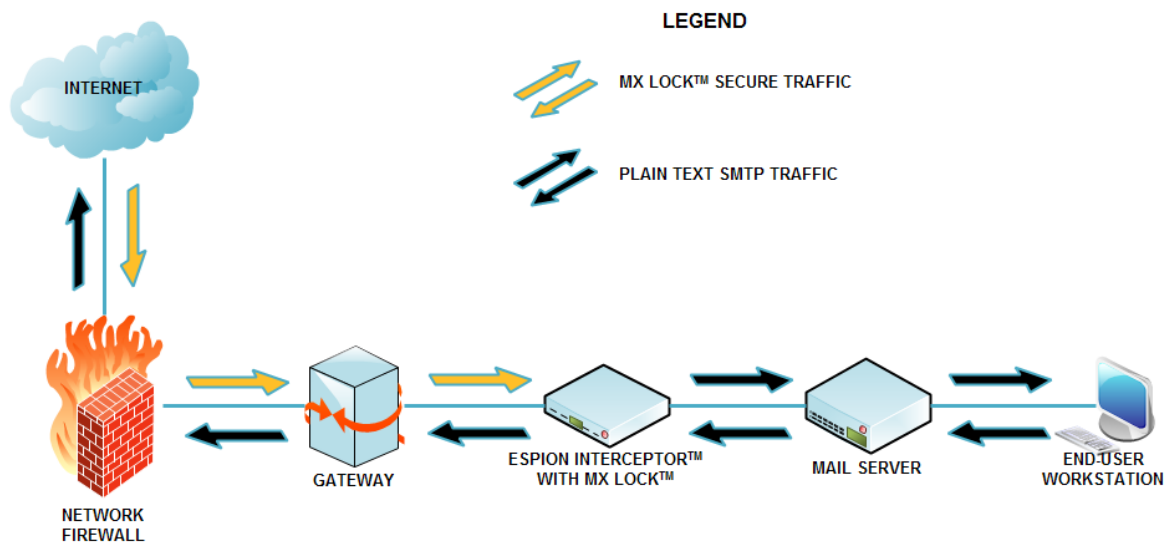


MX LOCK™- Email Encryption System

Locking Your Email Against Interception™

Interceptor™ with **MX LOCK** supplies the highest level of data security for emails carrying confidential and proprietary information. MX LOCK uses Espion's powerful Interceptor platform (and is also available through Espion's hosted services – **Paladin MX™**) to supply the highest level of email data security at your company. MX LOCK provides automatic and selective data security by enforcement of outbound email content and attachment rules. Once an email is scanned for restricted content, the email and any attachments are encrypted with a highly secure 1024-bit dual-key encryption technique used by the U.S. and Canadian Governments and their military. Content filtering rules prevent infractions of compliance for **HIPAA** (Health Insurance Portability and Accountability Act) and **GLBA** (Gramm-Leach-Bliley Act) as well as enforce custom IT management policies. MX LOCK prevents data leakage and off-loads the mail server resulting in improved system performance. All secure emails are encrypted and stored on the Interceptor thereby ensuring data security.



MX LOCK™ DATA FLOW ARCHITECTURE

Additionally, an Interceptor equipped with MX LOCK allows emails of unlimited sizes to be sent very securely to trusted recipients over the Internet. Employees can send very large files to anyone located inside or outside the

corporate email system. Emails to trusted recipients located outside the corporate email system may be accessed over any Internet connection, on any computer OS, on any browser and still have secure access to these large files, regardless of the recipient's mail system limitations **AND** there are no software or hardware modifications required on the recipient's workstation . These same trusted recipients can send oversized files in an encrypted reply, even if the trusted recipient's email system has file size limitations. This is very important for sending X-rays, CT scans, CAD drawings, photographs and other large attachments.

Rules based partitioning permits firewalling of email traffic based on the content of emails and attachments. Various departments can be partitioned to prevent data leakage between employees and outside contractors. Rules based partitioning allows employees with different job functions such as R&D, Marketing, Finance, etc. to be located virtually anywhere in the world.

