



# Cisco Web Security Appliance

---

# Contents

Virtual appliance	3
Features and benefits	3
Product specifications	6
Deployment	8
Licensing	8
Services	10
SMARTnet Support services	10
Warranty information	11
Cisco Capital	11
For more information	11
Acknowledgments	11

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.

## Virtual appliance

With the growth of video and other rich media, traffic has become less predictable, resulting in overages and degraded performance. Addressing these and other issues, administrators face long lead times when buying and installing hardware, remote installation challenges, customs duties, and other logistical issues, especially in multinational organizations.

The Cisco WSAV significantly lowers the cost of deploying web security, especially in highly distributed networks, by letting administrators create security instances where and when they are needed. The Cisco WSAV is a software version of the Cisco WSA that runs on top of a VMware ESXi, KVM hypervisor, Microsoft Hyper-V and Cisco Unified Computing System™ (Cisco UCS®) servers. You will receive an unlimited license for the Cisco SMAV with the purchase of any of the Cisco Email or Web Security software bundles, along with the corresponding SMA software license.

With the Cisco WSAV, administrators can respond instantly to traffic spikes and eliminate capacity planning. There is no need to buy and ship appliances; new business opportunities can be supported without adding complexity to a data center or requiring additional staff.

## Features and benefits

Feature	Benefits
Talos Security Intelligence	<p>Receive fast and comprehensive web protection backed by the largest threat detection network in the world, with the broadest visibility and largest footprint, including:</p> <ul style="list-style-type: none"><li>• 100 TB of security intelligence daily</li><li>• 1.6 million deployed security devices, including firewall, IPS, web, and email appliances</li><li>• 150 million endpoints</li><li>• 13 billion web requests per day</li><li>• 35% of the world's enterprise email traffic</li></ul> <p>Providing a 24x7 view into global traffic activity to analyze anomalies, uncover new threats, and monitor traffic trends. Talos prevents zero-hour attacks by continually generating new rules that feed updates to the WSA every three to five minutes, enabling industry-leading</p>

Feature	Benefits
	threat defense hours and even days ahead of competitors.
<b>Cisco Web Usage Controls</b>	Combine traditional URL filtering with dynamic content analysis to mitigate compliance, liability, and productivity risks. Cisco's continuously updated URL filtering database of over 50 million blocked sites provides exceptional coverage for known websites, and the Dynamic Content Analysis (DCA) engine accurately identifies 90 percent of unknown URLs in real time; it scans text, scores the text for relevancy, calculates model document proximity, and returns the closest category match. Administrators can also select specific categories for intelligent HTTPS inspection.
<b>Advanced Malware Protection</b>	Advanced Malware Protection (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. It takes advantage of the vast cloud security intelligence networks of both Cisco and Sourcefire® technology. AMP augments the malware detection and blocking capabilities already offered in the Cisco WSA with enhanced file reputation capabilities, detailed file-behavior reporting, continuous file analysis, and retrospective verdict alerting. The Cisco <a href="#">AMP Threat Grid</a> delivers malware protection through an on-premises appliance for organizations that have compliance or policy restrictions on submitting malware samples to the cloud. The Layer 4 Traffic Monitor continuously scans activity, detecting and blocking spyware "phone-home" communications. By tracking all network applications, the Layer 4 Traffic Monitor effectively stops malware that attempts to bypass classic web security solutions. It dynamically adds IP addresses of known malware domains to its list of malicious entities to block.
<b>Cognitive Threat Analytics</b>	Cisco Cognitive Threat Analytics is a cloud-based solution that reduces time to discovery of threats operating inside the network. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection. Take advantage of Cisco Cognitive Threat Analytics with a simple add-on license to your Web Security solution. Reduce complexity while gaining superior protection that evolves with your changing threat landscape.
<b>Application Visibility and Control (AVC)</b>	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. The WSA supports visibility of activity across an entire network. New: Customers can deploy customized bandwidth and time quotas per user, per group, and per policy.
<b>Data Loss Prevention (DLP)</b>	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. The Cisco WSA also supports Secure ICAP to encrypt the traffic exchanged between WSA and third-party DLP solutions.

