Addressing Advanced Web Threats:

Protect Your Data and Brand

What You Will Learn

From collaboration to communication to data access, the web is a mission-critical business tool. Enterprises rely on the web not only to innovate and compete but also to conduct business. But the web poses significant security risks that are easily encountered by users, yet not so easy to detect.

To address web security challenges effectively, enterprises need a comprehensive solution. Cisco® web security is one such solution. It provides:

- Cloud-based intelligence
- Context-based policy and management
- Network enforcement

Challenges

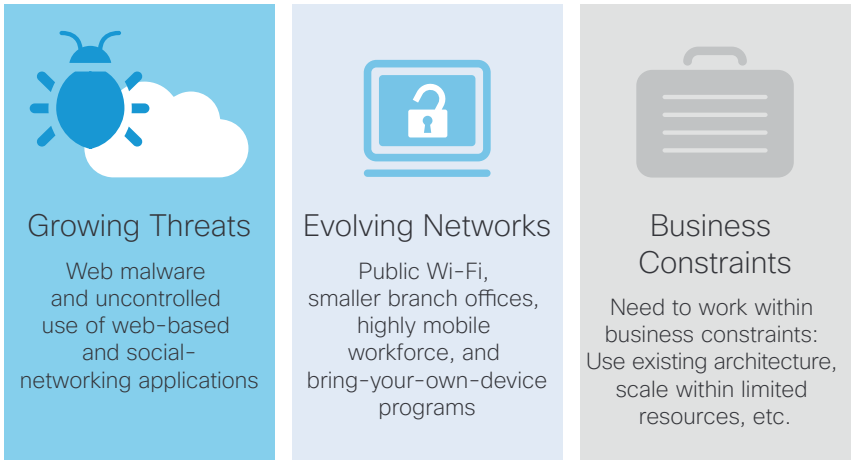
Some of the most sophisticated web-based threats are designed to hide in plain sight on legitimate and well-trafficked websites. According to research by Cisco Talos Security Intelligence and Research Group (Talos) for the *Cisco 2015 Annual Security Report*, adversaries who use some of today's leading exploit kits, like Angler and Sweet Orange, rely on malvertising to redirect users to websites—including legitimate sites—that host those exploit kits.[1]

While organizations of every size are at risk for web malware exposure, research by Talos shows that the largest enterprises (25,000 employees or more) have more than two and a half times the risk of encountering web malware than smaller companies. The wealth of intellectual property and other high-value information—such as financial and customer information and big data—that these organizations generate, collect, and store makes them prime targets for cybercriminals. As recent news reports have shown, entities around the world, including companies and even nation-states, are engaging hackers to help facilitate corporate espionage and other types of "intelligence gathering."

Once an organization's network is compromised, it can take weeks, months, or longer for an advanced persistent threat (APT) enabled through web malware to be detected in the network. Meanwhile, the targeted organization continues to lose data—and is at risk of facing significant damage to its finances and reputation.

Protecting the network, data, and the workforce from web-based threats has never been more difficult for enterprises due to the constantly evolving threat and network landscape and a challenging business landscape (see Figure 1).

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



Trends dissolving the traditional network security perimeter include:

- 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 risks
- Expansion of unsecure public Wi-Fi
- A growing population of smaller branch offices
- A highly mobile workforce
- Bring-your-own-device (BYOD) policies

[1] *Cisco 2015 Annual Security Report*, Cisco, Jan. 2015.

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

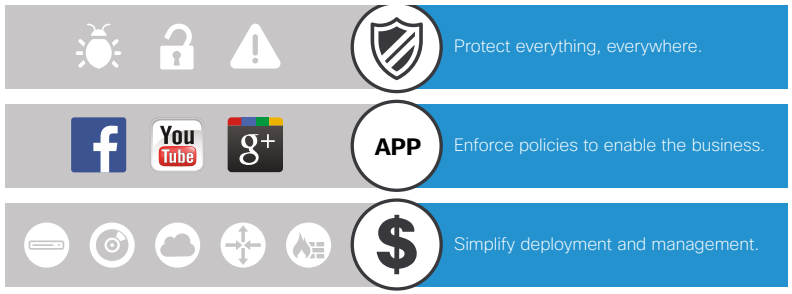
A Comprehensive Approach

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. Simply consider the fact that cybercriminals are building 4 new pieces of web malware per second: 240 per minute, 15,000 per hour, 300,000 per day.[2]

To address web security challenges effectively, enterprises need a potent, pervasive solution (see Figure 2) that can:

