Web Security:

A Buyer's Guide

Introduction

From communication to data access, the web has become a mission-critical business tool. But with more businesses doing work online, the web is also now a popular attack vector. Today's threats aren't limited to questionable websites or bad URLs. Some of the most sophisticated threats are designed to hide in plain sight on legitimate and well-trafficked websites. And threats outside of the network aren't the only concern. Users inside the business may be putting the organization at risk by consuming excess bandwidth and accessing content like social media, videos, and personal applications outside acceptable use policies.

Modern businesses need a web security solution that provides continuous monitoring and analysis across the extended network, and protection before, during, and after an attack. This document examines requirements businesses should consider when purchasing a web security solution that will meet the challenges of today's advanced threat landscape.

Buyer's Criteria for Web Security

When evaluating web security solutions, organizations should assess the following criteria to ensure they will receive the deeply layered protection needed to defend their business from today's advanced threats and targeted attacks:

- Big data analytics and collective global security intelligence
- Reputation filtering
- Real-time malware scanning
- Web usage controls
- Application visibility and control (AVC)
- Data loss prevention (DLP)
- Threat protection and remediation
- Flexible deployment options

Requirement 1: Big Data Analytics and Collective Global Security Intelligence

Malware can no longer be identified based on what it "looks" like, because a file that is categorized as benign today could easily become malicious tomorrow. Traditional solutions like "cloud-assisted antivirus" do not address the evolution of advanced malware designed to evade signature-based detection. This is why true protection can only be achieved with a web security solution that provides continuous analysis. And if a file's disposition does change, constant monitoring of all traffic is what helps security personnel trace the infection back to its origin.

The Cisco Approach:

- Protection backed by millions of malware samples gathered globally every month
- Analysis by the Cisco® Talos Security Intelligence and Research Group and Cisco Collective Security Intelligence (CSI) teams
- Identification of malware based on what it does, not what it looks like, allowing detection of even the newest zero-day attacks
- Cisco Advanced Malware Protection (AMP) to provide deeper visibility, control, and retrospection

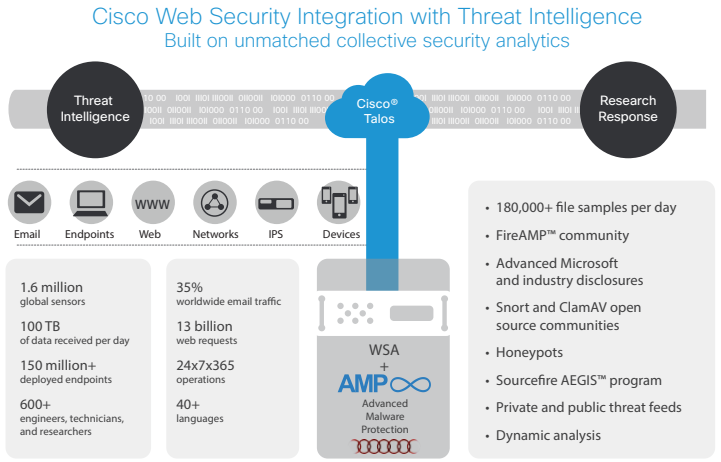

Figure 1. "Cisco Web Security: Protection, Control, and Value."

*Cisco 2015 Annual Security Report, Cisco, Jan. 2015:

Requirement 2: Web Reputation and Categorization

Modern web security requires the ability to block malware from both suspicious and legitimate sites before it reaches a user. Business tools that increase productivity can significantly increase the probability that users will encounter malware. Even legitimate websites can pose a threat by malware designed to hide in plain sight. Web security in this environment must be capable of dynamic reputation and behavior-based analysis. It also must be nuanced enough to support policies that give employees customized access to the sites they need while selectively denying the use of undesired sites and features like web-based file sharing.

The Cisco Approach:

- Dynamic analysis of unknown URLs to block malicious content
- Web reputation filters that analyze and categorize the risk associated with a site the instant a web request is made
- Reputation scoring to block, allow, or deliver with warning a particular site

*Cybercriminals are building 4 new pieces of web malware per second–240 per minute; 15,000 per hour; 300,000 per day**

Requirement 3: Real-Time Malware Scanning

As businesses expand their use of the web, they increase their exposure to tangible risks, like zero-day malware, that can ultimately affect their data, brand, operations, and more. To provide the best defense from known and new malware, a web security solution should provide both dynamic reputation analysis and behavior-based analysis. Businesses need the ability to scan all inbound and outbound web traffic in real time for malware and analyze every piece of web content accessed. Solutions with content-aware, policy-based DLP, and encryption capabilities are critical to achieve protection.

