Data sheet
Cisco public

Cisco Security Cloud Control for Government Data Sheet

Contents

Organizations face a critical challenge today: Attackers are exploiting the weakest links in their networks, such as unsecured users, devices, and workloads. This threat landscape is complicated by the shift from traditional data centers to a distributed environment, where protecting dispersed data across multiple touchpoints becomes complex.

To address these threats, many organizations resort to using multiple security tools, leading to siloed teams, tech stacks, and management systems that hinder effective security. This fragmented approach results in unnecessary costs, longer deployment times, inconsistent security, and critical gaps.

Without a centralized platform, gaining a holistic view of security is challenging. Manual identification of misconfigurations is error-prone and can lead to breaches. There is a lack of skills, time, and resources to fully utilize security features and maximize ROI. Resolving access or policy issues is lengthy due to diverse security products. Admins spend excessive time crafting similar policies across different platforms. Operational issues are often addressed reactively, leading to downtime and suboptimal performance. Non-actionable alerts and overwhelming data cause analysis paralysis and hinder decision-making, with a missing sense of urgency.

A unified security platform aims to alleviate these issues by providing a comprehensive view of the security landscape, enabling consistent policy enforcement, simplifying troubleshooting, and improved end-user productivity through actionable insights.

To meet the unique needs of various organizations and support diverse network firewall configurations, the focus is on three core objectives: simplifying operations, enhancing security, and improving clarity. We aim to streamline security management processes, strengthen defenses with advanced Zero Trust and offer clear, actionable insights to protect against vulnerabilities.

Security Cloud Control for Government

Security Cloud Control is Cisco's unified, cloud-native security management interface for the Cisco Security Cloud. It simplifies and strengthens defenses by centralizing security solutions into a single, cohesive interface. This approach eliminates silos, reduces complexity, and provides end-to-end visibility, empowering organizations to proactively address security challenges across their entire infrastructure.

Security Cloud Control for Government unifies management across:

- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Secure Firewall Adaptive Security Appliance (ASA), both on-premises and virtual
- Cisco Multicloud Defense for Government

Security Cloud Control also incorporates the cloud-delivered version of Firewall Management Center (FMC), providing a fully unified experience between on-premises and cloud-based firewall management. This expands management of policy and configuration to Cisco Secure Firewall Threat Defense (FTD) and Adaptative Security Appliance (ASA), both on-premises and virtual.

Setup is easy, fast, and frictionless, allowing customers to onboard and start managing hundreds of devices within hours. The intuitive user interface and focus on simplicity means that training requirements are minimal, with a learning curve measured in hours rather than days.

Because it's a cloud-based solution, Security Cloud Control for does not require capital expenditures, rack space, or manual patching and upgrading, dramatically reducing your operational costs.

It doesn't matter whether your organization has 5 or 5000 security devices. Security Cloud Control provides network operations teams with the ability to reduce time spent managing and maintaining security devices, enabling them to focus on what is most important to your core mission.

Unified dashboard that enables our customers to gain a real-time, holistic perspective of their entire network and cloud security ecosystem. Customers can efficiently manage tens of thousands of security devices, coordinating multiple tenants under a centralized global administrator.

The level of visibility and management from Security Cloud Control helps to deliver these outcomes. From taking intent-based policies in one place and translating them throughout all the control points in your network to streamlining, troubleshooting and recommending policies that span multiple solutions, Security Cloud Control helps with it all.

Security Cloud Control benefits

Security Cloud Control simplifies network security management through centralized visibility, streamlined policy deployment, and real-time monitoring. It enhances operational efficiency by harmonizing security policies across multiple devices, ensuring consistent protection and rapid response to threats.