A SUMMARY OF MX LOCK FEATURES

- **Secure Email Encryption** – Auto enforcement and conditional programming
- **Email Filtering by Content** – Custom scanning to block non-compliant outbound emails
- **Secure via TLS** – Transmit confidential emails over a secure channel
- **Secure File Transfer** – Outbound attachment transfer security with virtually no size limitations
- **Secure Policy Encryption** – User transparent key management - RSA 1024-bit dual key
- **HIPAA/HITECH/ARRA/SOX/GLBA Compliant** – Forced transparent compliance
- **Customizable security questions, user screens, graphics, logos and more**
- **Auto Load Balancing** – Clustering of local and off-site Interceptors while keeping uniformity in configuration
- **Unlimited Logical Redundancy** – 100%, 200%, 300%, 400% and greater with clustering
- **Log Files** – View of various live mail flow components
- **Mail Flow Graphs and Reports** – Detailed administrative reports on live mail flow, security attacks, system resources and more
- **Self Healing Configuration**
- **Auto Scaling – Scale-up/down** with clustering
- **Identity Management**
- **Firewall** – Added layer of security for the company's email infrastructure
- **Network Tests** – Network trouble shooting tools (trace route and MX record lookup)
- **Sanity Checks** – Trouble shoot email flow problems (validate connectivity, check time, etc.)
- **Intrusion Prevention** – Protect ALL ports from hack attacks
- **Hardware Health Monitoring** – In-depth real-time view of server hardware components
- **Alerting System** – Selectable administrative alerts for system or network mail flow issues
- **Backup and Restore** – Export and import Interceptor settings

COMPLIANCE ENFORCEMENT

AUTOMATIC AND CONDITIONAL ENFORCEMENT

The Interceptor is your most comprehensive solution for compliance enforcement. Stop intentional and accidental GLBA and/or HIPAA violations.

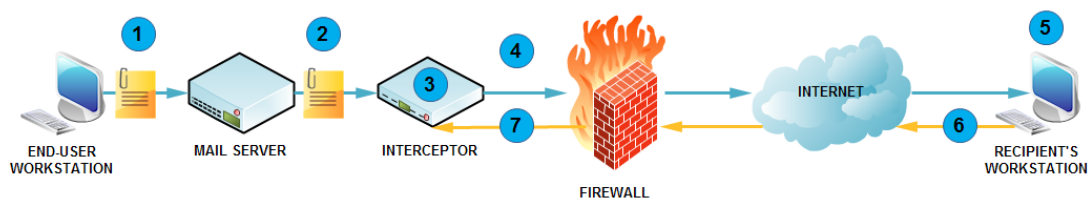
The MX LOCK system is designed specifically to allow IT managers to mix in-house rules and methodologies with industry compliance rules such as for Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act of 2002 (SOX) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act and the American Recovery and Reinvestment Act (ARRA).

[CLICK HERE](#) to read more about meeting compliance requirements using MX LOCK.

FILE TRANSFER WITHOUT SIZE LIMITATIONS

EMAIL LARGE ATTACHMENTS WITH ZERO PROBLEMS

Clients can now send emails, with attachments, of virtually no size limit, regardless of those limitations imposed by the sender's and receiver's mail servers. This translates to end-users having the ability to securely send large email file attachments such as medical images, X-rays, CAD-CAM diagrams, books and other digital records. Email users do not need to leave the company's IT infrastructure to send large emails which could potentially violate HIPAA, GLBA and even SOX guidelines. Recipient's are verified as "Trusted Recipients" and can only access these documents after proper certificate verification and login authentication.



- 1 End-user at your company emails a large attachment to a recipient outside your network. Email is sent to the mail server.
- 2 The mail server forwards the email (with attachment) to Interceptor™ MX Lock™.
- 3 MX Lock™ encrypts the email (with attachment) and stores it (encrypted) on-disk.
- 4 A secure link is sent via email to the intended recipient.

- 5 The recipient receives the secure link email to his/her email inbox.
- 6 The recipient clicks on the link and a secure connection is created between the web browser and the Interceptor.
- 7 Upon proper authentication, the recipient can view the contents of the email message (and download the attachment) in a web browser.

A recipient's access to these sensitive documents and attachments are over private and secure links. This ensures that emails and attachments are compliant with HIPAA and GLBA policies. Client emails are forced into

IT conformance rules, transparent to the Client. MX LOCK provides an added bonus to the performance of the mail server. The Interceptor stores all outbound encrypted emails and attachments locally in an encrypted form for protection against physical theft of the Interceptor. Potential HIPAA and GLBA violations are blocked and notices are routed to the appropriate management, all of which is easily and highly customizable.

