

E-Mail/IM Compliance and Encryption

KEY BENEFITS

- Robust, flexible and scalable, risk-based “real time” monitoring and archiving of outgoing / incoming external & internal E-Mail, attachments, Bloomberg and Instant Messages.
- General/“tailored” content scan-ning via continually updateable key-word and lexicon appropriate for the securities, banking, insurance, health, etc. industry to which it is applied.

KEY FEATURES

E-Mail Compliance

- Notification engine with multiple alternative levels of interdiction to quarantine “red flagged” e-traffic as part of pro-active, enterprise-wide supervision and general compliance efforts.
- Secure, tamper-proof audit trail for the “life” of e-communication and evidence of reviews to ensure full compliance with SEC, FINRA, FRCP GLB, and other applicable current/ future regulatory requirements in the U.S., EU, Asia, etc.

Data Security / Encryption

- Revolutionary, first-in-industry automated system to open and retain encrypted E-Mails and attachments to ensure integrity of proprietary client information on receipt by firm and during internal review process.
- SAS 70-certified data center storage available.
- Sharing and collaboration
 - Automatic username generation
 - Free readers for recipients
- Chain of custody records
 - Audit trail
 - Continuous control
- Dynamic permission control
 - Continuous control
 - Enterprise digital rights management
 - Invocation, revocation, modification

New Approach to Corporate Security

Effective regulatory compliance and data protection for today’s enterprise email and data must address multiple regulations and requirements while offering business efficiencies. New realities dictate that in order to comply with government regulations, companies must move beyond passive policy management and perimeter-only, point-of-origin security models. The new approach demands proactive, automated products that provide continuous security and corporate compliance—for distributed data-at-rest & outbound data-in-motion.

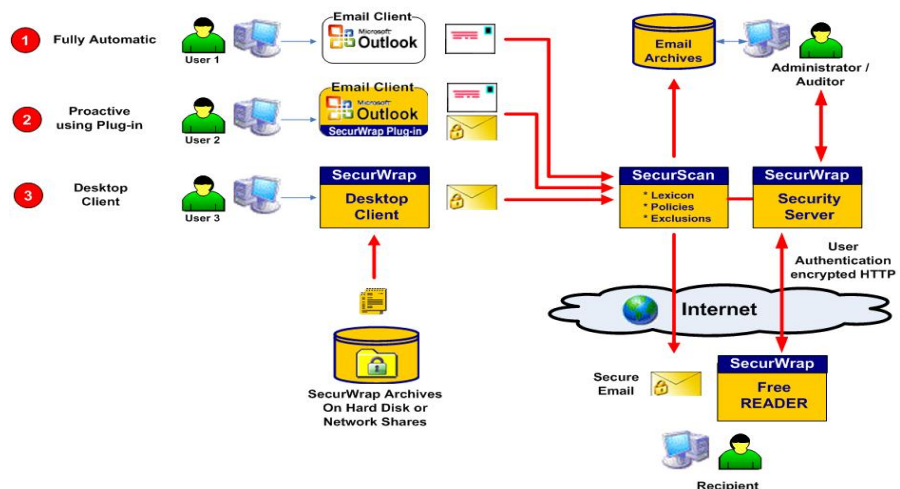
A Comprehensive Solution

PolicyBridge™ from DISC is the first product of its kind to integrate email monitoring technology; archive, retrieval and policy-based compliance with strong encryption enriched with enterprise digital rights management capabilities. These are powerful security mechanisms that extend and enforce regulatory and corporate security policies to the desktop, email, removable media and recipients.

PolicyBridge as an integrated solution provides a complete approach to challenges associated with email compliance regulations. PolicyBridge also protects confidential data, customer files and transactions, and other strategic business data from external threats or non-malicious actions.

How does it work?

