

# ***Modus™ Secure Email Management***

**By Paul Vanbosterhaut**  
Managing Director

December 1, 2004



**VIRCOM**  
E U R O P E

# Contents

- OVERVIEW ..... 3**
  - THREAT PREVENTION ..... 4
  - EMAIL FILTERING ..... 4
    - Policy management*..... 4
    - Anti-Spam filtering*..... 4
- TECHNICAL DESCRIPTION ..... 6**
  - MULTI-LAYERED TECHNOLOGY OVERVIEW ..... 6
- THE PACKAGES ..... 9**
  - SOFTWARE PACKAGES ..... 9
  - MODUSAPPLIANCE ..... 9
- KEY PRODUCT/SERVICE STRENGTHS..... 10**
  - CATCH RATE PERFORMANCE & FALSE-POSITIVE PROTECTION ..... 10
  - LOWEST TCO..... 10
  - STATISTICS & MONITORING..... 11
  - CUSTOMIZATION OPPORTUNITY ..... 11
  - CLUSTERED CONFIGURATION FOR MAXIMUM AVAILABILITY ..... 12
  - INDEPENDENT DELIVERY ..... 12
  - VIRCOM-RELATED DIFFERENTIATORS..... 13
    - Vircom’s eMail Background*..... 13
    - Product Maturity*..... 13
    - Vircom’s Support*..... 13

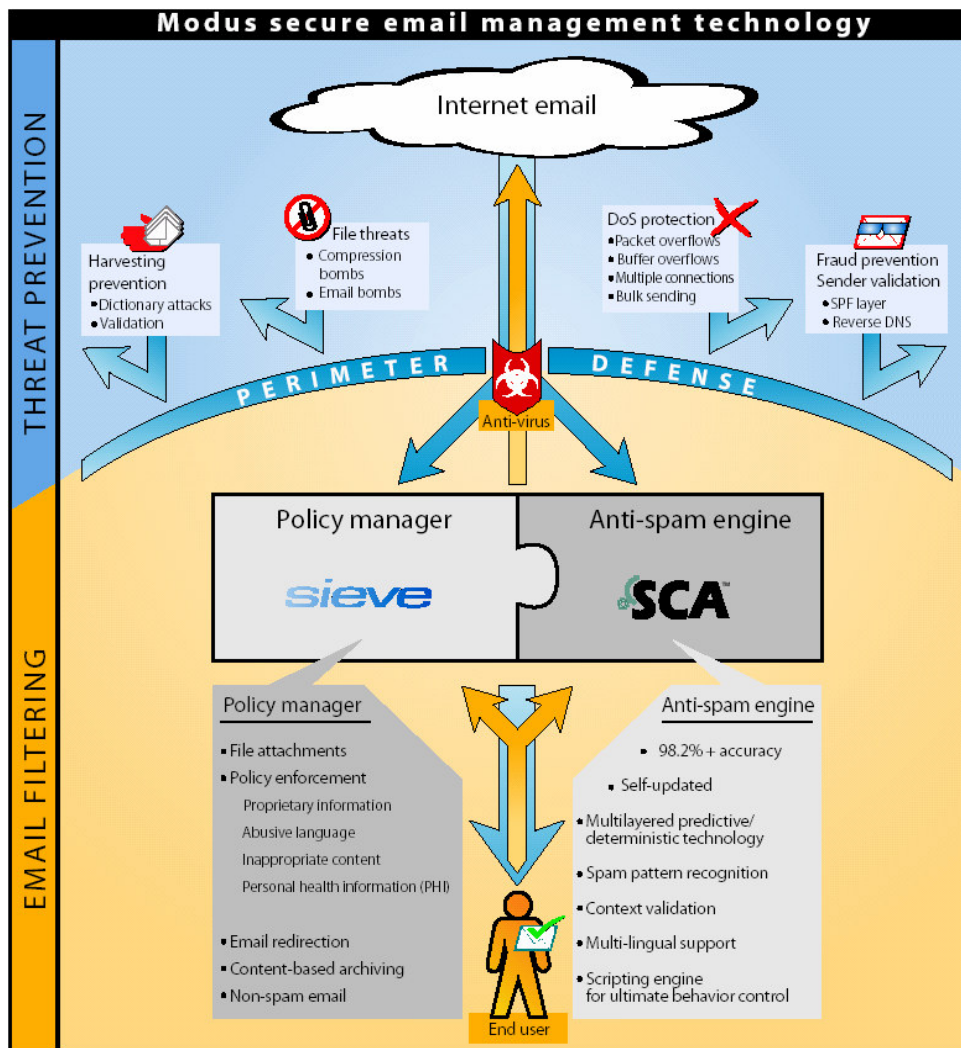
## Overview

The growing quantity and sophistication of today’s spam, viruses and other malware present many challenges for email 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, making victims of those targeted by these underhanded and illegal practices. Additionally, address harvesting and denial of service (DoS) attacks are on the rise and causing increased network instability.

