

Cisco FireSIGHT Management Center

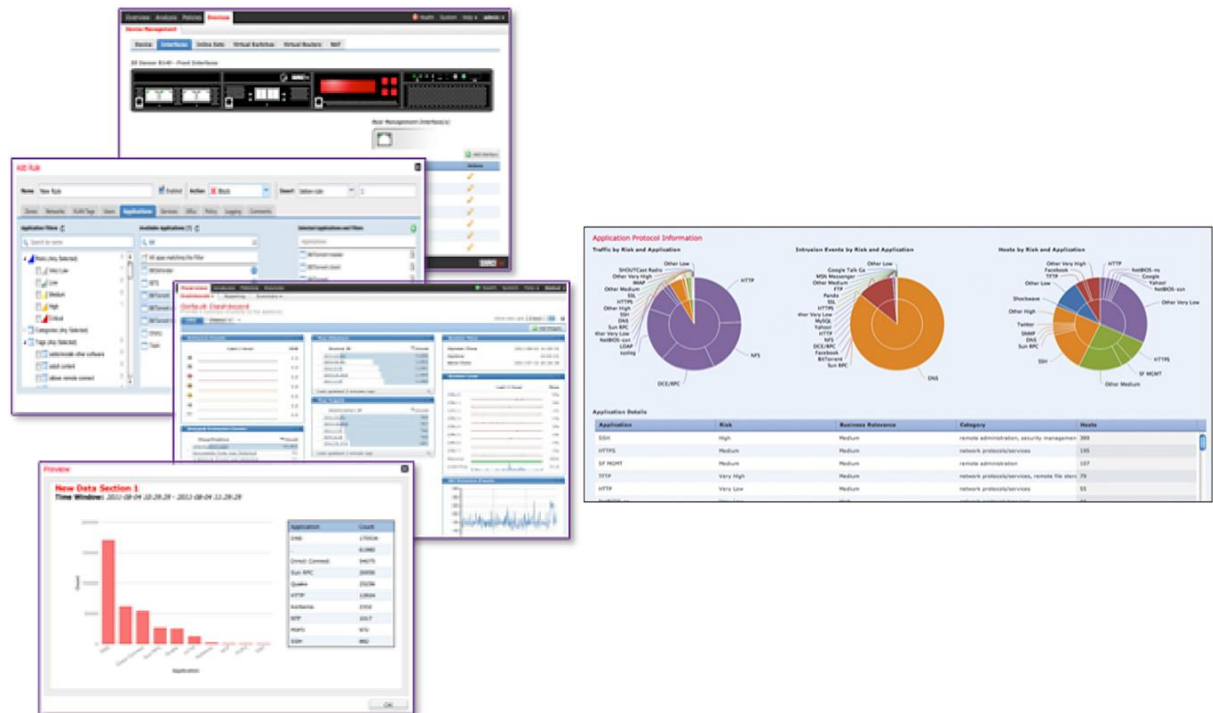
When it comes to effective threat prevention, a window into your network is invaluable. The Cisco FireSIGHT™ Management Center provides just that.

Product Overview

Gain total visibility into everything on your network, including physical and virtual hosts, operating systems, applications, services, protocols, users, geolocation information, content, network behavior, network attacks, and malware with the Cisco FireSIGHT Management Center. This security management console (Figure 1) is the centralized point of event and policy management for your intrusion prevention security operations. It allows you to automatically aggregate and correlate information generated by Cisco's next-generation firewall, Cisco® ASA with FirePOWER™ Services, and by Cisco's next-generation Intrusion Prevention System (NGIPS), Cisco FirePOWER NGIPS. The Cisco FireSIGHT Management Center centrally manages network security and operational functions, including event monitoring, analysis, incident prioritization, and reporting, so that you can better protect your business. It also reduces your costs by streamlining operations and automating many commonly recurring security analysis and management tasks.

Enterprise-Class Management

Figure 1. Cisco FireSIGHT Management Center: Centralized Policy, Event, and Device Management



Cisco FireSIGHT Management Center discovers real-time information about changing network resources and operations to provide you with a full contextual basis for making informed decisions (see Table 1). In addition to providing a wide breadth of intelligence, the Cisco FireSIGHT Management Center delivers a fine level of detail, including:

- **Trends and high-level statistics:** Helps managers and executives understand security posture at a moment in time as well as how it's changing, for better or worse.
- **Event detail, compliance, and forensics:** Provides an understanding of what happened during a security event to improve defenses, support breach containment efforts, and aid in legal enforcement actions.
- **Workflows:** Easily exports data to support responses to an event, improving response management.

Unparalleled Visibility and Insight

Table 1 illustrates the breadth of contextual awareness provided by Cisco FireSIGHT Management Center into threat vectors that more traditional security technologies do not detect.