- **Simplify management:** Streamline security policy and device management across your extended network.
- **Proactive, Not Reactive:** Traditionally, we've flooded you with alerts, leaving you to figure out how to mitigate issues. Now, we're shifting to a proactive approach. Using AI, we predict when your system might hit its max capacity, identify the apps causing problems, and offer solutions to avoid downtime.
- **Write Once, Apply Everywhere:** You only need to create network objects (like malicious IPs or URLs) once. These can be shared across different security products, ensuring comprehensive protection across your entire network.

Security Cloud Control features

Security Cloud Control strengthens your security posture by aligning policies throughout your organization. Our solution addresses the challenge of staying on top of your policies when adding security tools. This is especially helpful for organizations with geographically dispersed locations as well as hybrid network environments.

The solution eliminates the time-consuming complexity of managing policies across distributed security devices. It helps prevent inconsistencies and gaps in your security.

You can manage from anywhere with a highly secure, always available, highly reliable, and scalable multitenant cloud solution. It frees up capacity for other priorities by strengthening and maintaining security posture in less time and with fewer resources.

Optimization for your existing platforms: Upon onboarding, Security Cloud Control will immediately be able to identify and flag common issues across firewalls that have been in production for years. After assessing and identifying all risks, you will now be able to swiftly remediate issues across all devices in bulk – bringing your devices to a consistent and more secure state. Security Cloud Control helps to correct the following issues:

- **Unused objects** are objects that will never be hit and cause issues during troubleshooting as well as add to potentially unwanted questions during audits.
- **Duplicate objects** are often found on a device and associate different names to the same IPs. Removing duplicate objects can improve the overall performance of the appliance.

- **Inconsistent objects** are objects that get represented differently across deployed firewalls. This is typically the most important object issue from a security perspective. For example, if you had an object name “block list” and all devices are supposed to have this object with matching variables or IPs, Security Cloud Control will quickly validate this. If the object is not consistent across firewall devices, Security Cloud Control will alert you and allow you to resolve the issue in seconds.
- **Shadow rules** are rules that will never be hit due to preceding rules that supersede them.

Templates for consistent policy design: Using Security Cloud Control, you can now create, apply, and manage a consistent policy design across disparate devices from a single place. Our template feature allows you to create a “gold configuration” that can be replicated and customized. Once you are done, you can export and apply your standardized configuration to any new platform.

Simplified firewall OS upgrades: Often one of the most time-consuming and frustrating challenges that our customers face is maintaining the firewall OS for both features and vulnerabilities. Using Security Cloud Control, you can reduce the time it takes to perform Cisco ASA or Cisco Threat Defense (FTD) image upgrades by up to 90 percent. We take the guesswork out of planning and enable you to perform the upgrade in bulk across all your devices at once.

CLI in bulk: In addition to an intuitive web-based UI, we also provide our Command-Line Interface (CLI) users with a streamlined user experience as well. Security Cloud Control’s CLI Tool gives users the ability to perform CLI commands in bulk across many devices at once, including the ability to create user-defined macros or shortcuts for your most common commands.

Audit of changes with change log: Customers can track changes through our change log to review what change was made, when, and who performed the change. All changes made in both the Security Cloud Control UI and the CLI Tool are captured.

Remote-access VPN monitoring and management: Visibility across remote user sessions and head-end devices with a historical view over 90 days for capacity planning. Extend visibility of user traffic by leveraging Cisco Security Analytics and Logging.

Cloud-delivered version of Firewall Management Center: Offers the same look -and feel as on-premises and virtual versions of Firewall Management Center, with:

- **Comprehensive visibility and policy control:** Provides exceptional visibility into what is running in your network and cloud so you can see what needs to be protected. Using this visibility, you can create and manage firewall rules and control thousands of web and custom applications used in your environment.
- **Automated security for dynamic defense:** Continually monitors how your network is changing, streamlining operations, and improving your security so you can focus on the threats that matter.

