

10 Key Considerations for a Messaging Gateway Security Solution

1. Complete product family for messaging infrastructure
2. Integrated, secure and scalable architecture with advanced technologies
3. Sophisticated anti-spam with zero administration
4. Advanced malware protection for anti-virus, zero-day and zombie protection that is predictive, preventative *and* reactive
5. Comprehensive corporate policy and regulatory compliance with minimal impact on users
6. Integrated policy-based encryption
7. Multi-protocol protection including instant messaging, VoIP, and mobile devices
8. Enterprise readiness with maximum flexibility and minimum administration
9. Low total cost of ownership
10. Market leader and vendor viability

Encryption

The IronMail encryption engine provides granular policy definition, leveraging LDAP or Active Directory groups and policies, and message characteristics including content, attachments, recipient, domain, and header information. Both B2B and B2C policy-based encryption technologies are supported, ensuring that recipients who have no encryption capabilities are still able to receive and reply to secure email. Because encryption is applied at the gateway instead of at the desktop level, Secure Computing's multiple encryption options remove the burden of determining encryption requirements from the end user. This also avoids common pitfalls associated with end-users forgetting to encrypt sensitive data.

Edge

Secure Computing's Edge™ email security appliance was designed specifically to address the issue of rising spam volumes. Positioned at the perimeter of the mail system, Edge controls traffic at the network border, using patented TrustedSource data to accept or reject email connections based on the reputation of the sending computer. By dropping connections based on reputation, Edge eliminates 50%-80% of email traffic before it has to be processed by any other systems. Edge also blocks hacker assaults that use methods such as denial-of-service attacks, Telnet or ping attacks and buffer overflow attacks.

IronIM

The IronIM™ instant messaging security appliance is the first and only solution that integrates policy to secure, log, monitor and encrypt enterprise IM communications, even over public IM networks. IronIM allows administrators to control and manage the use of public and enterprise IM from a single management platform to eliminate risks from IM-borne threats, ensure compliance with various industry and government regulations, and monitor for information leakage or other policy violations. IronIM supports multiple instant messaging networks (including AOL Instant Messenger, MSN Messenger, Yahoo! Messenger, and corporate IM solutions including Microsoft LCS and IBM SameTime) and does not require deployment of a new IM client.

IronNet

To combat the threats posed by outbound traffic, Secure Computing has developed the IronNet™ appliance to monitor all outbound internet traffic. Outbound traffic is reviewed for compliance violations and subjected to enforcement of corporate policies regarding compliance violations across all messaging protocols company wide, including Webmail services such as MSN Hotmail, Yahoo! Mail and Google gMail, message board and blog postings, peer-to-peer and Voice over Internet Protocol (VoIP) services such as Skype, and FTP transmissions to prevent unauthorized protocol use before the infraction occurs.

RADAR

RADAR™ receives a real-time stream of behavior-based intelligence from TrustedSource, Secure Computing's global threat reputation system. TrustedSource analyzes data from a massive global array of sensors, including more than 110 billion messages per month. RADAR uses the reputation scores from TrustedSource to detect deviations from expected behavior for all senders, and provides real-time alerting to customers, including company risk assessments, internal threat monitoring, and investigative assistance.

Features and Benefits of Secure Computing's Messaging Gateway Security

Advanced Technologies	<ul style="list-style-type: none"> Powered by TrustedSource 	<p>Global intelligence provides an unequalled view of threats worldwide.</p> <p>Provides the advantage of proactively identifying new threats before any other system and automatically ensuring all messaging systems are instantly protected.</p>
	<ul style="list-style-type: none"> Preventive, proactive, and reactive protections to protect against viruses, Trojans, worms, zombies, DoS attacks, directory harvests, phishing, spam, spyware, and malicious content in one solution 	<p>New attacks are neutralized even before signature files are updated, preventing damage and ensuring network integrity.</p>
	<ul style="list-style-type: none"> Protects every messaging protocol that your users might use: email, IM, Webmail, P2P, FTP, VoIP, wireless devices 	<p>Saves money, streamlines maintenance and provides a higher, more consistent level of compliance without having to manage and deploy multiple devices.</p>
Appliance-Based	<ul style="list-style-type: none"> No software to deploy and maintain 	<p>Reduce data center and IT staffing by deploying a turnkey, ease-to-use appliance.</p>
	<ul style="list-style-type: none"> Inbound and outbound protection in one comprehensive appliance 	<p>Reduce load on email servers by controlling all incoming and outgoing mail in one best-of-breed appliance.</p> <p>Reduces costs by combining email security functionality into one best-of-breed solution from one vendor.</p>
	<ul style="list-style-type: none"> Designed for high availability with global scalability and unmatched processing speed 	<p>Peace of mind that your messaging network is protected against threats that may come down the road, no matter how large the enterprise is or how many facilities and users have to be protected.</p>
	<ul style="list-style-type: none"> Positioned at the corporate gateways 	<p>Prevents attacks before they reach vulnerable email servers; ensures that no attacks will infiltrate the network or users.</p> <p>Saves costs on hardware, bandwidth, and networking infrastructure.</p> <p>Gateway protection doesn't interfere with users normal business functions; no end user training required ensures faster adoption.</p>
Outbound Content Filtering	<ul style="list-style-type: none"> Performs advanced content filtering, pattern matching, fingerprinting, clustering, adaptive lexical analysis on both words and phrases, and image scanning and analysis 	<p>Ensures that protected information is automatically discovered and appropriately managed, with no end user training, and no IT overhead.</p> <p>Enforces corporate policies and government regulations without disrupting normal business processes.</p>
	<ul style="list-style-type: none"> Provides multiple encryption standards, as well as "push" and "pull" security 	<p>Automatically and transparently enforce regulatory and corporate compliance with minimum user involvement and administration overhead.</p> <p>Meets the varying needs of different customers and partners in one comprehensive solution.</p>
Market Leader	<ul style="list-style-type: none"> Over 100 patents issued in the U.S. and other countries, Common Criteria EAL2 Certified, Positioned in the leaders quadrant of Gartner's "Magic Quadrant for E-Mail Security Boundary, 2006"¹, IDC's Market Leader, winner of 2006 Best Products awards of SC, Information Security, PC, Network World and SearchSecurity Magazines, and over 19,000 customers in 106 countries, including more than 57% of the Fortune 500 	<p>Guarantees that Secure Computing actually performs as promised.</p> <p>Peace of mind in working with proven technology from a public, stable partner.</p>

