

Cisco Web Security: Protection, Control, and Value



Benefits

- **Strong protection:**
Protects every device through a sophisticated global threat-intelligence infrastructure, which includes Cisco Talos Security Intelligence and Research Group (Talos)
- **Complete control:** Helps enable advanced control of all web traffic, including dynamic web content such as social media applications
- **Investment value:**
Delivers more for your security investment and lowers the total cost of ownership (TCO) for web security, offering flexible deployment options, smooth integration with existing security and network infrastructure, and world-class 24-hour support

The World Wide Web is a wonderful thing. It's also insecure. But how do you protect your devices and resources while also using social media and web applications?

We believe that one solution isn't enough. You need a variety of protections against today's fast-evolving cyberthreats. But that introduces complexity and bigger operational workloads to your IT environment, right? Not with the Cisco® Web Security Appliance (WSA) (see Figure 1). Cisco WSA is an all-in-one highly secure web gateway that brings you strong protection, complete control, and investment value. It also offers an array of competitive web security deployment options, each of which includes Cisco's market-leading global threat intelligence infrastructure.

Figure 1. Cisco Web Security Appliance



Strong Protection

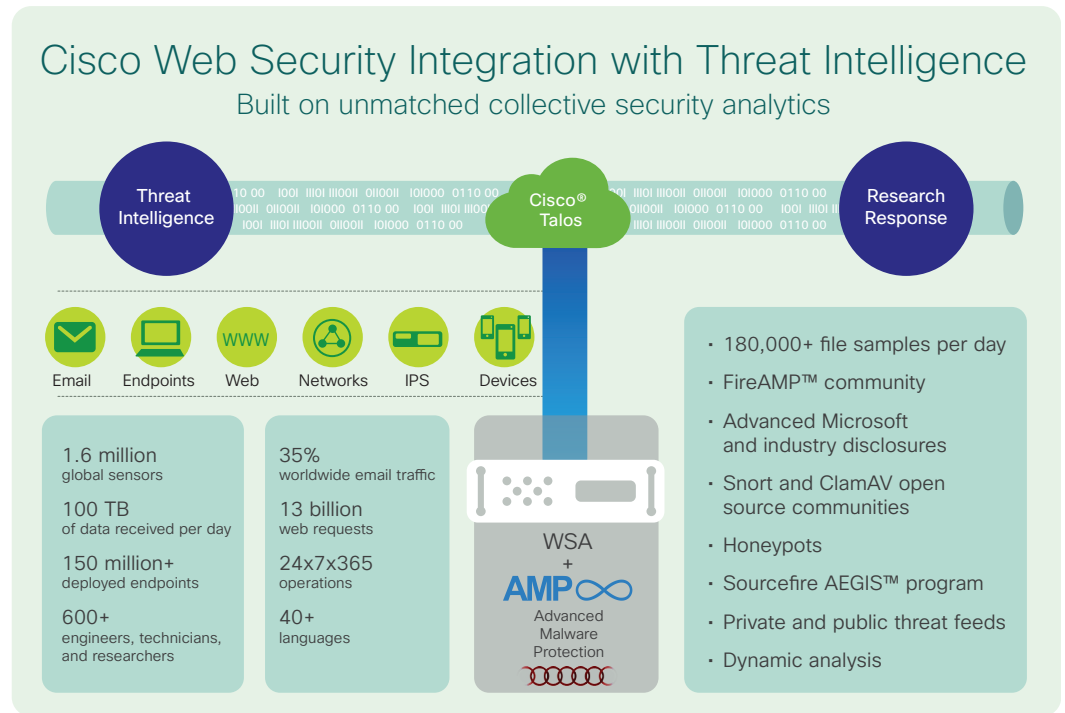
Advanced Threat Defense

Cisco Web Security is powered by Cisco Talos Security Intelligence and Research Group, the industry's largest collection of real-time threat intelligence, with the broadest visibility and largest footprint. Talos discovers where threats are hiding by pulling massive amounts of global information across multiple attack vectors (see Figure 2). This information gathering encompasses:

- 100 TB of security intelligence daily
- 1.6 million deployed security devices, including firewall, intrusion prevention system (IPS), web, and email appliances
- 150 million endpoints
- 13 billion web requests per day
- Hundreds of applications and 150,000 microapplications
- 35 percent of the world's enterprise email traffic

Talos delivers early-warning intelligence, threat and vulnerability analysis to help protect organizations against zero-day advanced threats. It continually generates new rules that feed updates every three to five minutes so that Cisco Web Security can deliver industry-leading threat defense hours and even days ahead of competitors.

