# Cisco Secure Web Appliance

## Protection, Control, Visibility, and Value

### The internet is indispensable, but not secure. How do you confidently protect your devices and resources while also allowing users access to the web, social media, and SaaS applications?

You need a variety of protections against today's fast- evolving cyber threats, malware, and ransomware. Only Cisco provides:

- An all-in-one web gateway, when you need a physical or virtual appliance, with class-leading threat intelligence and more comprehensive control than is offered by next-gen firewalls
- A seamless user integration when you also require cloud-delivered web gateway protection, with Cisco Umbrella
- Integration and entitlement to Cisco SecureX, our open orchestration and XDR platform that accelerates incident response

## Benefits

- **Protects devices with** sophisticated global threat intelligence from the Cisco Talos® threat research team
- **Comprehensive control** of web traffic, including dynamic web content like social media applications
- **Enhanced threat response with** greater visibility and automation that speeds incident response, with included Cisco SecureX™ entitlement
- **Rapidly check system status** and troubleshoot via the System Health Dashboard
- **Seamless identity,** the Cisco Umbrella® Seamless ID feature enables Cisco® Secure Web Appliance to pass the user identification information to Cisco Umbrella Secure Web Gateway after successful identity authentication.
- **More investment value for** your security with Cisco Umbrella and SecureX integration, flexible deployment options, and award-winning 24-hour support.

Disparate point security solutions from multiple vendors introduces complexity and massive operational overhead into your IT environment. But not so with Cisco Secure Web Appliance (see Figure 1). It not only offers you strong protection, control, enhanced visibility, and investment value on its own, it's also part of the larger Cisco Secure platform, which you can choose to adopt at your own pace to strengthen your security posture.

Figure 1. Cisco Secure Web Appliance

## Strong protection

### Threat defense

Cisco Secure Web Appliance's threat intelligence is powered by Cisco Talos, one of the industry's leading threat research and analysis teams. Talos discovers where threats are hiding by pulling a massive amount of global information across multiple attack vectors.

Talos delivers early-warning intelligence, threat, and vulnerability analysis to help protect organizations against zero-day advanced threats. It continually generates new rules that feed updates every three to five minutes so that Cisco Secure Web Appliance can deliver industry-leading threat defense hours and even days ahead of competitors.

### Comprehensive website reputation analysis

Secure Web Appliance correlates threats collected across Cisco's global presence to produce a behavior score upon which to act. It applies and enforces web reputation scores on parent sites and subsites.

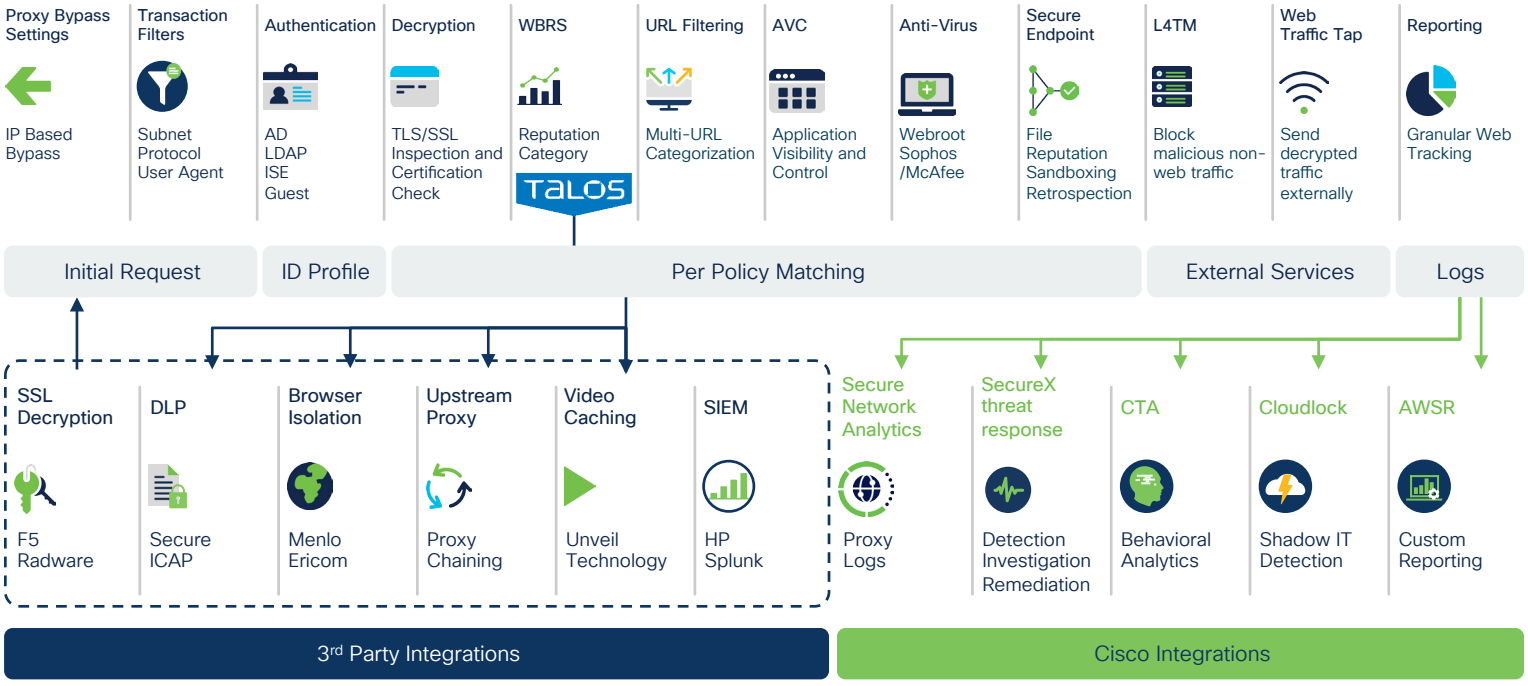
Together with threat intelligence from Talos, web reputation filters defend against zero-day web malware through dynamic reputation analysis. The feature selects the most relevant scanner in real time – based on URL reputation, content type, and the efficacy of the scanner – and improves the catch rate by scanning high-risk objects first during increased scan loads.