¹ Gartner, Inc., "Magic Quadrant for E-mail Security Boundary, 2006", by P. Firstbrook and A. Hallawell, Sept. 25, 2006.

The Gartner Magic Quadrant is copyrighted Sept. 25, 2006 by Gartner, Inc., and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Before IronMail, **Cox Communication's** postmaster was spending 20 hours a week just maintaining content lists. Today, time spent has dropped to three hours a week, they have reduced mail volume by 40%, block on average 25 viruses per week, eliminated the need for 20 new servers, reduced administrative time by over 90%, all with zero false positives.

Donald Wasylyna, manager of information security for the **H. Lee Moffitt Cancer Center and Research Institute** found IronMail to be a cohesive solution, "There weren't services that conflicted with one another. Typically, you'll have five different features but not all five features can be used at the same time." Wasylyna also finds the company's support and customer responsiveness to be excellent. "IronMail was one of the few pieces of security infrastructure that was a true win for us."

Southwest Airlines had the challenge of streamlining their system with a mass transition to a new platform. They also wanted to stop spam, reduce the number of vendors and ease their administrative burdens. "At first we were concerned about putting so many mail groups on our IronMails. But as we went forward with the migration, we found that our concerns were baseless—IronMail didn't even blink. It was wonderful—it did not go down and did not have a huge queue length. Every email was delivered within a minute. We could not have done it without IronMail," said Vasu Salem, systems engineer at Southwest Airlines. Bottom line: Southwest Airlines saved approximately \$300,000 per year, as well as blocking over 90% of incoming mail as spam.

Exeter hospital has 2,500 email users. They needed a solution that could help them comply with HIPAA as well as provide policy-driven encryption to Webmail users. "We needed a solution that was so intuitive and easy-to-use that even my grandmother could easily access encrypted email," said Paul Wolf, Sr. Network Administrator at Exeter Hospital. With IronMail and encryption providing both gateway-to-gateway and gateway-to-user encryption capabilities they are able to provide policy-based compliance and encryption transparently to end-users.



For more information

Contact your local reseller,
or Secure Computing at:
1-800-379-4944 (inside U.S.)
1-408-979-6100 (worldwide)
sales@securecomputing.com

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100
Fax: +1.408.979.6501

European Headquarters

Berkshire, UK
Tel: +44.(0).870.460.4766

Asia/Pacific Headquarters

Wan Chai, Hong Kong
Tel: +852.2598.9280

Japan Headquarters

Tokyo, Japan
Tel: +81.3.5339.6310

For a complete listing of all our global
offices, see www.securecomputing.com/goto/globaloffices

Product Comparison Chart

Features	IronMail*	IronIM	Edge	IronNet	RADAR
Anti-spam protection	X	X	X	X	
Anti-virus protection	X	X	X	X	
Anti-phishing protection	X	X	X	X	X
Anti-zombie					X
Outbound compliance protection	X	X		X	
Powered by TrustedSource	X	X	X	X	X
Supported email platforms	All, including: Microsoft Exchange, Lotus Notes and Domino, and Novell Groupwise	N/A	All, including: Microsoft Exchange, Lotus Notes and Domino, and Novell Groupwise	All, including: Microsoft Exchange, Lotus Notes and Domino, and Novell Groupwise	N/A
Supported instant messaging networks	N/A	AOL Instant Messenger, MSN Messenger, Yahoo! Messenger, Microsoft LCS and IBM SameTime	N/A	N/A	N/A
Supported protocols	SMTP	AOL Instant Messenger, MSN Messenger, Yahoo! Messenger, Microsoft LCS and IBM SameTime	SMTP	HTTP, HTTPS, FTP, Webmail, blogs, P2P, VoIP	N/A
Forensic capabilities	Real time alerts, real time dashboards, detailed historic reporting	Real time alerts, real time dashboards, detailed historic reporting	Real time alerts, real time dashboards, detailed historic reporting	Real time alerts, real time dashboards, detailed historic reporting	Real time alerts, internal IP address monitoring, identifies sources of phishing attacks and destination URLs
High throughput	Up to 60,000 messages/hour (full content analysis)		3 million per appliance per hour		
Encryption	X	X	N/A	X	N/A
Desktop footprint	Zero	Zero	Zero	Zero	Zero
Enterprise class	X	X	X	X	X
Small-medium business	X	X		X	X
Carrier class	X		X	X	X

*Description of IronMail includes advanced compliance and encryption options.