

Secure Computing® is a global leader in Enterprise Security solutions. Our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.

The Industry's Leader in Every Way

Secure Computing's Secure Mail portfolio has passed multiple tests by analysts, independent researchers, and customers



"Best Encryption Solution for Healthcare"



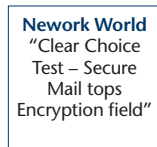
Best Buy 2007: "For its power and relatively low cost of ownership, we rate this product our Best buy."



"Best Email Security Appliance"



"Most impressive arsenal of features"



"Secure Mail tops Encryption field"



COMMON CRITERIA EAL2 CERTIFIED

Web vers. Mar08

Block the Bad; Guard the Good

To combat the real business risks posed by the growing number of messaging security threats, Secure Computing® has developed a layered security solution against inbound and outbound threats that can occur over a messaging infrastructure. These innovative, policy-based security, encryption, and compliance appliances protect multiple messaging protocols, including email, Webmail, file transfers, and other HTTP- and FTP-based communications.

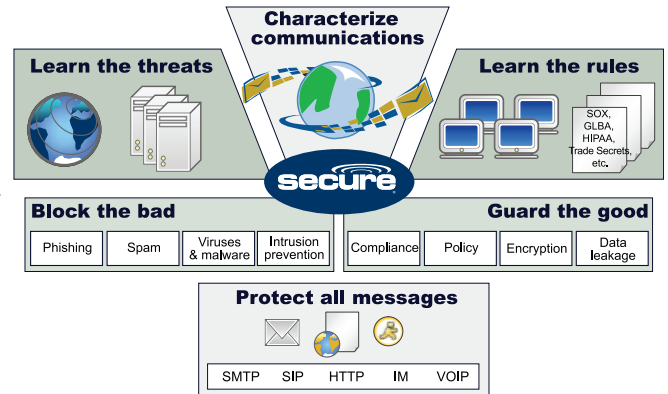


Figure 1: Secure Mail – Inbound and out, regain control of your email messages, their content, compliance, and secure delivery

TrustedSource – Global Intelligence to Protect Your Organization

Secure Computing's TrustedSource™ technology is the cornerstone of our solutions. The most precise and comprehensive Internet host reputation system in the world, TrustedSource characterizes Internet traffic and makes it understandable and actionable. TrustedSource's unrivaled effectiveness is a direct result of Secure Computing's unique view into enterprise Internet traffic. By accumulating huge amount of data daily from over 7000 sensors located in 82 countries, TrustedSource creates a profile of all "sender" activity on the Internet and then utilizes this profile to watch for deviations from expected behavior. The system then generates a "reputation score" based on the behavior of the sending host. This score is incorporated into Secure Computing products to enable them to quickly and accurately reject unwanted traffic.

Secure Mail Portfolio

Secure Mail (IronMail)

Enterprise email systems are prime targets for a host of costly attacks, including inbound threats such as spam, viruses, hacking, worms, and Trojan horses, and outbound threats like corporate or regulatory policy abuse and corporate espionage. Trusted by the world's largest and most respected organizations, including more than 40% of the Fortune 500, the Secure Mail gateway appliances provide the most effective, comprehensive protection for enterprises, small-to-medium businesses, and carrier class environments. Secure Mail (IronMail) combines the critical elements of a comprehensive email security approach into a hardened platform that provides immediate ROI and meets the high-performance demands of today's busy messaging networks.

10 Key Considerations for a Secure Mail 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-layered protection
8. Enterprise readiness with maximum flexibility and minimum administration
9. Low total cost of ownership
10. Market leader and vendor viability

Advanced Compliance

Going beyond simple preservation of sensitive information, industry and government regulations dictate that companies exercise close control over many types of electronic data. Secure Mail's Advanced Compliance Profiler uses multiple sophisticated content analysis engines to monitor and prevent the potential leakage of sensitive data, as well as private, protected customer data. Customers easily train Advanced Compliance to automatically recognize sensitive information in more than 250 document types in 8 different languages. Advanced Compliance can recognize types of data such as social security numbers or bank account numbers. Using fingerprinting, adaptive lexical learning, clustering, and image analysis technologies, it can detect protected documents even if they've been intentionally modified in an attempt to escape detection. Advanced Compliance can detect sensitive information even in the event of:

- Intentional modification of content (both miss-spellings and re-arranging of words)
- Copying and pasting of sensitive data to a different file or to the mail body
- Content leakage in a different version/variation of the trained document (Quarterly Financial reports, modified engineering drawings, modified source code, etc.)

