

Call Us Today

Canadian Headquarters
4101 Yonge Street
Suite 708
Toronto, ON, Canada
M2P 1N6
416.226.8600

North American Toll Free:
1.888.697.3246

United States
1870 The Exchange
Suite 1000
Atlanta, GA
30339
1.770.578.6540

Europe
27 Old Gloucester Street
London, United Kingdom
WC1N 3AX
+44.020.7419.8763

ABOUT ECHOWORX™

Leading Provider of Encryption Software

Echoworx is a leading provider of managed encryption services to protect confidential information from unauthorized viewers and makes the encryption of digital information easy. Echoworx' complete encryption strategy for privacy encompasses much more than just data loss prevention. It protects all forms of disparate email data, whether on mobile devices, desktops, in the cloud or on exchange servers.

Echoworx is Deloitte, Microsoft, CCTM and PCI certified. As a SaaS (software as a service) model; is built on best-of-breed technology. Echoworx is the encryption service provider of choice for leading security software and telecommunications and hosted exchange providers, including BT Global Services, Symantec Hosted Services, AT&T, McAfee, Verizon, and Apptix among other global businesses.

www.echoworx.com



Policy-Based Encryption Secure Email Communications at the Gateway...

Encrypted Mail Gateway Policy-Based Encryption Solution

Encrypted Mail Gateway is a policy-based managed encryption solution that provides organizations with an easy way to enforce email encryption without disrupting the day-to-day workflow of their employees.



It puts the control back in the hands of the IT department by enabling them to manage the organization's entire email infrastructure. At the same time it enables users to read their encrypted email from their desktop or mobile device.

This policy-based encryption engine not only encrypts messages based on pre-defined corporate policies, it re-directs and prevents confidential information from being distributed over the Internet to the wrong people.

The reporting capabilities allow IT managers to audit how employees are sharing confidential information and to make the necessary changes to meet organizational policies and compliance requirements.



Because every organization has a unique way of reporting information, Echoworx' highly customizable policy engine can be configured to suit specific business needs. Echoworx engineers will work with company compliance officers to transition existing policies into policy templates and add more policies as needed.

The policy engine automatically enforces compliance, all encrypted messages are digitally signed and can be validated to prove compliance as and when required.

All outbound emails are monitored to ensure confidential information is encrypted before it is distributed over the Internet.

Echoworx Encrypted Mail Gateway also provides the ability to associate rules with the content of outbound email to help protect enterprises from liabilities associated with



privacy and data security regulations such as The Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), PCI Compliance, and Securities and Exchange Commission (SEC) rules.

Highlights

- Enables policy-based managed encryption solution
- Enforces email encryption based on pre-defined policies
- Allows emails to be read on all desktop and mobile devices
- Puts control back in the hands of IT
- Re-directs and prevents confidential email from being distributed to the wrong people
- Reporting feature enables IT to audit employee usage and make changes
- Supports industry standard encryption
- Allows encrypted messages to be digitally signed and be validated for compliance purposes
- Provides engineering support to work with Compliance Officer to enable and add new policies
- Enables rule association with outbound email content and helps protects organizations from liabilities associated with privacy and security
- Hides encryption complexities from the end user ensuring ease of use
- Supports 14 languages

English, German; Spanish; French (Canada); French (France); Italian; Dutch; Japanese; Korean; Portuguese (Brazilian); Portuguese (Portugal); Russian; Chinese (Traditional); Chinese (Taiwanese)



Hands-free approach to Policy-Based Encryption

Encrypted Mail Gateway now offers a self-provisioning feature to support multi-level resellers and customers. With this feature, Echoworx partners can take a hands-free approach to policy-based encryption, and allow their resellers and customers to easily set up, manage and brand their own accounts.

Without self-provisioning, an Echoworx partner would license the product, sell it to their reseller or customer and then they would have to work with Echoworx directly to set up the customer account, manage the account and even develop the branding. With self-provisioning, the reseller has the option of doing all the work or handing it off to their customer.

The reseller or the customer can self-brand their interface by browsing their desktop for company logos and graphics, as well as easily add themes and corporate colors using the drop down color wheel or customizing colors based on pantones or RGB codes.

Reseller customer accounts can be managed and/or branded from a single screen. Reseller customers are listed in an easy-to-access drop down menu.



The administrator sets policies by creating matching conditions that will trigger policy actions. Accounts can also be managed by:

- Choosing the number of email notifications they would like to receive based on incoming messages and expiring messages
- Selecting the language preferences from more than 14 languages
- Determining if notifications should be digitally signed
- Determining how many times a password can be keyed in before the user is locked out of the system
- Reviewing a variety of reports including usage, access levels, etc



Powerful web-based Administration Console

The powerful web-based Administration Console allows managers to set, review and customize their organization's privacy policies so confidential content is automatically encrypted. The intuitive user interface ensures that policies can be easily managed.

The user simply composes an email and the content and attachments are automatically scanned to detect whether the message should be encrypted or otherwise processed before it is sent.

Built-in features also include a wide variety of commonly used rules, dictionaries and expressions. Complex rule chains can be created to suit an organization's business needs.

In addition to encrypting messages, administrators can monitor all messages and reject those that do not comply with company policies and procedures.

Multiple domain deployment

Encrypted Mail Gateway allows for multiple domain deployment - i.e. where multiple domain names (or multiple organizations) share the same deployment with separate sets of rules.

Analytics

The analytics tool tracks every single message that has been processed and can provide snapshots of the system through summary diagrams. Detailed searchable reports identify important information such as the most flagged policies, the highest offenders, top keywords, and the percentage of flagged messages.

Third-party S/MIME keys

Encrypted Mail Gateway supports third-party S/MIME or PGP credentials to accommodate automatic encryption/decryption of messages at the gateway.

Technical Specs

The Policy Engine can run onsite as a virtual appliance.

The minimum specs are as follows:

- Operating System requirements: one of: Red Hat Linux (2.6 kernel), 32 bit Microsoft Windows 2003 Server, 32 bit Microsoft Windows XP, 32 bit, Microsoft Windows Vista 32/64 bit, Microsoft Windows 7 32/64 bit
- Minimum Memory requirements: 2GB RAM
- Minimum Installation Disk Space requirement: 250 MB
- MySQL (GA release) database Outbound SMTP email delivery relay/smarthost