



Product Assessment

Secure Computing Secure Mail (IronMail) 6.7

Secure Messaging in Enterprise Security

Andrew Braunberg

Research Director, Enterprise Software and Security

Contents

- Summary
- Strengths and Weaknesses
- Product Buying Criteria
- Point/Counterpoint
- Product Metrics

Current Analysis
Outsmart your competitors

Secure Computing Secure Mail (IronMail) 6.7

Analyst:

A. Braunberg

Date Updated:

July 22, 2008

Product Class:

**Secure Messaging in
Enterprise Security**

■ Summary

Current Perspective: Threatening

Secure Computing Secure Mail, previously known as IronMail, is threatening to competitors, because the gateway, policy-based appliance includes leading secure messaging technology, powered by the TrustedSource reputation service. The product also supports outbound protection to enable policy compliance, and it is powered by TrustedSource reputation service. Secure Computing acquired the product in 2006 from CipherTrust, one of the industry's leading e-mail security providers that focuses on the world's largest enterprises.

CipherTrust, now fully integrated into Secure Computing, has consistently been a market leader in technological product innovation. The company has driven its success early on by incorporating functionality such as anti-spam, encryption, and policy and regulatory compliance into its e-mail security product. Secure Computing's product suite provides comprehensive security for messaging, including e-mail, and Web-based mail. The product no longer supports instant messaging protection, as that functionality has been moved into Secure Computing's Secure Web product. Secure Mail competes most closely with Barracuda at the low end and with Symantec and IronPort at the high end.

Secure Computing's focus is on meeting the messaging security needs of enterprise and ISP customers, largely through its TrustedSource global threat correlation engine that protects against spam and email borne threats like malware, viruses, phishing, and zombies. Secure Mail also applies advanced compliance policies to outbound content by monitoring it and/or preventing red-flagged messages from being sent. In its most recent releases, Secure Computing has focused on enhancing features around policy management and enhanced spam detection. The company claims to have more enterprise mailboxes than any of its competitors based on its customer base of 3,000 global organizations, including more than one-third of the Fortune 500 organizations.

■ Strengths and Weaknesses

Strengths

- Secure Mail includes a comprehensive e-mail security package, including anti-spam and anti-virus protection, outbound protection, and integrated Webmail support.
- Secure Computing has focused recent development on more granular policy management capabilities such as whitelisting TrustedSource look-ups, faster performance, enhanced reporting, and tools to empower administrators.
- Secure Mail combats spammers largely through its TrustedSource Reputation Service, with reputation data that covers not only sender IPs, but also message reputation and message

Product:

content (URLs, attachments, domains, and images).

**Secure Computing
Secure Mail 6.7**

- Secure Mail offers greater than 99% spam detection accuracy.

Secure Messaging
in Enterprise Security

Weaknesses

- Secure Computing, a leader in the large enterprise space, needs to better market this product to the mid-market and SMB space.
- Like others in this industry, Secure Computing faces a consolidating market, with rivals adding advanced capabilities including data leakage, encryption, and mail archiving.

Buying Criteria



Anti-spamming Functionality: OUTSTANDING

- Secure Mail includes a comprehensive e-mail security package: virus and anti-spam protection, policy and content compliance for data loss prevention, e-mail privacy, and secure e-mail gateway capabilities. The product’s Compliance Control feature helps ensure compliance to regulations such as HIPAA, Gramm-Leach-Bliley Act, and Sarbanes Oxley.
- Secure Mail’s filtering engine is called SpamProfiler, and the technology is the company’s fundamental correlating engine for filtering not only spam but also viruses, phishing, and other threats. SpamProfiler uses 12 detection techniques, analyzing thousands of attributes of each, including zero-day protection (created in-house) and signature-based technologies provided by anti-virus partners Authentium, McAfee, and Sophos. The content extraction engine has been updated to scan, detect and identify over 350 distinct file formats for attachments including extraction of embedded file types recursively.
- The technology examines the source of the e-mail and the message content in a pattern-matching and heuristic approach, using methods such as Bayesian filtering. Other techniques used to identify legitimate e-mail include its proprietary reputation engine, blacklists/whitelists, sender policy framework (SPF), DKIM, and sender identification.

