



WHITE PAPER

# Safeguarding your Email Infrastructure

INSIDE MODUS™ TECHNOLOGY

# Table of Contents

Executive Summary .....	3
Vircom's modus™ Technology.....	3
Multiple Layers of Protection .....	3
Perimeter Defense .....	4
Protocol-level Filters.....	4
Content Filters .....	4
Predictive Methods.....	4
Deterministic Methods .....	5
Summary.....	5
Compliance and Policy Management .....	5
Deployment Best Practices .....	5
modusGate™ .....	5
modusGate™ Appliance .....	6
modusMail™ .....	7
Management, Monitoring and Reporting .....	7
Where Vircom Brings Value.....	8
Conclusion .....	8
About Vircom.....	8

## Executive Summary

Most organizations consider their e-mail security solution to be the center point of control over all aspects of their inbound, outbound, and internal acceptable communication policies. Spam threats make up 80% of email traffic<sup>1</sup>. As such, it is imperative that email security solutions continually update their spam definitions and must be flexible, scalable and easily managed. Successful solution providers are proactive problem solvers, ensuring that spam and other email borne threats never adversely affect their clients.

Sophisticated techniques used by spammers make it challenging for email security solutions to keep pace. Few vendors have the expertise to understand the principle mechanics of spam. Vircom's modus™ technology addresses this issue by providing a highly performing solution that analyzes all inbound and outbound email traffic to counteract spam, phishing, viruses, spyware, out-of-policy communications and other email threats. Vircom's products ensure that email communications are never compromised.

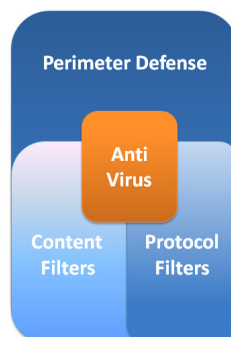
Botnets, fast flux and phishing attempts are examples of email-borne threats, and effective anti-spam technology must be able to respond to up-to-the-minute attacks, and incorporate deterministic and adaptive capabilities.

The following white paper describes Vircom's modus™ technology and why its multi-layered architecture makes it a leading turnkey solution.

## Vircom's modus™ Technology

Vircom's proprietary technology is at the heart of all of its products - designed to address spam, virus and policy violations and to quickly adapt to new threats as they emerge. modus™ provides a full suite of filtering options, including perimeter defense, sender authentication and accreditation layers, Denial-of-Service protection, hacking prevention, and attachment blocking. Powerful filtering engines ensure optimal and unparalleled accuracy in blocking threatening email and providing versatile email policy management.

### Multiple Layers of Protection



Multi-layered Architecture

Spammers continuously look for new techniques to ensure delivery of their messages. Some techniques elude content filters while other methods bypass protocol filters. Email filtering solutions must therefore work at different levels to be effective.

Vircom's modus™ architecture combines several layers of security that, when used in conjunction with anti-virus protection from Norman® Data Defense and McAfee® promises superior email security:

## Perimeter Defense

This first layer provides network-level protection, acting as the first line of defense. Vircom's proven network-level filtering rejects high volumes of unwanted mail and blocks the most obvious spam without ever receiving the email message. Network layer protection includes connection blocking and limiting which prevents simultaneous connections from a single IP.

Administrators can specify real-time blacklists (RBLs) while excluding trusted IP addresses from lookup. Enabling Reverse DNS ensures that users sending mail to your server are from legitimate domains. Another form of email authentication, DKIM (Domain Keys Identified Mail) is also used at the network layer. DKIM uses public keys and the DNS to establish the origin of a message, tracking and detecting domains and thus aiding in identifying those from which forged or fraudulent email originates.

In addition, Vircom's Sender Reputation System (SRS) provides predictive and proactive defense for new waves of spam threats. SRS quickly identifies spammers by predicting the legitimacy of the sender using a set of identifiers, such as IP address, domains and URLs, at the connection level. Dynamic by nature, SRS is designed to act quickly to changes in behavior based on the identifiers. Vircom believes in the importance of reputation on a global scale, and is working with recognized partners to improve upon reputation systems for the benefit of the entire Internet community.

