

Cisco Security Cloud Control

Centralize security management for Cisco solutions

In today's complex network security landscape, managing diverse environments often leads to inefficiencies and errors, particularly when juggling multiple solutions across hybrid and multicloud environments. Organizations need a unified interface to streamline security policy management while strengthening their overall security posture. Cisco Security Cloud Control addresses these challenges by providing a single solution for managing Hybrid Mesh Firewall and Universal Zero Trust Network Access (ZTNA), enhancing security outcomes and reducing misconfigurations.

Security Cloud Control transforms security operations with its cloud-native design and AI-driven features. By consolidating security and automating tasks like device provisioning and policy updates, it improves visibility, scalability, and efficiency. It provides unified management for Hybrid Mesh Firewall, a highly distributed security fabric that stops advanced threats, protects applications, and enforces zero trust segmentation across data centers, campuses, and IoT environments.



Benefits

- Centralize management of Cisco Secure Firewall (ASA and FTD), Cisco Multicloud Defense, Cisco Hypershield, Cisco Secure Access, Cisco Secure Workload, and Cisco AI Defense for enhanced control across environments.
- Gain real-time visibility into network traffic and threats, while automating operational tasks like device provisioning and updates.
- Simplify scalability and deployment with cloud-assisted device onboarding and SaaS-based continuous feature delivery.
- Improve resilience through AI-driven insights, reducing misconfigurations and optimizing network policies.
- Utilize a single AI Assistant to streamline policy enforcement, troubleshooting, rule analysis, access control, and more across products, eliminating silos and reducing operational complexity.

Additionally, Security Cloud Control enables Universal ZTNA, ensuring seamless zero trust enforcement across cloud and on-premises environments. By converging network and security, it delivers a simplified experience for hybrid workforces with consistent ZTNA policies enforced per application.

This integrated approach unifies security across multiple devices and products. The Cisco AI Assistant further reduces complexity in rule management and mitigates risk. Security Cloud Control establishes a robust, adaptive defense system that evolves with the network, optimizing both security and operational efficiency.

Unify policy administration and simplify security management for strengthened protection

Security Cloud Control provides an integrated approach to streamline and enhance your security management. With its advanced features, Security Cloud Control simplifies operations, improves visibility, and boosts efficiency, ensuring your network remains secure and agile.

Centralized management

Streamline operations and ensure policy consistency.

- Manage Cisco security products from a single interface, simplifying policy and object management, in addition to role-based access control (RBAC) across multiple devices.
- Support security policy management across on-prem, public cloud, private cloud, and hybrid environments for consistent protection.
- Use one AI Assistant to optimize policy enforcement, resolve issues, analyze rules, and manage access control across products.

Holistic visibility

Facilitate faster threat identification and remediation.

- Obtain real-time visibility into network traffic and security events to monitor and respond promptly.
- Use advanced analytics for insights into remote user traffic, including visibility and geographic distribution.
- Provide centralized visibility for managed service providers (MSPs), reducing complexity and supporting client onboarding.

Advanced predictive insights

Enhance network performance with intelligent forecasting for Secure Firewall.

- Leverage AIOps for policy analysis and optimization to address misconfigurations and traffic spikes.
- Gain predictive insights into network performance through traffic insights and capacity forecasting.
- Guide remediations to potential issues, preventing downtime and improving network security.

Increased operational efficiency

Simplify security functions and save IT team time.

- Automate tasks such as device provisioning, object updates, and policy enforcement.
- Migrate seamlessly from on-premises Firewall Management Center (FMC) to the cloud, including policies and licenses.
- Facilitate easy migration from ASA or third-party firewalls to FTD, reducing manual effort.

Scalable, cloud-native design

Benefit from scalable and adaptive cloud security.

- Access Security Cloud Control from any location with an internet connection for remote collaboration and real-time response.
- Receive continuous updates and new capabilities automatically to maintain up-to-date protection.
- Scale your security infrastructure efficiently to accommodate growing networks and evolving security needs.

Security Cloud Control transforms security management, addressing the problems of the past by offering centralized, scalable, and automated security policy enforcement. It provides a forward-looking, proactive approach that aligns with the ever-changing demands of the modern digital world.

Additional resources

- [Announcement blog](#)
- [Solution overview blog](#)
- [AI Assistant for Security blog](#)
- [AIOps blog](#)
- [Hybrid Mesh Firewall blog](#)