Ⓘ **IRONPORT**®

ADVANCED THREAT PREVENTION, SPAM AND VIRUS BLOCKING, AND CORPORATE EMAIL POLICY ENFORCEMENT.

IronPort C660 Email Security Appliance for Large Enterprises and ISPs

OVERVIEW

As the battle to protect the corporate email perimeter continues, two trends emerge: higher mail volumes and more resource-intensive scanning. The *IronPort C660*™ is purpose-built, on the foundation of the *IronPort AsyncOS*™ operating system, to provide power for today's volumes and high-performance scanning for tomorrow's threats. This unparalleled performance delivers dial-tone availability—saving hours of productivity and thousands of dollars during peak traffic times, such as damaging virus outbreaks or spam attacks.

Fortune 500 and Global 2000 companies need a secure and easy-to-manage email security solution that protects all facets of their complex email infrastructures. The *IronPort C660* provides IronPort's exclusive preventive filters and signature-based reactive filters (combined with data loss prevention and best-of-breed, onbox encryption technology) to enable the highest level of email security available today—while delivering unprecedented visibility and management tools.

FEATURES

The *IronPort C660* provides the world's most powerful multi-layered approach to email security.

SPAM PROTECTION

IronPort® provides defense in depth against spam by providing two layers of protection — a preventive layer of reputation filters, followed by reactive filters.

IronPort Reputation Filters™ provide an outer layer of defense using *IronPort SenderBase*® data to perform a real-time email traffic threat assessment and identify suspicious email senders.

IronPort Anti-Spam™ **Filters** utilize the industry's most innovative approach to threat detection, based on IronPort's unique *Context Adaptive Scanning Engine*™ *(CASE)*. *IronPort's CASE* examines the complete context of a message, including: "What" content the message contains, "How" the message is

constructed, "Who" is sending the message, and "Where" the call to action of the message takes you. By combining these elements, *IronPort Anti-Spam* stops the broadest range of threats with industry-leading accuracy.

The IronPort Spam Quarantine™ is a self-service end-user solution, with an easy to use Web or email-based interface. This feature provides end-users with their own safe holding area for spam messages and integrates seamlessly with existing directory and mail systems.

VIRUS PROTECTION

IronPort Virus Outbreak Filters™ identify and quarantine viruses hours before traditional virus signatures are available.

Sophos Anti-Virus technology provides a fully integrated second layer of virus protection with the highest-performance virus scanning technology in the industry.

▶

McAfee Anti-Virus technology is fully integrated to provide an additional layer of protection (either in conjunction with, or as an alternative to, Sophos) for maximum virus security.

DATA LOSS PREVENTION

Integrated Compliance Filters allow customers to address PCI, HIPAA, GLB, SOX and other regulatory compliance requirements. IronPort's easily-deployed and easily-managed solution also enables intellectual property protection and enforces organizations' acceptable use policies.

IronPort Email Encryption gives administrators the ability to secure confidential data and comply with partner, customer or regulatory requirements. *IronPort PXE*™ technology enables simple, secure communication from the gateway to any recipient inbox — while TLS, PGP and S/MIME technology provide security between partner email gateways.

Compliance Quarantine provides delegated access to emails that have been flagged by the content scanning engine.

EMAIL AUTHENTICATION

DomainKeys Identified Mail (DKIM), and DomainKeys verification and signing digitally process messages to establish and protect identities with email senders and receivers on the Internet.

IronPort Bounce Verification™ tags messages with a digital watermark to provide filtering of bounce attacks at the network edge.

Directory Harvest Attack Prevention tracks spammers who send to invalid recipients and blocks attempts to steal email directory information.

ENTERPRISE MANAGEMENT TOOLS

Email Security Manager™ is a powerful, graphical management tool that provides fingertip control to manage all email security – including preventive and reactive anti-spam and anti-virus filters, email encryption and content filtering.

Intuitive GUI enables unprecedented visibility and control. The integrated Web-based user interface enables real-time and historical reporting along with the ability to configure policies, search, and selectively release quarantined messages.

Centralized Management eliminates a single point of failure with superior "peer to peer" architecture and makes managing multi-box installations of IronPort email security appliances simple. The ability to manage configuration at multiple levels allows organizations to manage globally while complying with local policies.