## Protocol-level Filters

The second layer of filtering occurs at the protocol level, during the SMTP transaction. Filters, such as block scan attack, can be enabled allowing administrators to limit the number of recipients for incoming mail. This effectively prevents spammers from sending messages with an unusually high number of recipients as well as slowing down and blocking dictionary attacks. SMTP Authentication can be configured and requires user authentication prior to email being relayed.

## Content Filters

modus™ offers various content filters to further detect potential email threats. modus™ scans attachments and automatically blocks password-protected encrypted files. It also blocks attachments according to their extension types.

Custom scripts can be created, using Vircom's Sieve™ scripting feature, to further intercept forbidden content. Additionally, modus™ is available with anti-virus protection from industry leaders Norman® Data Defense and McAfee®.

## Predictive Methods

Unique to modus™ is Vircom's proprietary and adaptive Sequential Content Analyzer (SCA™) engine which scans message contents. The SCA™ performs an analysis against the latest spam identification rules, updated automatically by Vircom's security team. The SCA™ uses machine-learning artificial intelligence allowing it to detect spam that it has not seen before.

## Deterministic Methods

Using information gathered from spam messages, these reactive methods, such as keyword filtering and checksum databases, effectively lower the occurrence of false-positives and are more efficient in countering new spam techniques.

## Summary

While some decisions can be made at a very early stage, such as when a sender is blacklisted, others require a correlation of several factors. It is the synergy between the features and the layers that ensure email filtering efficiency.

modus™ optimizes treatment efficiency with its multiple cross-connected filtering engines, each one providing the others with valuable decision-making information and each capable to make a decision as early as possible to optimize performance. This flexible and scalable architecture allows Vircom to update, enhance and add engines to counter new threats quickly.

## Compliance and Policy Management

Key to most organizations is the ability to protect information, both inbound and outbound. This reduces the risk of fraud and allows them to conform to government regulations regarding privacy of information.

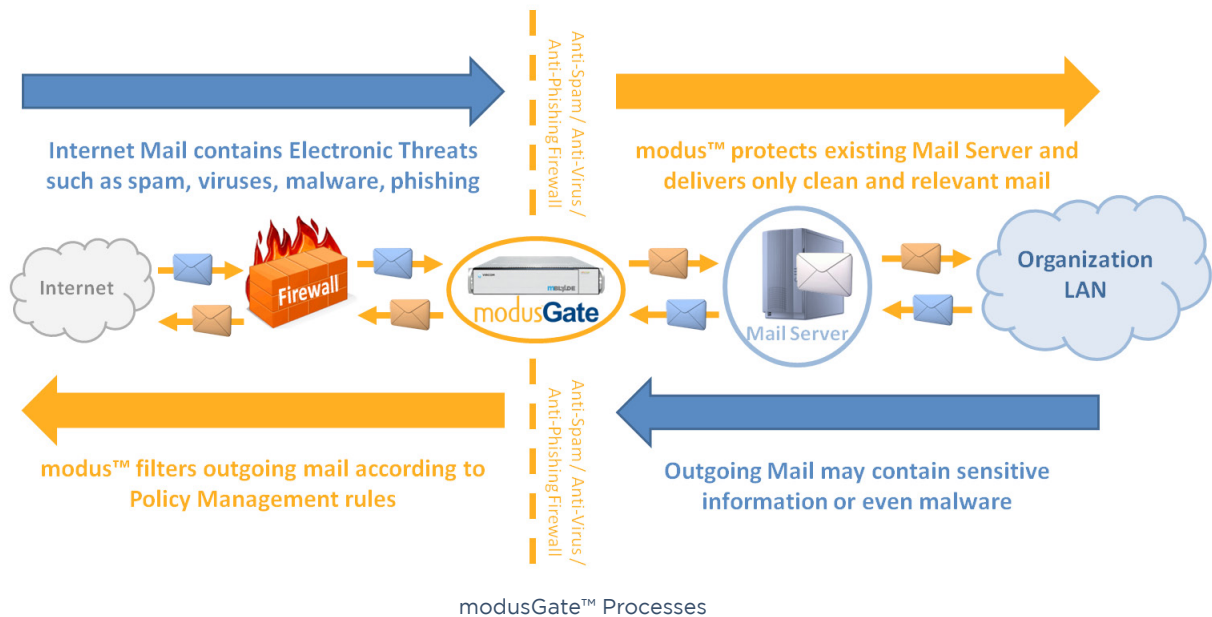
Vircom's Sieve™ scripting engine allows administrators to create customizable filters for restriction-free policy management to support regulatory standards such as PCI-DSS, SOX and HIPAA. Furthermore, logging functions generate and retain copious amounts of information, which includes records for server performance, configuration, operation, security, spam and virus scans, authentication activity and audits of message transactions.