Secure Mail Encryption

The Secure Mail 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.

Secure Mail Edge

Secure Mail Edge email security appliance was designed specifically to address the issue of rising spam volumes. Positioned at the perimeter of the mail system, Secure Mail Edge controls traffic at the network border, using patented TrustedSource data to accept or reject email connections based on the reputation of the sender. By dropping connections based on reputation, Secure Mail Edge eliminates 50%-80% of email traffic before it has to be processed by any other systems. Due to this, the next hop servers see a reduced constant flow eliminating the need to upgrade hardware every 6 to 8 months owing to the rise in spam volumes. Secure Mail Edge also blocks hacker assaults that use methods such as denial-of-service attacks, Telnet or ping attacks, and buffer overflow attacks. There are myriads of regulations that require archiving of all received messages irrespective of them being spam or not. As Secure Mail Edge drops emails at the connection level and never opens the packet, it aids in huge savings when it comes to archiving costs. Secure Mail Edge has been intentionally designed to work with any email security solution and any customer environment.

Table 1: Features and Benefits of Secure Computing's Secure Mail Solution

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, Webmail, 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>

Table 1 continued on page 3

Table 1 continued

Appliance-Based	<ul style="list-style-type: none"> No software to deploy and maintain 	Reduce data center and IT staffing by deploying a turnkey, ease-to-use appliance.
	<ul style="list-style-type: none"> Inbound and outbound protection in one comprehensive appliance 	Reduce load on email servers by controlling all incoming and outgoing mail in one best-of-breed appliance. Reduces costs by combining email security functionality into one best-of-breed solution from one vendor.
	<ul style="list-style-type: none"> Designed for high availability with global scalability and unmatched processing speed 	Peace of mind, whether you're a global giant or 25-person start-up, that you have inbound and outbound messaging protection, powered by TrustedSource. Two categories (S and E class) of Secure Mail appliances are available.
	<ul style="list-style-type: none"> Positioned at the corporate gateways 	Prevents attacks before they reach vulnerable email servers; ensures that no attacks will infiltrate the network or users. Saves costs on hardware, bandwidth, and networking infrastructure. Gateway protection doesn't interfere with users normal business functions; no end user training required ensures faster adoption.
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 	Ensures that protected information is automatically discovered and appropriately managed, with no end user training, and no IT overhead. Enforces corporate policies and government regulations without disrupting normal business processes.
	<ul style="list-style-type: none"> Provides multiple encryption standards, as well as "push" and "pull" security 	Automatically and transparently enforce regulatory and corporate compliance with minimum user involvement and administration overhead. Provides Encryption to Anyone (yahoo accounts, gmail accounts, patients, law clients, etc.), Anywhere (email client, Web browsers, PDAs, etc).
Market Leader	<ul style="list-style-type: none"> Over 100 patents issued in the U.S. and other countries, Common Criteria EAL2 Certified, IDC's Market Leader, winner of 2007 Best Buy award of SC, winner of 2006 Best Email Security for Healthcare award 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 	Peace of mind in working with proven technology from a public, stable partner.

Case Studies

Before Secure Mail, IT administrators at **FW Murphy** had to dedicate too much time to monitor and troubleshoot spam traffic, costing precious time and money. After deployment of Secure Mail Chris Ditto, Network Administrator at FW Murphy said—"Secure Computing's Secure Mail (*IronMail*) has helped us to exponentially increase productivity by eliminating the clutter and wasted time associated with today's abundance of spam email." Secure Mail (*IronMail*) reliability allowed for only one Exchange server and prevented the need to install an edge transport server. FW Murphy evaluated other products as well but found that—"Secure Mail (*IronMail*) was the clear choice for its price, its effectiveness and its ease of use. IronPort's spam filtering did not catch nearly as much spam as Secure Mail caught plus it was more difficult to manage. "

Donald Wasylyna, manager of information security for the **H. Lee Moffitt Cancer Center** and Research Institute found Secure Mail (*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. "Secure Mail (*IronMail*) was one of the few pieces of security infrastructure that was a true win for us."

