

E-mail Compliance and Data Protection

KEY BENEFITS

- Address regulatory compliance guidelines: SOX, SEC, GLB, HIPAA, FRCP
- Ease discovery and auditing of communications with simplified and efficient data retrieval
- Reduce policy infractions with proactive enforcement
- Secure sensitive data stored on- or off-network, within email, laptops and removable media
- Eliminate costly point solutions

KEY FEATURES

Email Compliance

- Automatic enforcement of corporate policies
- Surveillance of inbound, outbound and internal email
- Centralized administration consoles
- Compliance archival and tamper-resistant audit trail
- Intelligent, context-based lexicon
- Multi-tiered permission settings
- Supports MS Exchange, Lotus Notes, Instant Messaging and Bloomberg Messaging
- Hosted Solution or Onsite Solution

Data Security

- Data encryption
 - Automatic or proactive
 - Data-at-rest and in-motion
 - Post delivery protection
- Option for SAS 70-certified data center storage
- Share and collaborate
 - 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—both for distributed data-at-rest and outbound data-in-motion.

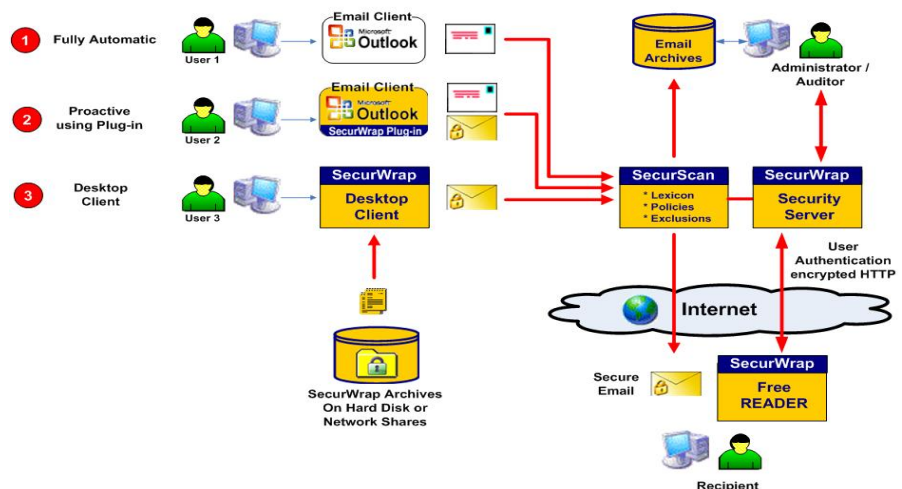
A comprehensive solution

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

How does it work?

PolicyBridge™ II is comprised of two software components: SecurScan™ for scanning and archival and SecurWrap™/Magic KeyRing Security System™ for data protection. PolicyBridge™ II 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™ II 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™ II

SecurScan™ for Email Compliance and Archival

SecurScan scans inbound, outbound and internal email for regulatory compliance risks. SecurScan can operate as either a post-process surveillance and archival solution or in real-time, performing active scanning, policy enforcement and archival. In pre-process mode, SecurScan allows companies to stop at-risk communications and decide what action to take. SecurScan 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 email:

- (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

SecurScan automatically archives and indexes all email and attachments while providing integrated email retrieval features. PolicyBridge™ II 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™/Magic KeyRing Security System™ Encryption for Data Security

SecurWrap/Magic KeyRing provides easy-to-use yet powerful data encryption for desktops, laptops, file servers, and removable media. SecurWrap/Magic KeyRing 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/Magic KeyRing Email Plug-In

SecurWrap/Magic KeyRing 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 allows users to protect email and attachments.

Security Server

SecurWrap/Magic KeyRing Security Server provides consolidated user management, identity management and key exchange between senders and recipients of sensitive content. A powerful tool, the SecurWrap/Magic KeyRing 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).

About Digital Info Security Company® (DISC)

Founded in 2005 to provide hosted compliance solutions for the financial industry, today DISC provides secure email compliance and data storage solutions to small and mid-sized organizations across numerous regulated industries. DISC's state-of-the-art data center and technical infrastructure backs DISC's services with the highest level of security and redundancy. DISC is led by a management team with more than 25 years of experience in Internet security, SEC, HIPAA, and other regulatory compliance solutions and currently trades as DGIF on the Pink OTC Markets.

ONSITE SOLUTION SYSTEM REQUIREMENTS

Languages

- English and Japanese

Desktop Client

- Microsoft Windows NT® 4.5.1, 2000, XP Professional
- Microsoft Outlook 2000 and higher
- IBM Lotus Notes v5.0.6 and higher

Reader

- Windows 98SE, ME, NT 4.5.1, 2000, XP Pro and Home
- Microsoft Outlook 2000 and higher
- Lotus Notes v5.0.6 and higher

Server

- Windows 2000 Advanced Server™

Database

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

Hardware

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