Cisco Security Cloud Control for Government

Benefits

- Unify management for all Cisco Secure Firewall form factors—on-premises, in the cloud, or across hybrid environments—for streamlined federal security operations.
- Gain real-time visibility into network activity, security threats, and policy events to quickly identify and remediate potential issues, supporting mission-critical government operations.
- Automate critical tasks such as firewall provisioning, object updates, and fleet management to reduce operational overhead and minimize configuration errors.
- Scale with confidence using a SaaS-based interface that accelerates feature delivery and adapts to evolving federal infrastructure requirements.
- Ensure compliance with federal security standards such as Federal Risk and Authorization Management Program (FedRAMP), Federal Information Processing Standards (FIPS) 140, and National Institute of Standards and Technology (NIST) frameworks, providing assurance of regulatory adherence.

Centralized security management for simplified protection

Cisco Security Cloud Control is the cloud-delivered unified management interface for Cisco security. It offers centralized visibility, policy enforcement, and automation across hybrid and multicloud environments—helping organizations reduce complexity, strengthen threat response, and simplify day-to-day operations.

Security Cloud Control for Government extends these capabilities to meet the unique needs of federal agencies. In its first phase, it delivers consolidated management of all Cisco Secure Firewall form factors and Cisco Multicloud Defense, supporting both operational resilience and regulatory compliance.

Achieving FedRAMP Moderate authorization for the firewall management capabilities within Security Cloud Control demonstrates Cisco's commitment to meeting the federal government's security standards. This milestone enables agencies to begin securely adopting cloud-based operations with confidence.

Looking ahead, Cisco will continue to pursue FedRAMP authorization for the full suite of Security Cloud Control platform services. This expansive deployment will deliver deeper context across solutions, greater visibility, and increased operational efficiency—empowering agencies to strengthen their security posture and evolve toward a fully integrated security framework over time.

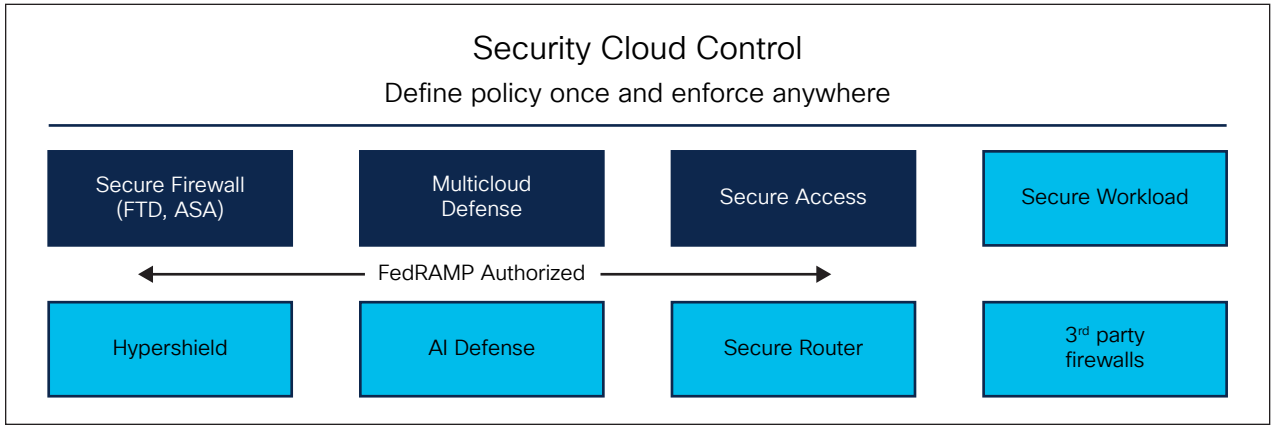

Figure 1. FedRAMP authorized solutions within Security Cloud Control

Unify management and enhance security for federal, state, and local government agencies

Centralized management

Enforce consistent security policies across on-premises, public, private, hybrid, and multicloud environments to maintain a unified security posture.

Establish Role-Based Access Control (RBAC) across all firewalls to simplify administration and ensure consistent enforcement of user and device permissions.

Ensure seamless access to new features, performance enhancements, and security updates through SaaS delivery—minimizing disruption and maintenance effort.

Firewalling (physical and virtual)

Centrally configure and manage Firewall Threat Defense (FTD) and Adaptive Security Appliance (ASA) rule sets across hardware, virtual, and container-based firewalls.

Use real-time dashboards, analytics, and unified logging to detect threats, monitor usage, and accelerate incident response.

Simplify deployment with Zero-Touch Provisioning, enabling faster rollout of firewalls across distributed government sites and agencies.

Cloud firewalling

Continuously discover and evaluate cloud assets to ensure policies remain aligned with evolving multicloud workloads.

Enforce firewall policies across Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI) from a unified management interface for comprehensive visibility and control.

Integrate automated threat intelligence to defend against cloud-native attacks with minimal manual intervention.

Regulatory compliance

Meets FIPS 140 requirements as part of the FedRAMP Moderate for government security standards.

Alignment with Trusted Internet Connections (TIC) 3.0 Policy Enforcement Points, Executive Order 14028, and Office of Management and Budget (OMB) Memo M-22-09—Zero Trust and Protective Domain Name System (DNS).

Complies with state mandates such as TX-RAMP (Level 2 certified) and NIST 800-53 security control baselines.

Holds Cybersecurity Maturity Model Certification (CMMC) and meets the NIST Cybersecurity Framework.

Learn more

- Cisco Security Cloud Control webpage
- Cisco Secure Firewall webpage
- Cisco Multicloud Defense webpage
- Cisco solutions for government webpage

C45-5330105-00 08/25