The Cisco Approach:

- Enhanced malware defense coverage
- Most robust antimalware inspection on the market
- Process-speed optimization
- Adaptive and prioritized scanning
- Real-time malware analysis

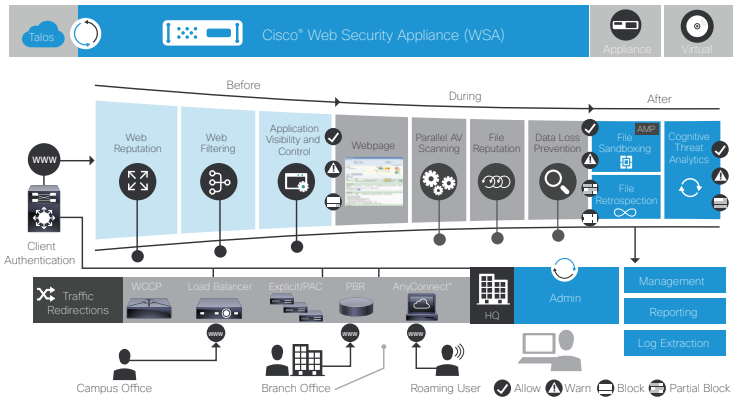

Figure 2. "Cisco Web Security: Protection, Control, and Value."

*Source: Cisco T alos.

Requirement 4: Web Usage Controls

Today's organizations need superior web usage controls that allow them to manage bandwidth usage by employees and guest users. Targeted campaigns deploy malware designed to steal high-value data and ultimately gain access to data centers. Businesses must be able to deploy web usage controls that can shut down user access dynamically when a site that is known to host malware is requested.

The Cisco Approach:

- Combination of traditional URL filtering and real-time analysis
- User access based on URL filtering policies checked against Cisco's database of more than 50 million known malicious URLs
- Bandwidth and time quotas deployed by user, group, or policy

Requirement 5: Web Application Visibility and Control

A modern web security solution should give enterprises complete control over how end users access Internet content. Web security solutions that offer AVC help administrators create and enforce detailed policies within websites that contain embedded applications and microapplications without hindering workforce productivity or burdening IT resources. In addition, web security solutions must be able to control application behavior such as uploading, tagging, or posting a video, helping to reduce exposure to web-based malware and prevent data loss.

The Cisco Approach:

- AVC that delivers deep visibility into evolving application and microapplication content
- Granular control over application usage and behavior
- Identification and classification of hundreds of the most relevant and widely used Web 2.0 and mobile applications, such as Facebook, and more than 150,000 microapplications, such as Facebook games

Requirement 6: Data Loss Prevention

A modern web security solution should give enterprises complete control over how end users access Internet content. Web security solutions that offer AVC help administrators create and enforce detailed policies within websites that contain embedded applications and microapplications without hindering workforce productivity or burdening IT resources. In addition, web security solutions must be able to control application behavior such as uploading, tagging, or posting a video, helping to reduce exposure to web-based malware and prevent data loss.

The Cisco Approach:

- Customized content access based on business needs and regulatory compliance
- Context-based rules for basic DLP or Internet Content Adaptation Protocol (ICAP) that allow deep content inspection and enforcement of DLP policies
- On-board DLP capabilities through data scanning by title, metadata, and size, and upload prevention to webmail and file-sharing services in the cloud
- Custom policy creation according to the desired degree of restriction

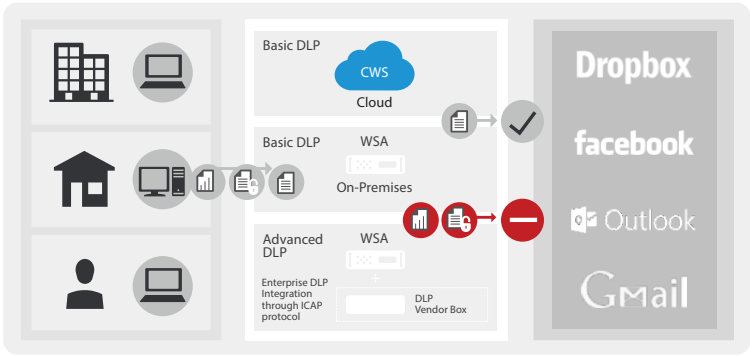

Figure 3. "Cisco Web Security: Protection, Control, and Value."

Requirement 7: Web Application Visibility and Control

Even with a layered approach to web security, some sophisticated attacks will manage to get through. Continuous analysis and retrospective security are needed to identify malicious files that have so far evaded detection, and to help determine the scope of the attack so it can quickly be contained and remediated.

