

[www.securecomputing.com](http://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.

“IronMail has helped us secure our patient information and transmit critical messages without worrying about whether we are violating a policy or regulation.”

– Jim Donaldson, Baptist Health Care Corporation

#### Encryption benefits

- **Enables secure e-mail communication in any environment, regardless of the recipients' encryption capabilities**
- **Policy-driven encryption ensures that sensitive information is protected without requiring end-user action**
- **Easy to install and compatible with any type of messaging server, including Exchange, Notes and Domino**
- **Robust reporting and analysis tools provide instant insight into e-mail traffic crossing the enterprise gateway**
- **Multiple encryption options for business-to-business or business-to-user communication assures compatibility with any intended recipient**

© October 2006 Secure Computing Corporation. All Rights Reserved.  
 CT-Encryption-PO-0ct06vF, Bess, enterprise strong, IronMail, MobilePass,  
 PremierAccess, SafeWord, Secure Computing, SecureOS, SecureSupport, Sidewinder  
 G2, SmartFilter, Softoken, StrikeBack, Type Enforcement, CyberGuard, and Webwasher  
 are trademarks of Secure Computing Corporation, registered in the U.S. Patent and  
 Trademark Office and in other countries. Anti-Virus Multi-Scan, Anti-Virus PreScan,  
 Application Defenses, Edge, G2 Enterprise Manager, Global Command Center, IronMail,  
 IronNet, Live Reporting, Message Profiler, MethodMix, On-Box, Outbreak Defender,  
 Power-It-On!, Radar, RemoteAccess, Secure Encryption, SecureWire, SmartReporter,  
 SnapGear, Threat Response, Total Stream Protection, TrustedSource, TrustedSource  
 Portal, and ZAP are trademarks of Secure Computing Corporation. All other trademarks  
 used herein belong to their respective owners.

## Secure Computing Encryption

### Policy-based protection for messages outside of the network

While few will debate the value of encrypting messages that contain sensitive information, many security officers have resisted installing an encryption solution on their enterprise e-mail network due to difficulties in deployment and administration of existing solutions. Typically require bypassing of corporate messaging security infrastructure such as anti-virus and content filtering controls. Secure Computing® Encryption™, available as a component of the IronMail® appliance, removes the barriers to deploying an encryption solution. Offering a robust policy driven encryption solution that supports multiple encryption technologies Secure Encryption is the breakthrough secure messaging solution organizations have been seeking.

- **Business-to-business encryption:** The default standard for Secure Encryption gateway-to-gateway secure delivery is TLS/SSL. Server-side S/MIME and open PGP support enables interoperability with legacy systems.
- **Business-to-user encryption:** Simple and easy to use, Secure Encryption is the perfect solution for sending secure messages to any recipient. No cumbersome key management is required, making encryption transparent to the end users. Encryption can be assured regardless of the recipient's decryption capabilities, opening up the e-mail communications channel with patients and clients protected by government privacy regulations, as well as with business partners with whom sensitive corporate information is shared.
- **Policy-driven encryption:** Effective encryption relies as much on defining what messages need to be protected as it does on the method used to protect the message. IronMail's robust policy engine provides granular policy definition leveraging LDAP/Active Directory groups and policies, and message characteristics including content, attachments, recipient, domain, or header information.
- **Precise, accurate policy enforcement:** IronMail's detection and enforcement capabilities are the most precise, complete technologies available on the market today. IronMail relies on multiple layers of detection technologies to determine a compliance score for every outbound email. Based on this score IronMail enforces encryption policies.
- **Ease of administration:** As an enterprise solution, IronMail was designed to reduce the strain on your IT networking staff by eliminating the need for end-user training. IronMail eliminates the headache of key management with an automated approach that updates encryption keys from a central console. Because it integrates seamlessly with your existing infrastructure through LDAP or Active Directory, IronMail provides a solution that works with any environment.
- **In-depth reporting and analysis:** IronMail's MTA provides administrators with automated logging and reporting, saving time and money. Instantly, administrators can access statistics on who is sending what type of e-mails to whom and when messages and attachments are opened. The IronMail dashboard provides a comprehensive view of the entire messaging infrastructure, giving administrators full visibility into message traffic.
- **Scalable and enterprise-ready:** From the beginning, Secure Computing has designed products specifically for enterprise deployments, and Secure Encryption follows that trend. The Secure Encryption solution is ideal for any size environment, from a few hundred users to a few hundred thousand.