## Deployment Best Practices

Vircom's modus™ suite of products can be adapted to suit your email environment. Available as an email server with webmail, an integrated gateway software installed on your own hardware and placed in front of an existing mail server or a turnkey appliance, modus™ is designed for flexible deployment options. It can be used in a blockade when redundancy or high availability is required, as a virtual server and as an SDK.

## modusGate™

Vircom's modusGate™ email gateway separates the security from the actual mail server. It integrates seamlessly with Microsoft® Exchange, Lotus® Domino or any standards-based email-server and offers powerful MTA features. At its core are the acclaimed multiple layers of filtering and message scanning functions for which modus™ is known.



Installed on a separate server or delivered as an appliance, modusGate™ resides between the firewall and the mail server. Incoming messages are first processed by modusGate™ to undergo security checks and message content scanning. Legitimate messages are then relayed to the mail server for delivery to local mailboxes.

modusGate™ can authenticate users through SMTP, LDAP or Active Directory and can automatically create users to mirror the mail server. Microsoft's SQL Server Express, standard with all modusGate™ installations, facilitates access to data. Alternatively, modusGate™ can be integrated with an existing SQL Server for greater data storage or if replication or a cluster environment is required.

## modusGate™ Appliance

Vircom offers a portfolio of modusGate™ appliances from entry-level to an enterprise solution. Featuring all of the benefits of modusGate™, these scalable appliances are the perfect cost-effective solution for your email security requirements.

For the entry-level market, the m100 is equipped with an Intel® processor and will process up to a million messages a day. The m150, well suited for the mid-range market with the capability of processing over a million messages, comes with an Intel® Core Duo 4300 1.8 GHz processor, up to 8G DDRII memory and RAID-1 support.

The mBlade™ is Vircom's definitive email gateway appliance. With four hot swappable SATA drives, 8G DDR II RAM and built-in RAID-5 for data integrity, it is our fastest and most powerful email security solution. An expandable appliance, the mBlade™ can support up to 8 SATA drives, two Quad Core processors and up to 32 G DDR II RAM and RAID-0, 1 or 10. For high capacity needs, with high traffic and stringent security requirements, the standard mBlade™ provides all of the modus™ features and is able to process up to 17 million messages per day. Deployed in high-availability mode, the mBlade™ will meet the requirements of the most demanding carrier grade and enterprise customers.

## modusMail™

modusMail™ comes bundled with everything required to deploy email: messaging services, an end-user interface, security controls and the best anti-spam/anti-virus protection available. modusMail™ features versatile deployment options and supports SMTP, POP3 and IMAP4 protocols. Authentication can be performed against various sources such as ODBC databases, Active Directory, LDAP and Radius. Because of its highly granular design, modusMail™ settings can be customized globally, per domain or per user and an unlimited number of domains are supported with no additional licensing.

modusMail™ also allows for easy integration with most billing software such as LogiSense, RODOPI, EcoBuilder, Platypus Billing System, and Emerald.