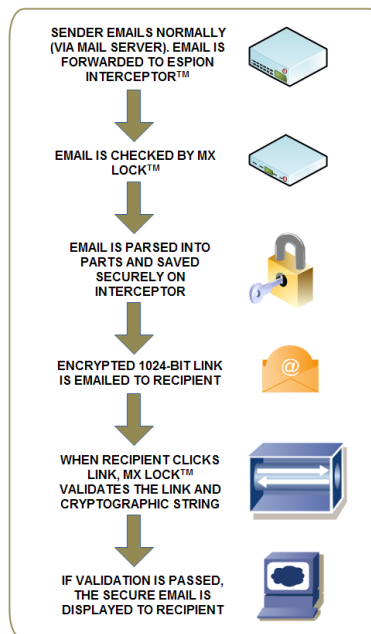
[CLICK HERE](#) to read more about Secure File Transfer.

TRUSTED RECIPIENT SYSTEM



PROTECTS CONFIDENTIAL DATA FROM HACKERS AND OTHER PRYING EYES

MX LOCK ensures that encrypted email content and attachments (such as medical patient information, corporate trade secrets, financial information and any other confidential or otherwise sensitive information) go only to the designated and trusted recipient and can only be opened by the trusted recipient to whom it was sent. MX LOCK secures the email (and all attachments) with an unbreakable dual-key encrypted exchange – the same level the U.S. and Canadian Governments use for their secure record encryption and storage. This dual-key encrypted exchange is very robust and requires proper credentials before the process of accessing the email can begin. This guarantees a hack-proof email system.



MX LOCK™ - EMAIL FLOW LOGIC

[CLICK HERE](#) to read more about the Trusted Recipient System.

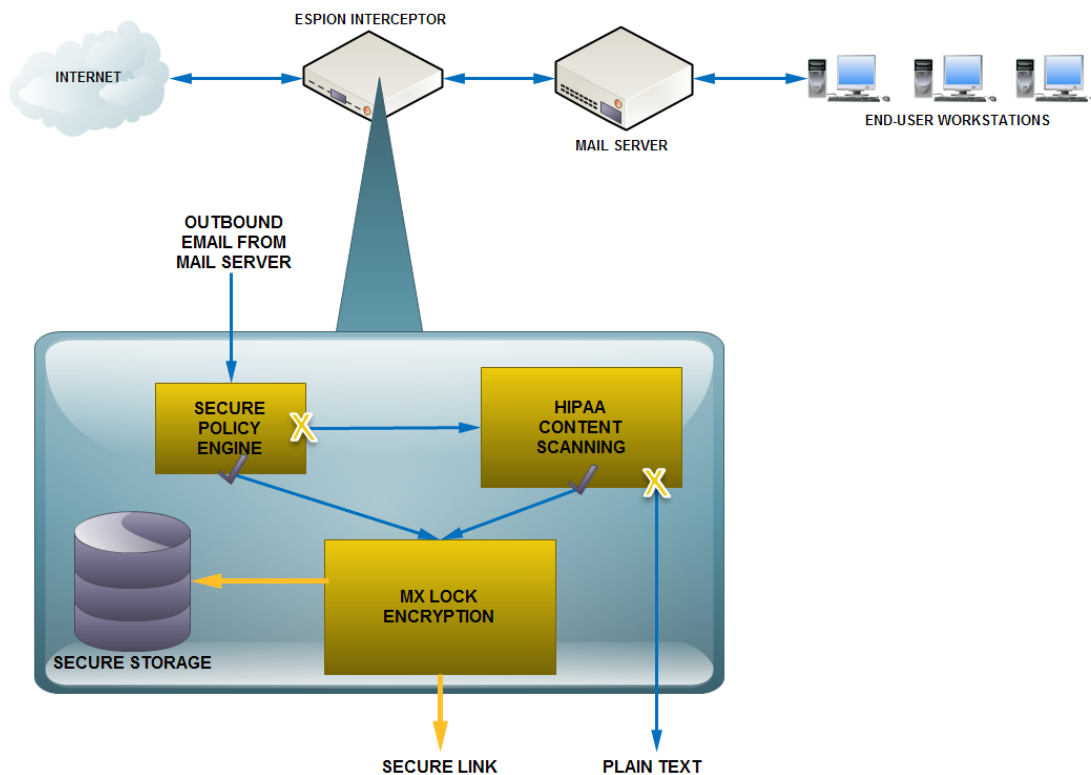
PROOF OF COMPLIANCE AND RECORDED RECEIPT

