



SecurExchange Perimeter™ Edition



Secure e-Mail & Content Monitoring for MS Exchange 2003, 2000 & 5.5

Just imagine what the disastrous consequences, cost and potential loss of credibility could mean to your organization from the exposure of sensitive, confidential or proprietary information, legal action over sexual or racial harassment or non-compliance with internal or external content policies? It all adds up to the very real risk of corporate liability, and it could cost your company time, money - or even your reputation, or your business.

Now more than ever, it has become absolutely critical to be able to monitor, analyze and control **all** the e-mail content flowing both into and out of your network. While almost all anti-spam and anti-virus products block unwanted incoming messages, very few of them can also monitor your outgoing e-mail content. The fact is, most vendors didn't anticipate these new requirements when they designed their products, and as a result, they are now stuck with outdated legacy products that simply can't adapt to meet new needs. For users of Microsoft Exchange, only a solution that has been designed specifically with intelligent content analysis and complete integration and operation with your Exchange Server in mind can offer you the reliable protection you need to safeguard both your outgoing and incoming e-mail traffic, at precisely the point where it matters the most: the perimeter of your Exchange network.

Nemx Software Corporation's SecurExchange Perimeter™ Edition is a powerful, cost-effective and comprehensive all-in-one secure e-mail and content monitoring solution, designed for companies running Microsoft Exchange. With SecurExchange Perimeter™, you don't just eliminate spam. You gain the ability to reliably protect your sensitive or confidential information, enforce compliance with corporate content policies, intelligently analyze all incoming and outgoing e-mail for content violations, and automatically execute real-time message actions based on predefined event conditions - giving you Total e-Mail Peace of Mind™.

SecurExchange Perimeter™ creates a rock solid first-level corporate defense against incoming and outgoing violations and abuses of e-mail, giving you the power to:

- Safeguard your sensitive, confidential, personal or financial information from deliberate or unintentional exposure via e-mail;
- Ensure all incoming and outgoing messages meet your acceptable use and content rules;
- Selectively archive critical messages in real-time based on their content or by user community, to ensure an accurate and complete audit log to meet specific compliance requirements, or simply as added corporate protection and risk management;
- Automate appropriate real-time message actions and apply them globally, by user or user group, or based on their message content;
- Minimize the impact and instantly notify your administrator if your Exchange Server is the target of an NDR, Recipient Directory or other interrogation attack;
- Create a safe working or learning environment free of harassment, aggressive behavior and inappropriate content;
- Dramatically lower the cost of your e-mail and Exchange administration; and
- Stamp out spam while guaranteeing your important business partner and customer messages get delivered without fail.

Need advanced anti-virus protection too? Bundle one of our SecurExchange Anti-Virus products with SecurExchange Perimeter™ for complete protection in a totally integrated solution!

**"Managing our enterprise messaging is only one of my responsibilities;
thankfully Nemx has made that job a lot easier."**

K. GOLLINGER, WAYNE COUNTY COMMUNITY COLLEGE DISTRICT.



Simplicity at its best!

SecurExchange Perimeter™ is the only “all-in-one” secure e-mail and content monitoring solution created exclusively for the Microsoft Exchange Server. SecurExchange Perimeter™ integrates and operates seamlessly with Exchange’s native facilities, services and connectors. All configuration and operations are performed directly from the System Manager or Exchange Administrator, meaning no special commands, new applications or interfaces you have to learn. Your existing Exchange security settings and rules are automatically honoured, so you never need to perform time-consuming modifications or reconfigurations to Exchange. Plus, with SecurExchange Perimeter™, there’s no extra proxy server/gateway or additional PC required, making installation a breeze - and saving you money! That’s why we can promise that SecurExchange Perimeter™ has the lowest administration and operating costs of any product available.

Key features

Real-time scanning: automatically scans all messages in real-time to detect and prevent content violations BEFORE they can occur. SecurExchange Perimeter™ actively monitors the content, message body and attachments of both outgoing and incoming messages, allowing you to prevent the kind of content breach that could spell disaster for your business.

