

Modus™ Description

The growing quantity and sophistication of today's spam, viruses and other malware present many challenges for e-mail communications. While inundations of spam cripple unprotected networks and drain valuable IT resources, other Email-borne menaces pose important financial and security risks for organizations and end users.

Identity theft - commonly known as Phishing - and fraud are fast becoming serious threats. More and more scammers are impersonating reputable organizations or spoofing IP addresses for illegal practices.

Address harvesting and denial of service (DoS) attacks are on the rise and causing increased network instability.

Image spam becomes an increasingly common and sophisticated network nuisance. Most spammers combine image serializing with the use of millions of spam zombies or "bots" - infected desktop PCs, located all over the world, which spammers secretly commandeer to relay their emails.

The need has never been greater for robust e-mail technology that addresses every aspect of security including its administration. Vircom's Modus™ is that technology.

I - Technology & Performance

Perimeter Defence

A proactive approach is the first step towards secure e-mail management. By creating a rock-solid perimeter defence, Modus™ annihilates the potential for damage caused by harmful emails that otherwise would penetrate to network level.

This perimeter defence protects against major e-mail threats:

- **Mailbox validation**

Through its standards-based address-validation process, Modus fortifies the mail server by reducing the number of messages that require network-level treatment.

- **DoS Attacks**

Modus strengthens your system against attacks created to crash the system or render it unavailable for legitimate tasks. It prevents packet and buffer overflows by ending suspicious connections or transactions that provoke exaggerated delays or that solicit too many system resources.

Additionally, Modus constantly monitors the number and status of connections and slows any suspicious activity (like dictionary attacks) making it impossible for hackers to overwhelm your system's resources or hijack available server threads.

- **Harvesting attacks**

Modus protects your network against address harvesting by detecting the pattern of validation attacks, which consist of sending large numbers of transaction requests to a server and tracking only the accepted receivers to validate their addresses. Modus progressively slows the connection with the requesting server, making the task of collecting addresses so time-consuming that it becomes counterproductive for spammers and harvesters.

- **Reputation & Validation Filters**

ModusGate supports multiple third-party accreditation and authentication services to check the sender's reputation. Based on his reputation, the sender can either be blocked, trusted (and bypass the anti-Spam layer) or just treated normally without any special action.

Modus also fortifies your server against e-mail frauds by using Sender Policy Framework (SPF) to validate the sender's e-mail address (versus the sending IP address) which makes it impossible for spammers and con artists to spoof the address and impersonate trusted organizations with an SPF registry.

The perimeter defence alone can reduce unwanted email traffic and processing of unwanted email traffic by as much as 70%!

Email Filtering

File threats

Not only does Modus block e-mails carrying forbidden file attachments, but it also protects networks against compression and e-mail bombs.

These potentially dangerous files are used to disable servers by overwhelming them with infinitely long code or files that consume the available CPU power until the server can no longer support the task and crashes.

Viruses

All e-mails are scanned by the SandBox-powered Anti-Virus engine from Norman Data Defence®, by the anti-virus engine from McAfee® or both. The anti-virus layer is automatically updated, 24/7, ensuring an optimal protection against sudden breakthroughs of viruses, Trojans, worms and other malicious codes potentially carried by incoming e-mail.

Sender Scrutiny

Modus next determines whether email should be blocked (block lists) or passed (trusted lists) based on sender information. User configurability ensures a versatile, multi-level, and secure scrutiny of emails.

Content Purification & Analysis

Modus proprietary "purification" processes then examine message contents through two distinct analysis engines to neutralize any form of hidden code or identify spam characteristics with the email structure.

Multi-layered multi-technology SCA

Modus passes the email through its Sequential Content Analysis (SCA™) engine. This proprietary process performs a statistical analysis of the content of the email message using a binary, dictionary-less, language agnostic method to access spam patterns. Combining predictive and deterministic technologies, Modus detects spam patterns within messages instead of instances of spam making it a proactive mechanism compared to conventional anti-spam engines.

Bottom line: Vircom's multilayered SCA™ engine outperforms any other filtering engine in the industry and delivers an outstanding out-of-the-box accuracy of 98.2% with less than 0.1% false-positives.