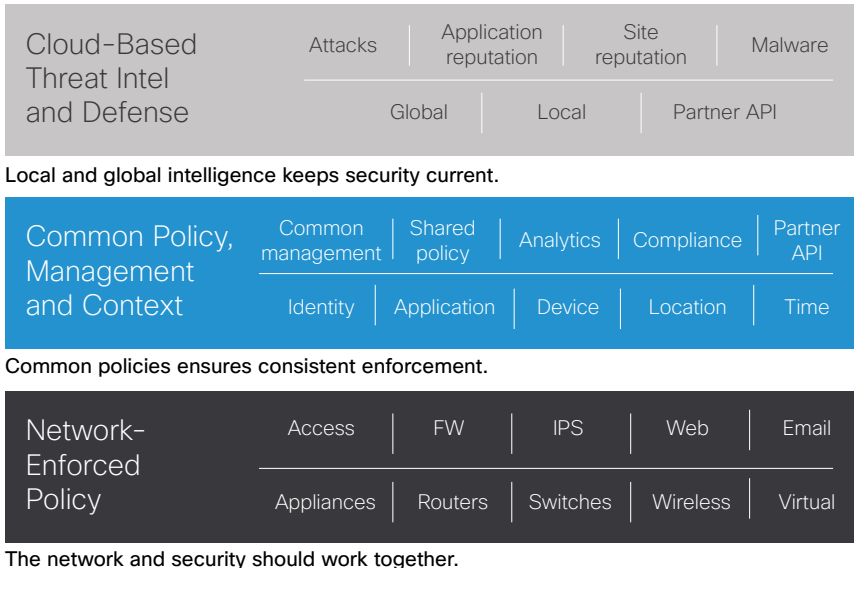
- Protect everything, everywhere—including traditional users in the corporate office, BYOD users, remote offices, and public wireless access points.
- Enforce use policies that will grow with business, rather than inhibit it.
- Be deployed easily within the limitations of the corporate network as well as the business environment.

Figure 2. Critical Elements of Comprehensive Web Security



Protecting every device, every user, and every bit of data that crosses the enterprise network requires an adaptive and responsive—as well as architectural—approach. Cisco network-based security architecture is that approach. Its components (see Figure 3) present a closed-loop solution that allows 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. Cisco Network-Based Security Architecture



[2] Source: Cisco Talos.

The Cisco network-based security architecture comprises:

- **Cloud-based intelligence** – Adaptive and consistent threat protection delivered months ahead of threats, avoiding the problems associated with pure signature and patch cycles
- **Context-based policy and management** – Intelligent security policy based on rich context (user, device, location, posture, application) rather than "whitelists" and static provisioning
- **Network-enforced security** – Consistent enforcement of security policies across the entire network infrastructure

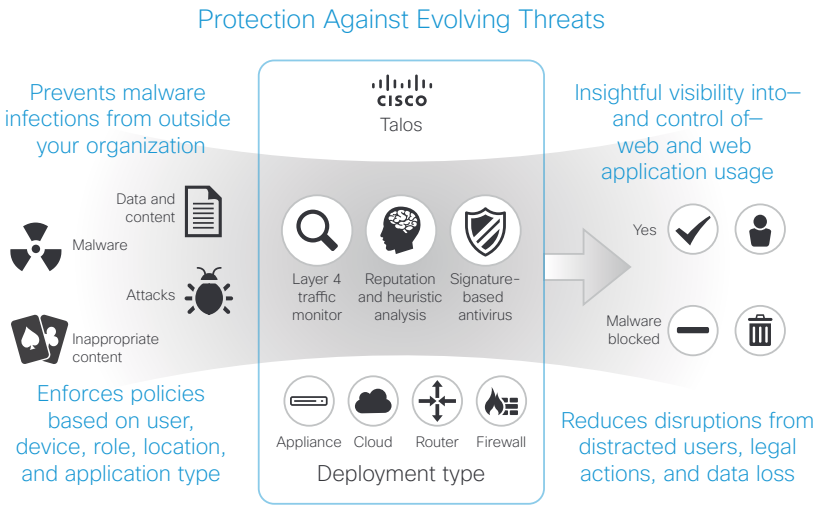
Advanced Malware Protection

Advanced Malware Protection (AMP) adds to the sophistication of Cisco web security, helping to provide continuous monitoring and analysis across the extended network. AMP is a detection system that does not rely on malware signatures, which can take weeks or months to create for each new malware sample. Instead, it uses a combination of file reputation, file sandboxing, and retrospective analysis (described later in this paper) to identify and stop threats across the entire attack continuum—before, during, and after an attack.

Cisco Web Security

Cisco web security, which supports Cisco network-based security architecture, protects against threats that can disrupt organizations (see Figure 4). Named by Gartner as the leading Secure Web Gateway for 2014, Cisco web security 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 remote and mobile users, including security for smartphones and tablets, with the Cisco AnyConnect® Secure Mobility Client—a lightweight, highly modular security client providing easily customizable capabilities based on the individual needs of the business.

Figure 4. How Cisco Web Security Works



Cisco web security uses reputation and zero-day threat intelligence from Talos. Composed of leading threat researchers, Talos is the primary team that contributes threat information to the Cisco Collective Security Intelligence (CSI) ecosystem, which includes Threat Response, Intelligence, and Development (TRIAD), Managed Threat Defense, and Security Intelligence Operations. Cisco CSI is shared across multiple security solutions and provides industry-leading security protections and efficacy.

Talos calls on an unrivaled telemetry data set of billions of web requests and emails, millions of malware samples, open-source data sets, and millions of network intrusions to create intelligence that provides a holistic understanding of threats. This capability translates to the industry-leading effectiveness for Cisco security

solutions. Our security intelligence cloud produces "big intelligence" and reputation analysis for tracking threats across networks, endpoints, mobile devices, virtual systems, web, and email.