Next Steps:

Are there Zombies in Your Network That You Are Unaware of?

Get your free Domain Health Check report to find out about your Mail and Web reputation:
<http://www.securecomputing.com/dhc>

What is Domain Health Check?

The Domain Health Check™ is a free service from Secure Computing that provides information on the publicly observed messaging and Web traffic on your domain and any associated net blocks that you provide. The information in this report comes from the Secure Computing TrustedSource service, a global reputation service that tracks messaging and Web activity for every domain on the Internet.

Weekly Webinars (live product demos)

Attend Secure Computing's Weekly Webinars (http://www.securecomputing.com/weekly_webinar.htm). In a 45-minute session, you will learn how each of our enterprise security products can protect your organization from email and Web threats, including both known and unknown threats.

Visit TrustedSource (http://www.trustedsource.org)

Visit TrustedSource, the industry's most complete Internet reputation system, everyday to:

- Know about latest malware threats
- See global message volume
- Monitor rise in spam volumes
- Read blogs from experts
- Calculate ROI on reputation service
- Check the reputation of any domain, IP, URL, etc.
- Find out about top spam senders
- Fingerprint your site to monitor the risk of being phished
- And much more ...



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).1344.312.600

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](http://www.securecomputing.com/goto/globaloffices)

Before Secure Mail (*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.

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 Secure Mail (*IronMail*) appliances. But as we went forward with the migration, we found that our concerns were baseless—Secure Mail (*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 Secure Mail (*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 Secure Mail 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.

The City of London was faced with the problem of employees being forced to waste time dealing with ever-increasing volumes of spam in their email and the generic accounts. According to Zah Edah-Tally, Messaging Team Leader, City of London, "we were experiencing a growing volume of spam email that was exceeding 50% of our total email volume. This volume was exacerbated by the fact that we actively promote the service account email addresses, such as info@cityoflondon.gov.uk, on our Web site." "We carefully researched all independent sources of information, including industry analyst assessments such as the Gartner Magic Quadrant for messaging security," commented Zah. "We concluded that Secure Mail (*IronMail*) from Secure Computing was best placed to deliver the service and features we require."

Baptist Health System, one of the largest healthcare systems in Alabama and one of the state's largest employers needed help with increased mail flow ability to transmit e-mail messages containing PHI securely to help ensure HIPAA compliance. "We decided to explore Secure Computing's Secure Mail (*IronMail*) as an option a year ago in an effort to proactively defend our users against spam," said Phillip M. Moses, Exchange administrator for Baptist Health System. "Not only did the total cost of ownership (TCO) of Secure Computing meet our needs, but the company and its products had an incredible reputation. The results we saw during our onsite evaluation showed us that the appliance could do exactly what we needed it to, efficiently and effectively."

American Casino & Entertainment Properties, LLC (ACEP) doesn't gamble on messaging security with Secure Computing. ACEP, the parent company of the Stratosphere and Arizona

Charlie's Casinos had two major concerns when it came to protecting its email infrastructure: blocking inbound threats such as spam, viruses and phishing attacks, and securing sensitive outbound email messages. Their concerns were rightly addressed with Secure Mail (*IronMail*).

"We evaluated solutions from Secure Computing and Proofpoint, and found that Secure Computing is able to provide us with high quality anti-spam and anti-virus capabilities, as well as granular policy and encryption capabilities that can't be beat. Additionally, the sales team that we were working with was always available to help us or work with us on fine-tuning the appliance to fit our needs. Overall, the company's support is what really solidified our decision to select Secure Computing as our messaging security provider. The reporting included with the Secure Mail (*IronMail*) product is rich and granular, our previous solution was very simplistic and provided very little viable information," said Mike Essig, Executive Director of Information Technology for ACEP.