

Mitigating Web Threats with Comprehensive, Cloud-Delivered Web Security

Overview

For collaboration, communication, and data access, the web has become a mission-critical business tool. But the web also poses significant security risks to the enterprise that are easily encountered yet not so easy to detect.

Some of the most sophisticated web-based threats are designed to hide in plain sight on legitimate and well-trafficked websites. For example, “malvertising” is the new industry term for disguising malware as online advertisements. Watering hole attacks conceal malware on member-based sites, phishing campaigns target individuals with personal details, and botnets take control of victims’ devices.

Research conducted by Cisco® Talos found that 93 percent of customer networks access websites that host malware.¹ These types of attacks often represent malicious code on trusted webpages that users may visit every day.

The Challenges

All organizations of every size are at risk for web malware exposure, but research shows that the largest enterprises (with more than 25,000 employees) have more than 2.5 times the risk of encountering web malware than smaller companies. These organizations generate, collect, and store a wealth of intellectual property and other high-value information such as financial and customer information and big data. This information makes them prime targets for cybercriminals.

But no organization is immune. Entities around the world, including companies and even nation-states, are engaging hackers to help them conduct corporate espionage and other types of “intelligence gathering.” Hacking is an industry.

And as companies transition away from traditional IT models, remote users need protection beyond the firewall. Security is no longer only about safeguarding data centers; it’s now also about protecting devices.

The traditional assumption that threats come only from outside the firewall is no longer valid. Advanced attacks access information from inside the network through infected guest, employee, or even company devices.

Once an organization’s network is compromised, it can take weeks, months, or longer for an advanced persistent threat (APT) to be detected in the network. Some threats are so sophisticated that they may sit doing nothing for weeks, like sleepers, before they get to work. Meanwhile, the targeted organization continues to lose data and is at risk of facing significant financial or reputational damage.

¹ [Cisco 2015 Midyear Security Report](#).

Figure 1. Overview of Web Security Challenges for Today's Enterprises



Protecting the network, data, and the workforce from web-based threats has never been more difficult for enterprises. They face both a constantly evolving threat and network landscape and a challenging business environment (see Figure 1). Trends dissolving the traditional network security perimeter include:

Cisco Security in Action

Threats are becoming more sophisticated, but sometimes a low-tech attack is highly effective. The String of Pearls campaign uses basic tactics with a modern twist. It combines spear phishing and exploit attempts to trick users.

The approach is simple: Send users seemingly legitimate emails with attachments in order to download executable files and take over their machines.

Attackers target specific high-profile and money-rich industries. They send specific individuals emails disguised as invoices from well-known shipping companies. Upon opening the attachment, users are prompted to enable macros in order to continue. (Microsoft has disabled macros that run automatically upon opening documents to prevent this from happening.) The enabled macros then download executable files from Drop box and launch them on the victims' machines.

Cisco Talos has hundreds of feeds of raw threat intelligence, ranging from suspicious URLs, files, hashes, and more. It takes that intelligence data and applies selection logic to it to identify samples that are worthy of review.

Talos collected 45 days' worth of samples and clustered them together according to a set of alert criteria. It reduced more than a million detailed sample reports to just over 15 thousand clusters of samples that exhibited similar behavior. This process uncovered the Microsoft Word document that downloaded and executed a secondary sample, which began beaconing to a command-and-control server.

Once the executable files were identified, Talos updated all of Cisco's security solutions against the latest and most advanced threats. Cloud Web Security now blocks the download of these files so administrators can restrict access to identified malicious domains.

- Uncontrolled use of web-based and social networking applications by employees, which opens the door not only to web malware but also to compliance and data security risk
- Expansion of unsecure public Wi-Fi
- A growing population of smaller branch offices
- A highly mobile workforce

- “Bring your own device” (BYOD) policies

Other factors also make it difficult for enterprises to identify and defend against web-based threats. These include the rapidly ballooning volume of web traffic that must be inspected and the increasing number of virtualized business applications. Many organizations are challenged further by the need to develop more robust security policies within rigid business constraints. For example, they must use the existing architecture and often limited resources to scale web security to remote and branch offices, which typically have little or no IT support on site.

A Comprehensive Approach

Today’s enterprises need to harness the power of the web without undermining business agility or web security. But as they expand their use of the web, they increase their exposure to tangible risks that can affect their brand, operations, data, and more.

To address web security challenges effectively, enterprises need a potent, pervasive solution that can:

- Address current web security demands. It must deliver strong protection against today’s threats and address how modern users access information.
- Adapt to meet the changing threat landscape. It must detect new forms of malware and address anything that bypasses perimeter defenses.
- Meet both the constraints and needs of the business. It must fit with current infrastructure and scale as the business grows.

Figure 2 illustrates how these capabilities work to address web security challenges.

Figure 2. Key Elements of Comprehensive Web Security



Securing every device, every user, and every bit of data that crosses the enterprise network requires an adaptive and responsive - as well as an architectural - approach. Cisco’s network-based security architecture is that approach.

The components (Figure 3) fit together in a comprehensive solution that helps enterprises to defend against, discover, and remediate threats originating from the web. It also helps enterprises better manage the security risks of borderless networks, so workers can globally access the network with their device of choice and use the applications and information they need to do their jobs.

