Cisco Security Services
A Solution Overview
Cisco Public

Security (ESA, WSA and SMA) Solution Overview

Cisco Email Security

Product Overview

Customers of all sizes face the same daunting challenge: email is simultaneously the most important business communication tool and the leading attack vector for security breaches. Cisco® Email Security enables users to communicate securely and helps organizations combat Business Email Compromise (BEC), ransomware, advanced malware, phishing, spam, and data loss with a multilayered approach to security.

The Cisco Email Security Difference

Cisco Email Security includes advanced threat protection capabilities to detect, block, and remediate threats faster; prevent data loss; and secure important information in transit with end-to-end encryption.

With Cisco Email Security customers can:

- Detect and block more threats with superior threat intelligence from Talos™, our threat research team.
- Combat ransomware hidden in attachments that evade initial detection with Cisco Advanced Malware Protection (AMP) and Cisco Threat Grid.
- Drop emails with risky links automatically or block access to newly infected sites with real-time URL analysis to protect against phishing and BEC.
- Prevent brand abuse and sophisticated identity-based email attacks with Cisco Domain Protection (CDP) and Cisco Advanced Phishing Protection (CAPP) services.
- Protect sensitive content in outgoing emails with Data Loss Prevention (DLP) and easy-to-use email encryption, all in one solution.
- Gain maximum deployment flexibility with a cloud, virtual, on-premises, or hybrid deployment or move to the cloud in phases.

Cisco Web Security Appliance

Product Overview

For security, your network needs malware protection, application visibility and control, acceptable use policy controls, insightful reporting and secure mobility. Cisco offers this protection, all on a single platform: the Cisco® Web Security Appliance (WSA).

In our highly connected and increasingly mobile world, more complex and sophisticated threats require the right mix of security solutions. Cisco delivers security for all layers of network infrastructure with the strong protection, complete control, and investment value businesses need. We also offer a broad set of web security deployment options, along with market-leading global threat intelligence. The Cisco WSA simplifies security with a high performance, dedicated appliance, and the Cisco Web Security Virtual Appliance (WSAV) lets businesses deploy web security quickly and easily, wherever and whenever it's needed.

The Cisco WSA was one of the first secure web gateways to combine leading protections to help organizations address the growing challenges of securing and controlling web traffic. It enables simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs. "Set and forget" technology frees staff after initial automated policy settings go live, and automatic security updates are pushed to network devices every 3 to 5 minutes. Flexible deployment options and integration with your existing security infrastructure help you meet quickly evolving security requirements.

The Cisco Web Security Difference

With Cisco Web Security customers can:

- Receive fast and comprehensive web protection backed by, Talos, the largest threat detection network in the world, with the broadest visibility and largest footprint.
- Combine traditional URL filtering with dynamic content analysis to mitigate compliance, liability, and productivity risks.
- Integrate with Advanced Malware Protection (AMP). AMP is an additionally licensed feature available to all Cisco WSA customers. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting
- Utilize Cisco Cognitive Threat Analytics is a cloud-based solution that reduces time to discovery of threats operating inside the network.
- Easily control the use of hundreds of Web 2.0 applications and 150,000+ micro-applications. Granular policy control allows administrators to permit the use of applications such as Dropbox or Facebook while blocking users from activities such as uploading documents or clicking the "Like" button.
- Prevent confidential data from leaving the network by creating context-based rules for basic DLP. The Cisco WSA also uses Internet Content Adaptation Protocol (ICAP) to integrate with third-party DLP solutions for deep content inspection and enforcement of DLP policies.
- Protect roaming users by integrating with the Cisco AnyConnect® Secure Mobility Client, which provides web security to remote clients by initiating a VPN tunnel that redirects traffic back to the on-premises solution.

Cisco Content Security Management Appliance

Product Overview

Centralize management and reporting functions across multiple Cisco® Email Security Appliances (ESAs) and Cisco Web Security Appliances (WSAs) with the Cisco Content Security Management Appliance (SMA). The integration of Cisco SMA with Cisco ESAs and WSAs simplifies the planning and administration of email and web security, improves compliance monitoring, makes possible a consistent enforcement of acceptable-use policies, and enhances threat protection.

Organizations must often coordinate the management and administration of multiple appliances across geographically dispersed teams with a limited staff and budget. Built on a robust platform optimized for reporting and tracking, the Cisco SMA delivers high performance and scalability plus industry-leading protection and control for long-term investment value.

Comprehensive Threat Protection

The Cisco SMA delivers a comprehensive view of an organization's security operations, providing better threat intelligence, defense, and remediation. Important features include the centralized management of email spam quarantine, comprehensive threat monitoring across multiple web security gateways, web reputation scoring, and botnet detection. The Cisco SMA's reporting capabilities can also be used to help administrators identify and address activities involving data loss prevention (DLP).

Upgrade your Content Security appliance in three easy steps

1. Confirm your current Cisco Content Security model and refresh needs.
2. Review the recommended migration path.
3. Contact your trusted Cisco Security account manager or partner to get started.

