Data Sheet

Cisco Cloud Web Security

Today’s highly connected and fast-moving world is filled with complex and sophisticated web security threats. Cisco delivers the strong protection, complete control, and investment value that businesses need. We offer the broadest set of web security deployment options in the industry, each of which brings to bear Cisco’s unparalleled global threat intelligence infrastructure. With a proven mature and scalable platform, Cisco has a proven track record of stopping more malware than any other cloud security service.

Overview

Cisco® Cloud Web Security (CWS) provides industry-leading security and control, with best-in-class uptime, unmatched zero-day threat protection, and advanced policy capabilities that enable dynamic, context-based application controls. Administrators can select specific categories for intelligent HTTPS inspection, and a single management interface delivers global control and comprehensive reporting. When using CWS, ssers are protected everywhere, all the time through Cisco’s worldwide threat intelligence footprint. CWS also comes with Cisco’s award-winning 24-hour support.

As a cloud service, Cisco Cloud Web Security offers ease of deployment, a 30 to 40 percent lower cost than on-premises products, and the ability to centrally set and enforce policies for an entire organization, regardless of where users are located. CWS also uses the power of cloud computing to stop threats.

Cisco Cloud Web Security enhances the Cisco network infrastructure by using its built-in connector capability to tightly integrate with Cisco ASA firewalls, Cisco ISR Generation 2 (ISR G2) routers, Cisco Web Security Appliances, and the Cisco AnyConnect® Secure Mobility Client. This integration enables web traffic to be redirected to the CWS cloud using criteria such as user identity, empowering businesses to extend web security across their infrastructure, including branches and devices used by roaming users.

Features and Benefits

Threat Intelligence	Receive fast and comprehensive web protection backed by the largest threat-detection network in the world, with the broadest visibility and largest footprint, including • 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 percent of the world's enterprise email traffic Cisco Security Intelligence Operations (SIO) provides a 24-hour view into global traffic activity that enables Cisco to analyze anomalies, uncover new threats, and monitor traffic trends. Cisco SIO generates new rules and updates every three to five minutes, providing threat defense hours and even days ahead of competitors.
Real-Time Malware Scanning	Defend against malware and advanced persistent threats using multiple layers of antimalware technologies and intelligence from Cisco SIO updated every three to five minutes. Cisco Cloud Web Security detects and proactively blocks threats in real time through a comprehensive approach. Signature inspection is used to identify known threats. Intelligent multiscanning optimizes efficiency and the catch rate by determining which scanning engine to use for signature inspection based on reputation and content type. Cisco Outbreak Intelligence, a heuristics-based engine, identifies unusual behaviors and zero-hour outbreaks. Outbreak Intelligence works by running webpage components in a separate test area before permitting user access. Using proprietary "scanlet" engines for Java, Flash, PDF, and more, Outbreak Intelligence opens up the individual components of a webpage to determine how each component behaves and to block malware present.
Application Visibility and Control	Control the use of hundreds of Web 2.0 applications, such as Facebook, and more than 150,000 microapplications, such as Facebook games. Cisco Cloud Web Security combines identity, time, content, location, and outbound compliance to build and maintain an application policy.
URL Filtering, Dynamic Content Analysis, Real-Time Categorization	Defend against compliance, liability, and productivity risks by combining traditional URL filtering with real-time dynamic content analysis (DCA). Cisco's continuously updated URL-filtering database of more than 50 million blocked sites provides exceptional coverage for known websites, while the DCA engine accurately identifies top categories of unknown URLs in real time.
Secure Mobility	Protect roaming users by integrating with the Cisco AnyConnect Secure Mobility Client, which dynamically initiates a highly secure tunnel that directs all external web traffic to the closest Cisco Cloud Web Security proxy for real-time analysis prior to permitting access.
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, offer granularity down to the user level, and enable administrators to spotlight potential issues quickly.
Outbound Content Control	Block sensitive information from leaving the safety of the network, helping to ensure compliance and reduce risk. Cisco Cloud Web Security protects data by controlling the type of web content that is uploaded, using criteria such as file name, file type, webpage keywords, or other preconfigured IDs to identify and mitigate potential risks. This content control is in addition to the Cisco Application Visibility and Control monitoring of outbound content such as file-sharing applications.
Industry-Leading Uptime	Help ensure data protection with 99.999 percent availability and uptime. Cisco Cloud Web Security requires less time spent troubleshooting. With automatic updates from Cisco SIO, CWS stays tuned against the latest threats without intervention. Once initial automated policy settings go live, staff are freed up to focus on other priorities.