Feature	Benefits
<b>Roaming-User Protection</b>	<p>The Cisco WSA protects roaming users by integrating with the Cisco AnyConnect<sup>®</sup> 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 AnyConnect technology analyzes traffic in real time prior to permitting access.</p> <p>The Cisco WSA is also integrated with Cisco Identity Services Engine (ISE). With this exciting enhancement, customers can now take advantage of the power of Cisco ISE for Cisco WSA upon request. Cisco ISE integration allows admins to create policy on the Cisco WSA based on profile or membership information gathered by Cisco ISE through its single sign-on process.</p>
<b>Centralized Management and Reporting</b>	<p>Receive actionable insights across threats, data, and applications. The Cisco WSA provides an easy-to-use, centralized management tool to control operations, manage policies, and view reports.</p> <p>The Cisco M-Series Content Security Management Appliance provides central management and reporting across multiple appliances and multiple locations, including virtual instances. <a href="#">Cisco<sup>®</sup> Web Security Reporting Application</a> is a reporting solution that rapidly indexes and analyzes logs produced by Cisco Web Security Appliances (WSA) and Cisco Umbrella. This tool provides scalable reporting for customers with high traffic and storage needs. It allows reporting administrators to gather detailed insight into web usage and malware threats.</p>
<b>Flexible Deployment</b>	<p>WSA can be an effective protection against web-based threats for your workloads running in the cloud. Alternatively, if your organization uses on-premises WSA for web security, as a good security practice you can deploy a similar security stack for your cloud-based applications using WSAV on AWS. Furthermore, using Security Management Appliance virtual (SMAV) on AWS, <b>you can configure and monitor</b> a large number of WSA farms in your cloud environment itself.</p> <p>The Cisco WSAV offers all the same features as the Cisco WSA, with the added convenience and cost savings of a virtual deployment model, including instant self-service provisioning. With a Cisco WSAV license, businesses can deploy web security virtual gateways without being connected to the Internet, by applying the license to a new Cisco WSAV virtual image file stored locally. Pristine virtual image files can be cloned, if needed, to deploy several web security gateways immediately.</p> <p>Run hardware and virtual machines in the same deployment. Small branch offices or remote locations can have the same protection the Cisco WSA provides without having to install and support hardware at that location. Custom deployment is easily managed with the Cisco M-Series Content Security Management Appliance.</p>

## Product specifications

Tables 1 and 2 give Cisco WSA performance and hardware specifications, respectively.

**Table 1.** Cisco WSA performance specifications

	Model	Disk Space	Raid Mirroring	Memory	CPUs
Large Enterprise	S695	9.6 TB (16x600 GB SAS)	Yes (RAID 10)	64 GB, DDR4	2 x 2.6 Ghz, 12C
Large Enterprise	S690	4.8 TB (8x600 GB SAS)	Yes (RAID 10)	64 GB, DDR4	2 x 2.5 Ghz, 12C
Midsize Office	S395	2.4 TB (4x600 GB SAS)	Yes (RAID 10)	32 GB, DDR4	1 x 2.3 Ghz, 12C
Midsize Office	S390	2.4 TB (4x600 GB SAS)	Yes (RAID 10)	32 GB, DDR4	1 x 2.4 Ghz, 6C
SMB and Branch	S195	1.2TB (2x600 GB SAS)	Yes (RAID 1)	8 GB, DDR4	1 x 2.1 Ghz, 8C
SMB and Branch	S190	1.2TB (2x600 GB SAS)	Yes (RAID 1)	8 GB, DDR4	1 x 1.9 Ghz, 6C

**Table 2.** Cisco SMA hardware specifications

Hardware Platform	 Cisco S695	 Cisco S690	 Cisco S395	 Cisco S390	 Cisco S195	 Cisco 190
Form Factor	2RU	2RU	1RU	1RU	1RU	1RU
Dimensions	3.5 in. x 17 in. x 30.5 in.	3.4" x 19" x 29"	2 in. x 17 in. x 32 in.	1.7" x 19" x 31"	2 in. x 17 in. x 32 in.	1.7" x 19" x 31"
Redundant P/S	Yes	Yes	Yes	Yes	Yes, Accessory Option	Yes, Accessory Option
Remote Power Cycle	Yes	Yes	Yes	Yes	Yes	Yes
DC Power Option	No	Yes (930W)	No	No	No	No
Hot- Swappable H/D	Yes	Yes	Yes	Yes	Yes	Yes
Power Consumption	2216.5 BTU/hr	2216.5 BTU/hr	2626 BTU/hr	2626 BTU/hr	2626 BTU/hr	2626 BTU/hr
Power Supply	1050W	650W	770W	770W	770W	770W
Ethernet interfaces	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45	6 port 1G Base-T copper network interface (NICs), RJ - 45
Speed (Mbps)	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate	10/100/1000, auto negotiate
Fiber Option	Yes, separate	Yes, separate	No	No	No	No