1 Rack Unit (RU) 32" x 17" x 2"

ESA C195-C695F
WSA S195-S395
SMA M195-395

2 Rack Unit (RU) 30.5" x 17" x 3.5"

WSA S695, S695F
SMA M695, M695F

Legacy Cisco Content Security Appliances x170 & x80	Legacy Cisco Content Security Appliances x90	New Generation Content Security Appliances x95
ESA-C170-K9	ESA-C190-K9	ESA-C195-K9
ESA-C380-K9	ESA-C390-K9	ESA-C395-K9
ESA-C680-10G-FP-K9	ESA-C690-10G-K9	ESA-C695-K9
ESA-C680-10G-K9	ESA-C690-10G-K9	ESA-C695-K9
ESA-C680-10G-LF-K9	ESA-C690-10G-K9	ESA-C695F-K9
ESA-C680-1G-FP-K9	ESA-C690-1G-K9	ESA-C695F-K9
ESA-C680-1G-K9	ESA-C690-1G-K9	ESA-C695F-K9
ESA-C680-1G-LF-K9	ESA-C690-1G-K9	ESA-C695F-K9
ESA-C680-FP-K9	ESA-C690-K9	ESA-C695-K9
ESA-C680-K9	ESA-C690-K9	ESA-C695-K9
ESA-C680-LKFP-K9	ESA-C690-K9	ESA-C695-K9
SMA-M170-K9	SMA-M190-K9	SMA-M195-K9
SMA-M380-K9	SMA-M390-K9	SMA-M395-K9
SMA-M680-10G-K9	SMA-M690-10G-K9	SMA-M695F-K9
SMA-M680-10G-LF-K9	SMA-M690-10G-K9	SMA-M695F-K9
SMA-M680-1G-K9	SMA-M690-1G-K9	SMA-M695F-K9
SMA-M680-1G-LF-K9	SMA-M690-1G-K9	SMA-M695F-K9
SMA-M680-K9	SMA-M690-K9	SMA-M695-K9
SMA-M680-LKFP-K9	SMA-M690-K9	SMA-M695-K9
WSA-S170-K9	WSA-S190-K9	WSA-S195-K9
WSA-S380-K9	WSA-S390-K9	WSA-S395-K9
WSA-S680-10G-K9	WSA-S690-10G-K9	WSA-S695F-K9
WSA-S680-10G-LF-K9	WSA-S690-10G-K9	WSA-S695F-K9
WSA-S680-1G-K9	WSA-S690-1G-K9	WSA-S695F-K9
WSA-S680-1G-LF-K9	WSA-S690-1G-K9	WSA-S695F-K9
WSA-S680-K9	WSA-S690-K9	WSA-S695-K9
WSA-S680-LKFP-K9	WSA-S690-K9	WSA-S695-K9

General Orderability Date x95: May 10, 2019

ESA	SMB	Mid-Size Enterprise	Large Enterprise
Model #	C195	C395	C695/C695F
HD (quantity)	(2) 600GB HDD	(2) 600GB HDD	(8) 600GB HDD
Memory (quantity)	(1) 16GB DDR4-2666-MHz	(1) 16GB DDR4-2666-MHz	(2) 16GB DDR4-2666-MHz
CPU (quantity)	(1) 2.1 GHz, 85W, 8C	(1) 2.1 GHz, 85W, 12C	(1) 2.6 GHz, 125W, 12C

WSA	SMB	Mid-Size Enterprise	Large Enterprise
Model #	S195	S395	S695/S695F
HD (quantity)	(2) 600GB HDD	(4) 600GB HDD	(16) 600GB HDD
Memory (quantity)	(1) 16GB DDR4-2666-MHz	(2) 16GB DDR4-2666-MHz	(4) 16GB DDR4-2666-MHz
CPU (quantity)	(1) 2.1 GHz, 85W, 8C	(1) 2.3 GHz, 85W, 12C	(2) 2.6 GHz, 125W, 12C

SMA	SMB	Mid-Size Enterprise	Large Enterprise
Model #	M195	M395	M695/M695F
HD (quantity)	(2) 600GB HDD	(8) 600GB HDD	(16) 600GB HDD
Memory (quantity)	(1) 16GB DDR4-2666-MHz	(1) 16GB DDR4-2666-MHz	(2) 16GB DDR4-2666-MHz
CPU (quantity)	(1) 2.1 GHz, 85W, 8C	(1) 2.1 GHz, 85W, 12C	(2) 2.1 GHz, 85W, 8C

END OF SALE AND END OF SUPPORT FOR X90 HARDWARE APPLIANCES TIMELINE

Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.	May 31, 2019
End-of-Sale Date	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	June 12, 2019
Last Ship Date: HW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	June 25, 2019
End of New Service Attachment Date: HW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.	June 29, 2020
End of Service Contract Renewal Date: HW	The last date to extend or renew a service contract for the product.	September 25, 2023
Last Date of Support: HW	The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.	June 30, 2024

The last SW image release that would be supported for the x90 appliance platforms are as below

- Web Security Appliances: 14.x.x
- Email Security Appliances: 14.x.x
- Security Management Appliances: 14.x.x

Learn More

To learn more about Cisco Email Security Appliances, please visit https://www.cisco.com/go/emailsecurity

For product related questions please contact

esa-pm@cisco.com

wsa-pm@cisco.com

Datasheets can be found at

https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet_c22-739910.html

https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet-c78-729630.html

https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html

Cisco Content Security End of Sale Notifications

https://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/eos-eol-notice-c51-730832.html

https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/eos-eol-notice-c51-737103.html