Cisco Cloud Web Security: A Key Component of a Unified Security Architecture

Marketing/Technical description for services

Scope of the Service

Cisco Cloud Web Security (previously known as ScanSafe) builds on the value of the Cisco network infrastructures that customers have already deployed and encourages the incremental adoption of Cisco security solutions. Customers have the ability to procure the service based on the number of users or the expected monthly bandwidth consumption across all their locations.

As a cloud service, Cloud Web Security 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 detailed web-usage policies across an entire organization no matter where users are located or on what device. Through the Cisco AnyConnect$^{\text{®Secure Mobility Client}}$, Cloud Web Security extends its strong protection to roaming laptop users and enforces the same on-premises policies.

Web security products protect against both inbound malware threats and outbound data leakage threats and are increasingly tapped by other security components to leverage their threat intelligence data for better situational awareness. The underlying security functions remain the same, but the components are now increasingly able to communicate threat intelligence data. This interoperability results in the ability to automate the process of calibrating the security posture to changing threat conditions. Network, Web, and messaging security continue to address the common weak points targeted by attackers, but they can now fine-tune their detection mechanisms. This additional situational awareness enables identity, authentication, and authorization products to be extended to cloud-based services to bolster the user experience by tying together multiple services with single sign-on.

Cisco Threat-Focused Web Protection

Cisco's offerings include IronPort-branded Web security gateway appliances and Cisco Cloud Web Security, an SaaS solution. An on-premises/cloud configuration is also available for Cisco Web Security Appliance/Service deployments via a hybrid licensing offering.
Cisco added the AMP capabilities to its Web Security, Cloud Web Security, and Email Security gateways. The integration adds file reputation functionality, file analysis sandboxing via Cisco's ThreatGRID acquisition, and a feature called "file retrospection" to identify malicious files that are designed to appear benign to antimalware inspection engines but are programmed to become malicious at a later time. The features require an additional license.

Essential Guidance

Web security will continue to be the entry point of most attacks. The following measures could enable any organization to begin building the bridges necessary for a unified defense:

□ **Assess risk:** Thoroughly analyze existing security investments before rationalizing the purchase of emerging technologies. Consider ways to gain more value from existing security investments. Identify and evaluate technologies designed to bridge communication gaps in existing security solutions.

□ **Increase visibility:** Real-time content and security scanning is an essential part of Web security protection. Be more proactive about generating reports to gain visibility into which users and groups consistently generate the most risk. Assess the security infrastructure protecting the organization's key assets. Identify the at-risk employees with privileges to those key assets, and address the security policies and enforcement mechanisms that mitigate the increased risk posed by those employees.

□ **Monitor proactively:** Move from highly fragmented and poorly implemented defenses to predictive protection. This includes evaluating the usefulness of threat intelligence and contextual awareness gleaned from existing monitoring solutions deployed on the network.

□ **Examine response:** Identify process and technology gaps that hinder incident response and remediation from silicon to cloud. Give incident responders the right tools to efficiently carry out remediation activities. Review recent incidents and address process breakdowns. Consider improvements that extend existing policies and automate response as much as possible to give IT security time to address the most critical issues.

Features and Benefits by License

Several licenses are available. Cloud Web Security Essentials is the base offering for new and renewing customers. Other bundles and individual options are also available. The major features of each license are described in follow.

Table 1. 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 the 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 blocks any malware.
Web reputation	Restrict website access based on site reputation. 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 microapplications so that employees can access the sites needed for work without unnecessary distractions. Simultaneously prevent 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 dashboards and set 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, Cloud Web Security relieves web congestion at the headquarters, reducing bandwidth use while improving the end-user experience.

The Cloud Web Security Premium license, shown in Table 2, includes all the features from the Cloud Web Security Essentials bundle and adds AMP and Cognitive Threat Analytics.

Table 2. Premium License

Feature	Description
Cisco AMP (also available separately)	Protect against the latest and most advanced forms of malware with AMP's detection and blocking, continuous analysis, and retrospective alerting. AMP uses the vast cloud security intelligence networks of both Cisco and Sourcefire (now part of Cisco). AMP augments the antimalware detection and blocking capabilities already offered in Cloud Web Security 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.
Cognitive Threat Analytics (also available separately)	Reduce the time to discovery of threats operating inside the network. Cognitive Threat Analytics 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, it relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

Table 3. Advanced Threat Detection and A la carte Licenses

Feature	Description
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 typically available within 15 minutes of the event. Log extraction can be added to any existing Cloud Web Security license. It is ideal for customers with 4000 seats or more.
Data retention	Data for blocked web requests (policy or malware blocks) is retained for one year, and allowed data is retained for 45 days. Customers can retain data for longer periods to match the terms of their subscription.

Cloud Web Security Traffic Redirection Connection Methods

Cloud Web Security allows for flexible deployment options that include Cisco appliances... or not. There are many ways to redirect traffic to the Cloud Web Security web proxy. Redirection can be accomplished through the Cisco Adaptive Security Appliances (both physical and virtual), Cisco Integrated Services Routers (ISR) G2, Cisco 4000 Series Integrated Services Routers (through generic routing encapsulation over IPsec) and the Web Security Appliances (physical and virtual). These redirect traffic to Cloud Web Security for web security functions.

Next-Generation Firewall (Cisco Adaptive Security Appliances, physical and virtual): Capitalize on your Adaptive Security Appliance investments by offloading content scanning to Cisco's cloud through Cloud Web Security. Apply acceptable-use policy to the company, groups, or individual users.

Web Security Appliance (physical and virtual): Integrate Cloud Web Security and the Web Security Appliance so that identity information can be sent to the cloud. And extend other on-premises enterprise features to Cloud Web Security customers.

Cisco ISR G2: Save bandwidth, money, and resources and improve Internet speed at the branch 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 4000 Series ISR: Get the same benefits of redirecting through the ISR G2. At the same time, you reduce maintenance costs by adopting industry-standard GRE over IPsec technology that is reliable, well understood, and mature. See Controlled Availability notification for more information

AnyConnect Secure Mobility Client: Authenticate and redirect web traffic off the corporate network whenever the end user is. Cloud Web Security uses cached user credentials and directory information when users are away from the office or connecting through a VPN, helping to ensure that the same web usage policies are applied.

Standalone deployment: Deploy a simple web security solution that does not require additional hardware. Connect to the Cloud Web Security service using existing browser settings and Proxy Auto-Configuration (PAC) or Web Proxy Auto-Discovery (WPAD) files.

Every Cloud Web Security 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.

Announcing Email Security for Office 365

Did you know that Cisco customers moving to Office 365 can deploy the same industrial strength email protection they get from our Email Security Appliance (ESA) and it's called Cloud Email Security (CES) so these customers also have the added flexibility of having it delivered from the cloud!

For more information :

http://www.cisco.com/go/cws

Data Sheet :

http://www.cisco.com/c/en/us/products/collateral/security/cloud-web-security/data_sheet_c78-729637.html