Email Security Monitor™ delivers real-time threat monitoring and reporting. This technology tracks every system connecting to your IronPort appliance to identify Internet threats (such as spam, viruses and denial-of-service attacks), monitor internal user trends and highlight compliance violations.

SNMP Enterprise MIB facilitates hands-off monitoring and alerting for all system parameters including hardware, security, performance and availablility.

IRONPORT MTA PLATFORM

AsyncOS, IronPort's proprietary operating system, was built from the ground up to address the requirements of modern email gateways and to position customers for the future of SMTP. The *IronPort C660* supports thousands of simultaneous incoming and outgoing connections—ensuring that your email infrastructure is never overwhelmed, even during the largest outbreaks or attacks.

BENEFITS

Reporting Insight Proves ROI The *IronPort C660* offers very sophisticated management, monitoring and reporting tools designed to satisfy the large global enterprises and ISPs that make up IronPort's customer base. Each appliance has a unique reporting system, providing both a real-time and historical look at mail flowing through your email infrastructure. IronPort provides system administrators with the necessary information to make critical security decisions and demonstrate Return On Investment (ROI).
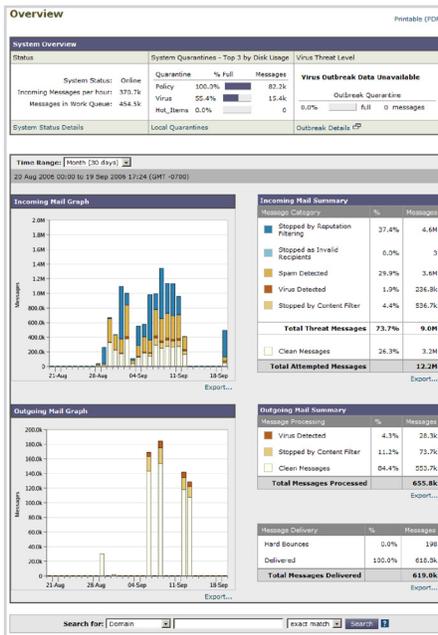

IronPort Email Security Monitor's intuitive graphical user interface enables real-time and historical visibility into your email traffic.

The *IronPort C660* integrates easily into existing messaging infrastructures—delivering defense-in-depth security with carrier-proven technology and the management capabilities required by large enterprises and ISPs.


Reduced TCO The *IronPort MTA* platform enables massive reduction in Total Cost of Ownership (TCO) by consolidating email operations and security into a single platform. Self-managing security services provide the lowest maintenance solution in the industry with minimal configuration requirements.

Increased End-User Productivity By securing the network at the gateway level, the *IronPort C660* acts as a "shock absorber," in front of the groupware server(s). This ensures that end-users are not bogged down by spam, viruses, and other threats. Unlike other solutions, IronPort security services do not rely on end-users to "train" the system. Instead, high accuracy is maintained through continuous and automatic rule updates.

Improved Administrative Efficiency IronPort's *Reputation Filtering* system was the first in the industry and remains the most sophisticated. In its default settings, the system will block over 80 percent of incoming mail at the connection level. By eliminating these unwanted messages, companies save bandwidth (the message is never accepted) and system resources. CPU-intensive spam and virus filters are used only when needed, and rate limiting is a very effective defense against "hit and run" spam attacks or denial-of-service attacks.

Minimized Downtime The comprehensive *IronPort C660* solution ensures the availability and security of your email infrastructure. IronPort offers a variety of security applications for spam and virus filtering, content scanning, and policy enforcement. Together these features reduce the risk and potential downtime posed by security threats.
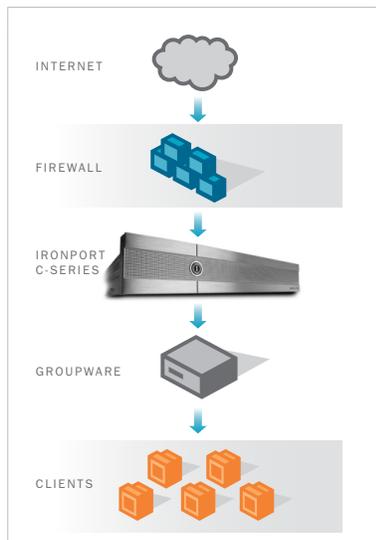
FIGURE 1.

