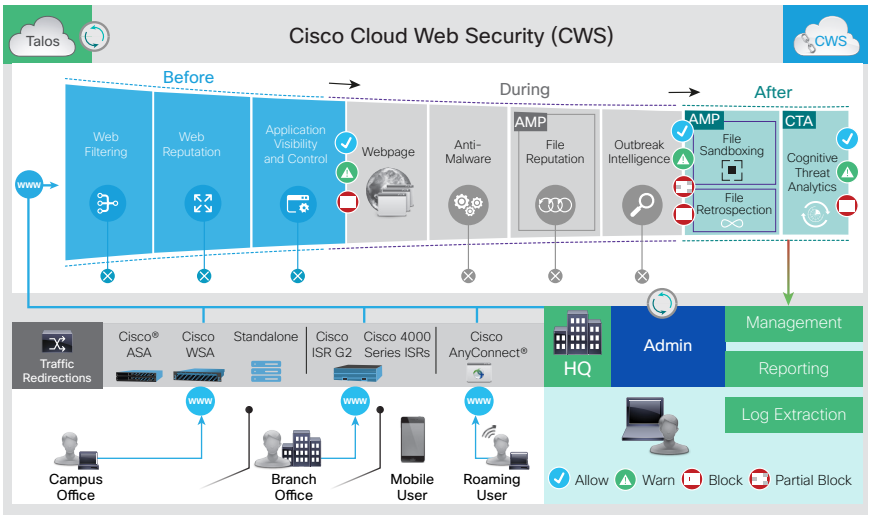
At-a-Glance

Cisco Cloud Web Security

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 as well as 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.

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 Web Security Pillars

Comprehensive Defense

Through web filtering and web reputation scoring, Cisco CWS controls access to more than 50 million known websites by applying filters from a list of more than 75 content categories. Our application visibility and control features include acceptable use policy that increases employee productivity and compliance. These controls cover access to web pages, individual web parts and microapplications so employees can access sites needed for work. Centralized policy management helps you enforce policies and manage the entire solution across all branches and users from a single centralized location that is accessible anywhere, at any time.

Real-time malware protection is based on the identification of unknown, unusual behaviors and zero-hour outbreaks through a heuristics-based, antimalware engine. Outbreak intelligence runs webpage components in a highly secure virtual emulation to determine how each component behaves and blocks any malware. Roaming users are protected with Cisco AnyConnect®, which enforces the same security features available with Cisco CWS in your company's offices. A secure mobile browser provides protection for mobile devices.

Advanced Threat Protection

Cisco AMP and Threat Grid 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 customer network. These fingerprints are sent to AMP's cloud-based intelligence network for a reputation verdict.

After an attack, 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 where it is currently located to 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).

You can also save time and money by redirecting traffic to Cisco CWS through existing Cisco products such as the Cisco Integrated Router G2 and ISR 4000, Cisco Adaptive Security Appliances (ASA and ASAv) next-generation firewalls, Cisco Web Security Appliances (WSA and WSAV), and the Cisco AnyConnect Web Security Module. You can also connect to Cisco CWS in a standalone deployment.

Next Steps

Find out more at http://www.cisco.com/go/cloudwebsecurity.

C45-730902-03 02/16