### Integrated, multilayer malware defense for adaptive protection

Effective web security used to mean simply blocking navigation to bad URLs. But today, you're more likely to get malware through legitimate websites. Cisco Secure Web Appliance defends against threats with multiple layers of antimalware technology and Cisco Talos threat intelligence, which is updated every three to five minutes. Every piece of web content accessed is analyzed using security and context-aware scanning engines.

Cisco Secure Web Appliance analyzes traffic in real time, breaks it into functional elements, and pushes elements to best-designed malware engines for inspection while maintaining high processing speed (see Figure 2).

Figure 2. Cisco SWA's Layers of Defense




## Sandboxing and continuous analysis

Cisco Malware Defense (formerly AMP for Networks) is an additional licensed feature for Cisco Secure Web Appliance. This capability provides malware detection and blocking, continuous analysis, and retrospective alert. It augments Secure Web Appliance's core malware detection and blocking. Customers additionally can sandbox PDF, Microsoft Office, and archive/compressed files, as well as Windows portable executable files.

# Complete control

## Centralized management

Cisco Secure Web Appliance's intuitive management interface centralizes policy management and reporting, offering unified global control.

## Deep web usage and application visibility

Get deep visibility into evolving application and microapplication content. Specifically, Cisco Secure Web Appliance identifies and classifies the most relevant and widely used web and mobile applications, such as Facebook, and more than 150,000 microapplications such as Facebook games. This is done by combining identity, time, content, location, and outbound compliance data to build and maintain application policy.

Coupled with this visibility, it offers precise control of application and usage behavior. It can regulate bandwidth consumption and apply conditional controls, such as throttling, based on the location, user profile, and device type. Additionally, it provides dynamic, context-based control of user access to applications based on user profile, device, and access mechanism. You can also set up policy to control Software-as-a-Service (SaaS) applications, such as Salesforce.com or Cisco Webex®.

Cisco Secure Web Appliance includes integration and license entitlement with Cisco SecureX, which is an open orchestration and XDR platform that integrates the Cisco Secure portfolio of network, email, cloud, and user protections. It delivers measurable reductions in threat dwell times, accelerated incident response, and other improved outcomes, like enhanced cross-team collaboration.

Cisco Secure Web Appliance Manager also includes the System Health Dashboard for rapidly determining system status and troubleshooting.

