.

REDUCING SECURITY COMPLEXITY:
Cisco SSE solutions offer a fully integrated, cloud-native solution with unified management of DNS-layer security that meets the Cybersecurity and Infrastructure Security Agency (CISA) mandate for Protective DNS. This is vital, but just the start of the comprehensive security protection delivered. Cisco supports government cybersecurity compliance by helping federal, state, and local agencies meet mandates like the Executive Order on Enhancing Cybersecurity, FedRAMP Rev 5, StateRAMP, and TxRAMP. These services ensure cloud offerings meet strict security standards for sensitive data protection. In addition, Cisco provides:

- **Secure Internet Access: Secure Internet Gateway (SIG)**, **secure web gateway**, and **cloud-delivered firewall** with **Snort 3.0** IPS — along with **CASB (Cloud Access Security Broker)** and **data loss prevention (DLP)** — providing comprehensive protection against cyber threats.
- **Secure Private Access:** Unified **Zero Trust Network Access (ZTNA)**, VPN as-a-service (VPNaaS), Single console covering all Secure Internet Access and Secure Private Access capabilities, Single Client for all capabilities, and unified policy management for all types of applications.

BASED ON DECADES OF EXPERIENCE:
"For almost 40 years, we've empowered government agencies of all sizes to tackle their distinct security and compliance challenges," states Jeff Scheaffer, Vice President, Cisco SSE Product Management. "We possess deep **insights into emerging threats** and their impact on cybersecurity strategies. The significance of **resilient and accessible** cybersecurity is paramount. Cisco's SSE solutions offer agencies reliable cloud-based security controls crucial for maintaining flexibility."

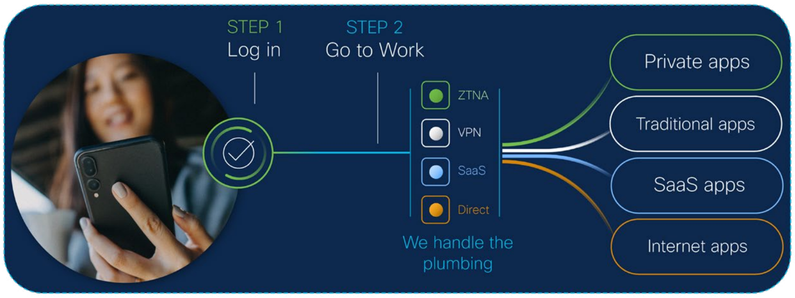
> **The significance of resilient and accessible cybersecurity is paramount. Cisco's SSE solutions offer agencies reliable cloud-based security controls crucial for maintaining flexibility."**

JEFF SCHEAFFER,
VP of Cisco Security Product Management

BY UNIFYING MULTIPLE SECURITY FUNCTIONS into a single cloud-delivered solution, managed from a single web interface and with a single client, Cisco SSE solutions reduce security complexity on the backend for administrators with security that is transparent to users on the front end. Over time, government agencies can flexibly add additional layers of security defenses customized to their needs. Cisco's SSE solutions:

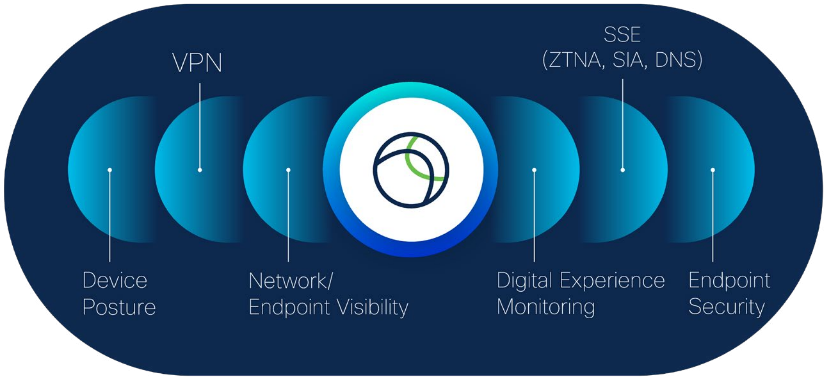
- **Provide secure access to all (not some) private apps:**
  Cisco SSE's ZTNA and VPNaaS enable seamless access from users (on-premise or remote; managed and unmanaged devices) to all apps, with zero-trust controls. On average, about 30% of applications cannot be supported by traditional ZTNA; such legacy apps with non-standard ports/protocols can be secured by VPNaaS, reducing or eliminating the hardware, management, and end-user hassles of on-premises VPN. IT can take a more pragmatic migration approach toward ZTNA as time allows, leveraging VPNaaS along the way.