Table 1. Cisco FireSIGHT Management Center: Full Stack Visibility

Category	FireSIGHT Management Center	Typical IPS	Typical Next-Generation Firewall
Threats	Yes	Yes	Yes
Users	Yes	Yes	Yes
Web applications	Yes	No	Yes
Application protocols	Yes	No	Yes
File transfers	Yes	No	Yes
Malware	Yes	No	No
Command-and-control servers	Yes	No	No
Client applications	Yes	No	No
Network servers	Yes	No	No
Operating systems	Yes	No	No
Routers and switches	Yes	No	No
Mobile devices	Yes	No	No
Printers	Yes	No	No
VoIP phones	Yes	No	No
Virtual machines	Yes	No	No

There are a number of Cisco FireSIGHT Management Center models. Choose the one that's right for your organization based on the number of sensor appliances to be monitored (both physical and virtual), the number of hosts in your environment, and the anticipated security events rate (see Table 2). All models provide the same management capabilities, including:

- Centralized device, license, event, and policy management
- Role-based management (segmented and isolated views and duties based on administrator role or group)
- Customizable dashboard with custom and template-based reports
- Comprehensive reporting and alerts for both general and focused information
- Event and contextual information displayed in hyperlinked tables, graphs, and charts
- Network behavior and performance monitoring

- Robust high-availability options to help ensure there's no single point of failure
- Correlation and remediation features for real-time threat response
- Open APIs for integration with third-party solutions and customer work streams, such as firewalls, network infrastructure, log management, security information and event management (SIEM), trouble ticketing, and patch management

Automate Security for Dynamic Defense

The Cisco FireSIGHT Management Center continually monitors how your network is changing over time. New threats are automatically correlated against the vulnerabilities that exist in your network to determine whether they can affect your business. This enables you to cut through all of the noise and focus your efforts on responding to the events that will have the most impact. Critical security activities such as policy tuning are also automated, saving time and effort, while adapting your network defenses to changing conditions. This results in optimized security policies that are specifically tailored to the network you have and the threats that you face.

Choice of Deployment Modes

Cisco FireSIGHT Management Center can be deployed as a physical or virtual appliance, allowing you to choose what options work best for your environment. Physical Cisco FireSIGHT Management Center appliances generally manage a higher number of sensors and provide greater event storage capabilities than their virtual counterparts. Virtual Cisco FireSIGHT Management Center appliances provide the convenience of being able to use your existing VM infrastructure. They can be easily deployed using VMware vSphere provisioning and can be used to protect assets in a physical network. Version 5.x virtual appliances can be hosted on VMware ESX and ESXi hypervisors and can manage up to 25 physical or virtual sensors.

Product Specifications

Table 2 compares the capacity and throughput for available Cisco FireSIGHT Management Center appliances, both physical and virtual.

Table 2. Cisco FireSIGHT Management Center Models



Feature	FireSIGHT FS750	FireSIGHT FS1500	FireSIGHT FS3500	FireSIGHT FS4000	FireSIGHT FS-VMW-SW
Maximum number of sensors managed	10	35	150	300	25 10 2
Maximum number of IPS events	20 million	30 million	150 million	300 million	Varies*
Event storage	100 GB	125 GB	400 GB	4.8 TB	Varies*
Maximum network map (hosts/users)	2,000/2,000	50,000/50,000	300,000/300,000	600,000/600,000	Varies*
Maximum flow rate (flows per second)	2,000 fps	6,000 fps	10,000 fps	20,000 fps	Varies*
High availability	Lights-out management (LOM)	RAID 1, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	Varies*

Note: A Cisco FireSIGHT Management Center appliance must be present for a sensor to function. All sensor licensing and management is handled by the Management Center. Additionally, all Cisco FireSIGHT Management Centers manage only the FirePOWER portions of Cisco ASA with FirePOWER Services deployments.

* Virtual Cisco FireSIGHT Management Center performance is highly dependent on the virtual environment chosen: CPUs, memory, storage, etc.

Ordering Information

Table 3 provides ordering information for virtual and physical Cisco FireSIGHT Management Center appliances and additional spare hardware.

Table 3. Cisco FireSIGHT Management Center Ordering Information

Cisco FireSIGHT Management Center (Hardware) Appliances	
Part Number	Product Description
FS750-K9	Cisco FireSIGHT Management Center 750 Chassis, 1RU
FS1500-K9	Cisco FireSIGHT Management Center 1500 Chassis, 1RU
FS3500-K9	Cisco FireSIGHT Management Center 3500 Chassis, 1RU
FS4000-K9	Cisco FireSIGHT Management Center 4000 Chassis, 1RU
Cisco FireSIGHT Management Center (Hardware) Spare	
FS-PWR-AC-650W=	Cisco FireSIGHT 650W AC Power Supply
Cisco FireSIGHT Management Center (Software) Virtual Appliance	
FS-VMW-SW-K9	Cisco FireSIGHT Management Center, Virtual (VMware) FireSIGHT License
FS-VMW-10-SW-K9	Cisco FireSIGHT Management Center, Virtual (VMware) FireSIGHT License, for 10 devices
FS-VMW-2-SW-K9	Cisco FireSIGHT Management Center, Virtual (VMware) FireSIGHT License, for 2 devices

To place an order, visit the [Cisco Ordering Homepage](#).

For More Information

For more information, please visit the following links:

- [Cisco ASA with FirePOWER Services](#)
- [Cisco FirePOWER Appliances](#)
- [Cisco FireSIGHT Management Center](#)
- [Cisco Security Services](#)



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 www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)