Cisco Cloud Web Security

Cisco® Cloud Web Security (CWS) is a different, more comprehensive, cloud-delivered web defense solution. It provides industry-leading, real-time protection and thorough enforcement of web usage policies.

Product Overview

Hacking has become a recognized industry today, supporting sophisticated and well-funded criminal enterprises. Attacks are also evolving continually, becoming more damaging and harder to detect. Traditional web security methods can block known threats but are not able to adapt to the changing threat landscape. And they don't address advanced malware.

Perimeter defenses don't address how your users access information and resources. Now it isn't just people outside your organization who are of concern; your own users may consume excess bandwidth or access inappropriate content that can put your organization at risk. Their personal devices may introduce malware from inside the firewall.

Built on an unrivaled global threat visibility network, Cisco CWS offers the most effective protection against advanced and targeted threats and continuous monitoring of both network and file behavior. It identifies threats operating in the environment with Cisco Advanced Malware Protection (AMP) and Cognitive Threat Analytics (CTA).

Cisco CWS controls web usage and blocks sites based on signature, reputation, and content analysis. CWS also delivers best-in-class malware scanning through outbreak intelligence, a heuristics-based engine that analyzes each webpage component in real time to block threats.

Cisco AMP protects against advanced malware threats, using file retrospection to track a file's disposition over time. Cisco CTA uses continuous capabilities to scan for symptoms of a breach, reducing the time to discover threats that bypass perimeter defenses.

As a cloud service, Cisco CWS delivers superior flexibility. You can easily deploy and scale the service with multiple connection options while using the existing infrastructure. A single management interface provides global control, providing enforcement of very detailed web usage policies across an entire organization no matter where users are located. Through Cisco AnyConnect®, Cisco CWS extends its strong protection to roaming laptop users and enforces the same on-premises policies.

Our advanced global threat visibility network continually updates Cisco CWS against the latest threats, and the most actionable cloud-delivered intelligence reporting helps ensure superior visibility into web usage. Top-tier data center facilities in 23 locations around the globe deliver a service-level agreement (SLA) of 99.999 percent uptime, so that information is always available. Cisco CWS also comes with Cisco's award-winning 24-hour support.

Features and Benefits by License

Several licenses are available: Cisco CWS Essentials (the base CWS offering for new and renewing customers), CWS Premium (for new and renewing customers, including all features from the CWS Essentials bundle in addition to AMP and CTA), Advanced Threat Detection, and Log Extraction à la Carte. The major features of each are described in Tables 1, 2, and 3.

Table 1. Cisco CWS Essentials License

Feature	Description
Web filtering	Control web access to more than 50 million known websites by applying filters from a list of over 75 web categories.
Malware scanning	Increase catch rate with an intelligent multiscanning technology that divides web traffic into functional elements and efficiently analyzes it in real time.
Outbreak intelligence	Identify unknown and unusual behaviors and zero-hour outbreaks through a heuristics-based antimalware engine. Outbreak Intelligence runs webpage components in a virtual emulation environment before permitting user access. Using proprietary "scanlet" engines for Java, PDF, executables, and more, outbreak intelligence opens up the individual components of a webpage to determine how each component behaves and block any malware.
Web reputation	Restrict website access based on site reputations. Analyze data such as the domain owner, the hosting server, the time created, the type of site requested, and more than 50 other distinct parameters to provide a reputation score for the site requested.[1]
Application visibility and control	Increase employee productivity by controlling access to webpages, individual web parts or micro applications so employees can access sites needed for work without unnecessary distractions while simultaneously preventing access to inappropriate content.
Dynamic content analysis	Defend against compliance, liability, and productivity risks by combining traditional URL filtering with real-time dynamic content analysis (DCA). The DCA engine automatically categorizes the content of an unknown URL by analyzing the content of the page itself, scoring relevancy to web categories (such as pornography, hate speech, gambling, and illegal downloads) and blocking the page if it conflicts with web security policies.
Centralized management and reporting	Receive actionable insight across threats, data, and applications. A powerful centralized tool controls both security operations, such as management, and network operations, such as analysis of bandwidth consumption. Administrators have access to a variety of predefined reports and can create customized reports and notifications. All reports are generated and stored in the cloud, so they are delivered in seconds as opposed to hours. Reports can be also be saved and scheduled for automated delivery. These capabilities provide flexibility, offering detail down to the user level, and help enable administrators to spotlight potential issues quickly.
Roaming laptop user protection	Protect roaming users with the same in-house policies through Cisco AnyConnect. AnyConnect® routes all roaming web traffic through an SSL tunnel directly to the closest Cisco cloud proxy and enforces the same security features that are on premises. By eliminating the need to backhaul web traffic through VPN, Cisco CWS relieves web congestion at the headquarters, reducing bandwidth use while improving the end-user experience.

