

# Cisco IronPort Email Security Appliances

## Why Is Email Security So Important?

The volume and sophistication of email-based threats continues to grow at an unchecked pace. Most organizations observe that as much as 90 percent of their incoming mail is invalid (spam, viruses, etc.), with the total number of incoming messages increasing every year - even as the number of employees stays constant. These email security threats are fueled by a powerful profit motive associated with spam, fraud, and information theft. This creates resources that bring professional engineers into the business of developing new threats, further exacerbating the situation. As this cycle does not appear to have a natural equilibrium, threats are expected to continue to grow in volume and sophistication for the foreseeable future.

There are no "silver bullets" to eliminate the flaws found in email. The ultimate answer will likely emerge as a mixture of many complementary solutions. The sustained viability of email demands a convergence of market-driven research and technological development.

## What Are Cisco's Email Security Products?

### Cisco IronPort Email Security Appliances

The Cisco IronPort® C-Series and Cisco IronPort X-Series Email Security Appliances are in production at eight of the ten largest ISPs and more than 20 percent of the world's largest enterprises. These industry-leading systems have a demonstrated record of unparalleled performance and reliability.

IronPort® email security appliances combine market-leading, best-of-breed antispam, antivirus, encryption, digital rights management, and archiving technologies. These solutions run on IronPort's revolutionary MTA platform, providing the highest levels of email protection, with exclusive preventive and reactive technologies and industry-leading email management tools.

With a complete portfolio of secure delivery methods, integrated key management, and the power of business-class email, IronPort technology also provides industry-leading encryption capabilities, enabling the comprehensive functionality necessary to protect even the most complex enterprise environments.

By reducing the downtime associated with spam, viruses, and blended threats, IronPort email security appliances vastly improve the administration of corporate email systems, reduce the burden on technical staff, and provide constant state-of-the-art network protection.

IronPort email security appliances provide a multilayer approach to stopping email-based threats:

- For spam protection, email and web reputation filtering technology is combined with industry-leading Cisco IronPort Anti-Spam feature.
- Cisco IronPort Outbreak Filters are paired with fully integrated traditional antivirus technology and patent-pending anti-targeted attack protection to ensure users are protected from the industry's more malicious attacks.

- Cisco Data Loss Prevention technology provides organizations with the broadest set of tools to enforce regulatory compliance and acceptable use policies accurately and efficiently.
- Cisco IronPort PXE encryption technology fulfills secure messaging, compliance, and regulatory requirements.

Figure 1 shows a typical Email Security deployment.

**Figure 1.**



IronPort email security solutions integrate easily into existing messaging infrastructures – delivering defense-in-depth security.

### What Is the Cisco SenderBase Network?

Cisco IronPort appliances harness the power of the SenderBase<sup>®</sup> Network. This powerful threat tracking database captures data from more than 100,000 organizations worldwide, providing a large and diverse sample of Internet traffic patterns.

- SenderBase receives over 30 billion queries daily.
- Using SenderBase data increases malware catch rates by more than 20 percent over signature-based scanning alone - an unprecedented increase in efficacy.
- For live threat updates and real-time access to your SenderBase Reputation Score (SBRS), visit: <http://www.senderbase.org>.

### What Are Cisco IronPort's Email Security Technology Differentiators?

**Cisco IronPort AsyncOS<sup>®</sup>** is a unique, high-performance software architecture designed to address concurrency-based communications bottlenecks and the limitations of file-based queuing.

**Cisco IronPort Reputation Filters** perform a real-time email threat assessment and then identify suspicious email senders. Suspicious senders are rate limited or blocked, preventing malicious traffic from entering the network.

**Cisco IronPort Anti-Spam** combines best-of-breed conventional techniques with IronPort's breakthrough context-sensitive detection technology to eliminate the broadest range of known and emerging email threats.

**Cisco IronPort Outbreak Filters** detect new virus outbreaks in real time, then quarantine suspicious messages - offering protection up to 42 hours before traditional antivirus solutions.