Hardware Platform	Cisco S695	Cisco S690	Cisco S395	Cisco S390	Cisco S195	Cisco 190
						
	SKU, 6-port 1GBASE-SX Fiber or 10GBASE-SR Fiber selectable upon ordering (modules included): WSA-S695F	SKUs, 6 port 1G Base-SX Fiber: WSA-S690-1G, 6 port 10G Base-SR Fiber, WSA-S690-10G				
HD Size	Sixteen 600 GB hard disk drives (2.5" 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Eight 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Four 600 GB hard disk drives (2.5" 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Four 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Two 600 GB hard disk drives (2.5" 12G SAS 10K RPM) are installed into front-panel drive bays that provide hot-swappable access for SAS drives	Two 600 GB hard disk drives (2.5" 10K SAS 4Kn) are installed into front-panel drive bays that provide hot-swappable access for SAS drives
CPU	Two 2.6GHz 12c 2666MHz processor	Two E5-2680 v3 processor	One 2.3GHz 12c 2400MHz processor	One E5-2620 v3 processor	One 2.1GHz 8c 2400MHz processor	One E5-2609 v3 processor
RAM	Four 16GB DDR4-2666 DIMM1	Eight 8GB DDR4-2133 DIMM1	Two 16GB DDR4-2666 DIMM1	Four 8GB DDR4-2133 DIMM1	One 16GB DDR4-2666 DIMM1	One 8GB DDR4-2133 DIMM1

Table 3 lists specifications of the Cisco WSAV, and Table 4 lists those for the Cisco M-Series Content Security Management Appliance.

Table 3. Cisco WSAV

Model	Disk	Memory	Cores
S000v	250 GB	4 GB	1
S100v	250 GB	6 GB	2
S300v	1024 GB	8 GB	4
S600v	2.4 TB	24 GB	12

Model	Disk	Memory	Cores
Servers		Hypervisor	
Cisco UCS		ESXi 5.0, 5.1, and 5.5 & 6.0	
Red Hat Enterprise Linux 7.0		KVM: QEMU 1.5.3	
Ubuntu 14.04.1 LTS		KVM: QEMU 2.0.0	
		Microsoft Hyper-V	

\*\* Applicable to the features Web Rep, URL filtering, Sophos and Webroot only. Additional features like AMP, TG, would put this model in evaluation mode.

Table 4. Cisco M-Series Content Security Management Appliance

Model	M659/690	M395/390	M195/190
Users (approximately)	10,000+	Up to 10,000	Up to 1,000

## Deployment

The Cisco WSA is a forward proxy that can be deployed in either Explicit mode (Proxy Automatic Configuration [PAC] files, Web Proxy Auto-Discovery [WPAD], browser settings) or Transparent mode (Web Cache Communication Protocol [WCCP], Policy-Based Routing [PBR], load balancers). WCCP-compatible devices, such as Cisco Catalyst® 6000 Series Switches, Cisco ASR 1000 Series Aggregation Services Routers, Cisco Integrated Services Routers, and Cisco ASA 5500-X Series Next-Generation Firewalls, reroute web traffic to the Cisco WSA.

The Cisco WSA can proxy HTTP, HTTPS, SOCKS, native FTP, and FTP over HTTP traffic to deliver additional capabilities such as data-loss prevention, mobile user security, and advanced visibility and control.

## Licensing

A Cisco WSAV license is included in all Cisco Web Security software bundles (Cisco Web Security Essentials, Cisco Web Security Antimalware, and Cisco Web Security Premium). This license has the same term as the other software services in the bundle and can be used for as many virtual machines as needed.

### Term-Based Subscription Licenses

Licenses are term-based subscriptions of one, three, or five years.

### Quantity-Based Subscription Licenses

The Cisco Web Security portfolio uses tiered pricing based on a range of users, not devices. Sales and partner representatives can help to determine the correct sizing for each customer deployment.