- **A better experience for end users:**
  End-user acceptance is critical for successful zero-trust adoption. By combining ZTNA with a complementary VPN-as-a-Service in a single secure client, with identity and posture checks, Cisco transparently delivers advanced, friction-free security for all applications. "Envision a government employee seamlessly accessing sensitive cloud applications, whether working remotely or in the office, without compromising security," says **Scheaffer**.



"Cisco's SSE for Government solution ensures this by rigorously verifying user identity, evaluating device security, and enforcing stringent access controls. It diligently monitors network traffic for any malicious activity, proactively blocking threats before they can reach the user's device or application. Acting as a vigilant 'security sergeant on the edge of networks,' it requires your workforce to merely login and get to work, eliminating any chance of bypassing security."

- **Uses one easy-to-manage client:**
  Delivering a broad set of security functions (DNS protection, SWG, VPNaaS + ZTNA, device posture, and more) to simplify the security process for managed devices. Also, the use of clientless zero-trust access extends least-privilege controls to BYOD and contractor devices.



- **Leverages a single console:**
  Making it easy to configure the broad set of Cisco SSE functions for both Secure Internet Access and Private Access. Consolidated reporting improves detection and reduces investigation time.

- **Provides comprehensive threat intelligence and deterrence:**
  Cisco SSE solutions give agencies advanced AI-assisted threat detection that helps predict new threat vectors. This capability utilizes statistical models, machine learning algorithms, and enormous volumes of threat intelligence data from **Cisco Talos**, one of the world's largest non-government threat intelligence teams. That leads to faster incident detection and stronger protection against existing and emerging attack tactics.

Building on Cisco's Broader Commitment to Government

CISCO SSE SOLUTIONS ADD A VITAL DIMENSION to Cisco's commitment to Federal, State, and Local government in supporting their networking, security, and AI needs. When you partner with Cisco, it's not about buying point products; it's about acquiring end-to-end platform solutions that will future-proof your IT investment. Cisco is known for consistently applying a product philosophy based on product excellence for greater experiences, an open platform advantage for better economical ingestion, and core AI across the portfolio for improved efficiencies.

In addition to Cisco's SSE for Government solutions, here are a few other examples of integrated Cisco offerings built for the public sector:

- **Cisco Security Cloud Control**, a cloud-based management solution that simplifies and centralizes the management of all Cisco Secure Firewall form factors (ASA and FTD), enhancing control of security policies and objects across multiple devices from a single, user-friendly interface. FedRAMP in process.

- **Cisco Splunk Platform,** offering a massively scalable and cost-effective data platfrom that helps Federal and State agencies make confident decisions and take action at mission speeds. You can ingest data and use it across multiple agency challenges being it cybersecurity, cisizen service or modernization initiatives. Proactively manage risk and meet various compliance mandates with its security analytics platform. FedRAMP authorized.

- **Cisco Software-Defined Wide Area Network (SD-WAN),** optimizes your wide area network, which means better experiences for customers and employees. It uses advanced, real-time analytics to guide users onto the best-performing path for optimal Software as a Service (SaaS) application performance, with up to 40% faster performance for Office 365. Cisco SD WAN delivers seamless automated government connectivity for Infrastructure as a Service (IaaS) in private and public clouds. It also automates on-demand connectivity to multiple sites and to the world's leading cloud provider networks through Software-Defined Cloud Interconnect (SDCI) providers. FedRAMP authorized.

