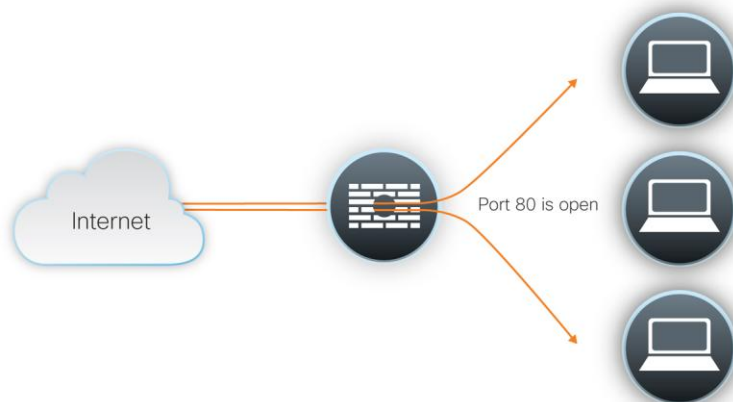


## Cisco IronPort Anti-Malware System

Malware is a real and costly problem most companies face today. Web and social media usage continues to grow exponentially, making it the key vector for online malware attacks. More than 90% of known malware appears on legitimate websites. Spyware and other types of malware can result in loss of confidential information, system and network downtime, reduced employee productivity, and escalating customer support costs.

The Cisco IronPort™ Anti-Malware System uniquely combines Cisco IronPort Web Reputation Filters, a critical first layer of preventative defense against new outbreaks, with best-of-breed signature-based verdict engines to provide powerful, fully integrated anti-malware defense. As the second layer of defense on the Cisco IronPort S-Series Web Security Appliance, the Cisco IronPort Anti-Malware System rapidly scans web content, as it is downloaded, against malware and virus signatures - eliminating the broadest range of known and emerging web-based threats. The combination of proprietary Cisco technology with multiple antivirus engines, including Sophos, Webroot, and McAfee, provides maximum security without compromising scalability.



### Industry-Leading Accuracy and Performance

The Cisco IronPort Anti-Malware System delivers exceptional performance in a single appliance. Cisco IronPort built the system to be fast and accurate, relying on a less computationally intensive single scan to evaluate a broad range of threats, including malware, phishing, pharming, rootkits, and more. With the industry's largest malware signature database located at the gateway, the Cisco IronPort Anti-Malware System provides enterprises with industry-leading protection against these threats.

Cisco IronPort's powerful dynamic vectoring and streaming (DVS) engine employs rapid object parsing and vectoring techniques, along with stream scanning, early exit algorithms, and reputation-based caching. This results in an unparalleled increase in scanning throughput over existing first-generation Internet Content Adaptation Protocol (ICAP)-based solutions.

---

To maximize efficacy, the Cisco IronPort Anti-Malware System supports verdict engines from multiple vendors.

**Broad threat categorization** identifies new and more sophisticated security threats, both on the request side and response side. The Cisco IronPort Anti-Malware System conducts deep archive scanning to detect viruses and malware obfuscated within archive packages. It also detects rootkits - hidden software that provides root-level access to, and control over, a computer without its owner's knowledge.

**Blocking threats at the corporate gateway** prevents infection and reduces cleanup costs. By stopping threats before they enter the network, the Cisco IronPort Anti-Malware System prevents initial and ongoing damage.

### The Broadest Range of Signatures

**Integrated scanning engines from Sophos, Webroot, and McAfee** allow you to scan for web-based threats in parallel, providing superior protection and performance.

The Sophos anti-malware engine offers traditional virus detection methods and complementary proactive protection through its Behavioral Genotype<sup>®</sup> technology, which defends against unknown or zero-day malware, including variants of known threat families. The Sophos malware scanning engine uses multiple detection techniques, including pattern matching, emulation technology, and behavioral genotype technology to accurately identify and block malware.

Sophos' Behavioral Genotype technology provides the best proactive protection by identifying new threats, enabling their in-house threat research teams to rapidly develop and test signatures and respond to blended threats before they infect corporate networks.

The Webroot scanning engine performs both request- and response-side scans. Efficacy and coverage are strengthened by Webroot's Phileas system, which identifies existing and new threats by intelligently scanning millions of sites daily.

The McAfee database includes virus and malware signatures and can be configured to perform both signature-based and heuristics-based scanning.

Cisco IronPort Anti-Malware System has the largest number of threat categories for the web gateway; this provides granular visibility into threat activity and specialized policy creation. Sixteen threat categories provide the enterprise with significant control to manage and balance risk management versus users needs.

IronPort DVS Anti-Malware Settings		
<input checked="" type="checkbox"/> Enable Suspect User Agent Scanning <input checked="" type="checkbox"/> Enable Webroot <input checked="" type="checkbox"/> Sophos		
<i>McAfee and Sophos cannot be enabled at the same time.</i>		
Malware Categories	Monitor	Block
	Select all	Select all
<input checked="" type="checkbox"/> Adware	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Browser Helper Object	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Commercial System Monitor	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Dialer	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Generic Spyware	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Hijacker	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Phishing URL	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> PUA	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> System Monitor	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Trojan Downloader	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Trojan Horse	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Trojan Phisher	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Virus	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Worm	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Other Malware	<input checked="" type="checkbox"/>	
Other Categories	Monitor	Block
	Select all	Select all
<input checked="" type="checkbox"/> Encrypted File	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Suspect User Agents	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Unscannable	<input checked="" type="checkbox"/>	

## Powerful Management Capabilities

A **web-based GUI** provides unprecedented control for initial configuration and ongoing management. The comprehensive, easy-to-use Cisco IronPort Anti-Malware System deploys in multiple modes, including “monitor only” or “monitor and block.”