Figure 2. Cisco Talos Security Intelligence and Research Group



Best Website Reputation Analysis

Cisco WSA correlates threats collected from Cisco’s network to produce a behavior score on which to take action. It applies and enforces web-reputation scores on parent sites and subsites.

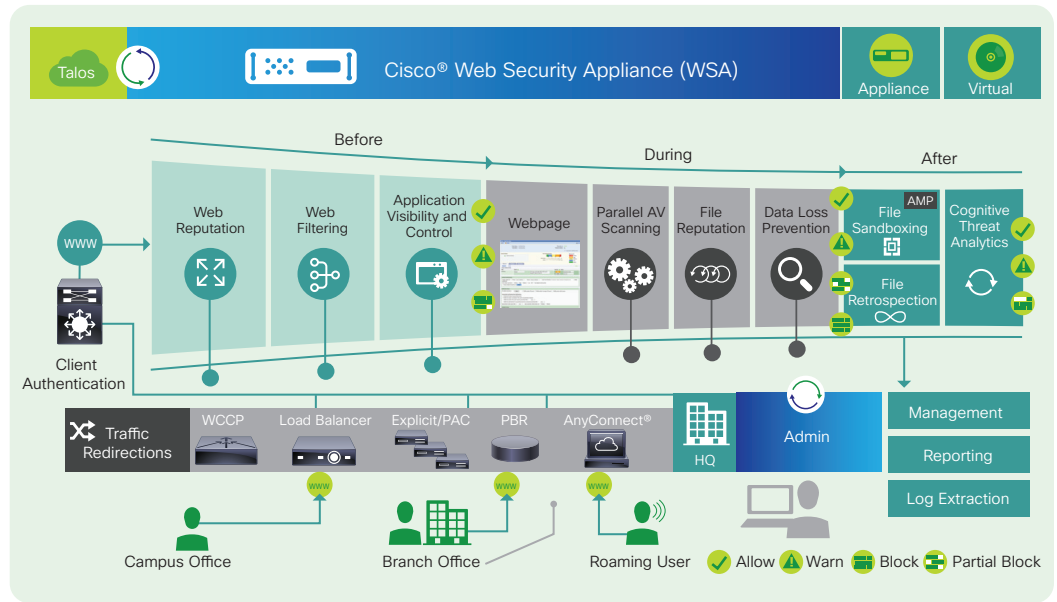
Integrated, Multilayer Malware Defense for Adaptive Protection

Effective web security used to mean blocking navigation to bad URLs. But today you’re more likely to contract a virus or download malware through legitimate websites. Cisco WSA defends against malware and advanced persistent threats using multiple layers of antimalware technologies and intelligence from Talos updated every three to five minutes. Every piece of web content accessed—from HTML to images to Flash files—is analyzed using security and context-aware scanning engines.

Cisco WSA analyzes traffic in real time, breaks it into functional elements, and pushes elements to best-designed malware engines for inspection while maintaining high processing speeds (see Figure 3).