Consequently, as spam and malware become more sophisticated, so must the technology designed to combat it. But the issue of security is not limited to inbound spam and other incoming email. Organizations in particular must also monitor and control the outgoing flow of email to prevent hostile work environments, information leaks and the illegal distribution of trade secrets and privacy-protected information. Additionally, email caching and failover set-ups are crucial for ensuring the robustness and full functionality of email networks.

Clearly, the need has never been greater for robust email technology that addresses every aspect of security. Vircom’s Modus™ is that technology.



*Figure-1: modus Secure eMail Management Overview*

## Threat prevention

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

This perimeter defence protects against:

- DoS Attacks (Packet overflow, buffer overflow due to bulk messages & multiple connections)
- File threats (Viruses, compression bombs, email bombs..)
- Harvesting attacks
- Spoofing (Prevention via Sender's Validation)

What's more, Modus™ fortifies emails server by reducing the number of messages that require network-level treatment. This amounts to considerable savings in bandwidth, CPU and IT resources.

## eMail Filtering

Once accepted into the network pipeline, emails undergo an exhaustive series of checks for policy management adherence, spam, viruses and other malware.

### Policy management

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

This policy management allows:

- Management of File Attachments (allowing several security levels)
- Policy enforcements
  - Proprietary information
  - Abusive language
  - Inappropriate content
  - Personal Health Information (PHI)
- eMail redirection
- Content-based archiving

### Anti-Spam filtering

What's more, with a dedicated, auto-updated anti-spam engine, Modus™ delivers up-to-the-minute protection against the latest email-borne threats.

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 no more than 0.001% false-positives. Combining predictive and deterministic technologies, the SCA™'s unique approach of detecting spam patterns within messages instead of instances of spam makes it a proactive mechanism compared to conventional anti-spam engines.



# Technical Description

## Multi-Layered Technology Overview

Vircom’s Modus3 technology is the only layered solution using multiple filtering technologies to identify, classify and manage spam messages. Figure-3 shows the trajectory of an email coming in from the Internet.

Before even arriving into your customer’s corporate system, it is checked by a 9-layer pre-protection that detects the basic forms of spam and malformed messages:

- The **Protocol filter** recognizes known header patterns and bounces them out automatically, without requiring any system resources.
- The **SMTP Security** automatically scans the sender’s information in search of accepted or rejected address patterns.
- The **Mail Relay** is a configurable IP-based authorization system that lets you control who can and cannot relay email on your corporate server.
- The **Block Scan Attack** layer counts the volume of transactions coming from a single source and either blocks or progressively slows the e-mail exchange process, thus making the server counter-productive to any spammer.

