

Cisco Web Security



Web technology provides innovative ways to market products, reach customers and suppliers, and reduce the cost of doing business. Unfortunately, many of these technologies contain security threats that can expose companies to significant business risks.

More Exposure, New Threats

Today, some of the most sophisticated web-based threats are designed to hide in plain sight on legitimate and well-trafficked websites.

- Online advertisements are now 182 times more likely to deliver malicious content than pornographic sites¹.
- Studies of traffic patterns show that criminal activity mirrors the “9 to 5” workday of its victims.
- The majority (83%) of web malware encounters in 2012 were malicious scripts and hidden iFrames - attacks representing malicious code on “trusted” webpages that users visit every day².

Ubiquitous web access creates new network entry points that blur the lines of historically segmented security layers. Employees once checked text-based email from workstations behind company firewalls, but today they interact with rich HTML messages from multiple devices, anytime and anywhere. Sophisticated blended email and web attacks capitalize on this vulnerability.

Once an organization's network is compromised, it can take weeks, months, or longer for an advanced persistent threat (APT) enabled through web malware to be detected in the network. Meanwhile, the targeted organization continues to lose data - and risks significant financial and reputation damage.

¹ 2013 Cisco Annual Security Report, January 2013, available for download at http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

² 2013 Cisco Annual Security Report, January 2013, available for download at http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

Increasingly Complex Web Scenarios

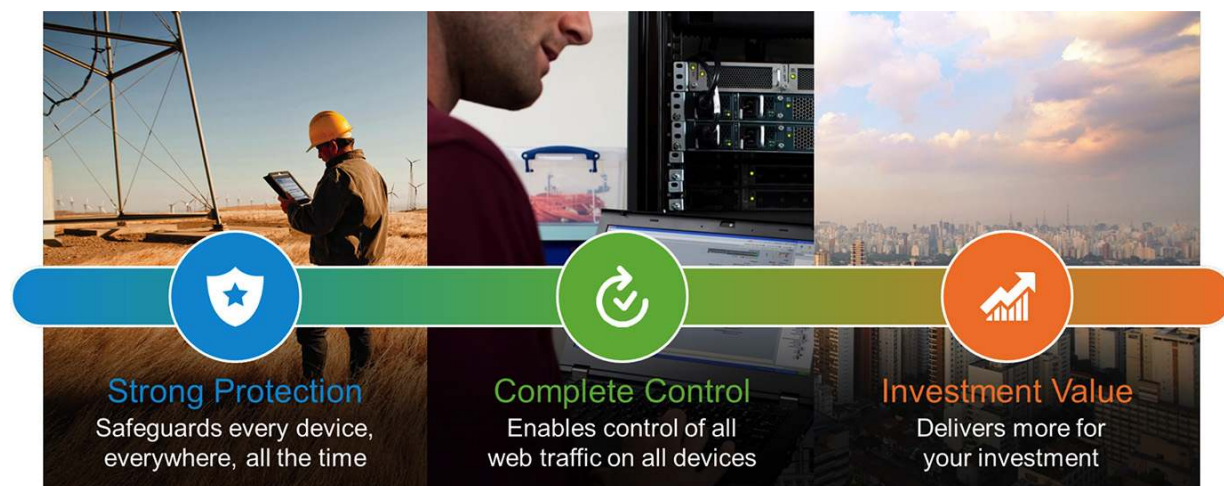
As a result of public Wi-Fi initiatives, smaller branch offices, remote workers, and the “bring your own device” (BYOD) movement, network perimeters are no longer clearly defined. Today’s employees expect to do business anywhere and with any device on hand, challenging traditional security and deployment models. However, uncontrolled use of social media and Web 2.0 applications by employees opens the door to web malware, data security risk, and productivity loss. And blocking sites altogether is not an option: Businesses need to harness the power of the web without undermining business agility or web security.

Growing Budget Pressures

Many organizations are challenged further by the need to develop more robust web security and policy within rigid business constraints. They must use their existing architectures and/or rely on limited resources to scale web security to protect the rapidly growing population of remote and branch offices, which typically have little or no onsite IT support.