**Cisco Data Loss Prevention technology** provides comprehensive DLP policies and remediation options, unparalleled accuracy, and easy deployment and management capabilities - meeting acceptable use policy and compliance requirements readily.

**Cisco IronPort PXE encryption technology** revolutionizes email encryption - meeting compliance requirements while delivering powerful business-class email features.

The **Cisco Threat Operations Center (TOC)** provides a 24x7 view into global traffic activity, enabling Cisco to analyze anomalies, uncover new threats, and track traffic trends.

Figure 2 shows the major elements integrated in an IronPort Email Security Appliance.

**Figure 2.**



IronPort email security appliances provide multi-layered security in a single solution.

### What Sets Cisco Apart from Other Email Security Vendors?

- IronPort technology provides the industry’s highest spam catch rate, greater than 99 percent, with a less than one in one million false positive rate.
- IronPort Reputation Filters eliminate 80 percent of junk email, before it enters your network.
- Cisco Ironport provides DomainKeys (DKIM) signing, directory harvest attack (DHA) prevention, and complete protection against bounced-message attacks.
- Cisco Ironport allows you to set different filtering policies for different groups within your organization.
- Real-time reporting allows administrators to be proactive about email security and modify policies if the organization is under network attack.

### Which Cisco IronPort Email Security Appliance is Right For My Organization?

- **Cisco IronPort Email Security Appliance X1070:** Built to meet the needs of the most demanding networks in the world.
- **Cisco IronPort Email Security Appliance C670:** Designed for organizations with more than 10,000 users.
- **Cisco IronPort Email Security Appliance C370:** Designed for organizations with 2000 to 10,000 users.
- **Cisco IronPort Email Security Appliance C170:** Designed for small businesses and organizations with up to 1000 users.
- **Cisco IronPort Encryption Appliance:** The most comprehensive email encryption gateway on the market.

**Table 1.** Specifications for Cisco IronPort C-Series and X-Series Email Security Appliances

	Cisco IronPort X1070	Cisco IronPort C670	Cisco IronPort C370	Cisco IronPort C170
<b>Chassis</b>				
<b>Form Factor</b>	2 RU	2 RU	2 RU	1 RU
<b>Dimensions (H x W x D)</b>	3.5" x 17.5" x 26.8"	3.5" x 17.5" x 26.8"	3.5" x 17.5" x 26.8"	1.67" x 16.9" x 15.5"
<b>Total Weight (lbs)</b>	57.5	52.2	49	26.96
<b>Power Supply</b>	870W, 100/240V	870W, 100/240V	870W, 100/240V	400W, 100/240V
<b>Redundant Power Supply</b>	Yes	Yes	Yes	No