### Web Security Software Licenses

Four web security software licenses are available: Cisco Web Security Essentials, Cisco Anti-Malware, Cisco Web Security Premium, and McAfee Anti-Malware. The major components of each software offering follow:

---

## Cisco Web Security Essentials

- Threat Intelligence via Cisco Talos
- Layer 4 traffic monitoring
- Application Visibility and Control (AVC)
- Policy management
- Actionable reporting
- URL filtering
- Third-party DLP integration via ICAP

## Cisco Anti-Malware

- Real-time malware scanning

## Cisco Web Security Premium

- Web Security Essentials
- Real-time malware scanning

## Cisco Web Security Shield

- Web Security Premium
- Advanced malware protection
- Cognitive threat analytics
- Threat Grid file analysis

## Advanced Malware Protection

- AMP augments anti-malware detection and blocking capabilities with file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for continuous analysis of threats.

## Cognitive Threat Analytics

- CTA relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

## McAfee Anti-Malware

- McAfee real-time malware scanning is available as a single, a-la-carte license.

## Software License Agreements

The Cisco End-User License Agreement (EULA) and the Cisco Web Security Supplemental End-User License Agreement (SEULA) are provided with each software license purchase.

## Software Subscription Support

All Cisco Web Security licenses include software subscription support essential to keeping business-critical applications available, secure, and operating at peak performance. This support entitles customers to the following services for the full term of the purchased software subscription:

- Software updates and major upgrades to keep applications performing optimally at the most current feature set
- Access to Cisco Technical Assistance Center (TAC) for fast, specialized support
- Online tools to build and expand in-house expertise and boost business agility
- Collaborative learning for additional knowledge and training opportunities

## Services

Table 5 lists Cisco Web Security services.

**Table 5.** Cisco Web Security services

<b>Cisco Branded Services</b>	<p>Cisco Security Planning and Design: Enables deployment of a robust security solution quickly and cost-effectively.</p> <p>Cisco Web Security Configuration and Installation: Mitigates web security risks by installing, configuring, and testing appliances to implement:</p> <ul style="list-style-type: none"><li>• Acceptable-use-policy controls</li><li>• Data security</li><li>• Reputation and malware filtering</li><li>• Application visibility and control</li></ul> <p>Cisco Security Optimization Service: Supports an evolving security system to address security threats, design updates, performance tuning, and system changes.</p>
<b>Collaborative/Partner Services</b>	<p>Network Device Security Assessment: Helps maintain a hardened network environment by identifying gaps in network infrastructure security. Smart Care: Provides actionable intelligence gained from secure visibility into the performance of a network. Additional services: Cisco partners provide a wide range of valuable services across the planning, design, implementation, and optimization lifecycle.</p>
<b>Cisco Financing</b>	<p>Cisco Capital<sup>®</sup> can tailor financing solutions to business needs. Access Cisco technology sooner and see the business benefits sooner.</p>

## SMARTnet Support services

Customers have the option to purchase Cisco SMARTnet<sup>®</sup> support for use with Cisco WSAs. Cisco SMARTnet support helps customers resolve network problems quickly with direct, anytime access to Cisco experts, self-help support tools, and rapid hardware replacement. For more information, visit <https://www.cisco.com/go/smartnet>.

## Ordering Cisco WSAv

Do the following to order Cisco WSAV:

1. Go to <https://www.cisco.com/go/wsa>. At right, under "Support", click "Software Downloads, Release, and General Information". Click "Download Software", then click on any model to see the downloadable virtual-machine images available. You will also see a downloadable XML evaluation license. You need to download one of the images and the XML evaluation license.
2. Download the following documentation from Cisco.com:
  - a. Cisco Security Virtual Appliance Installation Guide
  - b. Documentation for AsyncOS® 11.5
3. Follow the instructions in the Cisco Security Virtual Appliance Installation Guide to get started. Please note that content security virtual appliance evaluations are not covered under SMARTnet support and are therefore unsupported.

## Warranty information

Find warranty information on Cisco.com at the [Product Warranties](#) page.

## Cisco Capital

### Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. [Learn more](#).

## For more information

Find out more at <http://www.cisco.com/go/wsa>. Evaluate how the Cisco WSA will work for you with a Cisco sales representative, channel partner, or systems engineer.

## Acknowledgments

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: (<http://www.openssl.org>). This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**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>.

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: <https://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)