Time for a New Approach

A modern approach to web security requires the ability to block hidden malware from both suspicious and legitimate sites before it reaches users, as well as the ability to block high-risk sites. The approach must be nuanced enough to support policies that give employees access to the sites they need to do their jobs while blocking the use of undesired features, such as games and file transfers. It also needs to be backed by the best security intelligence to stay abreast of the changing threat landscape.



Cisco offers all of this in a flexible set of web security delivery options - all part of the Cisco security architecture that works together to provide a comprehensive set of cybersecurity solutions. Cisco® Web Security delivers the **strong protection, complete control, and investment value** that organizations of all sizes need today.

Strong Protection

Advanced Threat Defense

Cisco Web Security is powered by Cisco Security Intelligence Operations (SIO), an organization that detects and correlates threats in real time using the largest threat detection network in the world. SIO discovers where threats are hiding by pulling massive amounts of information across multiple vectors and looking across the global threat landscape through the broadest visibility and largest footprint:

- 100 TB of security intelligence daily
- 1.6 million deployed security devices, including firewall, IPS, web, and email appliances
- 150 million endpoints
- 13 billion web requests per day
- 35% of the world's enterprise email traffic
- Updates as often as every three to five minutes

Real-Time Malware Scanning

Cisco Web Security uses both dynamic reputation analysis and behavior-based analysis to provide businesses with the best threat defense from zero-day web malware. All inbound and outbound web traffic is scanned in real time for both new and known web malware. Every piece of web content accessed - from HTML to images to Flash content - is analyzed using security- and context-aware scanning engines.

Intelligent multiscanning determines which scanning engine to use based on reputation and content type, optimizing efficiency and catch rates. Traffic inspection engines analyze traffic in real time, breaking it into functional elements and pushing those elements to the malware engines best designed to inspect that sort of data.

An integrated Layer 4 Traffic Monitor available on Cisco Web Security Appliances and Cisco Next-Generation Firewalls scans all 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. In addition, the Layer 4 Traffic Monitor is able to dynamically add IP addresses of known malware domains to its list of malicious entities to block. Using this dynamic discovery capability, the Layer 4 Traffic Monitor can monitor the movement of malware in real time - even as the malware host tries to avoid detection by migrating from one IP address to another.

Cisco Web Security in action

In early September 2012, researchers with Cisco SIO warned of a critical zero-day vulnerability in Microsoft Internet Explorer (IE) versions 6, 7, and 9, which would allow an attacker to gain full administrator access to a vulnerable machine if a user simply visited a malicious webpage.

More than two weeks (16 days) after the vulnerability was widely known, antivirus vendors began issuing signatures. And nearly three weeks after Cisco SIO issued its vulnerability warning, IE was patched and a security advisory was issued. Meanwhile, users were left exposed.

On "day zero," Cisco automatically blocked the website hosting the IE exploit, protecting customers from ever visiting the site. Cisco reputation technology assessed the risk of the domain, which was pushed instantly out to Cisco customers.

Further analysis of the IE vulnerability by Cisco SIO researchers revealed a spike in traffic to a second malicious domain and the presence of malware - the vulnerability was actively being used.

Correlating this web data with intelligence from Cisco IPS, Cisco SIO issued a signature and blocked the command-and-control infrastructure for this threat.

Cisco's continuous intelligence from both automated systems and human analysis helped to prevent attacks before they could happen. For example, using this combined intelligence, Cisco SIO updated all devices within five minutes to block more than 40 "parked" domains registered by the same suspicious entity.