	Cisco IronPort X1070	Cisco IronPort C670	Cisco IronPort C370	Cisco IronPort C170
<b>Processor, Memory, and Disks</b>				
<b>CPUs</b>	2x4 (2 Quad Cores)	2x4 (2 Quad Cores)	1x4 (1 Quad Core)	1x2 (1 Dual Core)
<b>Memory</b>	4 GB	4 GB	4 GB	4 GB
<b>Disk Space and Count</b>	1.8 TB (300 * 6)	1.2 TB (300 * 4)	600 GB (300 * 2)	500 GB (250 * 2)
<b>Hot-Swappable Hard Disk</b>	Yes	Yes	Yes	Yes
<b>RAID Level and Controller</b>	RAID 10, hardware	RAID 10, hardware	RAID 1, hardware	RAID 1, software
<b>Interfaces</b>				
<b>Ethernet</b>	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	2 Gigabit NICs, RJ-45
<b>Speed (mbps)</b>	10/100/1000, Auto-Negotiate	10/100/1000, Auto-Negotiate	10/100/1000, Auto-Negotiate	10/100/1000, Auto-Negotiate
<b>Duplex</b>	Half or Full, Auto-Negotiate	Half or Full, Auto-Negotiate	Half or Full, Auto-Negotiate	Half or Full, Auto-Negotiate
<b>Serial</b>	1xRS-232 (DB-9), serial	1xRS-232 (DB-9), serial	1xRS-232 (DB-9), serial	1xRS-232 (RJ-45)
<b>Fiber</b>	Optional, 2 fiber ports (1000BASE-SX)	Optional, 2 fiber ports (1000BASE-SX)	Optional, 2 fiber ports (1000BASE-SX)	No
<b>USB</b>	0	0	0	2
<b>Configuration Logging and Monitoring</b>				
<b>Web Interface</b>	GUI-based (HTTPS)	GUI-based (HTTPS)	GUI-based (HTTPS)	GUI-based (HTTPS)
<b>Command Line Interface</b>	SSH or Telnet (command-based)	SSH or Telnet (command-based)	SSH or Telnet (command-based)	SSH or Telnet (command-based)
<b>Logging</b>	Syslog	Syslog	Syslog	Syslog
<b>Centralized Reporting</b>	Supported	Supported	Supported	Supported
<b>File Transfer</b>	SCP, FTP	SCP, FTP	SCP, FTP	SCP, FTP
<b>Configuration Files</b>	XML-based	XML-based	XML-based	XML-based
<b>Centralized Configuration</b>	Supported	Supported	Supported	Supported
<b>Monitoring</b>	SNMPv1-3, email alerts	SNMPv1-3, email alerts	SNMPv1-3, email alerts	SNMPv1-3, email alerts
<b>Environmental Operating Ranges</b>				
<b>Total Current (A)</b>	3.7	3	2.7	4.85 (max)
<b>Input Voltage (V)</b>	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
<b>Operating Power (W)</b>	394.8	325.4	287.6	400 (max)
<b>Total Heat Dissipation (BTU/Hr)</b>	1904	1904	1801.6	432.6
<b>Leakage Current (mA)</b>	3.5	3.5	3.5	3.5
<b>Fan Exhaust Volume (CFM)</b>	43.1	37.4	37.4	Idle at 24°C: 12.3 Full fan speed: 34.4
<b>Ambience Noise (bels)</b>	6.3	6.3	6.1	Idle: 41.3 dBa Stress: 64.2 dBa (max)
<b>Effective MTBF (Hours)</b>	94,400	94,400	94,400	107,356
<b>Operating</b>				
<b>Temperature (°C)</b>	10°C to 35°C	10°C to 35°C	10°C to 35°C	-5°C to 45°C
<b>Relative Humidity (%)</b>	20% to 80% (noncondensing)	20% to 80% (noncondensing)	20% to 80% (noncondensing)	20% to 80% (noncondensing)
<b>Altitude (m)</b>	3048	3048	3048	3000

	Cisco IronPort X1070	Cisco IronPort C670	Cisco IronPort C370	Cisco IronPort C170
<b>Vibration</b>	0.26 Grms at 5-350Hz	0.26 Grms at 5-350Hz	0.26 Grms at 5-350Hz	0.41Grms, at 3Hz-500Hz
<b>Non-Operating</b>				
<b>Temperature (°C)</b>	-40°C to 65°C	-40°C to 65°C	-40°C to 65°C	-25°C to 70°C
<b>Relative Humidity (%)</b>	5% to 95% (noncondensing)	5% to 95% (noncondensing)	5% to 95% (noncondensing)	5% to 95% (noncondensing)
<b>Altitude (m)</b>	10,600	10,600	-16 to 10,600	4570
<b>Vibration</b>	1.54 Grms at 10-250Hz	1.54 Grms at 10-250Hz	1.54 Grms at 10-250Hz	1.12Grms at 3Hz-500Hz
<b>Industry Certifications</b>				
<b>RoHS</b>	Yes	Yes	Yes	Yes
<b>Other Certifications</b>				Safety: cULus, CB, CCC, BSMI EMC:CE, FCC, VCCI, C-TICK, KC

### Where Should I Go For More Information?

To secure greater protection for your company's messaging system, participate in the "TRY BEFORE YOU BUY" evaluation program. To receive a fully functional evaluation appliance to test in your network, free for 30 days, visit: <http://www.ironport.com/try>.



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 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](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. (1110R)