- **Cisco Duo**, delivers strong cloud-based authentication and device visibility tailored to the demands of public sector agencies requiring FedRAMP authorization. This includes role-based and location-based access policies, biometric authentication enforcement, the ability to allow or deny access based on device hygiene and notifying users to self-remediate out-of-date devices.

THE BROADER BENEFITS FOR AGENCIES:
By providing modern, ubiquitous security and networking that works seamlessly behind the scenes, everyone engaging inside and across the agency remains safer and more secure. It also gives agency leaders greater assurance about reliable business continuity and resiliency while reducing the risk of reputation and financial impact of a breach.

In a world of sophisticated cyber threats, U.S. Federal, State, and Local government agencies need a trusted security and networking partner they can rely upon. With its long history of innovation, proven track record, and commitment to protecting government networks, Cisco is a trusted leader and partner for securing the nation's digital frontier.

Now, with Cisco's Security Service Edge (SSE) for Government solutions integrated with other Cisco products, agencies can gain a potent edge to stay ahead of the evolving threat landscape and protect their critical assets.

Learn more about Cisco SSE for Government and how Cisco can help your agency safeguard its data and operations better.

This special report was produced by Scoop News Group and sponsored by Cisco.

FEDSCOOP CISCO

SIDE BAR ON THE NEXT PAGE

Cisco's technological innovation, tailored solutions and reliability give agencies critical security and assurance

Cisco's long-standing track record as a global leader in networking, security, AI, and IT solutions and its ability to tailor solutions to the government's unique needs have established it as a trusted partner of federal and state government agencies for nearly 40 years. By leveraging advanced technologies and building products that comply with various industry standards and regulations such as CISA, NIST 2.0, TIC 3.0, CONUS, CMMC, FIPS 140-2, MITRE ATT&CK and FedRAMP. Cisco provides assurance and peace of mind that federal and state organizations can meet regulatory compliance requirements while operating within existing IT frameworks.

HARNESSING INNOVATION & TRUST

Cisco consistently leads the technology industry in developing advanced networking, security and IT solutions through:

- **Technology innovation: Developing cutting —** edge solutions such as Software-Defined Networking (SDN), the Internet of Things (IoT), and cybersecurity to enhance operational efficiency, resiliency and security.
- **Investment in R&D —** Cisco invests heavily in research and development (R&D). This commitment to innovation means that federal and state agencies can rely on Cisco to provide solutions and services that are current and at the forefront of technological advancement.
- **Cloud and AI integration —** Cisco has been at the forefront of integrating cloud and artificial intelligence (AI) capabilities into its products, providing organizations with scalable, intelligent solutions that enhance decision-making, streamline processes, and help organizations adapt to changing demands and optimize their IT infrastructure.
- **Comprehensive security measures —** Cisco prioritizes comprehensive security. Features available in Cisco Splunk, Cisco Security Service Edge solutions, Talos threat intelligence, Cisco Secure Firewall, and many others offer advanced protection against cyber threats and ensure network integrity, which is crucial for federal and state agencies handling sensitive information.
- **Training and support —** In addition to technological integration, Cisco recognizes the need for knowledge transfer and skill development by offering comprehensive training and support for IT personnel within government agencies. This ensures IT teams are well-equipped to manage and maintain their networking solutions effectively.

Cisco's tailored solutions are designed to seamlessly integrate with the existing infrastructures of federal as well as state and local governments. Cisco's Security Portfolio, for instance, has been instrumental in helping state and local entities enhance emergency response systems, disaster recovery and resilience infrastructure and surveillance and monitoring of public spaces to enhance public safety. Cisco's solutions not only improve operational capabilities but also provide the scalability needed to accommodate future growth and technological advancements.