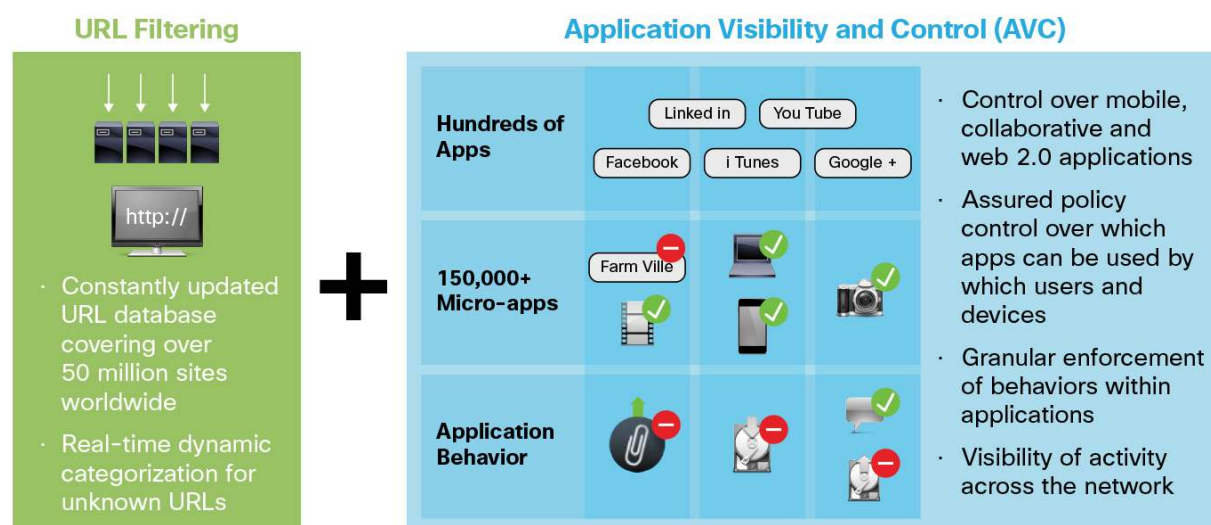
Complete Control

Granular Acceptable Use Controls

Cisco Web Security gives businesses complete control over how end users access the Internet. Identification of hundreds of applications and 150,000+ micro-applications allows administrators to create policies that match the nuanced business needs of today (Figure 1). Micro-applications are grouped into easy-to-use categories so that security administrators can easily allow or deny access to the relevant parts of the application. Specific features such as chat, messaging, video, and audio can be allowed or blocked, according to the requirements of business and users - without the need to block entire websites.

As an example, the Facebook Videos category can identify whether a user is uploading, tagging, or posting videos; administrators can choose which actions to allow (e.g., viewing and tagging videos, but not uploading them). The administrator can also deny any postings from users, effectively making Facebook read-only.

Figure 1. Acceptable Use Controls



Vital Data Loss Prevention

The Cisco Web Security Appliance (WSA) provides essential tools for a data loss prevention (DLP) strategy. Onboard capabilities allow administrators to create basic content control rules based on context.

Cisco WSA also integrates via Internet Content Adaptation Protocol (ICAP) with DLP solutions from leading vendors to ensure consistent enforcement of DLP policies and deep content analysis. Powerful engines inspect outbound traffic; analyze it for content markers such as confidential files, credit card numbers, or customer data; and prevent this data from being uploaded to the web.

Actionable Reporting

Controlling web security is not enough. It is also essential to analyze, troubleshoot, and refine security policies in order to stay ahead of threats. Cisco Web Security solutions provide powerful, centralized tools to control security operations, such as management, and network operations, such as analysis of bandwidth consumption.

Investment Value

Unified Security










Today's web-based threats are complex, but a better security infrastructure doesn't have to be. The security infrastructure and its elements must work together with more intelligence to detect and mitigate threats. Cisco's architectural approach to security is holistic: It allows organizations to retain their business agility by enabling the reuse of services and rapid deployment of new capabilities as business needs change.

Cisco Web Security delivers a better return on investment, whether the solution is deployed via appliance or through the cloud. Its close integration with the Cisco network infrastructure and other Cisco security products lets enterprises reuse existing assets to deploy web security in areas where it was too expensive or difficult to deploy previously. Cisco Web Security, with its simplified architecture, also reduces administrative burden by having fewer devices to manage, support, and maintain.

Flexible Deployment

Cisco Web Security is offered in a range of options, from basic firewall configurations to sophisticated cloud deployments with multiple connectors (Figure 2), so organizations can meet their business requirements without buying more than necessary.