Figure 3. The Network-Based Security Architecture

| Values | Content | Network | Access |
|---|---|--|---|
| Protection Protect against threats | Safeguards every device, everywhere, all the time | Protects networks before, during, and after attacks | Delivers context-aware, pervasive access protection |
| Control Control the environment | Support control of all web and email traffic on all devices | Offers exceptional visibility and control of network and application traffic | Simplifies access controls |
| Flexibility Support the business | Integrates transparently with existing security and network infrastructures | Provides agile, open, and scalable platforms | Secures access of an increasing number of endpoints |
| Framework | | | |
| Management and Intelligence Capabilities | Configuration Management | | |
| | Operation Management | | |
| | Security Intelligence | | |
| Security Solutions | Web Security | Site-to-site VPN | Remote Access VPN |
| | Email Security | NGIPS | Identity and Access Control |
| | | NGFW | Malware Protection |
| | | Firewall | |

Cisco's security architecture today includes three main sections:

- **Content security:** Web and email security solutions that monitor ingoing and outgoing web and email traffic and regulate employee web and application access
- **Network security:** Firewalls, VPNs, and intrusion prevention systems that manage companywide policies, regulate network access, and adjust automatically to alerts
- **Secure access:** Remote access solutions with identity and access controls to safeguard connections, enforce policies, and regulate remote and guest access to the network

Cisco Cloud Web Security

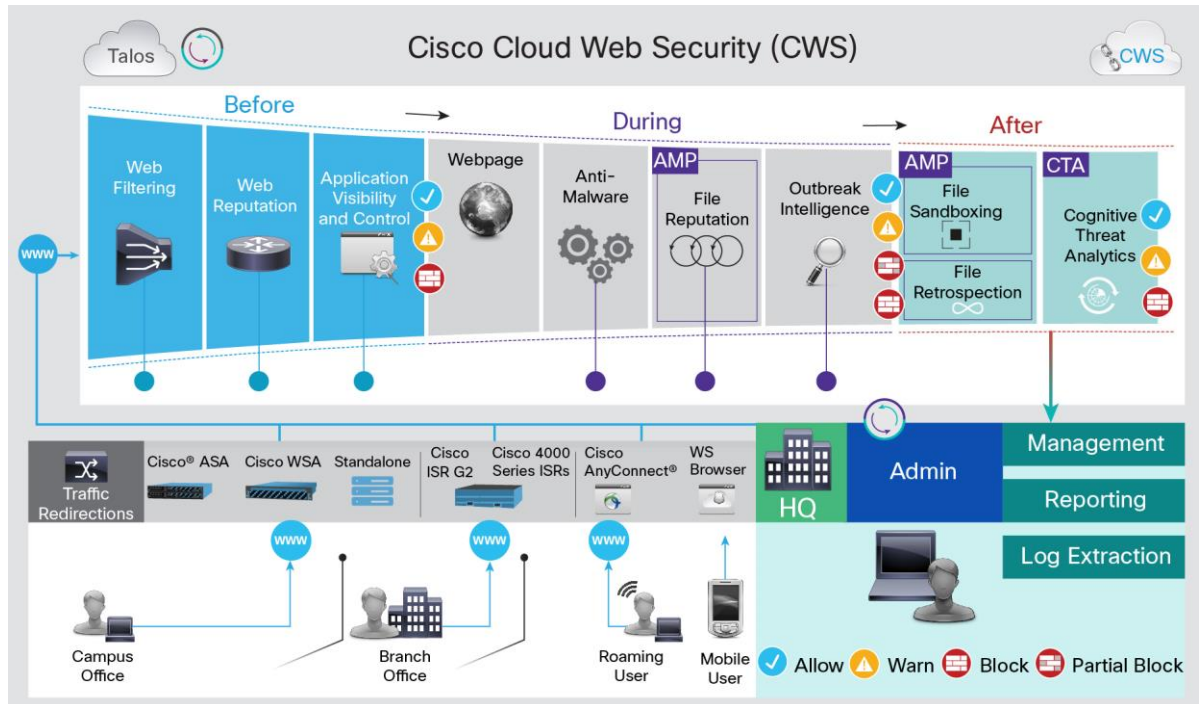
Cloud Web Security (see Figure 4) keeps malware off the network and helps organizations of all sizes more effectively control and secure web usage. It provides both inbound and outbound protection and extends web security to roaming users with the Cisco AnyConnect® Secure Mobility Client, a lightweight, highly modular security agent providing easily customizable capabilities based on the individual needs of the business.

Cloud Web Security pairs with Advanced Malware Protection (AMP) to protect against the latest and most advanced threats and analyze traffic in a highly secure environment in real time. Only AMP delivers the ability to track a file's disposition in a network over time to identify where malicious files may be hiding. Cognitive Threat Analytics adds continuous capabilities to scan the environment for symptoms of an infection and malware that bypasses perimeter defenses.

Furthermore, Cisco Cloud Access Security provides visibility and control for software-as-a-service (SaaS) application usage, cloud data loss protection, and anomaly detection for the growing risks created by the proliferation of cloud apps.

