



WHITE PAPER

More Than Just Email Filtering

WHAT YOU MUST KNOW BEFORE PURCHASING
YOUR EMAIL SECURITY SOLUTION

Table of Contents

Executive Summary	4
More than just email filtering.....	4
Deterministic, adaptive and predictive technology	5
Security and Protection	6
Monitoring and reporting.....	7
Policy Management and Compliance	7
Security as a Service.....	8
PlatinumPlus™ Proactive Support Plan	8
Conclusion	9
About Vircom.....	9

Executive Summary

Email security is more than just filtering spam. The evolving sophistication and rapid proliferation of email-borne threats advance too quickly to be countered with conventional methods. With more than 200 billion email messages exchanged daily¹, email is mission critical for businesses worldwide. However, as email communications continue to rise, networks become more vulnerable to malicious attacks and other threats.

As a result, organizations must deploy email security solutions that are complete and include several complementary features to be effective and manageable. This white paper will focus on the features of an effective email security system and how Vircom's comprehensive modus™ technology addresses these requirements.

More than just email filtering

What denotes an effective email security solution? A good solution is easy to deploy and manage. It integrates well with your existing environment and interfaces directly with email servers such as Microsoft® Exchange, Lotus® Notes and GroupWise®. It provides fail-safe methods to backup and restore your system or uses existing technologies to accomplish this. Finally, a good solution is backed by a provider who cares enough to use proprietary technology to protect your investment.

Straightforward setups are the most effective. In fact, ease of deployment should be considered when purchasing a solution. If setup is easy, so, too, will managing the solution. Subsequent to purchasing your solution, the most important step in securing your email infrastructure is deploying the solution.

An integral part of many organizations is business continuity planning (BCP), of which disaster recovery for their IT infrastructure is a part. Complicated solutions could present unintentional problems during recovery so, again, easily deployed and managed solutions are best.

Vircom's modus™ products are available as an email server with webmail, integrated gateway software installed on your own hardware and placed in front of an existing mail server or as a turnkey appliance. All were developed and optimized for a Windows environment and, as such, are easy to deploy effectively. Furthermore, modus™ can be deployed in a blockade for redundancy and high availability requirements.

Because modus™ runs on a Windows server platform, there is interoperability between the two. It can quickly be integrated into your Active Directory domain; is optimized to work with Exchange Server; can be used with your SQL Server (but comes standard with SQL Server 2005 Express) and it uses standard Windows® processes to backup and restore modus™. modus™ also makes use of Windows® features such as services and performance counters to manage and monitor your system. Built into the modus™ Console and WebMonitor, administrators are one click away from checking the status of their email infrastructure.

With Vircom, you have the freedom to use the management and storage tools with which you are already familiar. And, as a Microsoft® Certified Gold Partner, Vircom leverages assigned resources to ensure that the modus™ platform is hardened and is a solution that conforms to secure development practices.

Many appliance-based vendors use open source software as part of their offerings. As a result, they cannot provide a high level of platform hardening or integrate with existing application management systems. The consequence can be a product that is difficult to integrate within your existing infrastructure and challenging to manage. This could leave you vulnerable to email threats and network attacks.

Vircom's appliances are fully-integrated and completely Windows® hardened. The hardening process removes extraneous portions of the operating system that are not required to operate the appliance but can present possible security problems. OS hardening minimizes the appliance footprint to reduce memory and maximizes performance to virtually eliminate security vulnerabilities present in other platforms². Powered by modus™, our appliances allow you to remotely access your systems and backup quarantine data, user settings, and directory information with existing Windows® services.

Vircom's solutions are the only products on the market that allow users to build around SQL Server cluster and replication architecture and enable the use of all standard backup, copy, data mining and customer reports tools previously set in place. This allows for easy data access and an option to use Vircom's standard SQL Server 2005 Express database or integrate modus™ with your own SQL Server for more data storage.

Vircom's modus™ solutions provide unparalleled deployment flexibility by allowing for customized hardware setups (specialized servers, SAN/NAS storage, RAM disk), ongoing upgrades (RAM, CPU), virtual machine configuration and redundancy and high availability (MS SQL, server cloning). No competitor can match this.

modus™ is truly part of the network infrastructure and not just a black box in front of your email server. And Vircom's professional services experts are available to help you fine-tune your system to optimize your platform's capabilities.