TODAY'S EMAIL-BORNE THREATS consist of virus attacks, spam, false-positives, distributed denial of service attacks, directory harvest attacks, phishing (fraud), data loss and more. The *IronPort C660* email security appliance addresses the issues faced by large enterprises and ISPs, by uniquely combining powerful performance with preventive and reactive security measures that are easy to deploy and manage.

Power at the Perimeter:
The *IronPort C660* provides multi-layered security on a single appliance by combining IronPort's revolutionary technology with additional market-leading solutions.

MANAGEMENT TOOLS			
SPAM DEFENSE	VIRUS DEFENSE	DATA LOSS PREVENTION	EMAIL ENCRYPTION
THE IRONPORT ASYNCOS EMAIL PLATFORM			

SPECS

CHASSIS / PROCESSOR

Form Factor	19" Rack-Mountable, 2U rack height
Dimensions	3.5" (h) x 19" (w) x 29" (d)
CPU	Two Intel Multi-Core Processors
Power Supplies	Hot-plug redundant, 750 watts, 100/240 volts

STORAGE

RAID	RAID 1+0 configuration; Dual channel hardware with battery-backed cache
Drives	Four hot-swappable, 300 GB Serial attached SCSI
Capacity	70 GB queue capacity

CONNECTIVITY

Ethernet	Two Broadcom Gigabit BaseT and One Intel 10/100 BaseT Ethernet ports
Serial	One RS-232 (DB-9) Serial Port

MAIL OPERATIONS

Mail Injection Protocols	SMTP, ESMTP, Secure SMTP over TLS
Mail Delivery Protocols	SMTP, ESMTP, Secure SMTP over TLS
DNS	Internal resolver/cache; Can resolve using local DNS or Internet DNS servers
LDAP	Integrates with Active Directory, Notes, Domino and OpenLDAP servers.

INTERFACES/CONFIGURATION

Web Interface	Accessible by HTTP or HTTPS
Command Line Interface	Accessible via SSH or Telnet; Configuration Wizard or command-based
File Transfer	SCP or FTP
Programmatic Monitoring	XML over HTTP(S)
Configuration Files	XML-based configuration files archived or transferred to cluster

CRYPTOGRAPHIC ALGORITHMS

TLS (Encrypted SMTP)	56-bit DES, 168-bit 3DES, 128-bit RC4, 128-bit AES and 256-bit-AES
DomainKeys Signing	512, 768, 1024, 1536 and 2048-bit RSA
SSH for System Management	768 and 1024-bit RSA
HTTPS for System Management	RC4-SHA and RC4-MD5

PRODUCT LINE

SIZING UP YOUR EMAIL SECURITY SOLUTION

IronPort Systems provides industry leading email security products for organizations ranging from small businesses to the Global 2000.

IronPort X1060™	Built to meet the needs of the most demanding networks in the world.
IronPort C660	Designed for large enterprises and service providers.
IronPort C360™	Suggested for medium to large enterprises.
IronPort C360D™	Recommended for any company with unique outbound email communication needs.
IronPort C150™	An affordable, and easy to use, all-in-one appliance for small to medium enterprises.

SUMMARY

INDUSTRIAL STRENGTH EMAIL SECURITY

The *IronPort C660* is the most sophisticated email security appliance available today. IronPort appliances are in production at eight of the ten largest ISPs and more than 40 percent of the world's largest enterprises.

By reducing the downtime associated with spam, viruses and a wide variety of other threats, the *IronPort C660* enables the administration of complex corporate mail systems, reduces the burden on technical staff, and quickly pays for itself. It is the advanced technology within IronPort appliances that leads to the simplicity of management, and also the highest levels of security in the world. IronPort's email security appliances are carrier class offerings that can support and protect your email systems – not only from today's threats, but from those certain to evolve in the future.

CONTACT US

TRY BEFORE YOU BUY

Through a global salesforce and reseller network, IronPort offers a free "Try Before You Buy" program for the *IronPort C660*. To learn if you qualify call 650-989-6530 or visit us on the Web at www.ironport.com/try

IRONPORT C660
10/08
DOC RELEASE

(I) IRONPORT®

IronPort Systems
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, now part of Cisco, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use— providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

IronPort is now
part of Cisco.

ılıılıı
CISCO™