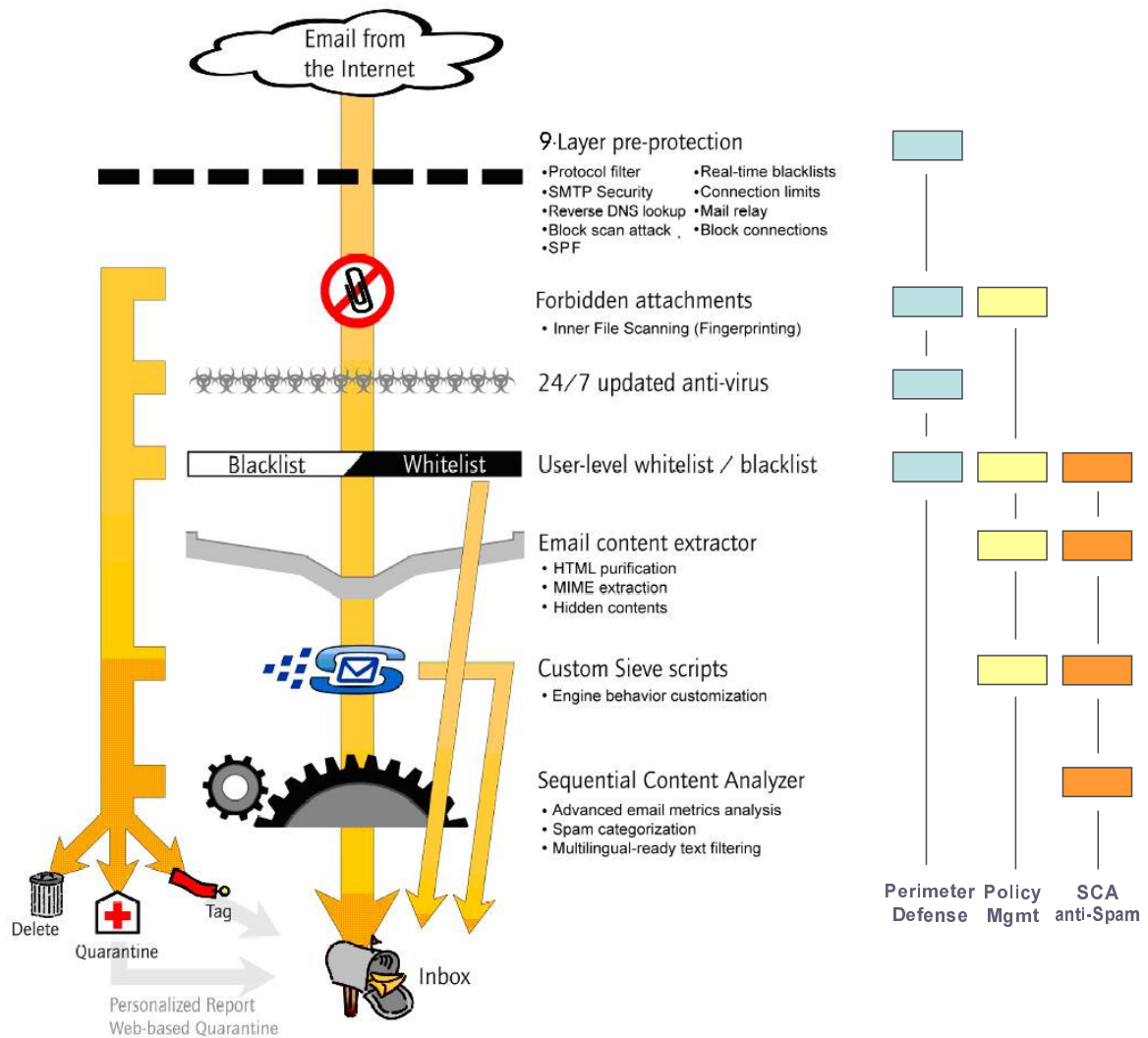


Figure-2: Multi-layered technology overview.

- The **SPF (Sender Protection Framework)** layer detects whether an email is being sent from a legitimate IP address and to block emails that are being sent from forged (or “spoofed”) IP or domain addresses.
- The **Reverse DNS Lookup** sends a request to the sender’s domain IP address before it accepts any e-mail. If the IP returns a negative check, the e-mail is bounced.
- The **Real-Time Blacklists** (or blackholes) layer compares the sender’s name to different spammer blacklists and blocks any e-mail processed by a blacklisted sender. This is an optional feature that can be set according to your corporate policies.
- The **Connection Limit** prevents a user (an IP address) to perform simultaneous operations in the server.
- The **Block Connections** layer is a configurable filter that blocks specific IP addresses or domain names from sending e-mail.

After these first 9 checks, email is rejected or accepted for treatment. If it is accepted, it is checked for **Forbidden Attachments**. This features comes with an out-of-the-box forbidden file extension list, but can be customized at the network, domain or user levels. Modus3 features a powerful inner file scanner that goes beyond the mere file extension and actually verifies the contents of the file to make sure it matches its extension.

The email is then scanned by the Anti-Virus engine, either from **Norman Data Defense**® or from **McAfee**®. 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 email.

Before being processed by the content extractor, the message is checked by the user-level **Whitelist / Blacklist**. If the sender of the message has been whitelisted, the email will go through the solution, whatever its contents. If the sender was blacklisted, the message will be either deleted, put in the user’s quarantine or tagged and sent to the user’s inbox.

After these first 4 verifications, the email is ready to be processed by the **Email Content Extractor** that purifies all MIME and HTML contents that can prevent the message from being properly analyzed by the solution. Any non-conforming or hidden content is thus removed, and the message is sent as purified text with added email metrics for further analysis.