Cisco Advanced Malware Protection

Cisco AMP is an add-on service to Cisco web security. AMP uses the vast cloud security intelligence networks of Talos to provide superior protection across the attack continuum—before, during, and after an attack. It is the industry's only proven zero-hour antivirus solution that protects against new viruses in less than 60 minutes.

File Reputation	Captures a fingerprint of each file as it traverses the web gateway and analyzes via the AMP cloud-based intelligence network for a reputation verdict
File Sandboxing	Provides ability to analyze unknown files in a secure sandbox environment to determine a file's threat level
File Retrospection	Allows surgical scoping, containment, and remediation of malicious files after an infection occurs
Collective Immunity	Sends threat intelligence from all AMP users to Cisco Talos to mark as malicious and protect all members of the AMP community from future infections

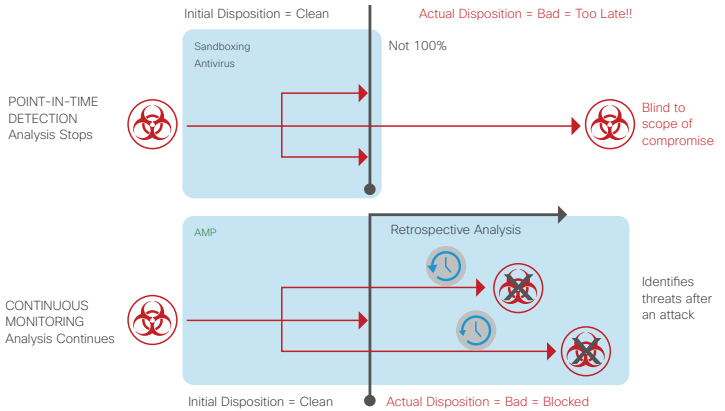

Figure 4. "Cisco Web Security: Protection, Control, and Value."

Requirement 8: Flexible Deployment Options

While today's web-based threats are complex, your security solutions should be simple and work together to detect and mitigate threats. Organizations need a web security solution that offers flexible deployment options—appliance, virtual, cloud, and hybrid—so they can protect all users in their organization and manage the solution in a way that makes the most sense for their business.

Cisco Web Security Solutions

Cisco web security provides consistent, high-performance web security and policy management 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 enables better data and brand protection and helps to ensure compliance.

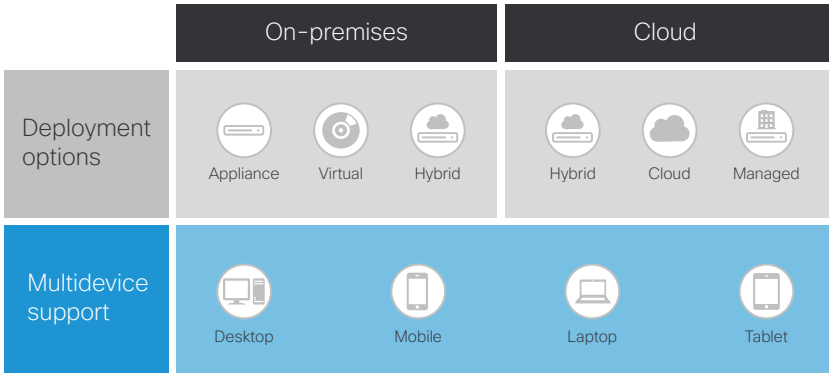

Figure 5. Web Security Deployment Options

Cisco Web Security Appliance (WSA)	Simplifies control with a high-performance dedicated appliance
Cisco Web Security Virtual Appliance (WSAv)	Allows administrators to create new appliance instances wherever and whenever they are needed
Cisco Cloud Web Security (CWS)	Delivers a simple web security solution that does not require any additional hardware; it can function standalone or can provide increases protection by connecting existing network equipment to cloud-based web security services using existing browser settings and PAC files

Conclusion

Protect your organization from advanced threats in today's highly connected and mobile environments by deploying Cisco web security. Both Cisco WSA and Cisco CWS deliver strong protection, complete control, broad deployment options, and investment value.

Cisco WSA and Cisco CWS provide advance threat defense through the work of Cisco Talos. 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 translating to leading security effectiveness for Cisco security solutions. The result is a security intelligence cloud producing "big intelligence" and reputation analysis for tracking threats across networks, endpoints, mobile devices, virtual systems, web, and email.

For more information on the Cisco web security portfolio, visit www.cisco.com/go/web-security. A Cisco sales representative, channel partner, or system engineer can help you evaluate how Cisco web security solutions will meet the unique needs of your organization.