The suite is comprised of two software components: PolicyBridge for scanning and archival and SecurWrap™ for data protection. PolicyBridge sits behind spam and anti-virus software in the SMTP gateway, actively scanning inbound, outbound and internal email and attachments. Using an industry-specific and customizable lexicon that contains relevant keywords, phrases, and associations, PolicyBridge scans all email traffic with a powerful parsing engine. It also flags messages according to user and group definitions. Based on corporate security policies defined in a rules database, the software then automatically implements various actions to protect data and enforce policies.



Components of PolicyBridge

PolicyBridge for E-Mail Compliance and Records Retention

PolicyBridge scans inbound, outbound and internal email for regulatory compliance risks. PolicyBridge can operate as a post-process surveillance and archival solution, or in real-time performing active scanning, policy enforcement and archival. In pre-process mode, PolicyBridge allows companies to stop at-risk communications and decide what action to take. PolicyBridge scans email using an intelligent, lexicon-based parsing engine to identify keywords, phrases or patterns such as account numbers and SSNs in email subject lines, body and attachments. Based on the policy database, SecurScan goes beyond basic blocking and allows for four actions based on what is found in the E-Mail:

- (1) Block the email and prevent the message from leaving the company
- (2) Quarantine the email until reviewed and approved for release
- (3) Let the email pass and log the action, or
- (4) Automatically encrypt the email and embed digital rights management enabling companies to later revoke or modify recipient privileges.

Compliance Grade Archival

PolicyBridge automatically archives and indexes all email and attachments while providing integrated email retrieval features. PolicyBridge supports industry standard storage solutions such as EMC Centera, StorageTek Libraries and all XFS compatible storage devices, such as NAS, SAN, WORM, and optical. The integrated console allows for streamlined review of emails (pre- and post-process) and also provides a comprehensive set of archive retrieval tools for efficient discovery.

SecurWrap® Encryption for Data Security

SecurWrap provides easy-to-use yet powerful data encryption for desktops, laptops, file servers, and removable media. SecurWrap allows users to share encrypted content with other users by encapsulating information in a “wrapper.” Our permission wrapper technology is a collaboration-enabling solution that provides a self-contained mechanism for encryption, digital rights management, audit, and authentication. It flexibly supports online and offline access to all types of files in email, on removable media, or at rest. The technology is designed to be simple to administer, without requiring you to distribute certificates, establish a public key infrastructure, or install any filter drivers.

SecurWrap E-Mail Plug-In

SecurWrap Email Plug-in is designed for users who want to proactively protect sensitive information within the email. Native buttons and menu operations integrated with Outlook and Lotus Notes allow users to protect email and attachments.

Security Server

SecurWrap Security Server provides consolidated user management, identity management and key exchange between senders and recipients of sensitive content. A powerful tool, the SecurWrap Security Server maintains a secure communication protocol with any sensitive data controlled in a permission wrapper and provides a comprehensive audit trail on sensitive data in use throughout and outside of the enterprise: user actions on the data, how that data has been shared, where it is located, and which users have access to it. Administrators may also revoke or expand user permissions directly from the Security Server console (e.g. if the recipient is no longer trusted).

ONSITE SOLUTION SYSTEM REQUIREMENTS

Languages

- Adaptable to many languages including English, French, Japanese, and others

Desktop Client

- MS Windows
- MS Outlook 2000/2003
- IBM Lotus Notes v5.0.6 and above

Free Reader

- MS Windows
- Microsoft Outlook 2000 and higher
- Lotus Notes v5.0.6 and above

Server

- Windows Server 2003 and above

Database

- SQL Server™ 2000 and above
- Oracle® 9i and above

Hardware

- 2+ Servers: Current generation Xeon Quad Processors, 4G min RAM, 250 GB min high speed disk

Support for EMC Centera, StorageTek libraries, all XFS compliant storage devices (WORM, SAN, NAS, Optical)



Digital Info Security Company
11030 CirclePoint Road
Suite 100
Westminster, CO 80020

1.866.841.5970

info@disecurityco.com
www.disecurityco.com