The Cisco CWS Premium license, shown in Table 2, includes all features from the Cisco CWS Essentials bundle and adds AMP and CTA.

Table 2. Cisco CWS Premium License

Feature	Description
Cisco AMP (also available as an add-on)	Protect against the latest and most advanced forms of malware with AMP's detection and blocking, continuous analysis, and retrospective alerting. It uses the vast cloud security intelligence networks of both Cisco and Sourcefire (now part of Cisco). Cisco AMP augments the antimalware detection and blocking capabilities already offered in Cisco CWS with enhanced file reputation capabilities, detailed file sandboxing, and file retrospection. The only solution with all of these capabilities, Cisco AMP tracks a file's disposition over time inside the network perimeter. If a file is later found to be malicious, file retrospection identifies where the file entered and where it traveled to help in the remediation process. Learn more.
CTA (only available packaged with AMP)	Reduce the time to discovery of threats operating inside the network. CTA addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection. Unlike traditional monitoring systems, Cisco CTA relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees and adapt over time. Learn more.

[1] Protect against URL-Based Threats.

Table 3. Advanced Threat Detection and à la Carte Licenses

Feature	Description
Log extraction can be added to any existing Cisco CWS license. It is ideal for customers with 4,000 seats or more.	
Log extraction API	Automatically pull web usage data quickly for highly secure analysis with an S3-compatible HTTPS API. Log data is compiled in W3C text format that can be correlated with existing data using a variety of reporting and analysis tools such as security information and event management (SIEM). Log information consisting of more than 20 attributes is available within 2 hours of the event.

Table 4. Web Security Bundle

Feature	Description
Web Security Bundle	The Web Security bundle is comprised of the WSA and CWS so customers can consume Cisco Web Security across Cloud or On Premises. The bundle includes: • **WSA Premium**: Combines URL filtering defense with deep content scanning (Web Usage Controls, Web Reputation, Sophos Anti-malware, Webroot Anti-malware and Software Subscription Support); includes license for Web Security Virtual Appliance. See WSA Datasheet for more details. • **CWS Essentials:** See above • **Web Reporting Application (optional):** The Cisco Web Security Reporting Application provides a single pane of glass for monitoring your web security regardless of deployment. It includes a customized Splunk application and a Splunk server 6.2.x in one seamless installation. It polls log data collected from multiple WSAs and CWS for Splunk's predefined reports. Customers can also perform ad hoc searches using the flash timeline view and web-tracking forms. • **Log Extraction (optional):** See above • **AMP:** See above

Advanced threat detection is an add-on license that includes Cisco AMP and CTA (see descriptions above) and is available to customers with a current CWS Essentials license.

These benefits are included with all Cisco CWS licenses.

Talos Security and Research Group: With a 24-hour view into global traffic activity, Talos analyzes anomalies, uncovers new threats, and monitors traffic trends. Talos generates new rules and updates every 3 to 5 minutes, providing threat defense hours and even days ahead of competitors. Receive fast and comprehensive web protection backed by one of the largest threat-detection networks in the world, with the broadest visibility and largest footprint based on:

- 130 billion web requests served by Cisco CWS per month
- 3.6 petabytes of bandwidth pumped through Cisco CWS monthly
- 100 TB of intelligence gathered daily
- 4.9 billion antivirus and web filtering blocks per month
- 1.6 million sensors
- Support on all major operating systems and platforms

World-class support: Resolve issues rapidly with direct, 24-hour access to Cisco experts available in more than 10 JD Power award-winning security support centers. Support for Cisco CWS software subscription includes:

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

Industry-leading uptime: Help ensure data protection with top-tier data center facilities that deliver an SLA of 99.999 percent uptime. With automatic updates from Talos, Cisco CWS stays current with the latest threat information. Security is always on and available, freeing your staff to focus on other priorities.

Deployment

Cisco CWS Traffic Redirection Connection Methods

Cisco CWS runs as a service on Cisco appliances, including the Cisco Adaptive Security Appliances (ASA and ASAv), Cisco Integrated Services Router (ISR) G2, and the Cisco Web Security Appliances (WSA and WSAv). These redirect traffic to Cisco CWS for web security functions.

Next-Generation Firewall (Cisco ASA/ASAv): Capitalize on your Cisco ASA investments by offloading content scanning to Cisco's cloud through Cisco CWS. Apply acceptable-use policy to the company, groups, or individual users.