KEEP TRACK OF THE SECURITY OF YOUR ENCRYPTED EMAILS

A validated record is made when a user's email (and attachments) is encrypted by MX Lock. This record includes intricate details such as:

- The sender's and recipient's email addresses
- Date and time of the sending of the secure message (by the sender)
- Date and time of the viewing of the secure message (by the recipient)
- IP address of the workstation where the secure message was viewed
- The content policy that triggered encryption
- And more

This record is highly powerful for meeting compliance requirements and extremely necessary to withstand a HIPAA and GLBA audit.



SARBANES-OXLEY COMPLIANCE

ARCHIVAL OF ALL EMAIL TRAFFIC

Under Sarbanes-Oxley Act of 2002 (SOX) Section 404, all inbound and outbound email must be archived and available in case of an audit. The Interceptor goes further to provide a complete transaction trail which includes the sender's email address, recipient's email address, date/time the email was sent, date/time the

email was viewed and more. For archiving of incoming email, the Interceptor needs to have MX Mercury enabled.

MX LOCK provides the capability and control necessary to comply with Sarbanes–Oxley Act of 2002 (SOX) Section 404 which requires the archiving of all outbound as well as inbound email. There are several configuration options available to IT management for routing SOX email to a storage or archival email address. Organized archiving of email records for SOX compliance can be as simple as routing a blind copy of all email based on custom settings. For example each email Client can have a “blind” copy of all sent and received email sent to a unique and undisclosed email address on the archiving storage system. In this case, all inbound and outbound email is organized by the archiving system. Alternatively, IT managers can take apply a more simple method of just routing a blind copy of all emails to a single email address.

[CLICK HERE](#) to read more about meeting SOX compliance using MX LOCK.

DATA LOSS PREVENTION (DLP)

DATA LOSS IS A PROBLEM

It is highly critical for you to keep confidential company data secure. MX Lock helps protect the following data from leaving your organization’s email infrastructure.

- **Data in Motion** – All company/proprietary data flowing through your internal network and going out to the Internet.
- **Data at Rest** – All company/proprietary data stored in-house (e.g., hard drives, tape drives).
- **Data at the End-Point** – All company/proprietary data located in various end-points of your internal network (e.g., USB drives).

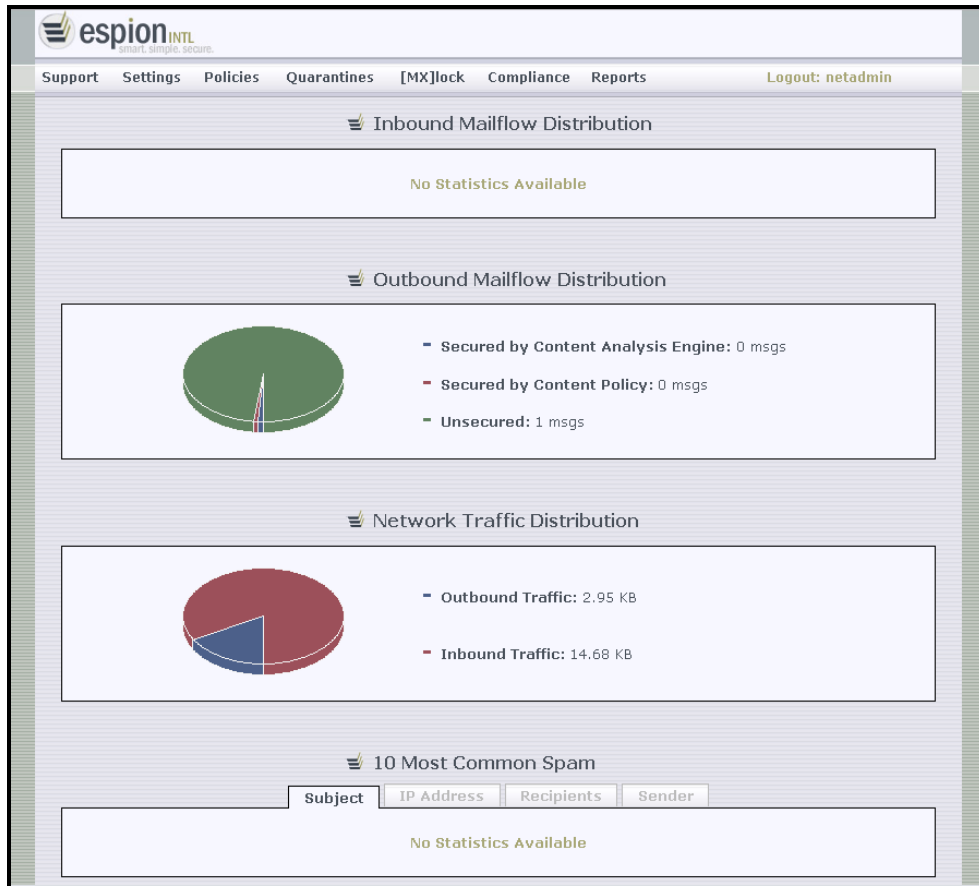
Data loss can occur through internal means (e.g., employees, consultants) or through external means (e.g., hack attempts, theft). A highly powerful and often overlooked data loss tool is your company’s email system which is often exploited by unwanted individuals. Scanning and filtering all emails leaving your network is your first step towards a data-loss-free environment.

