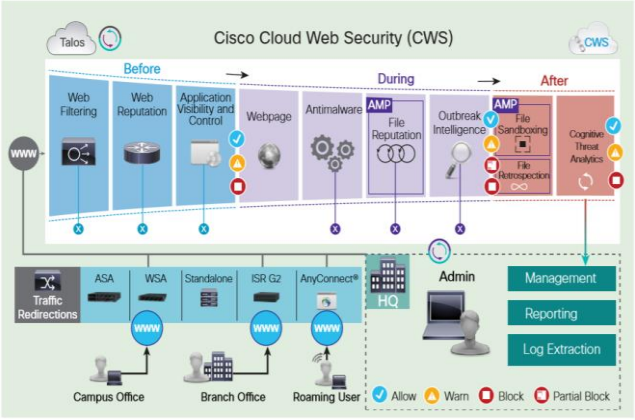
CISCO CLOUD SERVICES – WEB SECURITY

CLOUD MANAGED SECURITY

Cisco Cloud Web Security (CWS) provides comprehensive cloud-delivered web defence through industry-leading, real-time protection and the power of Cisco Advanced Malware Protection (AMP). Defend with best-in-class outbreak intelligence, malware scanning, and web and URL filtering, and get the easiest enforcement of granular web usage policies.

CWS provides superior flexibility to easily deploy and scale with multiple connection options using your existing infrastructure. Take advantage of the most local data center coverage and uptime, and leverage the most actionable cloud-delivered intelligence reporting, while knowing your web security is part of a broader Cisco Security solution.



DELIVER SECURITY AS A SERVICE

Meet a very different security approach from Cisco: comprehensive web security as a cloud service. With the Cisco Cloud Web Security (CWS) solution, Cisco is delivering intelligent cybersecurity for the real world. We provide superb visibility, consistent control, and advanced threat protection before, during, and after an attack.

As a cloud-delivered web security solution, Cisco CWS offers extensive security as a service (SaaS). Deployment is simple and fast. No maintenance or upgrades are required.

With Cisco CWS, administrators can set and enforce specific web use policies across the entire environment. Users can connect Cisco CWS to their existing infrastructure with flexible network integration options. Cisco CWS controls access to websites and specific content in Web pages and applications. Cisco's analysis engines deliver continual industry-leading antimalware and zero-day threat protection against web-based attacks. Our advanced global threat telemetry network continuously updates Cisco CWS against the latest threats.

Cisco Advanced Malware Protection (AMP) protects against advanced malware and tracks file disposition over time to see where malicious files travel. Cognitive Threat Analytics (CTA) scans web traffic for symptoms of an infection and addresses threats that bypass perimeter defenses. And centralized management and reporting provide increased visibility into web usage and threat information.

ADVANCED THREAT PROTECTION

Cisco AMP protects your environment across the attack continuum: before, during, and after an attack. The file reputation feature allows Cisco to capture a fingerprint of each file as it traverses the Cisco Content Security gateway during an attack. We send the fingerprints to AMP's cloud-based intelligence network for a reputation verdict.

After an attack, with the file sandboxing feature, you can run unknown files in a highly secure sandbox to determine the threat level and update other security components. Then, using file retrospection, you can track a file's disposition over time after it enters your environment. If it is found to be malware, you can discover where the file entered and traveled and mitigate future intrusions.

Our cloud-based CTA feature helps reduce threat identification time to minutes with its continuous efforts. CTA actively identifies symptoms of a malware infection through behavioral analysis, anomaly detection, and machine learning. And with the Cisco Talos Security Intelligence Research Group, among the largest threat detection networks in the world, leading researchers and systems continuously deliver security intelligence to Cisco CWS based on threat tracking across networks, endpoints, mobile devices, virtual systems, the web, and email around the globe.

SUPERIOR FLEXIBILITY

Cisco CWS is backed by a worldwide network and 23 data centers with service-level agreements (SLAs) based on 99.999 percent uptime. You can tailor visibility into your web usage with more than 10,000 customizable reports, updated every 10 minutes, and the ability to categorize traffic by user and application traffic. Web usage data may also be accessed quickly and with a high degree of security by a variety of reporting and analysis tools such as security information and event management (SIEM).

BENEFITS

- Granular web use policies: Set and enforce across the entire environment for applications, websites and specific webpage content.
- Easy to integrate: With flexible network integration options, you can connect Cisco Cloud Web Security (CWS) to your existing infrastructure.
- Real-time threat intelligence: Analysis engines deliver industry-leading antimalware and zero-day threat protection from web-based attacks. Our advanced global threat telemetry network continuously updates Cisco CWS to protect against the latest threats.
- Centralized management and reporting: Increased visibility into web usage and threat information.

CLOUD MANAGED SECURITY

The service is offering enterprise class web security solution in the cloud. Built on an unrivaled global threat visibility network and based on Cisco CWS it 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).

On top of that, ComuTel adds expert level planning, installation and design services as well as extended and pro-active support acting as a single point of contact for the customer problems. These services are built on the solid foundation, a set of services, rules and procedures for remote monitoring, precise diagnostics, timely troubleshooting and policy deployment bound to strict SLA.

COMUTEL ADDED VALUE

Expert level consultancy, planning, installation and design services during plan and design phases of the project.

Extended and pro-active support including single point of contact for the customer problems, incident tracking and resolution, configuration and change management, pro-active monitoring and regular reporting.

SERVICE FEATURES

- **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;
- **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;
- **Advanced Malware Protection** - Protect against the latest and most advanced forms of malware with AMP's detection and blocking, continuous analysis, and retrospective alerting;
- **Cognitive Threat Analytics** - 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, CTA relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees and adapt over time.

SERVICE PACKAGE OFFERINGS

- Standard: This package includes consultancy, planning, installation and design services during plan and design phases of the project as well as basic reactive support and warranty with SLA.
- Premium: This package incorporates all features of the standard offering as well as pro-active support services, consultancy and reporting with SLA.

PRICING STRUCTURE

Cloud Managed Security pricing components typically include one-time costs and monthly recurring costs

ONE-TIME COSTS

- Planning
- Design and deployment
- Physical Installation and cabling
- System setup and functional testing
- Hardware spares
- Fees for one time vulnerability scan

MONTHLY COSTS

- Management fees associated with incident, configuration and change management
- Vendor subscription costs
- Reporting
- Vulnerability scanning (if purchased as an option)