## Management, Monitoring and Reporting

Tools and engines alone cannot solve the complex email problems that threaten your organization's security and productivity. modus™ administration has been designed with ease-of-use in mind, providing administrators full control of their email security settings:

- **Engine updates:** Vircom's security team combines human analysis with a matchless self-learning mechanism to ensure that your spam engines are constantly and automatically updated. Additionally, up-to-the-minute anti-virus engine updates from Norman® Data Defense and McAfee® provide outstanding zero-day defense.
- **Delegation:** modus™ offers the greatest flexibility in the industry, allowing you to differentiate numerous settings at both the domain and user levels. To avoid complications, system administrators can delegate domain and users settings or force system-wide settings to avoid improper configurations. To avoid administrative overhead, modus™ inherits user account details, including alias information, from the mail or directory server.
- **Quarantine management:** By delegating elements of mailbox management to end-users, administrators are free to work on more pressing issues. Users can quickly review and release blocked messages, report false-positives, add senders to their trusted and blocked lists and schedule quarantine report delivery. Quarantine reports can be customized for maximum effectiveness and viruses, spam, phishing and attachments are all treated separately. Moreover, with quarantined items consolidated into a single report, end-users are not required to scour their junk mail folder for legitimate messages.
- **Reporting:** modus™ features extensive system, domain and user-level reporting. Reports include a system overview, security threats, trend analysis and tracking of top issues. Report scheduling allows administrators to generate reports on a daily, weekly or monthly basis. The reports can be printed, exported to PDF and Excel formats and emailed.
- **Web applications:** modus™ features WebMonitor, an application that provides information about system health and mail statistics using a real-time dashboard display, SNMP and Windows® performance monitors. At a glance, administrators can determine the system's complete operational status, view real-time usage statistics, audit email messages and see recent transaction history. The WebAdmin application provides Web access to the administrative functions of modus™. Mirroring a large part of the modus™ administrative console, IT administrators can use it to manage modus™ remotely or grant access to domain administrators to manage their own user settings. This can be useful for ISPs and organizations that host multiple domains.

## Where Vircom Brings Value

modus™ was designed for Windows® Server and continues to be optimized for it. It offers several deployment options and takes advantage of built-in Windows® features such as the backup facility, task scheduler and Remote Desktop. There are few, if any, additional costs as a result. It also allows Vircom to focus its efforts on email security features while still providing all of the tools necessary for disaster recovery.

Ferris Research<sup>2</sup>, in their 2007 The Cost of Spam report, estimates that spam will cost companies a total of \$100 billion worldwide. These costs are related to productivity loss from inspecting and deleting spam that is missed by filtering solutions, searching for legitimate email deleted in error by spam solutions (i.e. false-positives) and operations and help desk costs.

A 2007 survey conducted by Nucleus Research Inc. found that the annual cost of spam to American companies doubled to \$1,934 per employee, with employees spending more than 1% of their time managing spam in their inboxes every day.

While modus' high catch-rate and low rate of false-positives ensure outstanding filtering results, its granularity sets it apart. A one-size fits all approach to email security assumes that all users are alike and experience the same mail issues. Vircom offers a variety of deployment options to address the unique email security needs of any size organization. Delegating filter controls to end-users takes some responsibility from administrators and places it in the hands of those who can best determine individual needs. By setting their own quarantine report preferences and schedules, end-users decide how and when to deal with spam. This helps decrease the amount of time spent dealing with spam.

## Conclusion

Email is used in over 90% of corporate communications, and is now the most mission-critical communications element in system infrastructures. The ability to stop spam and prevent security threats, as well as track and report on system activity, greatly enhances an organization's ability to comply with regulations, ensure information is safe, and protect users from malicious attacks. Vircom's modus™ suite of products offer complete security, from spam and virus protection to perimeter defense and compliance.

With its team of security experts and leading technology, Vircom emerges as a leader in safeguarding email infrastructures and ensuring peace of mind.

## About Vircom

Vircom is a global leader in email security, specializing in software, appliance solutions and professional services. With over 15 years of experience, Vircom has been the first to market with several solutions, including technology to block image spam and predictive email content management.

Vircom's products include modusMail™, modusGate™ software, modusGate™ Appliance and are made available to several major security providers and deployed through third-party vendors to more than 6.6 million inboxes worldwide. For more information, visit [www.vircom.com](http://www.vircom.com).

2.Ferris Research, Industry Statistics, <http://www.ferris.com/research-library/industry-statistics/>