[CLICK HERE](#) to read more about Data Loss Prevention using MX LOCK.

COMPREHENSIVE SECURE ACCESS AND CONTROL

EASY-TO-USE CENTRAL ADMINISTRATION CENTER

All traffic between the administrative web interface and the Interceptor is via a 1024-bit RSA certificate based encrypted tunnel. Since Espion builds every Interceptor from the operating system up, the OS kernel is completely browser independent. As a result the Interceptor’s web interface is completely open to supporting all Internet browsers (e.g., Internet Explorer, Mozilla Firefox, Google Chrome, Opera and others). A one-time login provides IT administration the access to administer all Interceptors in a network.



Administrative control is very granular, allowing divisional responsibility privileges which are highly customizable by the administrator(s). Client level access is also very granular with various customizable privileges. The Interceptor implements a commercial grade dashboard which reports inbound and outbound

email flow statistics such as mail flow distribution (inbound vs. outbound) and much more. IT Management is provided a comprehensive set of programming tools to permit the development of custom content governance policies for access control on Outbound Email and Attachments. Content policy rules can be easily created, deleted, ordered and sorted with a single click. Other features include:

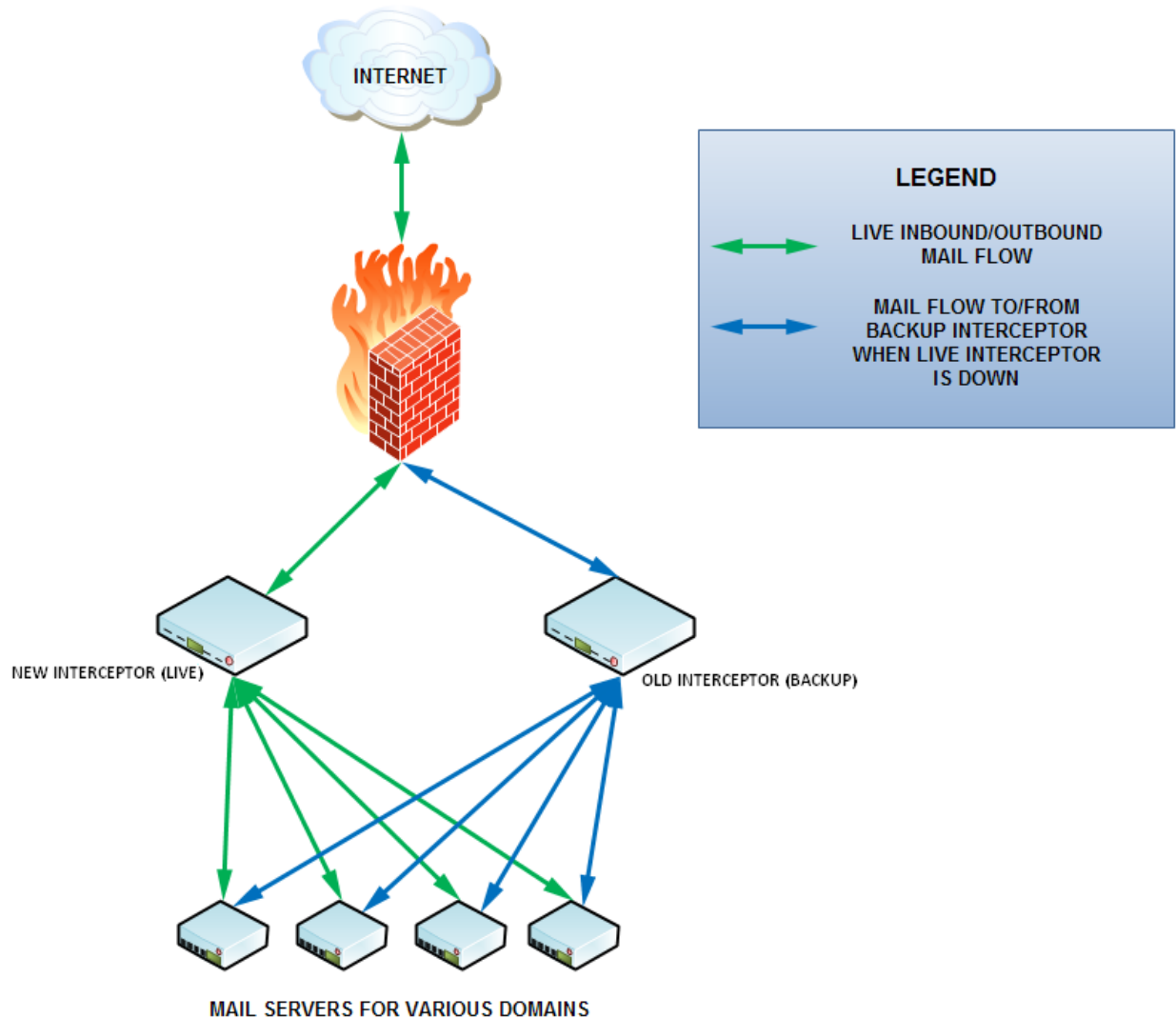
- Rules Wizards - Normal and advanced modes
- Address Rules Wizard - Rules for email from and/or to addresses
- Content Wizard - Rules for email subject and/or body

SCALING THROUGH CLUSTERING

EXPANSION WITH PRESERVATION

OLD INTERCEPTORS ARE NOT OBSOLETE