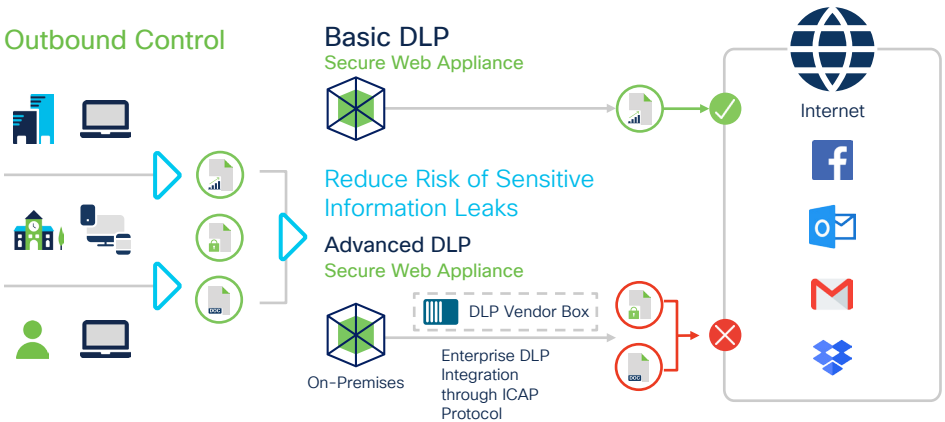
## Simplified configuration

Cisco Secure Web Appliance supports REST APIs for configuring network management and policies. With RESTful APIs you can also retrieve and modify configuration information or change, add, and delete configuration data without requiring libraries or additional software.

## Data loss prevention

Cisco Secure Web Appliance blocks sensitive information from leaving the safety of the network, helping to ensure compliance and reduce risk. This capability is in addition to the controls for outbound content such as file-sharing applications. You're able to prevent uploads to file-sharing services in the cloud, including iCloud and Dropbox. You can also stop confidential data from leaving the network by creating context-based rules for basic Data Loss Prevention (DLP) or by using the Internet Content Adaptation Protocol (ICAP) to integrate with any third-party DLP solution for deep content inspection and enforcement of DLP policies (see Figure 3).

Figure 3. Data loss prevention



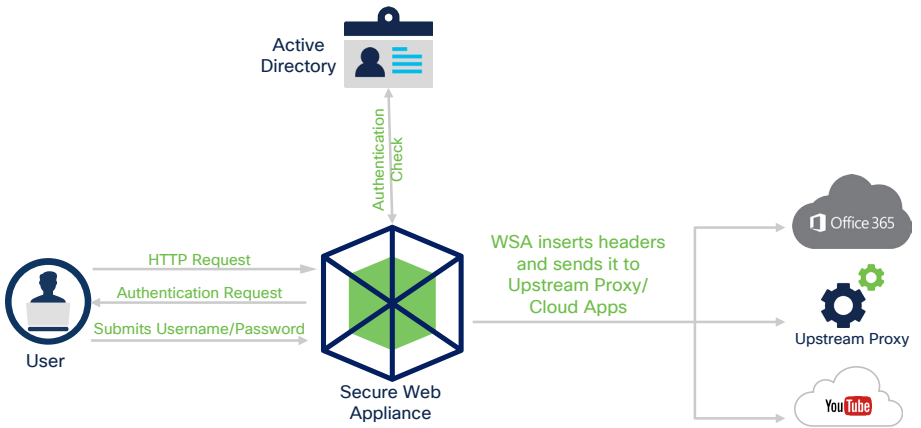

# Enhanced user experience

## Authentication efficiency

### Header rewrite

With Cisco Secure Web Appliance, custom header profiles can be configured for HTTP requests and multiple headers can be created under a header rewrite profile. The header rewrite profile feature enables the appliance to pass the user and group information to another upstream device after successful authentication. The upstream proxy considers the user as authenticated, bypasses further authentication, and provides access to the user based on the defined access policies (see Figure 4).