If **Custom Sieve Scripts** have been added, the message will be filtered according to the custom rules before it gets to the SCA engine, thus making it possible for IT administrators to modify the engine’s behavior or to implement custom corporate content policies.

At this point, the message has been checked outside of the corporate network, it has been made sure that it doesn’t carry a forbidden file format as an attachment, it is confirmed that it doesn’t carry viruses or other forms of harmful code and has been verified on the user’s whitelist / blacklist registry. Two types of email remain at this point: legitimate emails and the most advanced forms of spam.

To sort them, the **Sequential Content Analyzer** will use the data and metrics defined by the email content extractor as well as the purified text of the email to determine whether it is spam or a legitimate email. Using the advanced email metrics to judge the integrity of the original message, it will rate the likeliness of the message structure to be spam. Then, the SCA will extract sequences of the text contents and proof the structure against all forms of spam patterns.

The combined statistic likeliness of spam and result of the sequential content scanning are what finally discriminate the most advanced forms of spam from legitimate messages.

Once a message is identified as spam, it is categorized according to its contents.

Vircom currently classifies spam in 8 different categories:

- Hoax: Chain email, scams, fraudulent offers
- Adult: Pornography, sexually explicit contents
- Patterns: All messages that fit a typical spam pattern: Single link, image with URL, etc.
- Money: Loans, credit cards, debt consolidation, mortgages
- Goods: Various products for sale
- Health: Viagra and the likes, prescriptions, drug offers
- Custom: Spam caught through custom Sieve filtering
- Miscellaneous: All other types plus spam that potentially fits multiple categories.

At the end of this process, spam is identified and categorized. According to your settings, it is either: deleted, put in the user's quarantine or sent to the user's inbox with a defined tag in the subject field of the message.

Periodically, at your convenience, a quarantine report can be sent to end users to inform them of the contents of their quarantine. The one-click, easy-to-use interface of the email-based report allows them to release quarantined emails if desired.

# The Packages

After years of research and development, Vircom has developed a email infrastructure solution that capitalizes on the best of script, heuristic and statistic technologies to efficiently and reliably intercept and classify undesirable email without interfering with the normal flow of legitimate messages.

## Software Packages

The software solutions provided by Vircom are split within two main categories:

- modusMail (family of secure mail servers)
- modusGate (family of secure gateways)

Each family contains 4 different packages with different security levels.

They are described in the following table:

<b>modusMail</b> <b>Secure Email server</b> Complete e-mail server software	<b>modusGate</b> <b>Secure Gateway</b> Protects ANY e-mail server on ANY network
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

Both solutions are offered with various service packages:

- L:** Software package
- AS:** Software package + SCA™ anti-spam update service
- ASVN:** Software package + SCA™ anti-spam update service + 24/7 Anti-virus update service from Norman® Data Defense
- ASVM:** Software package + SCA™ anti-spam update service + 24/7 Anti-virus update service from McAfee

*Figure-1: Vircom’s Software messaging solutions.*

## modusAppliance

The power of modusGate is also integrated within a Dell-based appliance.

### modusGate



	Model	CPU	RAM	HD	Notes
Corporate (< 2000 users)	ModusAppliance20 series	2.8GHz P4	512M	Dual 36GB 15K SCSI	Rackmount 1U, Mirrored HD

*Figure-3: Vircom’s Appliance messaging solutions.*

## Key product/service strengths

### Catch rate performance & false-positive protection

Statistic technologies (such as heuristic methods) all constitute reactive methods to fighting spam. They are quite good in blocking variations of existing spam techniques. However, they are static and unable to adapt as quickly as the spammers do, and invariably fail to counter the latest spammer's tactics. Furthermore they will most likely have catastrophic results on false positives.

Deterministic methods (such as keyword filters) rely on humans and their judgment to constantly create new building blocks to update the anti-Spam solution. Although very efficient when performed by knowledgeable programmers, these solutions are inherently flawed and will inevitably lose their efficiency over time. As the spam volume increases and generates an ever-growing need for new updates, the number of rules, scripts or filters added to maintain the solution ahead of spammers will slow the treatment process up until it becomes a performance problem. Deterministic methods won't just do it alone anymore.