The Interceptor can guarantee your initial investment through clustering. As new Interceptor hardware platforms are deployed in your network, old Interceptor units can be configured to sync with the new units to provide redundancy and load balancing. Espion is able to provide a form of obsolescence insurance by virtue of being able to control all aspects of the system design, starting at the OS kernel and up. Although there is a practical limit to any given piece of hardware, we will often recommend placing the new Interceptor at a point front of the priority chain and allow the old Interceptor to stand duty as backup and load-balance.



CLUSTERING FOR SCALING UP/DOWN, LOAD BALANCING AND REDUNDANCY

REDUNDANCY

AN OLD INTERCEPTOR CAN BE CONFIGURED AS BACKUP

An old/existing Interceptor can be clustered with a new Interceptor to help maintain a standard and uniform configuration across all Interceptors in the cluster. While the new Interceptor can be used to handle live mail flow (as the hardware configuration is newer and more powerful), the old Interceptor can be used as a backup for if and when the new Interceptor is unavailable thereby providing highly effective passive redundancy.

LOAD BALANCING

OLD AND NEW INTERCEPTORS TOGETHER HANDLE TOTAL MAIL FLOW

Multiple Interceptors can be clustered together to help manage heavy email loads at your organization. Each Interceptor will process roughly the same amount of emails. If and when one of the Interceptors becomes unavailable, the other Interceptors in the cluster will take on the extra load with zero delays in email processing.

REMOTE CLUSTERING

CLUSTERING KNOWS NO GEOGRAPHICAL BOUNDARIES

An Interceptor is not bound by physical limitations. Multiple Interceptors can be clustered together across large geographical distances with the same ease as if they were within your network. The Interceptor AI based logic is self-learning. When fault tolerance is an issue, the Interceptor can be deployed worldwide but appear virtually local with centralized policy management.