Figure 2. Cisco Web Security Deployment Options

	On-Premises	Cloud
Deployment Options	 Appliance  Virtual  Next Generation Firewall	 Cloud
Connection Methods	 Roaming	 Router  Firewall  Appliance  Roaming



Cisco Web Security Appliance (WSA): Simplifies control with a high-performance dedicated appliance.



Cisco Web Security Virtual Appliance (WSAV): Allows administrators to create new appliance instances wherever and whenever they're needed.



Firewall Integrated: Offers protection without sacrificing performance by adding Web Security Essentials (WSE) and Application Visibility and Control (AVC) to an existing Cisco ASA next-generation firewall.



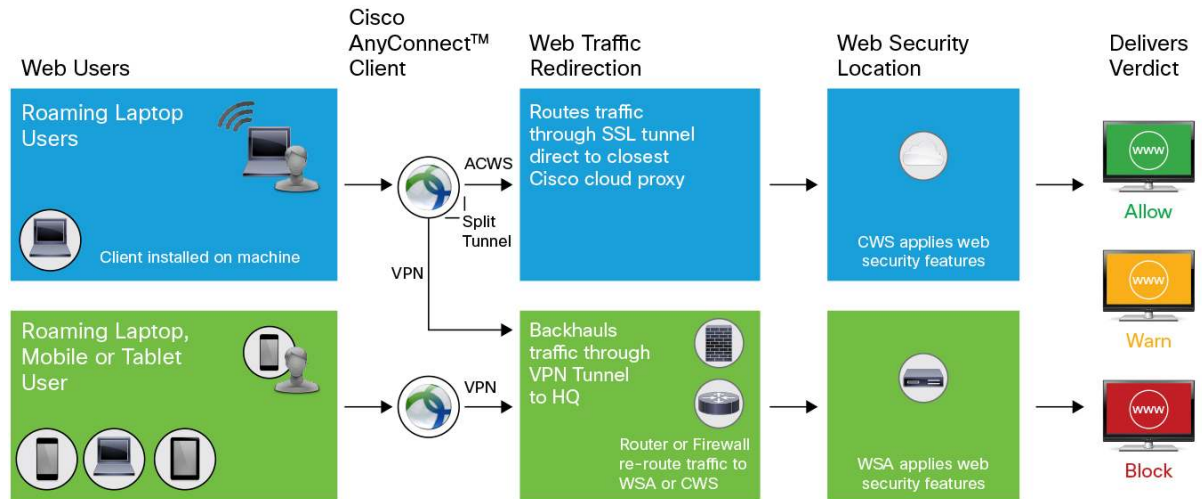
Cisco Cloud Web Security (CWS): Delivers a simple web security solution that does not require any additional hardware. It can function standalone or can provide increased protection by connecting existing network equipment to cloud-based web security services using existing browser settings and PAC files.



Cisco AnyConnect® Secure Mobility Client:

- On-premises: Enables remote clients to undergo web security services by requiring traffic to be redirected through a VPN tunnel back to the on-premises solution (Figure 3).
- In the cloud: Safeguards web-based transactions on mobile devices by dynamically initiating an SSL tunnel to redirect web requests directly to the Internet via the closest data center (Figure 3).

Figure 3. Protect Roaming Users with the Cisco AnyConnect Secure Mobility Client



Why Cisco?

In today's highly connected and increasingly mobile world, only Cisco Web Security delivers the strong protection, complete control, and investment value you need. Cisco Web Security solutions provide best-in-class uptime, zero-day threat protection, and seamless integration with Cisco's market-leading family of security offerings. Users are protected everywhere, all the time, with Cisco's unparalleled global threat intelligence infrastructure. A single management interface delivers global control with policies that provide dynamic, context-based control of web applications by assessing a user's location, profile, and device. Cisco Web Security minimizes costs with fewer devices, faster integration, and simplified training. Resolve issues and avoid downtime with Cisco's world-class, 24x7 support.

For more information on Cisco Web Security solutions and deployment options, visit <http://www.cisco.com/go/websecurity>.



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.

Recycling symbol: 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)