By studying the individual advantages of various technologies and identifying their weak points, Vircom has come out with a solution that not only uses multiple technological layers, but also multiple engines offering the efficiency of the statistical analysis with the accuracy of the deterministic methods. Vircom therefore has raised the standard of anti-Spam solutions by **catching 98.2% of all spam while delivering 99.99% of false positive protection**. These are key results to fight the user productivity losses!

### Lowest TCO

Vircom's solutions have an historical presence at xSPs running services over its messaging implementations. We know that having the lowest Total Cost of Ownership (TCO) is of major importance for them.

This starts with providing the highest accuracy to avoid System Administrators to constantly trace wrongly handled e-mails. It continues with offering a fully self-managed implementation (making it "install & forget") in addition to delegation opportunities (allowing end-user to manage their own quarantine and/or anti-spam environments).

Here are some of the features that ensure a minimal TCO:

#### 1. Accuracy

Non-accurate solutions are not helping the problem: they just amplify it. Users loose their trust in the system, and either:

- Call system administrators to trace wrongly handled emails (or emails that were never sent)
- Manage two mail repositories (the inbox deleting remaining spam & the quarantine looking after legitimate emails).

#### 2. User-aware

##### a. User-aware Quarantine

Some anti-Spam solutions offer scheduled quarantine reports to each mail-address (or mailbox). Few however offer to users an access to their personal quarantine (like Vircom's WebQuarantine). This allows:

- users to check issues by their own (not disturbing SysAdmin)
- to build the trust (users control their emails)

b. **User-aware WhiteList/Blacklist**

Some solutions allow user-level whitelist and blacklist, but most of them require the SysAdmin to do the work.

With Vircom's solutions, users can easily define their personal blacklist & whitelist. They can do it as they read their Quarantine report (they will be asked to whitelist the sender when they release a message or to blacklist a sender when they delete a message) or from the WebQuarantine.

Both actions (like other user-allowed settings) must be authorized by the SysAdmin through the modus<sup>3</sup>' authority delegation settings.

### **3. Automated User Database Management**

When the modusGate receives a message, it checks the validity of the destination email address. This allows him to automatically build a table of valid and alias-aware mailboxes (the process is called "User Pre-Authentication")

When the mailbox is destroyed from the main mail-server, it will also be deleted from the Gate (either when that inexistent mailbox will receive a mail or with the daily automatic refresh).

This pre-authentication allows users to be fully recognized with their mailbox. So they receive only one quarantine report (even if they have several addresses/aliases for the same mailbox) and their user settings only need to be defined ones.

Vircom's implementation automates this process and frees the SysAdmin from managing an additional user database.

Similarly, when users want to connect to the WebQuarantine (or administrators to the WebAdmin) they will use their mail-account address and password. Again, this avoids:

- Users to remember an additional password
- SysAdmin to maintain an additional authentication DB.

These features and others (like the possible integration with billing and productivity tools) insure the Lowest TCO to corporations and ISPs.

## **Statistics & Monitoring**

Another important feature is Modus's statistics monitoring module, which records filtering behaviour at the server, domain and mailbox levels. At any time, end users and administrators can access email statistics, which are plotted per day, week and month.

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

## **Customization Opportunity**

Vircom's modus<sup>3</sup> technology has a "Custom Sieve Filter" layer that makes it possible for IT administrators to modify the engine's behavior or to implement custom corporate content policies.

Here are some examples on where to use these customized filters:

- During a new virus attack, and before AV vendors have found ways to stop it, the "custom Sieve Filters" could allow customers to block all messages based on the particular format conditions of the virus (fi: title contains "Re: Your

order” and attachment filename contains “Netsky” or attachment file extension is “.vs\*”...),

- Customer may want to archive or redirect emails based on particular content or rules,
- Customer may want to restrain the sending of inappropriate content or the usage of abusive language,
- ...

## Clustered Configuration for maximum availability

Whether you need a high performance messaging system, a scalable configuration, a redundant setup or a failover option as part of your disaster recovery plan, modusBlockade is the gateway-based security package you are looking for.

Vircom’s modusBlockade is the clustered implementation of modusGate to insure increased availability and performance.

