

Policy Management

Preventing Email Data Leakage and Abuse

With the increasing amounts of information transferred by email every day, data theft and leakage have become a growing threat for every corporation. The Forrester Research group indicates that corporate secrets comprise two-thirds of the value of firms' information portfolio. Yet, most companies are still under protected or focus their security budgets on compliance and protection of custodial data (customer personal information) rather than internal information (corporate and product strategy, financial reports).

Organizations tend to react to and manage scandals after the fact. They should instead be proactive and protect from data leakage before it happens and before they lose the secrets that generate their revenue. It's very much like buckling on your seat belt a microsecond after impact: unreliable and ineffective.

Protect Corporate Secrets

A corporate lawyer at Meraas Capital in Dubai has been accused of industrial espionage after allegedly revealing inside information about the company to a competitor through email. Another data theft scandal involves Ferrari mechanic who had several hundred technical data email exchanges with McLaren chief designer. Recently, a businessman and Republican gubernatorial hopeful came under fire after sending out racist and trashy emails to friends and colleagues.

All these cases have one thing in common: email abuse and data leakage.

“Corporate Secrets comprise two-thirds of the value of firms’ information portfolios“

“Employee theft of sensitive information is 10 times costlier than incidents caused by accidents”

Forrester Research, “The Value of Corporate Secrets”



Comprehensive Inbound and Outbound Policy Management

Vircom's Policy Management is an add-on module to modus-Gate™ email security gateway and modusMail™ integrated anti spam mail server. Designed to help protect against data leakage of personal, financial or proprietary information through email, it will:

- Allow organizations to protect their valuable information against theft and accidents
- Enforce and monitor company policies to prevent abuse and misuse
- Keep a trace of what is being sent and received

This complete solution enables organizations to control what content can and cannot leave or enter their local network through email, and how it should be processed.

- Policy Management scans both inbound and outbound directions
- Rules examine subject, body and attachments of emails
- Rules use standard dictionaries which can be commercially-available lists of terms specific to an industry (tax and accounting terms, ICD medical codes and terms) or custom created to fit organisations' precise requirements (project codes, corporate credit card numbers, customer lists)
- Policies apply to specific users, groups (locally created or imported from Active Directory) or domains

“Data Leakage Protection is often easier (and less expensive) to acquire from archiving or e-mail security vendor as an add-on to existing solution”

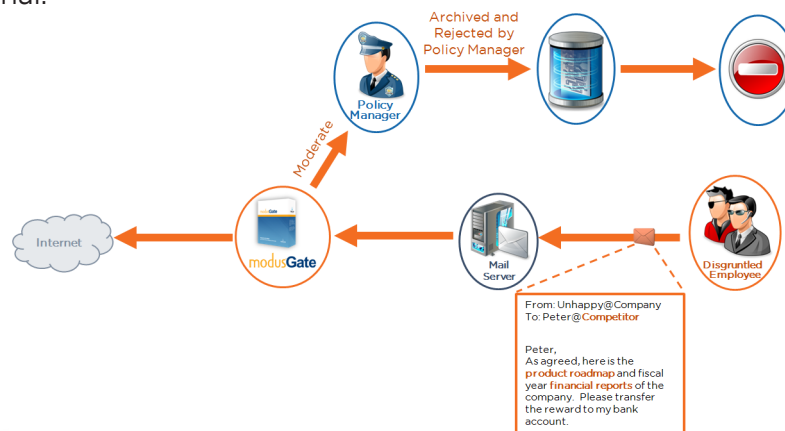
- Scan Incoming and Outgoing messages
- Provide comprehensive message handling
 - Quarantined and forwarded to policy officer
 - Issue a warning and reject
 - Delivered
 - Encrypted
- Scan attachments

The Radicati Group, E-mail Security Market, May 2010

Message Handling

Because most data in motion is time sensitive, all emails, including suspect or flagged messages, need to be delivered or moderated quickly.

In addition, the variety of content types and confidentiality of information means a single moderator cannot appropriately identify and classify proprietary data, or decide who is allowed to send or receive such material.



In order to expedite message handling, maximize confidentiality and ensure sensitive information is kept secure, each policy can be assigned to a specific moderator that will regulate the flow of intercepted emails.

These Policy Managers can administer and moderate a group of policies that apply to specific departments, or policies that apply to a specific topic or type of information.

Any message triggering one of the rules making up a policy is handled by any of these actions:

- Block the message which is returned to the sender as an attachment to a policy violation notice
- Send to moderator for revision
- Deliver and copy to moderator

In addition, optional auditing, archiving and encryption can be performed on matching rules:

Inbound

Delivery Setting	Audit	Archive	Encryption
Bounce (Return to Sender)	n/a	n/a	n/a
Moderate	✓	✓	n/a
Deliver and CC to moderator	✓	✓	n/a

Outbound

Delivery Setting	Audit	Archive	Encryption
Bounce (Return to Sender)	✓	n/a	n/a
Moderate	✓	✓	n/a
Deliver and CC to moderator	✓	✓	Ext.rcpt only

Policy Management is available in multiple email security solutions

- **modusGate™**: Email security gateway software
- **modusGate™ VM**: Hardened virtual appliance for VMware® hypervisors
- **modusGate™ Appliance**: Hardware appliance in 1U or 2U
- **modusMail™**: Integrated spam filtering mail server software

Top Rated



Contact Details

Americas: 1.888.484.7266
 World: +1.514.845.8474
 Web: www.vircom.com