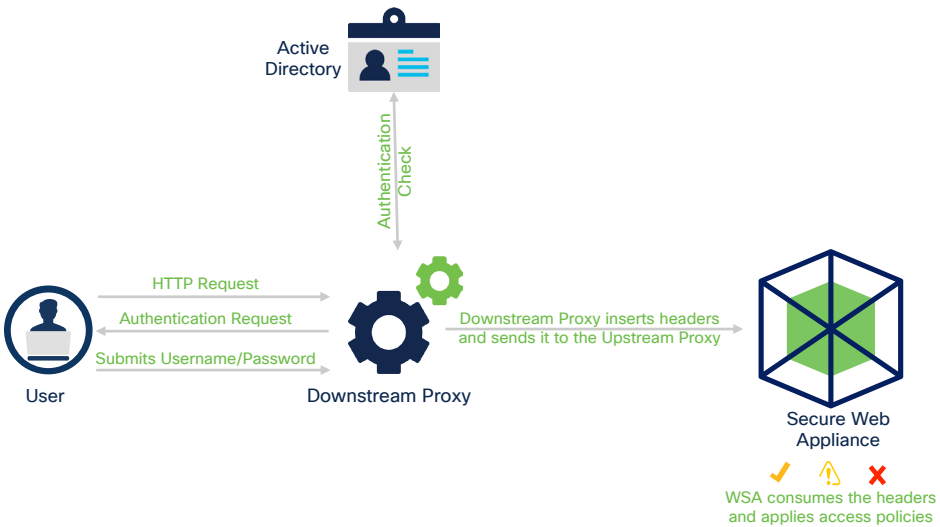
Figure 4. Header rewrite



## X-Authentication header consumption

Also, with Cisco Secure Web Appliance, the header-based authentication scheme can be configured where the downstream devices perform authentication and send the authentication information to WSA using authentication headers. Secure Web Appliance now processes this header information to identify users and applies the corresponding policies, eliminating the need for reauthentication (see Figure 5).

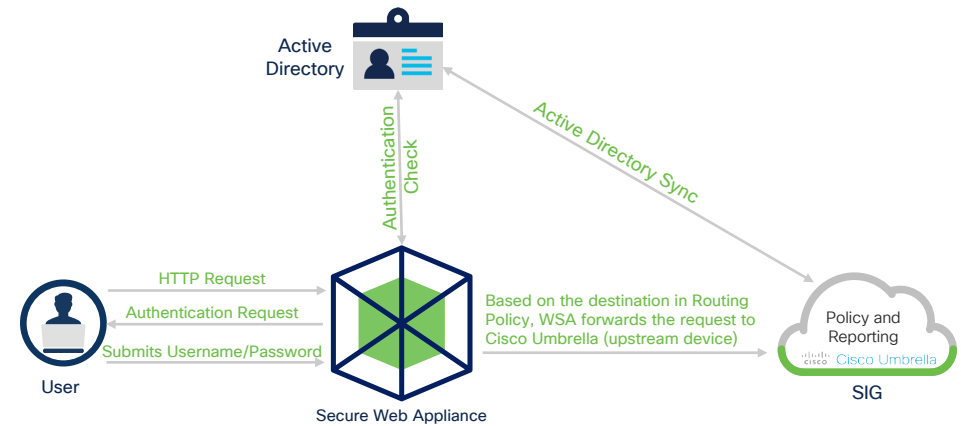
Figure 5. X- Authentication Header Consumption




## Cisco Umbrella Seamless ID

The Cisco Umbrella Seamless ID feature enables Secure Web Appliance to pass the user identification information to the cloud-delivered Umbrella Secure Web Gateway after successful authentication. Umbrella Secure Web Gateway checks the user information in the active directory based on the authenticated identification information received from the Secure Web Appliance. Umbrella considers the user as authenticated and provides access to the user based on the defined security policies. Secure Web Appliance passes the user identification information to Umbrella using HTTP headers (see Figure 6).

Figure 6. Umbrella Seamless ID



## Investment value

### Lower total cost of ownership

Cisco Secure Web Appliance delivers a consolidated solution in a single appliance, unlike other solutions that often require additional devices for new features and functions. You spend less time troubleshooting, with 99.999 percent availability and uptime. You save time with automatic updates from Talos and stay tuned against the latest threats without intervention. Lastly, you can use your existing VMware infrastructure in an unlimited number of deployments of Cisco Web Security Virtual Appliance.

## Models and available options

Please consult the Secure Web Appliance data sheet for the latest details on available configurations.

## Next steps

Find out more at the following link. Evaluate how Cisco Secure Web Appliance will work for you with a Cisco sales representative, channel partner, or systems engineer.

## For more information

**Learn more about Secure Cloud Analytics can use VPC Flow Logs to protect your cloud environment at https://www.cisco.com/go/SecureCloudAnalytics.**



C45-730937-00 09/21