Product:**Secure Computing
Secure Mail 6.7**Secure Messaging
in Enterprise Security

- Relying on historical accuracy rates and the analysis of Secure Computing researchers, the SpamProfiler's weighted analysis and correlation are used to compile what the company calls an aggregate spam confidence value, used to determine actions. Secure Mail's analytics do not rely so much on globally based honey pots anymore, but on the data being collected by the Secure Mail units (and other Secure Computing and partnering products) used in the field, analyzing over 110 billion messages per month.

Management Features: OUTSTANDING

- Secure Mail includes domain-based administration, which allows large IP-based companies, such as ISPs, to create administrators who have control over the entire appliance and the ability to create virtual host-based administrators. Secure Mail assigns one or more domains to the virtual host-level administrator; it assigns roles to them. Virtual host-level administrators can also create virtual host-specific policies.
- Every function of Secure Mail is managed through a browser-based interface, so administrators can centrally manage all computers running the software from a Web browser. The Web-based interface provides a dashboard view of the entire system.
- Secure Mail includes advanced reporting capabilities, including a customizable dashboard view with drill-down capabilities and enhanced internationalization/localization capabilities. The company has recently provided administrators with additional reports that show how many messages are being blocked at the connection layer (to illustrate how effectively TrustedSource is performing).
- Secure Mail has a multi-pronged encryption solution tied into its policy engine, which includes the ability to scan outgoing messages for gateway-to-gateway encryption or endpoint encryption. The technology dynamically determines the right encryption solution for a particular situation. This feature is not reliant on end user action, and because it is policy-based, it can be part of a compliance solution. Secure Mail supports very granular policy, which allows administrators to set up different rules for various groups.
- The encryption of e-mail communications also helps companies comply with applicable regulations, such as HIPAA regulations, the Gramm-Leach-Bliley Act, and Sarbanes-Oxley.

Architecture: STRONG

- The latest version of Secure Mail ships with a configuration that Secure Computing claims can provide more than 99% spam detection in most cases. Administrators do not need to touch the pre-configured settings unless they wish to create custom policies to meet internal business requirements. The company is continually improving its architecture to simplify installation and licensing, better combat new spam threats, improve message flow, and enhance management capabilities.
- Secure Mail has added a series of compliance engines that complement one another to offer advanced e-mail security functionality. One of these engines expands on its outbound message filtering capabilities with the addition of a data leakage prevention compliance engine, which lets organizations stop suspicious messages versus simply monitoring their activity. We expect this functionality to become even more meaningful to customers (and more of a differentiator to competitors' DLP offerings) as the company builds out the capabilities to include learning mechanisms. This technique trains on an organization's

Product:**Secure Computing
Secure Mail 6.7**Secure Messaging
in Enterprise Security

sensitive documents, automatically recognizing sensitive data leaving the company and building policies off that information. It is important to note is that Secure Mail does not store the sensitive documents on which it trains; it only stores the hashes (or resulting calculations) so that storage is optimized and sensitive documents are protected.

- Secure Mail includes a fingerprinting compliance engine that watches outbound e-mail attachments. The engine translates documents into a series of algorithm-generated hashes called a “document fingerprint,” which looks for exact replicas of protected documents, or to detect modifications to protected documents. Secure Mail complements its fingerprinting function with an adaptive lexical analysis engine, which examines documents for lexical structures such as frequency of words and position of words with respect to each other.
- Secure Mail appliances are extremely scalable, with no limit to the number of e-mail users they can support. Throughput per appliance is 200,000 unique messages per hour, depending on the configuration. This level of scalability is a key differentiator for the company, which filters mail for over 3,000 global organizations and claims one-third of the Fortune 500 as customers.
- Secure Computing has made several significant changes to the Secure Mail family of appliances. Secure Mail (IronMail) is available on the following appliances: S10D, S120, E2200, and E5200, which are targeted at the SMB and enterprise markets, respectively. The high end E5200 is described by Secure Computing as a carrier-grade appliance.