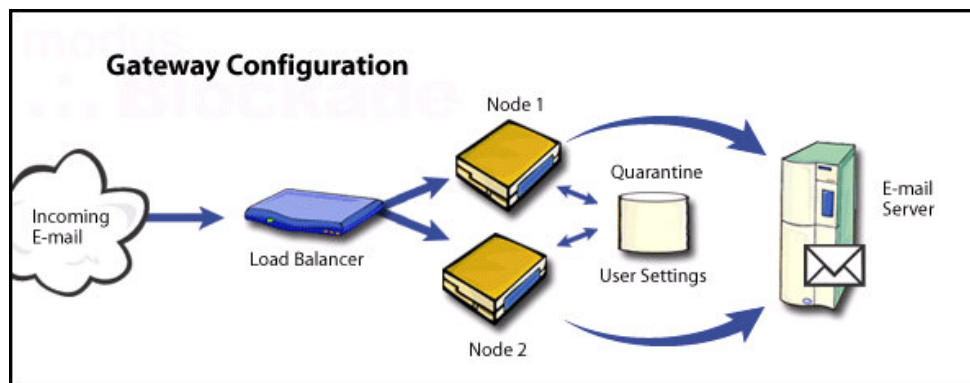


Figure-3: Multi-layered technology overview.

As shown in the above figure, a modusBlockade scenario would imply additional:

- SMTP load-balancer (could also be done via DNS/MX)
- Additional modusGate(s) (for redundancy)
- External database(s) for quarantine & user settings.

## Independent delivery

Because message delivery is technology-independent, Modus™ is compatible with any email system, whether it is used as a server, a gateway, comes integrated with a hardware appliance or is offered as a hosted service through our MSSP Partners.

Vircom’s software solutions are running on Microsoft Windows Server 2000/2003. Any engineer that is Microsoft certified should be able to install and support the modus<sup>3</sup> solutions. For standard configuration, the modus solutions can be installed in 15 minutes.

Vircom’s modusGate appliance is even easier to set-up. Pre-installed on a industry-leader PowerEdge 750, it just requires two wires to be plugged and IP addresses to be set.

In this case, corporates will use the Vircom solution hosted by one of our MSSP Partners across Europe (a list can be obtained at [sales@vircom-europe.com](mailto:sales@vircom-europe.com)). Emails just need to be redirected to the modus-based MSSP email scanning service, often just requiring a change of the MX records in the DNS.

## Vircom-related Differentiators

### Vircom's eMail Background

Spam is a complete mail problem. The way spammers perform scan-attacks to harvest email addresses is a mail problem; the way spammers send their messages (bulk messages) is a mail problem; the way spammers hijack mail servers to send their spam is a mail problem; the way spam annoys and reduces productivity of millions of users is a mail problem.

Most of the anti-Spam companies are coming from a content filtering background. But there is more required to fight spam: one need to assimilate the complete mail process and its issues.

That is why Vircom, a company that has focused on Secure Messaging since 1997, is one of the best positioned to offer powerful and accurate eMail scanning solutions today.

### Product Maturity

Vircom introduced its 1<sup>st</sup> generation anti-Spam solution in 1998. It already included advanced anti-spam tools such as filtering based on content or headers, selective mail blocking, multiple real-time blacklists such as ORBS or MAPS, and anti-bulk and anti-relay filtering.

In 2001, Vircom introduced its 2<sup>nd</sup> generation anti-Spam technology (called modusSieve<sup>2</sup>) based on the powerful Sieve technology (a standard Internet scripting language - RFC 3028 - defined for email filtering), later evolving into Automated Intelligent Content Filtering (AICF) for sophisticated anti-spam solutions.

In October 2003, after years of messaging security-focused research and development, Vircom launched and deployed its 3<sup>rd</sup> Generation anti-Spam technology (called modus<sup>3</sup>). Its powerful Sequential Content Analyzer (SCA) anti-spam engine, combining multiple statistic & deterministic technologies, is capable of remarkable accuracy and performance. The SCA outperforms single-technology solutions by performing 98.2% out-of-the-box spam catch rate while offering 99.99% false positive protection!

### Vircom's Support

We will leave it to our customers to comment on our support:

"I have contacted Vircom's support and the experience is always good. Most often the answers I am looking for are there on the first call. Personally, I have maintained Vircom mail servers for 3 years now and have had a few problems here and there which can be expected with the dynamics we deal with on the internet. Vircom has always been there to help when a new problem arises..."

*Chad Rowlee, Director of ISP Operations, CDC.Net Inc.*

"I have contacted Vircom Europe for several reasons. You always expect to have a good sales support, but your main concerns are on the technical support. I have to say that we experienced an excellent service on both ends. I am really happy!..."

*Rudolf Korntner, Technical Director, Infotech EDV-Systeme GmbH, Austria.*