Deployment

The Cisco Cloud Web Security service forwards web traffic to assigned proxies in CWS data centers, which scan it for malware and policy enforcement. An organization can connect to the CWS service directly or through connectors integrated into Cisco network products. CWS scales with the number of users employing the service.

The Cisco Cloud Web Security solution can be deployed by using a proxy auto-configuration (PAC) file either as an explicit proxy or as a transparent proxy using existing Cisco ISR G2 routers, ASA firewalls, and WSA devices as connectors. Deploying CWS using a transparent proxy through a connector enables a business to get the most out of its existing infrastructure and offloads scanning from the hardware appliances to the cloud, lessening the burden on the hardware and reducing network latency. CWS is also effective when deployed directly, providing every benefit of Cisco's industry-leading web security solution with 99.999 percent uptime and no hardware installation or maintenance.

Direct to Cloud

Cisco Cloud Web Security

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

Cloud Connection Methods

Includes software for on-premises appliances like Cisco ASA 5500-X Series Next-Generation Firewalls, Cisco ISR Generation 2 (ISR G2) Routers, and Cisco Web Security Appliances, redirecting traffic to CWS for web security functions.

Cisco ISR G2 Router with CWS Connector

Saves bandwidth, money, and resources by intelligently redirecting Internet traffic from branch offices directly to the cloud to enforce security and control policies.

Cisco ASA Firewall with CWS Connector

Integrates Cisco ASA Software Release 9.0 with Cisco Cloud Web Security to solve the combined problems of performance and breadth of security without affecting data center and network complexity.

Cisco Web Security Appliance with CWS Connector

Moves processing to the cloud, lifting the content scanning and policy load from the on-premises WSA and centralizing the management of access policies in the cloud.

Cisco AnyConnect Secure Mobility Client

Safeguards web-based transactions on roaming devices by dynamically initiating an SSL tunnel to redirect web requests directly to the Internet via the closest data center.

Although only one deployment method is needed, Cisco Cloud Web Security can integrate with multiple Cisco network infrastructure elements to enhance flexibility and capability. For example, you can deploy CWS through ISR G2 routers at branch offices to easily extend security coverage without backhauling Internet traffic. You can use a WSA at headquarters to take advantage of advanced proxy capabilities. Or you can deploy the AnyConnect Secure Mobility Client to protect roaming users.

Every Cisco Cloud Web Security deployment option has built-in user authentication methods that enable end-user identification. These include authentication built into connectors, as well as clientless cookie-based authentication methods that work independently or with a connector. The range of authentication options makes available a variety of methods for directory integration, including NT LAN Manager (NTLM), Security Assertion Markup Language (SAML), and IP surrogates. These directory integration methods allow you to set granular policies based on usernames and groups as well as to log the web activity of each individual.

Licensing

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 the number of users, not devices. Sales and partner representatives can help to determine the correct tier for each customer deployment.

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, highly secure, and operating at peak performance. This support entitles customers to the services listed below for the full term of the purchased software subscription:

- 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
- Additional knowledge and training opportunities through collaborative learning

Services

Cisco Branded Services	Cisco Security Planning and Design: Enables deployment of a robust security solution quickly and cost-effectively. Cisco Web Security Configuration and Installation: Mitigates security risks by installing, configuring, and testing solutions. Cisco Security Optimization: Supports an evolving security system to address security threats, design updates, performance tuning, and system changes.
Collaborative/Partner Services	Network Device Security Assessment: Helps maintain a hardened network environment by identifying gaps in network infrastructure security. Smart Care: Provides actionable intelligence gained from highly secure visibility into a network's performance. Additional services: A wide range of valuable services provided by Cisco partners across the planning, design, implementation and optimization lifecycle.
Cisco Financing	Cisco Capital® can tailor financing solutions to business needs. Access Cisco technology sooner and see the business benefits sooner.

Warranty Information

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

For More Information

Find out more at http://www.cisco.com/go/cloudwebsecurity. Evaluate how Cisco Cloud Web Security 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