Cisco Web Security Appliance (WSA/WSAv): Integrate Cisco CWS and Cisco WSA to so that identity information can be sent to the cloud, and extend other on-premises enterprise features to CWS customers.

Cisco ISR G2: Save bandwidth, money, and resources by intelligently redirecting Internet traffic from branch offices directly to the cloud to enforce security and control policies. Apply acceptable-use policy to all users regardless of location.

Cisco AnyConnect Secure Mobility Client: Authenticate and redirect web traffic whenever the end user is off the corporate network. Cisco CWS uses cached user credentials and directory information when they are away from the office or VPN, helping to ensure that exactly the same web usage policies are applied.

Standalone Deployment: Deploy a simple web security solution that does not require any additional hardware. Connect to the Cisco CWS service using existing browser settings and Proxy Auto-Config (PAC) or Web Proxy Auto-Discovery (WPAD) files.

Every Cisco CWS deployment option includes directory authentication methods that enhance end-user identification, enabling administrators to apply precise filter controls at the user or group level and run detailed log reports.

Subscriptions

All Cisco Cloud Web Security subscriptions are term-based subscriptions of 1, 3, or 5 years.

Seat-Based Subscription

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

Bandwidth-Based Subscription

Customers can consume Cisco CWS on a bandwidth basis by aggregating the total traffic across various deployment sites that will be directed to CWS data centers.

Security Enterprise License Agreements

Cisco Security Enterprise Licensing Agreements (ELAs) offer simplified license management and license costs savings through a single agreement. Customers with ELA v3 can add CWS Essentials, and customers with ELA v4 can add CWS Premium, all at no additional cost. To learn more about Security Enterprise License Agreements, talk to your Cisco account representative.

Software Subscription Support

Every Cisco CWS subscription also includes the following support benefits:

- Automatic application of patches, software updates, and maintenance to the Cisco cloud to keep applications and platform software current
- Access to the Cisco Technical Assistance Center (TAC) 24 hours a day, 7 days a week
- Online repository of application tools, technical documents, and training
- Registered access to Cisco.com for online technical information and service request management

Services

Cisco takes a threat-centric approach to security to protect network infrastructures and assets on the network. Our services help you take full advantage of security appliances and systems you've installed.

Cisco Branded Services

We've identified four actions that are essential for successful security deployments: assessment, integration, optimization, and management.

Cisco Security Planning and Design Service: Helps you develop and implement a robust security solution quickly and cost-effectively with:

- Security technology readiness assessment
- Security design development
- Security implementation engineering
- Security knowledge transfer

Cisco Web Security Configuration and Installation Service: Helps mitigate web security risks by installing, configuring, and testing to implement:

- Acceptable use policy (AUP) controls
- Reputation and malware filtering
- Data security
- Application visibility and control

Cisco Security Optimization Service: Helps you evaluate and strengthen your network's ability to prevent, detect, and mitigate threats. This service combines network security assessment, design, support, and learning activities in one comprehensive subscription package.

Cisco Managed Threat Defense: Provides dynamic real-time detection and remediation against known vulnerabilities as well as advanced persistent threats. Cisco provides the hardware, software, and expertise to deliver threat defense in a subscription-based model through a global network of security operation centers.

Collaborative/Partner Services

A wide range of valuable services from Cisco partners is available across the planning, design, implementation, and optimization lifecycle. These include:

Cisco Network Device Security Assessment: Helps you implement and maintain a hardened network device environment by identifying gaps in your Cisco network infrastructure security.

Smart Care Service (provided by a Cisco Certified Partner): Helps you simplify network maintenance through proactive network monitoring, assessments, software repairs, and technical support.

Other Services

Cisco Product Security Incident Response Team (PSIRT): The Cisco PSIRT is a dedicated global team that manages the receipt, investigation, and public reporting of security vulnerability information related to Cisco products and networks.

Cisco Secure Development Lifecycle (CSDL): This is a repeatable and measurable process designed to increase the resiliency and trustworthiness of our products.

More information on Cisco Services is available at: http://www.cisco.com/en/US/products/hw/vpndevc/services.html.

Financing

Cisco Capital® is uniquely positioned to provide highly competitive financing options for Cisco hardware, software, and services. Financing solutions can be customized according to your specific needs and include competitive rates, flexible terms, and migration options. This flexibility helps reduce the overall cost of acquisition, preserve capital, proactively manage lifecycles, and protect against obsolescence.

Warranty Information

Find warranty information on Cisco.com at the Product Warranties page.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

Find out more at http://www.cisco.com/go/cws. Evaluate how Cisco CWS 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.

Printed in USA C78-729637-05 08/15