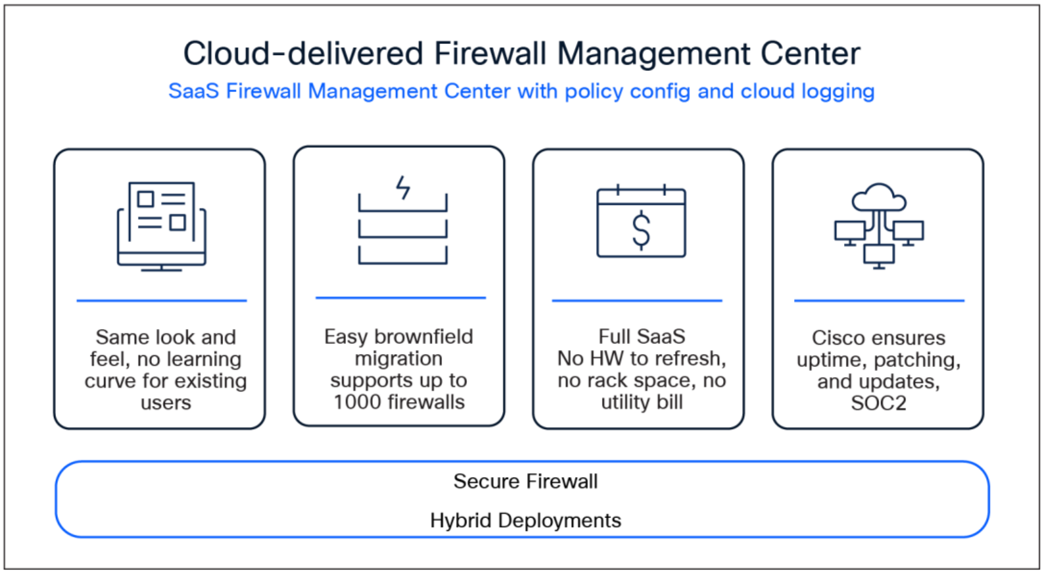
Cloud-delivered Firewall Management Center
SaaS Firewall Management Center with policy config and cloud logging
Same look and feel, no learning curve for existing users
Easy brownfield migration supports up to 1000 firewalls
Full SaaS No HW to refresh, no rack space, no utility bill
Cisco ensures uptime, patching, and updates, SOC2
Secure Firewall
Hybrid Deployments

Figure 1.
Benefits of cloud-delivered Firewall Management Center via Security Cloud Control for Government.

For more information, visit the Secure Firewall Management Center Data Sheet.

For more information on Multicloud Defense for Government, visit product webpage

Table 1. Features and benefits

Objective	How we can make it happen
Fast deployment and device onboarding	• Security Cloud Control accounts are assigned in 24 hours, and you can start onboarding devices almost immediately. Devices can be onboarded as just a configuration, single device, or thousands of devices through bulk imports with no associated downtime. • Low-touch provisioning streamlines large-scale remote deployments. Available for Firepower 1000/2000/3000 Series running FTD version 7.0.3 and later (excluding 7.1).
Unified dashboard - A Comprehensive view of firewall and security services	• To gain a real-time, holistic perspective of their entire network and cloud security ecosystem. Customers can efficiently manage tens of thousands of security devices, coordinating multiple tenants under a centralized global administrator.
Object and policy analysis for optimization of existing devices	• At onboarding, Security Cloud Control will uncover areas for optimization and put the user in a position to quickly remediate the problems found. Common issues include duplicate, unused, and inconsistent objects across devices. We can also identify hit rates and shadow rules that will never be hit.
Options for proactive configuration and policy changes	• Security Cloud Control gives you options for how you can manage your devices centrally. If you prefer, you can deploy directly to the device immediately using the CLI Tool, enabling the use of “bulk” deployments, macros, and/or shortcuts for your most common commands. Next, you can also use the UI to provide a simple way to “stage” changes in the cloud during normal business hours and then push these changes out at your next maintenance window.
Security templates	• Leveraging an existing “gold configuration,” you can design and manage templates for easy, consistent deployment of your new devices.
Global search	• Allows you to quickly locate and navigate to devices managed by Security Cloud Control. It scans all the devices and objects in the system and displays them with indexing. With event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.
Change log	• Track changes to the configuration being made within Security Cloud Control for accountability, auditing, and troubleshooting purposes.