Vendor Support: STRONG

- Secure Mail is updated via Secure Computing’s ThreatResponse Updates (TRU). ThreatResponse updates are provided as quickly as every 20 minutes based on constant analysis and trends detected by the TrustedSource research team. This provides the highest level of responsiveness to new and emerging threats and spam outbreaks with no administrator effort required.
- Secure Mail’s TrustedSource Reputation Service provides information on the specific reputation of an IP, message, and domain/URL address at each local gateway, as well as the global reputation based on its research team aggregating the data. The service typically blocks between 60% and 85% of connections based on reputation data. The security intelligence is collected from the company’s more than 10,000 sensors located in over 82 countries.
- CipherTrust was acquired by Secure Computing in August 2006, and it has access to the company’s large distribution base, including its 2,500 reseller channel partners, and cross-selling opportunities through Secure Computing’s 22,000-customer base.
- Secure Computing has placed a lot of emphasis on customer support of this product. The company offers 24-hour customer service and technical support. Local resellers also provide local language support in Japan, Singapore, UK, France, Germany, and Dubai.
- Email Protection is now sold on a subscription-based per user pricing model on top of the appliance rather than a perpetual bundle with appliance. Email Protection includes Antispam, TrustedSource, basic compliance, ThreatResponse updates, software updates, technical support, webmail protection, gateway to gateway encryption and image analysis.

Product:

■ Point/Counterpoint

**Secure Computing
Secure Mail 6.7**

Secure Messaging
in Enterprise Security

Point: Secure Mail has been criticized for being difficult to manage and configure, because there are a number of different engine rules to set up and tune.

Counterpoint: Obviously, not everyone wants to be a spam expert, so while Secure Mail's customers love the product for its variety of functions, the company realized there was so much capability that people had to spend too much time on it. Secure Computing has focused on this issue, so instead of spinning 1,000 dials and knobs, ThreatResponse Updates provide automated updates optimized for the customer's box, which includes a number of dynamic elements (since everyone's gateways are different). Secure Computing provides updates as quickly as every 20 minutes so that administrators require virtually no touch. The updates are based on a combination of data pertaining to specific gateways, global data the company collects, and Secure Computing's research analysis, called Genetic Optimization, which looks at over 1,000 characteristics of a message. The company has also eased installation through the new SmartStart wizard, which provides a simple setup procedure for optimal performance.

Point: Secure Mail does not have as many end users as some competitors.

Counterpoint: Secure Mail has over 3,000 global organizations, which Secure Computing believes is the largest network of enterprise e-mail boxes for any anti-spam vendor. On the other hand, Secure Mail's ISP customer base is limited, so Secure Computing does not have an extra 30 or 40 million e-mail users that it can use to pad its numbers. Secure Computing is happy to focus on the enterprise, because e-mail coming into a large Fortune 100 financial institution looks very different from the e-mail coming into an individual at Yahoo.com. Instead, Secure Computing has focused its efforts on addressing the issues of the most security-minded organizations in the world. These organizations select Secure Mail over less robust, less flexible competitors.

Point: Secure Mail is no longer a best-of-breed product within a pure-play secure messaging company since its acquisition by Secure Computing.

Counterpoint: Secure Computing is a pure-play security company; Cisco is not. Furthermore, from a purely technical perspective, Secure Mail can benefit from collaborating with the Secure Web (formerly known as Webwasher) team, because that product is an application layer gateway also. Secure Web also has an extremely powerful anti-malware engine, which will be incorporated into Secure Mail in order to gain better zero-hour protection through advanced heuristics and behavioral technology. The multi-product approach has also improved Secure Mail's ability to combat blended threats from multiple vectors effectively.