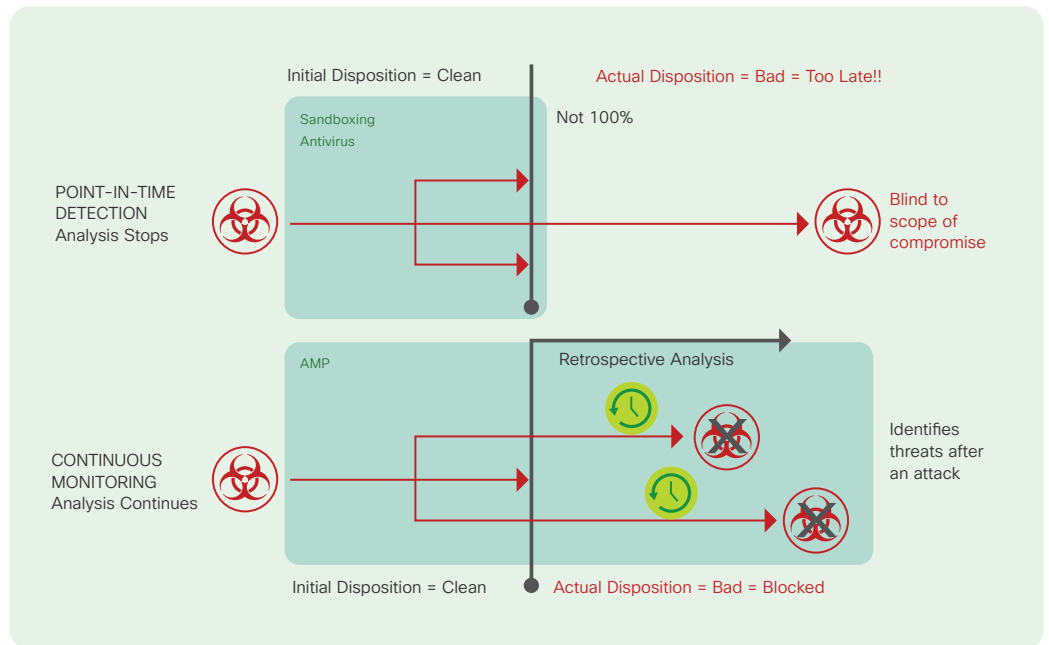
Figure 3. Cisco WSA's Layers of Defense



Sandboxing and Continuous Analysis

Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco WSA customers. AMP is a comprehensive malware-defeating solution that provides malware detection and blocking, continuous analysis, and retrospective alerting (see Figure 4). 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. Customers now have the ability to sandbox PDF, Microsoft Office, and archive/compressed files files, in addition to Windows portable executable files.

Figure 4. Retrospective Analysis with AMP





Complete Control

Centralized Management

The Cisco WSA's intuitive management interface centralizes policy management and reporting, offering global control from a simple-to-use single interface.

Deep Web Usage and Application Visibility

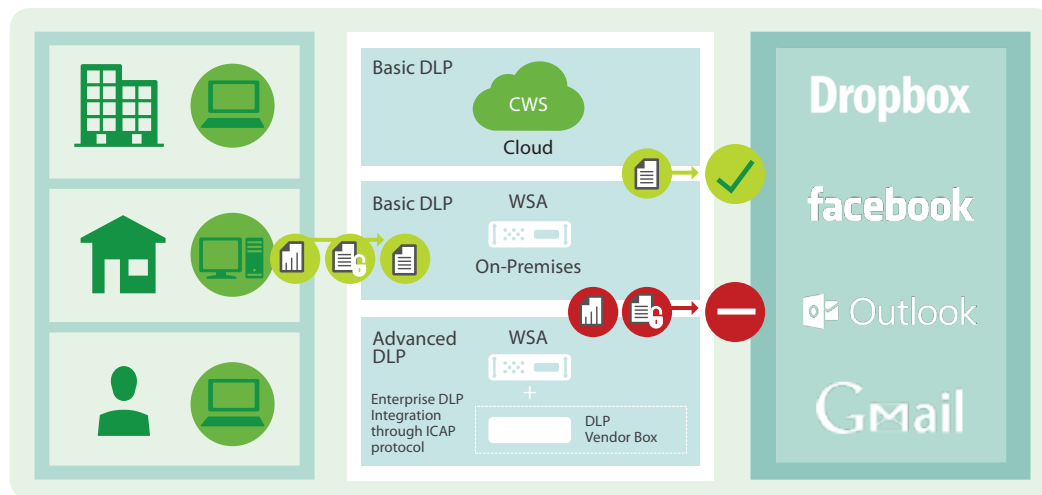
With the Cisco WSA, you get deep visibility into evolving application and microapplication content. Specifically, Cisco WSA identifies and classifies the most relevant and widely used web and mobile applications, such as Facebook, and more than 150,000 microapplications, such as Facebook games. This is done by combining identity, time, content, location, and outbound-compliance data to build and maintain application policy.