Intelligent Content Analysis (ICA): dramatically improves the effectiveness of all monitoring and filtering applications, whether to detect content policy violations or as an anti-spam measure. While most other vendors’ products scan for simple keywords or phrases that can easily be tricked or compromised, SecurExchange Perimeter™ with ICA also uses natural language processing queries and techniques including dictionary, thesaurus and prefix/suffix stripping methods. Among other advantages, ICA provides the foundation for Nemx’ unique and highly effective “Concept-based” content monitoring, which can dramatically improve the results while providing substantially greater flexibility. Offering the only truly *intelligent* content monitoring and filtering solution, SecurExchange Perimeter™ with ICA technology allows you to:

- Monitor all e-mail content in accordance with predefined concepts rather than simply looking for key words or phrases that can be misleading or easily camouflaged;
- Selectively archive messages by user, user group or based on the message content, to ensure corporate compliance with internal or applicable external policies;
- Use content-based parameters to invoke specific Smart Action Triggers™ for more refined and granular message control and exception handling;
- Flexibly and efficiently define, monitor and enforce your corporate use and content policies; and
- Significantly enhance the effectiveness of your anti-spam capabilities, while guaranteeing that legitimate mail from customers, partners and others is delivered without fail.

Smart Action Triggers™: automatically take any number of actions with e-mail that meets predefined event conditions. Multiple Smart Action Triggers™ can be defined and assigned as default actions to various content policy and filter definitions. Plus, automate routine and exception message handling using Smart Action Triggers™ to perform such tasks as:

- Selectively archive messages and attachments into an MS SQL server or other ODBC compliant database;
- Add an entry to your e-mail audit log;
- Delete or quarantine the message;
- Forward the message to another user(s) or public folder;
- Remove any or all attachments;
- Send a reply message to the sender;
- Send a copy or alert your staff to potential security breaches, insider threats or exposure to liability;
- Automatically white list friendly domains and safe senders depending on the Spam Confidence Level (SCL); and
- Intelligently categorize messages, moving messages to different folders within a user’s mailbox depending on their content.



AutoContent Manager: automatically inserts predefined text or graphics such as a corporate signature or disclaimer to the beginning and/or end of a message, to ensure a consistent look and feel to your corporate e-mail correspondence. Different auto-content can be defined and applied globally to all messages, or only to messages originating from a particular user or user group. For instance, AutoContent Manager can ensure that all e-mail from your finance department includes an appropriate disclaimer, while a special corporate promotional offer is appended to the messages from your sales and marketing teams.

Reporting: provides statistical information on the number of incoming and outgoing messages, the number of messages triggering an event (rule), and the frequency that each rule is being triggered - all valuable information to assist you in refining the effectiveness of your content policies.

IMF Management: extends the Microsoft IMF with much-needed flexibility, to provide more granular control and management of messages triggered by the IMF. With SecurExchange Perimeter™, you can be absolutely certain that legitimate e-mail from business partners, customers and suppliers will be delivered, because it enables you to:

- Minimize the false positives that would otherwise be generated by the Exchange IMF through global, group or "self-sensing" white listing and friendly domains;
- Define any number of SCL thresholds and assign different actions to each, providing individualized SCL threshold management;
- Perform predefined actions on IMF triggered messages, such as rerouting or moving them to a sub-folder, copying them to another user or sending another message; and
- Define safe sender lists to prevent Exchange IMF from archiving or, worse yet, deleting messages on the SMTP gateway/front end server that exceed the gateway's IMF threshold.

Eliminate Spam: stops spam dead in its tracks by combining Intelligent Content Analysis and concept scanning with all of SecurExchange's other advanced anti-spam measures, including header recognition techniques, Reverse Blacklist (RBL™) database lookup, Spam URL Blacklists (SURBL) and our constantly updated predefined "rule packs." More importantly, Nemx' Intelligent Content Analysis capabilities mean SecurExchange Perimeter™ also guarantees that the mail from customers, partners and others that should get delivered, gets delivered, without fail!

SecurExchange Perimeter™ provides your organization with a rock solid first level defense system for e-mail content monitoring and control of inbound and outbound messages.

System requirements

- Microsoft Exchange 2003, 2000 or 5.5. All service packs are supported.
- Minimum 128 MB RAM (256 MB recommended).
- Minimum 10 MB free disk space.

SecurExchange Perimeter™ Edition Total E-Mail Peace of Mind™.



14 POPLARWOOD AVENUE, OTTAWA, ONTARIO, CANADA K2S 1V3
Tel: (613) 831-2010 Fax: (613) 831-1898 e-mail: info@nemx.com