Product Metrics

Product: Secure Computing Secure Mail 6.7

Anti-spam Performance	Value
Claimed Effectiveness	99%
Claimed Accuracy	Eliminating false positives is a core competency, since this issue is extremely important to enterprises. Secure Computing tests its releases to a point of achieving zero false positives. Of course, much of it depends upon how the organization defines 'false positive.' Secure Computing has customers that can speak to their specific experiences, as well as reference customers that have never had a false positive.
Email Accounts/Volume Limits	There are no limits on the number of e-mail users IronMail can support, since its appliances are highly scalable and can support the largest environments. Throughput per appliance is 200,000 messages per hour, depending on configuration.
Messaging Security Functionality	Value
Encryption	Yes
DoS Attack Detection and Prevention	Yes
DHA Attack Detection and Prevention	Yes
SMTP Connection Management	Yes
Anti-spam Functionality	Value
Header Analysis	Yes
"Reputation" Filters	Yes, TrustedSource is the only multi-identity reputation engine available; it checks reputations for IP, domain, URL, message, and image.
Heuristics	Yes
URL Filters	Yes
Content Scanning	Yes
Real Time DNS Block List	Yes
Signatures	Yes
Custom Domain Safe/Block Lists	Yes
End User Safe and Block Lists	Yes
Keyword and Phrase Lexicon	Yes
Bulkmail Checking	Yes
Baysian Filtering	Yes
Tuning necessary	Product is automatically/dynamically tuned via the Threat Response Updates for optimal performance and effectiveness - administrators have option to manually tune as appropriate as well
Block Non-English Spam	Yes
Languages supported	Language independent so multiple from all global regions
Blocks Phishing Messages	Yes

Continued

Product Metrics (Continued)

Product: Secure Computing Secure Mail 6.7

Realtime Look-up on Messages	Yes
Spam Filter Updates	Auto updated on daily basis and updated in real-time as new threats, new techniques, outbreaks, etc. necessitate
Number of New Rules/Day	Not rule-based, updates provide real-time lookups for reputation, signatures, and optimization settings.
Outbound Anti-Spam	Yes (including anti-phishing and anti-porn)
Message Disposition Options	Value
Message Disposition	Block, quarantine, deliver, reroute, tag relabel, copy, log, deliver securely, forward
Central/End-user Quarantine	Both
Email Digest Sent to Users	Yes
Release Quarantine w/Email Digest	Yes
Configurable Scoring Sys for Spam	Yes
Configurable at Group/User Level	Yes - both
Disposition Configurable	Administrator
Anti-virus Filtering	Value
Antivirus Signature Supplier(s)	McAfee, Authentium, Sophos
Virus Protection	Zero-Day virus protection is included in the base appliance; AV signatures are optional
Virus Filter Updates	Zero-day automatically/dynamically; regular updates hourly
Mass-mailing Worm Auto Deletion	Yes
Virus Signature Updates	From Secure Computing/anti-spam vendor
Attachment type Filter by Extension	Yes
Emerging Threat Detection	Yes
Message Content/Subject Filter	Yes
Outbound Anti-virus	Yes
End User Controls	Value
End User Access to Quarantine	Yes
End User Mgmt of Safe/Block List	Yes
End User Mgmt of Spam Policy	Yes
E-mail Aliases Supported	Yes
Administration	Value
Policy Control Levels	Yes - by domain, group and individual
Event-driven Alerts	Yes

Continued

Product Metrics *(Continued)*

Product: Secure Computing Secure Mail 6.7

Multiple servers/Single Mgmt Console	Yes
GUI Web-based Mgmt Console	Yes
Multiple Administrator Roles	Yes
Directory Support	Yes (LDAP, AD)
Automated/Manual Update Service	Automated
Failover across Multiple Servers	Yes
Proprietary MTA or 3rd Party	Proprietary MTA (IronMTA) integrated with hardened operating system (IronOS) to achieve security and high performance.
Authentication Support	Value
SPF Support	Yes
Sender ID Support	Yes
Domain Keys Support	Yes
Content Compliance	Yes
Content Filtering	Value
Customize Content Filters	Yes
E-mail Part Inspection	All (header, msg body, attachment)
Attachment Filters (Content/File Type)	Both
Dictionary Filters	Yes
Custom Disclaimers	Yes
Attachment Blocking	Yes
Archiving	Yes
Notifications	Yes
Outbound Content-Filtering	Yes
Reports	Value
Stored Reporting Data	yes, flexible via GUI and exportable
Default Reports Available	20
Published/Emailed Reports	Yes
Database Type Supported	Yes
Single Database for Multi Servers	Yes
Report Aggregation (All Servers)	Yes
Automatic Report Generation	Yes
Support for Auto-export of Logs	Yes

Continued