Talos has a 24-hour view into global traffic activity to analyze anomalies, uncover new threats, and monitor traffic trends. Talos prevents zero-hour attacks by continually generating new rules that feed updates to the Cisco Web Security Appliance (WSA) every 3–5 minutes, providing threat defense hours and even days ahead of competitors.

Cisco web security is backed by the largest threat detection network in the world, with the broadest visibility and largest footprint, including:

- 100 terabytes (TB) of security intelligence daily
- 1.6 million deployed security devices, including firewall, intrusion prevention system (IPS), web, and email appliances
- 150 million endpoints
- 13 billion web requests per day
- 35 percent of the world's enterprise email traffic

Cisco web security uses both dynamic reputation analysis and behavior-based analysis to provide enterprises with the best threat defense from zero-day web malware. All inbound and outbound web traffic is scanned in real time for both new and known web malware. Every piece of web content accessed—from HTML to images to Adobe Flash® files—is analyzed using security- and context-aware scanning engines.

Cisco web security also gives enterprises complete control over how end users access Internet content. Precise control can even be applied to dynamic content, such as Facebook and Twitter content, 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 block entire websites.

Enhanced Malware Detection with AMP

The AMP add-on for Cisco web security provides malware detection and blocking, continuous analysis, and retrospective alerting to the Cisco WSA. Cisco AMP uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats across the attack continuum. Descriptions of Cisco AMP features follow:

- File reputation captures a fingerprint of each file as it traverses the Cisco web security gateway and sends it to the AMP cloud-based intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policies.
- File sandboxing lets you analyze unknown files that are traversing the Cisco web security gateway. A highly secure sandbox environment helps enable AMP to glean precise details about a file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into the AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection. Customers also now have the ability to sandbox PDF and Microsoft Office files, in addition to EXE files supported in the first AMP release.
- File retrospection solves the problem of malicious files that pass through perimeter defenses but are subsequently deemed a threat. It addresses the inherent weakness of most perimeter defenses: They are effective only at a single point in time. Even the most advanced techniques may fail to identify malware at the perimeter, because polymorphism, obfuscation, sleep timers, and other tactics are highly effective at helping files avoid detection as they cross the wire. Malicious files simply wait until they are inside the network to do their dirty work. These include files going in and out of your web traffic through software-as-a-service (SaaS) applications such as Dropbox and Box.
- Rather than operating at a point in time, file retrospection provides a continuous analysis of files that have traversed the security gateway, using real-time updates from the AMP cloud-based intelligence network to stay abreast of changing threat levels. Once a malicious file is identified as a threat, AMP alerts the administrator and gives visibility into who on the network may have been infected and when. As a result, customers are able to identify and address an attack quickly, before it has a chance to spread.

Additional Benefits of Cisco Web Security

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. The Cisco architectural approach to security, supported by Cisco web security, is holistic. It allows organizations to retain their business agility by helping to enable the reuse of services and rapid deployment of new capabilities as business needs change.

Cisco web security provides consistent, high-performance web security and policy regardless of where or how users access the Internet. It is the most effective defense against web-based malware and offers the best 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, Cisco web security provides better data and brand protection and helps to ensure compliance. It also helps to protect users, wherever they are, so they can safely and appropriately access the web.

Compared with individual point products, Cisco web security delivers a better return on investment, whether the solution is deployed by an appliance or through the cloud. (See Table 1 for deployment and licensing options.) Its close integration with the Cisco network infrastructure and other Cisco security products lets enterprises reuse existing assets to deploy web security in areas where it was too expensive or difficult to deploy previously.

Cisco web security, with its simplified architecture, also reduces your administrative burden by presenting opportunities for more operational efficiency, including 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.

Table 1. Cisco Web Security: Product Offerings

Product	Licensing Options
Cisco WSA – Premises-based web security gateway to protect all users, regardless of location. Powered by Talos for comprehensive zero-day threat protection. Web security, application control, proxy cache, and reporting fully integrated into a single appliance; available in three models.	*Advanced Web Security* - Application visibility and control (AVC), URL filtering, and reputation analysis, plus real-time antimalware protection and data loss prevention (DLP) integration.
Cisco Web Security Virtual Appliance (WSAv) – Virtual WSA for simplified, multilocation deployment; provides same functionality as WSA but with the flexibility of a virtual form factor.	*Advanced Web Security*
Cisco Cloud Web Security (CWS) – Cloud-based web security, powered by Talos, that provides comprehensive web defense through industry-leading, real-time protection and enforcement of detailed web usage policies. Multiple connector options make for easier deployments.	*CWS Essentials (includes web filtering, outbreak intelligence, AVC); CWS Premium (with AMP and Cognitive Threat Analytics)*

Conclusion

Security is more critical to your network 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. A highly secure network helps your employees embrace mobility and connect to the right information safely. It also allows your customers and partners to conduct business with you more easily.

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

For More Information

For more information on Cisco web security solutions and deployment options, visit www.cisco.com/go/websecurity.