Coupled with this visibility, the Cisco WSA offers the precise control over application and usage behavior. It can regulate bandwidth consumption and apply conditional controls, such as throttling, based on the location or profile of the user and the type of device. In addition, the Cisco WSA provides dynamic, context-based control of user access to applications based on user profile, device, and access mechanism. You can also set up policy to control SaaS applications such as Salesforce.com or WebEx.

Data Loss Prevention

The Cisco WSA blocks sensitive information from leaving the safety of the network, helping to ensure compliance and reduce risk (see Figure 5). This capability is in addition to the controls for outbound content such as file-sharing applications. You're able to prevent uploads to file-sharing services in the cloud, including iCloud and Dropbox. You can also stop confidential data from leaving the network by creating context-based rules for basic data loss prevention (DLP) or by using the Internet Content Adaptation Protocol (ICAP) to integrate with any third-party DLP solution for deep content inspection and enforcement of DLP policies.

Figure 5. Data Loss Prevention with Cisco WSA



Investment Value

Lower Total Cost of Ownership

The Cisco WSA delivers a consolidated solution in a single appliance, unlike other solutions that often require additional devices for new features and functions. You spend less time troubleshooting, with 99.999 percent availability and uptime. You save time with automatic updates from Talos and stay tuned against the latest threats without intervention. Lastly, you can use your existing VMware infrastructure in an unlimited number of deployments of the Cisco Web Security Virtual Appliance (WSAV).

Models and Options Available

Tables 1 through 4 provide specifications for the Cisco WSA, the Cisco Web Security Virtual Appliance (WSAV), and the Cisco M-Series Content Security Management Appliance.

Table 1. Cisco WSA Performance Specifications

	Users*	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large enterprise	6,000–12,000	S680	4.8 TB (8 x 600-GB SAS)	Yes (RAID 10)	32 GB	16 (2 octa core) 2.70 GHz
Midsize office	1,500–6,000	S380	2.4 TB (4 x 600-GB SAS)	Yes (RAID 10)	16 GB	6 (1 hexa core)
SMB and branch	Less than 1,500	S170	500 GB (2 x 250-GB SATA)	Yes (RAID 1)	4 GB	2 (1 dual core) 2.80 GHz

* Please confirm sizing guidance with a Cisco content security specialist to help ensure your solution will meet your current and projected needs.

Table 2. Cisco WSA Hardware Specifications




	S680	S380	S170
Hardware platform			
Form factor	2 rack units (2RU)	2RU	1RU
Dimensions	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm.)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm.)	1.64 x 19 x 15.25 in. (4.2 x 48.3 x 38.7 cm.)
Redundant power supply	Yes	Yes	No
Remote power cycle	Yes	Yes	No
DC power option	Yes	Yes	No
Hot-swappable hard drive	Yes	Yes	Yes
Fiber option	Yes (accessory)	No	No
Ethernet	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	2 Gigabit NICs, RJ-45
Speed (Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate

Table 3. Cisco WSAV Specifications




Web Users	Model	Disk	Memory	Cores
Less than 1,000	S000v	250 GB	4 GB	1
1,000–2,999	S100v	250 GB	6 GB	2
3,000–6,000	S300v	1024 GB	8 GB	4
Servers				
Cisco UCS 		ESXi 5.0, 5.1 and 5.5 Hypervisor		

Table 4. Cisco M-Series Content Security Management Appliance

Model	Cisco M680	Cisco M380	Cisco M170
Users (approx.)	10,000 or more	Up to 10,000	Up to 1,000

Next Steps

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.



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)

C02-733921-00 2/15