Deterministic, adaptive and predictive technology

Most solutions on the market are based upon open-source technologies that rely on traditional Bayesian logic to counter spam. With Bayesian analysis, the statistics do all of the work. This technique requires training, using both legitimate and unwanted mail to build a database of words to determine the probability that a message is spam. The downfall of this method is that it requires administrator intervention. Quarantined messages must be reviewed for false-positives and the filter must be retrained to prevent them.

Assuming that the emails received are homogenous in nature, the filter will make fewer errors in a relatively short amount of time. However, since spammers are constantly trying to outsmart statistics, it is a continuous game of catch-up. Therefore, it is advantageous to have a solution in place that proactively removes spam and continually receives updates for the latest threats.

Combining artificial intelligence-based technology and security experts who focus on evolving core technology every day, Vircom's modus™ technology has adaptive and predictive capabilities that require no filter retraining by the administrator. Unlike open-source based alternatives, hackers have no idea what they are dealing with and zero-day threats pose less risk to your data center.

Once deployed, Vircom's superior technology quickly becomes evident. At the core of modus™ technology is a unique scanning engine, the proprietary Sequential Content Analyzer (SCA™), with deterministic, adaptive and predictive capabilities. The SCA™ performs an analysis against the latest spam identification rules, which are updated automatically by Vircom's security team. The SCA™ uses machine-learning artificial intelligence allowing it to detect previously undetected spam. And with updates provided as soon as new spam waves are detected, Vircom's SCA™ technology is effective 24x7 to thwart even zero-day attacks.

Vircom's 99% catch rate and 0.001% false positive claims are backed by results from live traps that analyze spam samples worldwide, helping improve the technology on a daily basis. At the heart of the operation are security experts with specialized training whose objective is to analyze incoming data, add to the training sets that allow our software to adapt to evolving threats, and run statistical reports, all the while monitoring for new spam outbreaks.

Leading the change in sophisticated filtering and predictive technology, Vircom combines all of the above methods to provide the most complete level of security.

Security and Protection

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 and allow for granular control by the administrator. By doing so, Vircom Inc. 4 administrators maintain full control over their email infrastructure and can easily adjust their security for spam waves and other sporadic attacks.

Vircom's modus™ products include a myriad of settings to provide perimeter, protocol and content level defense. At the perimeter, modus™ can be configured for DKIM, to specify real time blacklists, and enable connection blocking and limiting, to name a few. In addition, the Sender Reputation System (SRS) provides 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.

Protocol level filters, such as block scan attack, can be applied to limit the number of recipients for incoming mail, thereby preventing dictionary attacks. SMTP Authentication can be configured and requires user authentication prior to email being relayed.

Content level filters further protect against 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®.

modus™ provides you with the most comprehensive email security and spam protection. By combining the industry's leading anti-spam technology and fully integrated multi-engine anti-virus, modus™ gives you the tools to effectively counter today's growing security threats, such as botnets, increasingly sophisticated phishing attempts, fast-flux attacks and image spam - allowing you take back control of your data center.

modus™ offers granular security and access control for both inbound and outbound messages. Administrators have complete control and can configure most settings at the system, domain and user levels. Furthermore, administrators have control over the strength of filtering which can be adjusted to normal, strong or extreme levels.

Administrators may want to customize settings or put temporary measures in place to react to a particular spam wave (attack). This can easily be accomplished using Vircom's Sieve™ scripting engine which allows administrators to create customizable filters. These filters are used to design site-specific settings for complete inbound and outbound security.

Monitoring and Reporting

Monitoring systems and reporting features allow IT administrators to oversee their email infrastructure activity. Monitoring systems should facilitate email tracking and provide an overview of system health while reporting features should provide information about elements such as security threats, statistics and trend analyses. IT administrators should assess these features when evaluating solutions as they can, among other things, simplify troubleshooting hardware and software problems and security issues.

The modus™ WebMonitor interface provides access to system health information, reporting and message auditing. The system health panel provides details about the system status for hardware resource usage and networking information; system activity for inbound/outbound connections, processing and message delivery queues and POP3 and IMAP connections; and performance rates for messages processed.

Vircom's reporting feature is an easy-to-use interface that permits administrators to quickly and effectively generate reports for an overview of their system and security threats. Reports are available for Vircom Inc. 5 the server as well as for all domains and users. Administrators can generate statistics reports for mail filters, security, senders and receivers, disk usage and questionable activities.