Objective	How we can make it happen
Out-of-band notifications	• Changes made via ASDM or CLI (SSH) will be identified by the Security Cloud Control administrator as an Out-Of-Band (OOB) change. The administrator can make the decision to keep this change or revert to the original configuration.
Backup and rollback of configurations	• Security Cloud Control backs up the configuration after every change and offers the ability to roll back to previous configurations.
Simple image upgrades	• Streamline the approach to performing OS upgrades for faster access to the latest patches and features.
Troubleshooting of potential issues	• Built into Security Cloud Control is the ability to pull live logs and run PacketTracer to help with troubleshooting of your devices.
Simple search	• See how policies are enforced across device types by searching for any object name, Access Control List (ACL) name, network, or application policy element.

Security Analytics and Logging (SAL) SaaS Overview

A cloud-delivered, Software-as-a-Service (SaaS) offering with a cloud-native data store, referred to as SAL (SaaS)

SAL (SaaS) is a full-feature offering providing cloud-based and cloud-delivered log management for NextGeneration Firewalls (NGFWs) running Cisco Firewall Threat Defense (FTD) software, as well as devices running the Adaptive Security Appliance (ASA) software, independent of their management platform. SAL (SaaS) enables event viewing via APIs in Security Cloud Control for firewall event logs.

Cisco Security Logging and Troubleshooting: Allows organizations to store firewall logs in the cloud and present visually in Security Cloud Control's event viewer. Correlate historical and/or live events from your firewall platforms for troubleshooting.

Required components and setup to run Cisco Security Analytics and Logging (SaaS):

Secure Event Connector: To capture Firewall Event Logs from cloud deployments, a Secure Event Connector (SEC) is needed. The SEC is a containerized application that can be installed on an on-premises or cloud Secure Device Connector (SDC), or even be set up to run in standalone mode. It receives events from Firewall Threat Defense (FTD) devices and Adaptive Security Appliance (ASA) devices and forwards them to Cisco SAL in the cloud. Installation instructions can be found here. While SEC remains the most scalable route to send logs to SAL (SaaS), firewall devices running Cisco Firepower version 6.5 or later can send event logs directly to SAL Cloud, without the need for an SEC. This capability has been found to reliably support sustained peak rates of up to 8,500 events per second (eps) per firewall device. The Cisco Firewall Management Center (FMC) version 7.0 supports this direct-to-cloud route of devices under its management through its "Integrations" settings.

Platform support matrix: Cisco security devices supported by Security Cloud Control for Government

Product	ASA software version	FTD version
Cisco Firepower 1010, 1120, 1140, and 1150	9.8 and later	7.0.3 and later (excluding 7.1)
Cisco Firepower 2110, 2120, 2130, and 2140	9.8 and later	7.0.3 and later (excluding 7.1)
Cisco Firepower 3105, 3110, 3120, 3130, and 3140	9.17.1 for 3100, 3120, 3130 and 3140, 9.19.1 for 3105 and later	7.1 and later
Cisco Firepower 4112, 4115, 4125, and 4145	9.4 and later	7.0.3 and later (excluding 7.1)
Cisco Firepower 4215, 4225, and 4245	9.20 and later	7.4 and later
Cisco Firepower 9300	9.4 and later	7.0.3 and later (excluding 7.1)
Secure Firewall Threat Defense virtual (FTDv): KVM, VMware, and Azure	NA	7.0.3 and later (excluding 7.1)

Ordering and provisioning information

To learn more about the detailed instructions on ordering Security Cloud Control Firewall Management for Government – refer to the Security Cloud Control Firewall Management for Government Ordering Guide

To place an order, visit the Cisco ordering homepage.