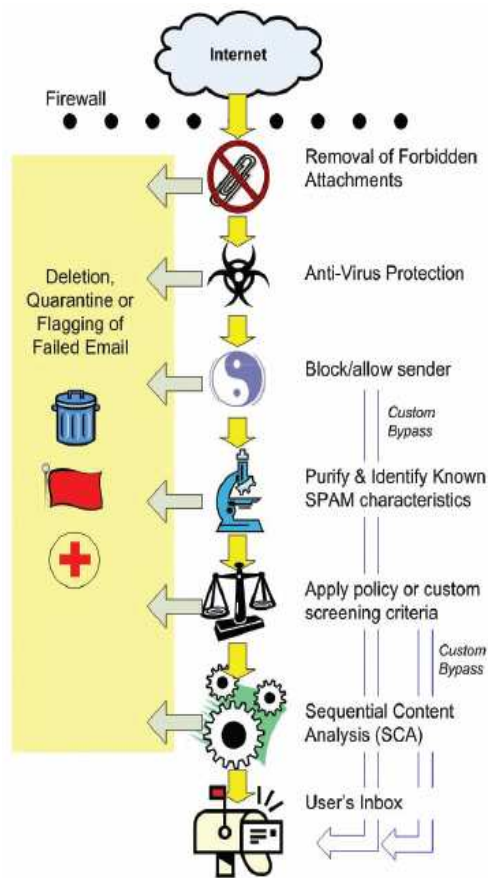


Figure 1: Modus Technology Description

Policies & Custom Rules

Although they can vary widely in nature and degree, corporate policies exist to ensure a hostile-free, professional work environment. Modus™ helps enforce your e-mail communications policies, protect your reputation and garner employee trust by analyzing e-mail for personal health information, abusive and inappropriate content, proprietary information and forbidden attachments.

- **Sieve™ scripts**

Modus compares administrator-customized scripts prepared through Vircom's Sieve™ facility to manage email against the internal policies or as a fallback to block worm or Trojan outbreaks.

These Sieve scripts can be based on message header, body and file names or types and can force a variety of actions, including: Email blocking, deletion or tagging, email redirection or moderation (for parental control, f.i.), email archiving and email encryption.

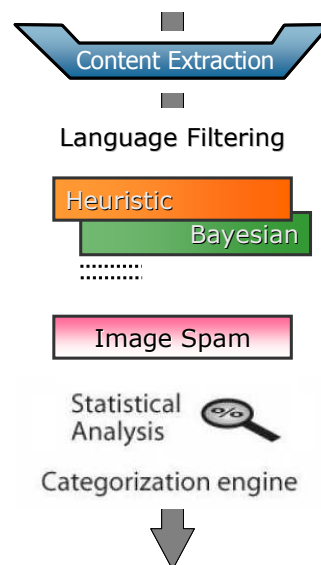


Figure 2: Multi-layered SCA™ Engine

- **Ultimate Flexibility**

Modus can choose which traffic to filter (inbound, outbound...) and when in the message processing sequence administrators want to run their scripts:

- Before content scanning (after the security checks are passed and the message is accepted for processing)
- Before anti-spam scanning (after the anti-virus scanning is complete)
- After all scanning

II - Effortless Administration

Automation

Automated User Database Management

Through standards-based lookups (SMTP, LDAP, MS Active Directory...), the ModusGate is aware of the user account and alias management done on the mail server and seamlessly inherits it without human intervention. This integrated management eliminates multiple quarantines and administration hassles.

Automated anti-Spam and anti-Phishing Updates

The SCA analysis is performed against the latest Spam and Phishing identification rules.

Vircom's SpamBuster team (not your staff) joins human analysis to a matchless self-learning mechanism to constantly update the SCA engine. They gather spammers and spam information through Internet monitoring, distributed honeypots and from millions of users reporting spam and false-positives.

This centralized approach insures that every lesson serves to all ModusGate systems and not just to one. More importantly, it offloads your staff from repeatedly training and tuning your own individual anti-Spam system...