Lastly, with WebMonitor's message audit, administrators can audit email messages and see the most recent mail processing transaction history. The message audit tracks message traffic - inbound external mail, outbound local mail and mail from local user to local user and displays all message transactions in a 1-line per message summary.

Policy Management & Compliance

Increasingly, organizations are changing their email strategy and implementing data loss solutions for better control and manageability over email security. New exploits that leverage email's inherent vulnerabilities surface constantly, necessitating an email security strategy that perpetually contends with emerging threats in a timely way.

Failure to react promptly to new attacks leaves organizations highly vulnerable. Because email is woven into business processes, creating sound email security means looking closely at workflows and dependencies. Securing email and the data contained in email is not simple.

With the introduction of regulatory requirements, such as Sarbanes-Oxley, the Data Protection Act (European Union) and Freedom of Information Act (UK), it is essential to have email compliance protecting your organization from potential litigation.

For organizations contending with regulatory compliance, it is not only imperative that they protect their information but also ensure that they have a means to identify every route email travels, map access to sensitive data against usage policies, and ascertain that sensitive data is delivered only to those with legitimate access.

Vircom addresses compliance with the modus™ Sieve™ interface that provides a flexible policy management interface to enforce acceptable use policies, regulatory compliance initiatives (HIPAA, SOX, Graham-Leach-Bliley, etc.), data loss prevention and federal and municipal laws (FRCP, etc.).

Additionally, WebMonitor's message audit feature complies with Sarbanes-Oxley regulations by recording all message transactions and storing them in a SQL database.

Security as a Service

Security is the first and foremost concern for administrators. However, it is not always easy to stay ahead of spammers and others who are forever looking for vulnerabilities and ways to infiltrate your network.

Vircom's Security Team of dedicated experts are continuously improving Vircom's unique anti-spam engine to ensure your complete protection. This team never sleeps, so that you can!

The data collected by Vircom's Security Team is instantly shared with the professional services team. Along with the expertise fostered internally, Vircom offers the most complete consulting and training packages designed to share that knowledge with its customers. Vircom offers remote installation services, training, system tuning and an industry-unique service plan, PlatinumPlus™. Vircom's compelling value is the combination of technology, flexibility and service that provides an unbeatable customer experience and email security.

PlatinumPlus™ Proactive Support Plan

An industry first, PlatinumPlus™ goes beyond 24x7 support by adding remote monitoring services: if you come under a targeted attack or for other issues, Vircom acts before you even realize it.

With PlatinumPlus™, your network is actively monitored around the clock. If a threat is detected, Vircom will immediately take action and, simultaneously, warn the network administrators of the situation. Often corrective measures are taken before the administrator is aware of any attack. PlatinumPlus™ also provides reports on system and network health.

Conclusion

While there are countless email security solutions on the market, only a few are dedicated solely to protecting your email infrastructure. Many solutions focus on hardware network protection with email security as an add-on. Contrarily, Vircom focuses exclusively on protecting your email network with their proprietary technology.

Staying ahead of threats and maintaining compliance requires a sophisticated, yet easily managed, solution. In addition to its straightforward and uncomplicated console and web interfaces, modus™ leverages a Windows® platform, which provides IT staff with familiar components for easy administration.

With its experienced team of security experts and engineers, Vircom continues to research email security best practices and develop powerful and effective solutions. Instead of relying on a singular scanning method to block spam, modus™ combines several technologies to provide the industry's best catch rates and lowest false positives. This alone makes modus™ a premium solution.

However, Vircom goes the distance by offering more than just spam protection and network security. modus™ incorporates tools and features that simplify administrative tasks and system monitoring and reporting. Additionally, with Vircom's Sieve™ scripting feature, IT administrators can create custom policies for compliance management and to increase modus™ effectiveness by creating scripts such as refined attachment blocking, redirecting mail and monitoring email for a specific email account. Sieve scripting allows for endless filtering opportunities which, in turn, can strengthen the efficacy of your email security.

Vircom clients are just a phone call or click away from some of the industry's best technology support experts. Whether you have a question or require help, Vircom's support staff is always available. And with PlatinumPlus™, problems are resolved before you are even aware of them.

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.

Their award winning, proprietary modus™ software technology is built to provide peace of mind to the organizations that present the highest risk, both to their operations and their shareholders.

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.