Security Cloud Control Firewall Management for Government License SKUs

Table 2.

Part number	Description
FWM-FED-SEC-SUB	Cisco Security Cloud Control Firewall Management for Government Subs
FWM-FED-BASE	Base Tenant entitlement: subscription of 12-60 months available
Cloud Management License with Unlimited Logging Storage and 90 days retention	
FWM- FED-ML-FP1010	Cloud Management and Logging for FPR1010 running ASA or FTD Image
FWM- FED-ML-FP1010E	Cloud Management and Logging for FPR1010E running ASA or FTD Image
FWM-FED-ML-FP1120	Cloud Management and Logging for FPR1120 running ASA or FTD Image
FWM-FED-ML-FP1140	Cloud Management and Logging for FPR1140 running ASA or FTD Image
FWM-FED-ML-FP1150	Cloud Management and Logging for FPR1050 running ASA or FTD Image

Part number	Description
FWM-FED-ML-1210CE	Cloud Management and Logging for FPR1210CE running ASA or FTD Image
FWM-FED-ML-1210CP	Cloud Management and Logging for FPR1210CP running ASA or FTD Image
FWM-FED-ML-1220CX	Cloud Management and Logging for FPR1220CX running ASA or FTD Image
FWM-FED-ML-1230	Cloud Management and Logging for FPR1230 running ASA or FTD Image
FWM-FED-ML-1240	Cloud Management and Logging for FPR1240 running ASA or FTD Image
FWM-FED-ML-1250	Cloud Management and Logging for FPR1250 running ASA or FTD Image
FWM-FED-ML-FP2110	Cloud Management and Logging for FPR2110 running ASA or FTD Image
FWM-FED-ML-FP2120	Cloud Management and Logging for FPR2120 running ASA or FTD Image
FWM-FED-ML-FP2130	Cloud Management and Logging for FPR2130 running ASA or FTD Image
FWM-FED-ML-FP2140	Cloud Management and Logging for FPR2140 running ASA or FTD Image
FWM-FED-ML-FP3105	Cloud Management and Logging for FPR3105 running ASA or FTD Image
FWM-FED-ML-FP3110	Cloud Management and Logging for FPR3110 running ASA or FTD Image
FWM-FED-ML-FP3120	Cloud Management and Logging for FPR3120 running ASA or FTD Image
FWM-FED-ML-FP3130	Cloud Management and Logging for FPR3130 running ASA or FTD Image
FWM-FED-ML-FP3140	Cloud Management and Logging for FPR3140 running ASA or FTD Image
FWM-FED-ML-FP4112	Cloud Management and Logging for FPR4112 running ASA or FTD Image
FWM-FED-ML-FP4115	Cloud Management and Logging for FPR4115 running ASA or FTD Image
FWM-FED-ML-FP4125	Cloud Management and Logging for FPR4125 running ASA or FTD Image
FWM-FED-ML-FP4145	Cloud Management and Logging for FPR4145 running ASA or FTD Image
FWM-FED-ML-FP4215	Cloud Management and Logging for FPR 4215 running ASA or FTD Image
FWM-FED-ML-FP4225	Cloud Management and Logging for FPR 4225 running ASA or FTD Image
FWM-FED-ML-FP4245	Cloud Management and Logging for FPR 4245 running ASA or FTD Image
FWM-FED-ML-F9K-S40	Cloud Management and Logging for FPR9K-SM40 running ASA or FTD Image
FWM-FED-ML-F9K-S48	Cloud Management and Logging for FPR9K-SM48 running ASA or FTD Image
FWM-FED-ML-F9K-S56	Cloud Management and Logging for FPR9K-SM56 running ASA or FTD Image
FWM-FED-ML-FTDV5	Cloud Management and Logging for FTDV Base Lic,100Mbps
FWM-FED-ML-FTDV10	Cloud Management and Logging for FTDV Base Lic, 1Gbps