**Malware categories and actions by verdict type** are managed within Cisco IronPort Web Security Manager. Administrators can create and easily manage custom anti-malware policies, and can enable or disable malware filtering on a per-user/per-group basis. The Cisco IronPort Anti-Malware System is the only solution to offer customers distinct settings for known and suspect malware and allow enterprises to set their own custom thresholds for malware-positive verdicts.

**Point-and-click functionality** is provided by Cisco IronPort Web Security Manager to enable/disable the service, select deployment modes, set thresholds, configure automated updates, and more. Automated, timely, and secure updates, which can be scheduled for as frequently as every five minutes, ensure coverage against the latest emerging virus and malware threats.

## Real-Time Monitoring and Comprehensive Reporting

**Real-time visibility** into trouble spots in a network’s web traffic requests are provided by the Cisco IronPort Anti-Malware System. Reports include top malware sites detected, malware threats, and categories identified/blocked. In addition, the reports provide actionable information, such as a list of top clients infected, as well as historical trends. Through IronPort Web Security Manager, administrators have comprehensive visibility and the ability to correlate malware activity with clients.

A **sophisticated alert engine**, included with every Cisco IronPort S-Series Web Security Appliance, also benefits the Cisco IronPort Anti-Malware System. Administrators can set up individual alert subscriptions for the system, based on severity levels. Alerts are calibrated in three categories: informational, warning, and critical. This provides administrators with clear visibility into the application and enables them to take appropriate and timely action, if required.

---

## Benefits

**Highest accuracy and lowest latency.** Optimized for accuracy and performance, the Cisco IronPort Anti-Malware System helps ensure industry-leading efficacy without any perceptible change to the end-user experience. The system combines the rapid parsing and vectoring capabilities of the Cisco IronPort DVS engine with extensive and accurate signature-based verdict engines from Sophos, Webroot, and McAfee.

The Cisco IronPort Anti-Malware System is updated in real time to ensure the most current protection available.

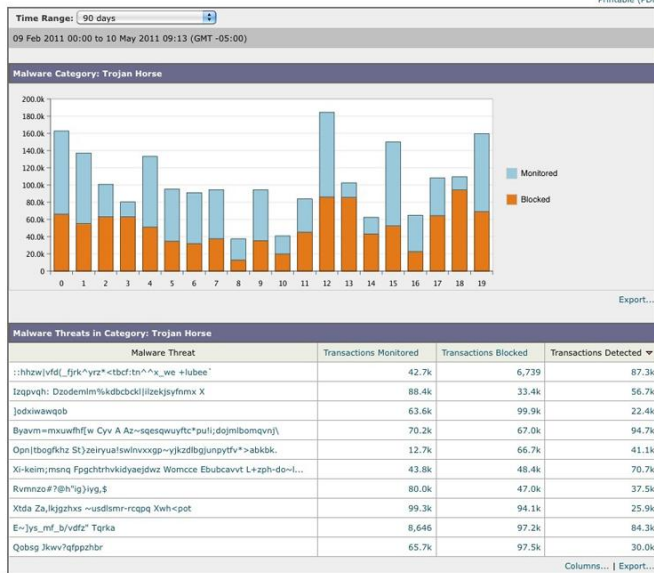
**Protection against the broadest range of web-based malware.** The Cisco IronPort Anti-Malware System quickly and accurately detects and blocks a full range of known and emerging threats, including viruses, adware, spyware, worms, Trojans, system monitors, keyloggers, rootkits, tracking cookies, browser hijackers, browser helper objects, phishing, and more - all in one single scan.

**Near-zero administrative overhead.** The Cisco IronPort S-Series web-based GUI makes initial configuration and setup simple. The Cisco IronPort Anti-Malware System's scanning accuracy virtually eliminates customer support calls and expensive desktop cleanup operations. Automated, timely, and secure updates reduce the need for ongoing manual tuning and maintenance to catch new and emerging threats.

**Comprehensive visibility.** Administrators and executive management may require information to better understand ever-evolving corporate threats. The Cisco IronPort Anti-Malware System's comprehensive reporting provides powerful insight into threats monitored or blocked, as well as the presence of infected clients. This reporting functionality also allows for a better view of user actions, providing data to help establish policies to further protect the network and corporate desktops.

**Low total cost of ownership.** First-generation, ICAP-based anti-malware solutions require ownership and administration of multiple servers. Unlike these products, the Cisco IronPort Anti-Malware System is delivered as a high-performance, single-appliance solution.

Malware Category  
Trojan Horse



Summary

The strong perimeter defense provided by the Cisco IronPort Anti-Malware System prevents client infections and greatly reduces cleanup costs. This is achieved with enhanced performance and security by utilizing multi-engine parallel stream scanning. As an important part of the Cisco IronPort S-Series, this solution combines unmatched accuracy and exceptional performance to deliver powerful protection with no perceptible change to the end-user experience.



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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://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. (1005R)