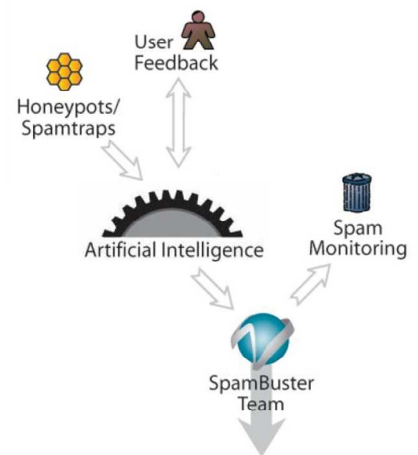


Figure 3: Auto-Updates

Personalization

Because your users are not all the same, Modus allows system managers to differentiate numerous settings (scanning severity, language filtering, attachment blocking, trusted lists, blocked lists...) at user and domain levels, offering the industry highest flexibility.

Through Modus' powerful authority delegation, administrators can allow advanced users to manage their individual settings themselves (via their WebQuarantine interface) avoiding administrative burden and force corporate-wide settings for less experienced users to avoid improper configurations.

Reporting and Tracking

Another important feature is Modus' WebMonitor module, which records system, traffic and email behaviour at the server, domain and mailbox levels.

System Health

At any time, corporate administrators can review the overall behaviour of their system. The new Modus System Health screen will show you information about:

- System Status (for the hardware Modus uses and interacts with).
- System Activity (for Inbound and Outbound connections, Processing and Message Delivery queues, WebQuarantine/WebMail Connections – and POP3 and IMAP4 Connections for the ModusMail product).
- Performance Averages (average performance rates for messages processed in the last second)
- Version Information (for Modus, your operating system, and about updates for the anti-spam/anti-virus engines)

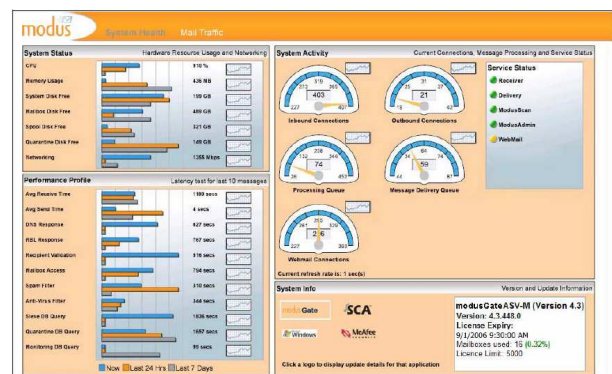


Figure 4: System Health in WebMonitor

Mail Traffic

At any time, end users and corporate administrators can access e-mail statistics, which are plotted per day, week and month.

The statistics module allows end users to consult their personal mailbox history, while corporate administrators can track all messages at the corporate or mailbox level. Detailed records of all e-mails scanned and stored enable system administrators to make informed decisions about network security based on documented trends in spam and other e-mail-borne threats.

Message Audit Log

System administrators can audit email messages and see the most recent transaction history, for mail processing, in the Message Audit view of the WebMonitor application.

The Message Audit displays a view of all message transactions in a 1-line per message summary. This feature tracks message traffic – inbound external mail, outbound local mail and mail from local user to local user (ModusMail only).

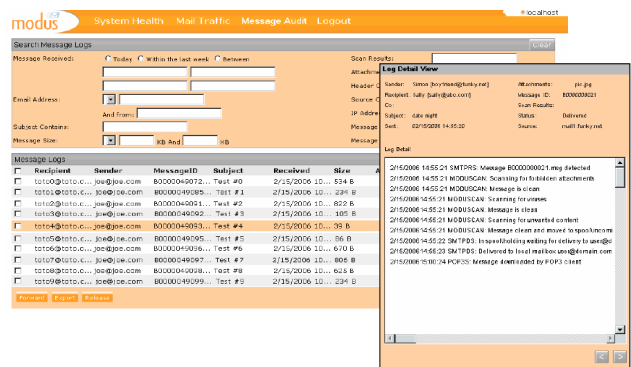


Figure 5: Message Audit Log in WebMonitor

III - Efficient User Interfaces

Advanced Quarantine Report

All users will receive an advanced quarantine report that will list the different blocked messages and the reason for them to be blocked.