Part number	Description
FWM-FED-ML-FTDV20	Cloud Management and Logging for FTDV Base Lic, 3Gbps
FWM-FED-ML-FTDV30	Cloud Management and Logging for FTDV Base Lic, 5Gbps
FWM-ML-FTDV50	Cloud Management and Logging for FTDV Base Lic, 10Gbps
FWM-FED-ML-FTDV100	Cloud Management and Logging for FTDV Base Lic, 16Gbps

Table 3. SAL Saas logging and troubleshooting XaaS license for logging entitlement

Part number	Description
SAL-FED-SUB	SAL XaaS Subscription
Security Analytics subscription of 1, 3, and 5 years available	
SAL-FED-SUB	Cisco Security and Analytics and Logging for Government
SAL-FED-ESS-1YR/2YR/3YR	Cisco Security and Analytics and Logging for Government Essentials Tier with 1 year, 2 year, or 3 year log retention period.
SAL-FED-PRE-1YR/2YR/3YR	Cisco Security and Analytics and Logging for Government Premium Tier with 1 year, 2 year, or 3 year log retention period.
SVS-SAL-FED-SUP-S	Basic Support for Cisco Security and Analytics and Logging for Government

Table 4. Firewall Management in Security Cloud Control: subscription of 1, 3, and 5 years available

Part number	Description
FWM-FED-FPR1010	Cloud Management for FPR1010 running ASA or FTD Image
FWM-FED-FPR1120	Cloud Management for FPR1120 running ASA or FTD Image
FWM-FED-FPR1140	Cloud Management for FPR1140 running ASA or FTD Image
FWM-FED-FPR1150	Cloud Management for FPR1150 running ASA or FTD Image
FWM-FED-FPRTD-V=	Cloud Management for Virtual FTD (FTDv5/10/20/30/50/100)
FWM-FED-FPR2110	Cloud Management for FPR 2110 running ASA or FTD Image
FWM-FED-FPR2120	Cloud Management for FPR 2120 running ASA or FTD Image
FWM-FED-FPR2130	Cloud Management for FPR 2130 running ASA or FTD Image
FWM-FED-FPR2140	Cloud Management for FPR 2140 running ASA or FTD Image
FWM-FED-FPR3105	Cloud Management for FPR 3105 running ASA or FTD Image
FWM-FED-FPR3110	Cloud Management for FPR 3110 running ASA or FTD Image
FWM-FED-FPR3120	Cloud Management for FPR 3120 running ASA or FTD Image

Part number	Description
FWM-FED-FPR3130	Cloud Management for FPR 3130 running ASA or FTD Image
FWM-FED-FPR3140	Cloud Management for FPR 3140 running ASA or FTD Image
FWM-FED-FPR4112	Cloud Management for FPR 4112 running ASA or FTD Image
FWM-FED-FPR4115	Cloud Management for FPR 4115 running ASA or FTD Image
FWM-FED-FPR4125	Cloud Management for FPR 4125 running ASA or FTD Image
FWM-FED-FPR4145	Cloud Management for FPR 4145 running ASA or FTD Image
FWM-FED-FPR4215	Cloud Management for FPR 4215 running ASA or FTD Image
FWM-FED-FPR4225	Cloud Management for FPR 4225 running ASA or FTD Image
FWM-FED-FPR4245	Cloud Management for FPR 4245 running ASA or FTD Image
FWM-FED-FPR9K	Cloud Management for FPR 9300 Series running ASA or FTD Image

Note: All the PIDs listed in Table 3 are available in 1,3 and 5-year subscription PIDs. Example: FWM-FED-FPR4225 is available as FWM-FED-FPR4225-1Y, FWM-FED-FPR4225-2Y, and FWM-FED-FPR4225-3Y

Additional resources

Cisco Security Cloud Control webpage

Cisco Secure Firewall Management Center webpage

Cisco Secure Firewall webpage

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-736847-17 09/25