### 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](mailto:sales@securecomputing.com)  
[www.securecomputing.com](http://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

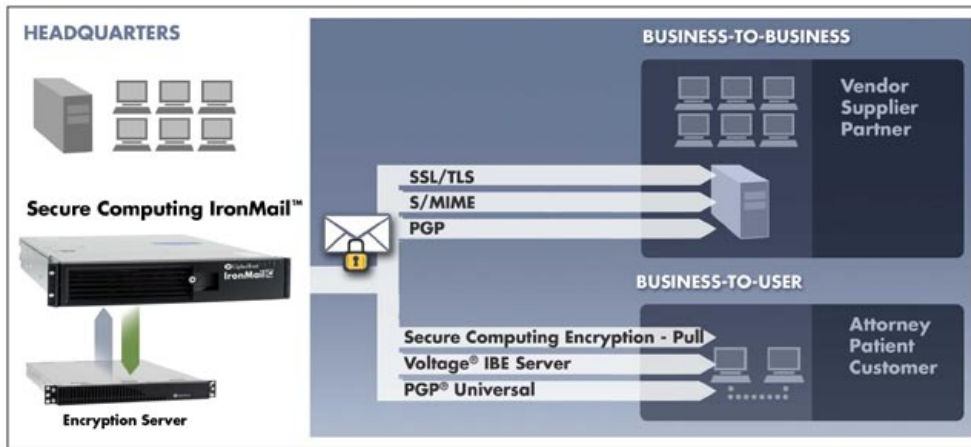


Figure 1

## Business-to-business encryption

IronMail supports multiple encryption protocols for secure e-mail communications between businesses:

- **SSL/TLS:** Secure Sockets Layer (SSL) is a protocol for encryption and authentication of Internet connections. Transport Layer Security (TLS) is the standardized version of SSL. IronMail uses SSL/TLS to create a secure “tunnel” for messages to travel through to the recipient server or client. This option is shipped native with each IronMail providing policy-driven encryption.
- **S/MIME:** IronMail offers support for S/MIME (Secure Multipurpose Internet Mail Extensions) to encrypt messages and send them securely. S/MIME requires key exchange between the sender and recipient servers that is managed by IronMail.
- **PGP:** IronMail customers can also select PGP (Pretty Good Privacy) technology to send encrypted messages. This solution combines IronMail’s market-leading message scanning and policy enforcement technology with PGP Universal’s world-class centrally managed encryption capabilities.

## Business-to-user encryption

Often, organizations need to communicate with recipients who do not have encryption capabilities. For these situations, Secure Computing offers several methods of encrypting messages that are effective regardless of the recipient’s encryption capabilities:

- **Encryption – Push:** The Push encryption module sends recipients a secure message as an attachment to an otherwise standard email. The recipient can view and respond to the message using any Web browser.
- **Encryption – Pull:** IronMail offers a secure staging server as a “pull” encryption option. With this method, an e-mail notifies the recipient that a message is waiting in a secure Web-based mailbox. The recipient logs into a secure Web page to retrieve, view and reply to any encrypted messages.
- **Voltage® IBE server:** By using well-known identities as public keys, IronMail’s Voltage IBE server eliminates the complexity of managing certificates, Certificate Revocation Lists (CRL), and other costly infrastructure.
- **PGP® universal automatic encryption and key management:** Customers who select the IronMail/PGP universal solution benefit from proven integration and joint policy configuration as well as single point of purchase, deployment and support.