COMPARTMENTALIZATION

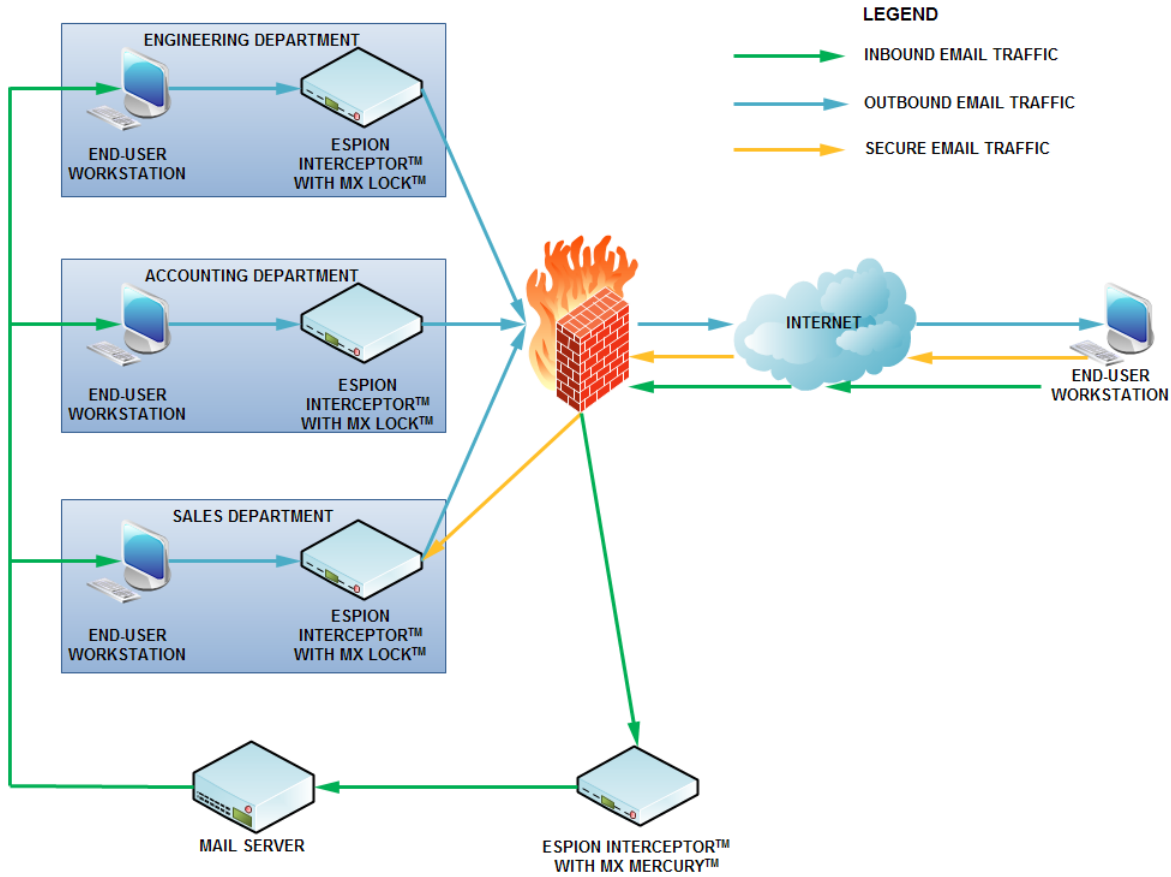
DIVIDE AND CONQUER

MX LOCK is very effective in allowing logical/functional departments to be constructed within the same email system to prevent data leakage between staff from varying departments as well as non-employees. This logical/functional filtering between internal and external users of the email system compartmentalizes email traffic based on content.

The figure on the next page shows the network configuration at a departmental basis where each department (Finance, Engineering, Production, & Sales) have dedicated compliance scanning and encryption. Each department's MX LOCK system is scanning emails and attachments from its own department before allowing them to leave the department. Each email is filtered based on customized policies.

Additionally, the figure shows an Espion Interceptor 1000™ behind the corporate firewall, scanning inbound email for spam, viruses and specific content.

[CLICK HERE](#) to learn more about Interceptor clustering.



EMAIL COMPARTMENTALIZATION FOR ADDED DATA SECURITY