Cloud Web Security is powered by Talos, part of the Cisco Collective Security Intelligence (CSI) ecosystem that uses dynamic analysis to deliver industry-leading security intelligence. Talos detects and correlates threats in real time. Its threat detection network, the largest in the world, comprises automated machine-learning heuristics and multiple scanning engines. Talos gathers 100 TB of intelligence from more than 150 million endpoints every day to build a detailed view, including the associated security risk, of each of the 13 billion web requests it sees daily.

Figure 4. How Cloud Web Security Works



Note: The products shown as traffic redirection methods include the Cisco Adaptive Security Appliance, the Cisco Web Security Appliance, the Cisco Integrated Services Router (Generation 2), and the AnyConnect Secure Mobility Client.

Cloud Web Security uses both dynamic reputation analysis and behavior-based analysis to provide enterprises with exceptional threat defense from zero-day web-based malware. All inbound and outbound web traffic is scanned in real time for both new and previously identified web-based malware. Every piece of HTTP and HTTPS web content accessed is analyzed by security- and context-aware scanning engines.

Cloud Web Security also gives enterprises complete control over how end users access Internet-delivered content, including SaaS applications. Precise control can even be applied to dynamic websites, such as Facebook and Twitter, as well as content from many other popular platforms and streaming media. Specific features such as chat, messaging, video, and audio can be allowed or blocked, according to the requirements of the business and users without the need to prohibit access to the entire website.

Traffic Redirection Methods

Cisco provides multiple traffic redirection methods so that customers can connect to existing infrastructure.

Traffic can be redirected by:

- **Cisco Integrated Services Routers (ISR G2 and 4000 Series with generic routing encapsulation [GRE] over IPsec):** Save bandwidth, money, and resources 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.
- **Next-Generation Firewall (Adaptive Security Appliances):** Improve the performance of your physical or virtual Adaptive Security Appliance by offloading your content scanning to Cisco's cloud through Cloud Web Security. Apply acceptable-use policy to the company, groups, or individual users.
- **Web Security Appliance:** Integrate Cloud Web Security with existing routers and firewalls through physical or virtual appliances to redirect traffic and enforce usage-control policies.
- **AnyConnect:** Extend your security border beyond the physical network, applying the same web-based security and usage controls for roaming laptop users.
- **Standalone deployment:** Deploy a simple web security solution that does not require additional hardware. Connect to Cisco's Cloud Web Security service using existing browser settings and Proxy Auto Configuration/Web Proxy Auto Discovery (PAC/WPAD) files.

Additional Benefits

Simple Integration in a Comprehensive Security Solution

Today's web-based threats are complex, but building a better security infrastructure doesn't have to mean building a more complex one. Instead, the infrastructure and the elements within it must work together with more intelligence to detect and mitigate threats. Cisco's architectural approach to security, supported by Cloud Web Security, is holistic. It helps organizations retain their business agility. Services can be reused, and new capabilities can be rapidly deployed as business needs change.

Strong Protection Regardless of User Location or Device

Cloud Web Security provides consistent, high-performance web security and policy regardless of where or how users access the Internet. It is a highly effective defense against web-based malware, and it offers exceptional application controls and URL filtering to manage data loss risks, employee productivity, and bandwidth usage. As part of a pervasive web security strategy for the enterprise, Cloud Web Security facilitates better data and brand protection and helps to ensure compliance. It also helps to protect users, wherever they are, so they can more safely, securely, and appropriately access the web.

Licensing Options

Cloud Web Security is available in subscriptions with seat-based or bandwidth-based pricing.

Seat-based pricing: Based on the number of users

- Cloud Web Security Essentials
- Advanced Malware Protection (AMP)
- Advanced Threat Detection (ATD)
- Cloud Web Security Premium
- Cloud Access Security on Cloud Web Security

Bandwidth pricing: Based on the total traffic across various deployment sites that will be directed to Cloud Web Security data centers

- Web Security Basic
- “Cloud” Web Security Intermediate

Cloud Web Security is also available to customers with current Enterprise License Agreements.

Lower TCO than On-Premises Solutions

Cloud Web Security delivers a better return on investment than individual point products. Its many web traffic redirection methods help enterprises reuse existing assets so they can deploy web security in areas where it was too expensive or difficult to deploy previously. As a true SaaS solution, Cloud Web Security also reduces administrative burdens by presenting opportunities for more operational efficiency. There are fewer devices to manage, support, and maintain. Additionally, the solution reduces the total cost of ownership through lower hardware, rack space, power, cooling, and repair costs.

Why Cisco?

Web security is more critical to your business than ever before. As threats and risks persist, along with concerns about confidentiality and control, security is necessary for providing business continuity, protecting valuable information, maintaining brand reputation, and adopting new technology. With protected web access, your employees can embrace mobility and connect to the right information with confidence. And your customers and partners can conduct business with you more easily.

No organization understands security like Cisco. Our market leadership, superior threat protection and prevention, innovative products, and longevity make us the right vendor for your security needs.

For more information on Cisco Cloud Web Security options, visit <http://www.cisco.com/go/cws>.




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.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)