

# Cisco IronPort Anti-Spam

ACCURATELY PROTECT AGAINST DIVERSE THREATS



Internet criminals constantly evolve techniques to penetrate an organization's defenses. Email threats have expanded beyond simply annoying spam to dangerous phishing and fraudulent spam. Cisco® IronPort Anti-Spam uses conventional techniques and innovative context-sensitive detection technology to eliminate a diverse range of known and emerging email threats.

## THE CISCO IRONPORT DIFFERENCE

Cisco IronPort® email and web security products and services are high-performance, easy-to-use and technically-innovative solutions, designed to secure organizations of all sizes. Purpose built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

Leveraging the Cisco Security Intelligence Operations (SIO) center and global threat correlation makes the Cisco IronPort solutions smarter and faster. This advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

## FEATURES

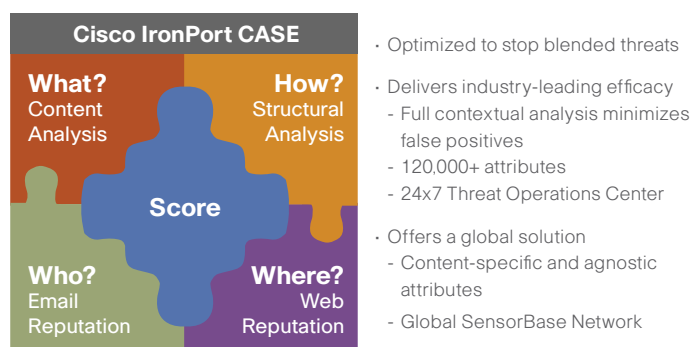
### Powerful Outer Layer of Defense

Cisco IronPort pioneered the technique of reputation filtering for a powerful outer layer of spam defense. Cisco IronPort Reputation Filtering stops 90 percent of incoming threats at the connection level. Cisco IronPort appliances and hosted services also support a unique rate-limiting capability to intelligently delay suspicious senders—greatly reducing spam without the risk of false positives.

### Accuracy with Context-Based Scoring

An innovative approach to threat detection helps separate Cisco IronPort Anti-Spam from the competition. In addition to reviewing sender reputation, the unique Cisco IronPort Context Adaptive Scanning Engine (CASE) examines the complete context of a message. In combination, the CASE score and sender reputation result in more accurate spam filtering than do traditional techniques.

Cisco IronPort Web Reputation technology measures the behavior and traffic patterns of a website to assess its trustworthiness. The Cisco IronPort CASE determines the reputation of any URL within a message body to facilitate an accurate analysis of messages. This technology helps to immediately protect Cisco IronPort Anti-Spam users from spam, malware, viruses, phishing, and spyware threats.



*Cisco IronPort CASE technology uses advanced machine learning techniques to emulate the logic used by a human that is evaluating the legitimacy of a message. A human reader, as well as the CASE, asks these four basic questions.*



## FEATURES (CONTINUED)

### Automatic Updates and Comprehensive Controls

**Automatic, timely, and highly secure rule updates** eliminate the need for ongoing manual tuning and maintenance to catch emerging threats. The Cisco update service helps ensure that Cisco IronPort solutions are running the most up-to-date engine

**Cisco IronPort Email Security Manager** can be utilized to set user- and group-specific policies. Administrators can easily configure the solution at a global level.

**The Cisco IronPort Spam Quarantine** gives end users direct access to check and manage messages or to review email digests that are mailed to them periodically. A powerful spam-reporting plug-in for Microsoft Outlook allows users to send missed spam directly to the Cisco Threat Operations Center for review.

**Marketing message detection** allows administrators to configure treatment of unwanted marketing messages.

### Real-Time and Centralized Reporting

**Cisco IronPort Email Security Monitor** delivers complete real-time visibility into who is sending email. It also alerts administrators to suspicious traffic so that they can take immediate action.

**Cisco IronPort Message Tracking** lets administrators find the status of any message that has crossed their email security solution. With this centralized reporting tool, administrators and support staff can quickly answer end-user inquiries such as, "What happened to my email?"

### Fast, Accurate Detection

**The Cisco 24-Hour Threat Operations Center** uses extensive technology and infrastructure to help ensure effectiveness. All together, the center's analysts speak more than 40 languages and have powerful tools to:

- Maintain email collection and analysis
- Manage a knowledge base of latest trends
- Publish real-time rule updates to help ensure that new spam, phishing and malware attacks can be blocked immediately
- Provide closed-loop verification of customer reports



*The Cisco Threat Operations Center provides the highest level of threat correlation—enabling users to collaborate with confidence.*

## BENEFITS

### Eliminates a Broad Range of Email Threats

Cisco IronPort Anti-Spam addresses a full range of known threats, including spam, spearphishing, and zombie attacks. It also addresses hard-to-detect, low-volume, short-lived targeted attacks such as 419 scams. Additionally, Cisco IronPort Anti-Spam identifies new and evolving blended threats, such as malicious content through a download URL or an executable file.

### Provides Great Accuracy

The key to effectiveness is data captured by the Cisco IronPort SenderBase Network, the world's first, largest, and most accurate traffic-monitoring system. In addition to exceptional technology, Cisco IronPort Anti-Spam is backed

by an interdisciplinary team of experts with backgrounds in email security, machine learning, and human genomics. As a leader in preventive threat detection techniques, Cisco employs security experts who constantly innovate to stay ahead of emerging threats. Cisco IronPort Anti-Spam is integrated with Cisco Security Intelligence Operations, which helps ensure a high level of accuracy and responsiveness.

Cisco is consistently recognized for superior email threat prevention through third-party tests and industry awards. On average, Cisco stops over 99 percent of spam, phishing and virus attacks with near-zero false positives.



## BENEFITS (CONTINUED)

---

### Promotes Ease of Use and Near-Zero Administration

Cisco's automatic, timely, and highly secure rule updates eliminate the need for ongoing manual tuning and maintenance to catch emerging threats. This time savings, combined with comprehensive reporting, gives administrators powerful insight into their email traffic.

### Adds a Global Solution

Cisco IronPort Anti-Spam uses locale-specific, content-aware threat detection techniques. It also takes full advantage of globally representative SMTP and HTTP content-independent data contributed by more than 120,000 ISPs, universities, and corporations on six continents.

### Delivers Industry-Leading Performance

Cisco IronPort spam-filtering technologies deliver industry-leading performance based on real-world mail streams. Cisco IronPort Reputation Filters:

- Decrease email bandwidth consumption by 90 percent or more
- Greatly improve system efficiency
- Reduce the number of messages that need to be processed

Additionally, the innovative Cisco IronPort CASE performs multiple evaluations simultaneously during a single message scan, eliminating unnecessary computational overhead.

## SUMMARY

---

### The Anti-Spam Solution

With email threats on the rise, and threat writers constantly evolving techniques to penetrate companies' existing defenses, a multi-layered spam defense provides companies with the most secure protection. Utilizing both best-of-breed conventional techniques and a revolutionary context-sensitive detection technology (that even filters the URL within a message body), Cisco IronPort Anti-Spam eliminates the broadest range of known and emerging email threats.

## CONTACT US

---

### How to Get Started

Cisco sales representatives, channel partners and system engineers are ready to help you evaluate how Cisco IronPort products can make your corporate network infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from these industry-leading products, please call 650-989-6530 or visit us on the web at [www.ironport.com/leader](http://www.ironport.com/leader).



**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).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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.  
(0908R)