Through the Quarantine Report, users can review blocked messages, open message in a safe environment, release messages, report false-positives and Whitelist senders in as much as two mouse clicks.

The quarantine report also allows users to:

- Select only the desired items to report
- Change the report frequency,
- Generate an updated report on demand...



Figure 6: Quarantine Report

Powerful WebQuarantine

The WebQuarantine component provides users with access to their quarantine contents from a web browser. WebQuarantine includes features such as message statistics and built-in access to scan preferences.

Through Modus' powerful authority delegation, administrators can therefore allow advanced users to manage their individual settings avoiding administrative burden and force settings for less experienced users to avoid improper configurations.

When authorized, power users can define numerous settings through their WebQuarantine, including:

- Scanning severity,
- Blocking actions (Delete, Tag...),
- Language filtering,
- Personal trusted and blocked lists,
- Quarantine report preferences...

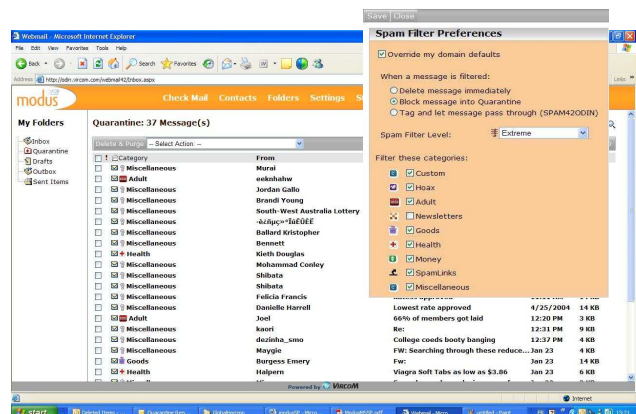


Figure 7: Web Quarantine Interface

Both Web Quarantine interfaces and Quarantine Report layouts are easily customizable in form and content (to match the corporate logo and colour schemes or to remove configuration options).

Conclusion

The Modus technology was created from the realization that there is no single tool that can adequately solve the complex problems that threaten email productivity today. As a result, Vircom's Modus™ technology combines several different tools to optimize spam and virus protection and offer administrators the powerful administration features you need.

Industry-leading catch rates, effortless administration and efficient user interfaces makes Modus™ your best buy:

- **Industry-leading catch rates**

This represents:

- Less spam in your user inboxes and less false positives for them to go retrieve
- Less requests or complaints to your help desk

- **Effortless administration**

Automation, delegation and monitoring greatly reduce the time you spend administrating the system, often making your Modus™ an "install & forget" solution.

- **Efficient user interfaces**

Ferris Research¹ estimated in a recent report that a typical medium-sized organization with good Spam protection spends about \$61 per user per year for quarantine management or... about 51% of the total cost.

Using Vircom's industry leading quarantine user interfaces will significantly reduce the time your users spent managing their quarantine and therefore significantly reduce the total cost!

Moreover, there is more. Vircom's Modus solutions (ModusMail™ mail server and ModusGate™ versatile email assurance gateways) offer additional sophisticated implementation and management features. These include integrated email caching or clustered implementation to improve availability, email encryption for respecting new confidentiality standards and regulations, advanced management features like alias management or disk space management and much, much more...

About Vircom

Vircom is not a typical software developer. They are a forerunner of email assurance. The company has been in the industry for over 10 years. It understands its markets, the e-mail challenges they face, the fact that there is more to email assurance than just anti-spam or anti-virus. That is why Vircom's own well-architected Modus technology is designed to address existing threats (spam, virus, Phishing, DoS...) but also to quickly adapt to new threats or standards as they emerge!

Throughout its development, Modus technology has earned numerous awards from industry experts including SC Magazine and Network Computing. Equally telling are the success stories of Vircom clients from all over the world - including NASA, Toshiba, Time Warner Cable, Sheraton Hotels & Resorts, The Hard Rock Café and the European Committee for Standardization (CEN) - who use and recommend Modus as their leading secure e-mail management technology.

¹ Ferris Research – Calculating Spam Cost in Your Organization - February 2005 - Report #511

