

www.securecomputing.com

Secure Computing[®] has been solving the most difficult network and application security challenges for over 20 years, and is uniquely qualified to be the global security solutions provider to organizations of all sizes.

Secure Computing IronIM

"Instant messaging could well be the dial tone of the future— albeit a silent one."

– The Wall Street Journal

IronIM benefits

- Satisfies regulatory compliance and corporate policy standards, and protects intellectual property by filtering all outgoing traffic
- Policy definition on a user, group or system-wide level
- Archives instant message conversations and attachment names for reporting and auditing purposes
- Transparent encryption to ensure the security of all messages without end-user intervention
- Stops viruses, worms and other threats from outside the enterprise before they reach the intended recipient

Secure Instant Messaging gateway

Instant Messaging (IM) has penetrated 90% of North American businesses, with over 80 million users logging on every day in organizations around the world. The real-time, interactive nature of IM makes it a valuable tool for collaborative efforts with business partners, customers and fellow employees. However, due to the consumer-oriented beginnings of the technology, IM has developed without the typical enterprise emphasis on manageability, reliability and security, leaving it vulnerable to attack.

In order to effectively combat the security threats presented by IM and ensure its manageability and reliability, Secure Computing[®] developed the IronIM[™] secure instant messaging gateway appliance.

- **Support for all public IM protocols:** Protects conversations over public IM protocols such as AOL Instant Messenger, MSN Messenger and Yahoo! Messenger; and corporate IM solutions such as Microsoft LCS and IBM SameTime. Protection is provided without the need for software installation on end-user machines.
- **Support for LCS and SameTime:** IronIM customers who use Microsoft Live Communication Server (LCS) or Lotus SameTime for internal IM can monitor all messages flowing across the internal network. These messages can be easily retrieved from the IronIM appliance using simple search functionality.
- **Corporate ID registration & mapping:** IronIM can access the corporate LDAP directory and map IM identities (screen names) to corresponding corporate LDAP names. IronIM will then require every IM user on the network to register with the IronIM appliance prior to communicating through the IM protocol.
- **Traffic encryption:** IronIM's patent-pending encryption technology automatically encrypts intra-company and IronIM-protected inter-company conversations, files and content without requiring end-user involvement.
- **Anti-virus support for file transfers:** IronIM scans files being transferred across IM using the Authentium anti-virus engine, allowing file transfers to take place without concern for infections of end-user machines or any other network elements.
- **Flexible policy administration:** IronIM provides an easy-to-use GUI interface that allows administrators to set and enforce defined corporate policies on a company-wide, LDAP group, or per-user level. Administrators can also determine which IM protocols should be allowed or blocked, and whether IM file transfers should be permitted.
- **Complete archiving:** IronIM monitors and logs all instant messaging traffic, including entire conversations; archives can be sent to third-party storage solutions on demand. Via IronIM's easy-to-use interface, administrators can set archiving policies and search for old content.
- **Hardened gateway appliance:** Built on the proven operating system that powers the IronMail e-mail gateway appliance, IronIM is designed from the ground-up with a focus on enterprise-grade security to withstand external attacks.



Figure 1: The Secure Computing IronIM appliance supports internal Instant Messaging protocols such as Microsoft Live Communications Server™ and Lotus Sametime™, as well as all major public Instant Messaging protocols such as AOL Instant Messenger™, MSM Messenger™, Yahoo! Messenger™, and Google Talk™, providing comprehensive protection for enterprises needing to manage the IM communications on their network. IronIM sits inside the enterprise firewall and does not require deployment of additional IM clients.

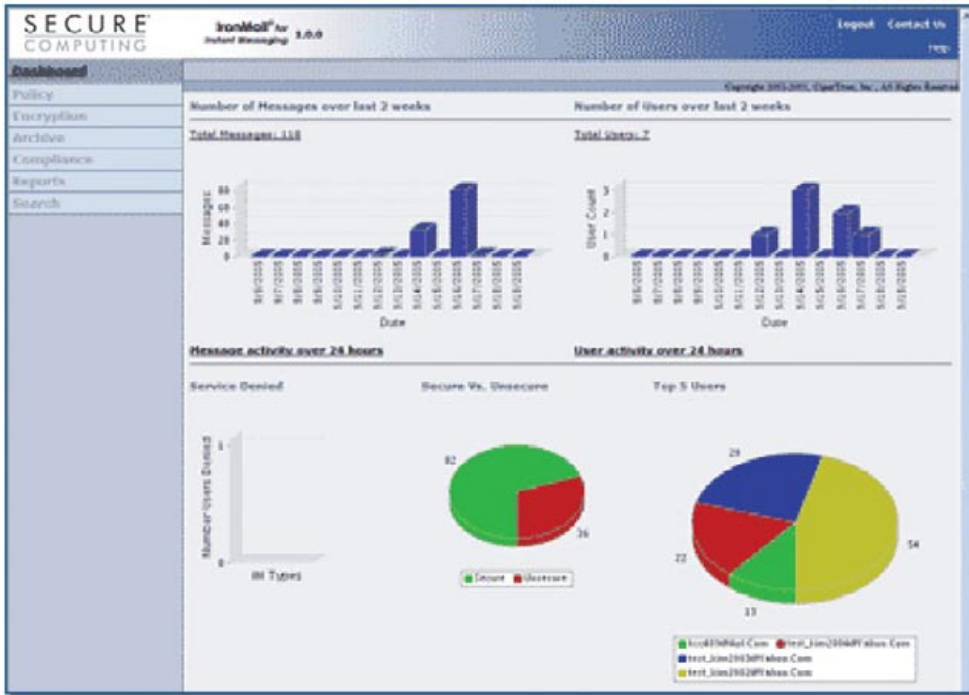


Figure 2: Secure Computing IronIM is easily managed through a simple at-a-glance dashboard. A full view of Instant Messaging activity and usage is provided on the first screen, and message activity and user activity is tracked and presented in graphical format for easy reference. Complementing the graphical dashboard is a full set of reports that drills down into the numerous areas of IM that concern security administrators and compliance or security officers.

Ongoing management of policies and the dictionaries used is made easy through the familiar and intuitive point-and-click interface.

SECURE COMPUTING

www.securecomputing.com



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
www.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
 No 1 The Arena
 Downshire Way
 Bracknell
 Berkshire, RG12 1PU UK
 Tel: +44.0.870.460.4766
 Fax: +44.0.870.460.4767

Asia/Pacific Headquarters
 Hong Kong
 1604-5 MLC Tower
 248 Queen's Road East
 Wan Chai Hong Kong
 Tel: +852.2520.2422
 Fax: +852.2587.1333

Japan Headquarters
 Shinjuku Mitsui Bldg. 2, 7F
 Nishi-Shinjuku 3-2-11
 Shinjuku-ku, Tokyo, 160-0023
 Japan
 Tel: +81.3.5339.6310
 Fax: +81.3.4496.4537

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