

Igaware Exchange Protector – for the email you want to receive

The Igaware Exchange Protector is a powerful appliance that filters email before it reaches your exchange server, keeping inboxes **free from spam, viruses and other malicious content**. Your exchange server will instantly be protected for greater reliability while staff productivity and morale will be boosted.

Anti-Virus

The Exchange Protector keeps your email free from viruses, trojans, malware and spyware by:

- Using award winning Clam AV and Kaspersky AV engines.
- Scanning each message along with its attachments..
- Intelligent attachment management engine with MIME checks..
- Attachment integrity testing for file type/extension/modification..
- Scanning an extensive database of known spyware & adware definitions.
- Sender throttling automatically controlled by domain and email address.
- Internal IP database with sender reputations and recent activity.

In effect, the most sophisticated protection mix available from using enterprise class antivirus technology with internal controls that learn from the experience of processing millions of messages every hour.

Anti-virus Engines

Exchange Protector can use two antivirus engines to scan each incoming message and its attachments because no two virus engines are the same. For example, some antivirus engines can detect more than just virus signatures and provide protection from malware, trojans and other online threats. More importantly, not all virus engines use the same virus signatures. Each antivirus engine lab has its own research department, its own honeypot network (list of email addresses and hosts used to collect random mail from the Internet to establish a sample of threats being sent around) and consequently some antivirus engines can detect viruses before others.

Exchange Protector uses ClamAV as standard and optional Kaspersky AV to process all incoming mail. We scan each message and attachment simultaneously by both engines. Our policy engine is flexible enough to search within archived attachments (.zip, .rar, .arj) and eliminate threats that try to bypass antivirus engines.

Community Spyware Databases

As web browsers have increased their effectiveness in blocking spyware accessible over the web, hackers and spammers have turned to distributing spyware via email. Exchange

Protector uses several community spyware databases to provide the same level of spyware protection for email as is available on the desktop.

Throttled Malware & Trojan Control

Malware & trojan distribution relies on the speed at which it is able to infect remote networks. Over the years malware, trojans and worms have morphed into almost an indistinguishable rolling threat but their core characteristic has remained the rapid distribution of identical messages. Exchange Protector has a built in identification system that tracks the message & attachment MD5 checksums and responds by temporarily delaying messages that match the bulk-mail criteria. Additionally, the system is always monitored for unusual activity as it is very unusual to process millions of messages with the same attachment name, size and checksum across the Internet.

Malware Attachment Filtering & Sanitation

The days of text-only SPAM are long gone. Today SPAM is distributed as a PDF, zip file, image, even an audio file! At the same time we use our email as more of a file sharing mechanism than a communications platform. Consequently, it is very important to understand the attachment type and what type of a threat it poses. Exchange Protector analyzes attachments on multiple layers, using checks for file names, file types, MIME headers and archives to assure we apply your corporate policy to all attachments.

There are literally thousands of different ways that spammers and hackers have been trying to bypass security systems over the past decade. First came the Microsoft Windows exploits related to long filenames. Then mismatched extensions. Followed by dangerous attachments encapsulated in archives. Finally, the culmination of it all - forged MIME headers, extensions, multiple extensions, etc. Attachment sanitation plays an incredible part of Exchange Protector functionality because in addition to protecting your mail flow it also reduces it significantly. Email messages tend to be several kilobytes in size while attachments can range in hundreds or thousands of that - multiplied by a few thousand, and for some, millions of messages a day, that results in a degradation of both the bandwidth and the performance of your exchange server. Exchange Protector helps return those resources back to you, with the majority of Spam and malicious emails not even downloaded.

Anti Spam

Exchange Protector helps you get back to business, ending tiresome interruptions by relying on:

- Bayesian filtering analyses text patterns of known SPAM messages..
- Internal honeypot network with over 5,000 email addresses collecting SPAM..
- Third party RBL (blacklists) help identify dangerous networks and senders..
- SPF/SenderID/DomainKeys frameworks help establish trusted relationships..
- Distributed Checksum Clearing Houses help identify bulk mail pieces..

- Internal RBLs, IP reputation lists, network checks establish sender reputation..

Truly, the combination of experience, high volume of mail processing, and constant monitoring and development deliver the most reliable flow of mail you actually want to read.

Comprehensive Mail Analytics

There is no single software or a single process that can successfully eliminate a significant amount of SPAM on its own. As SPAM and online threats evolve the gradual mail analytics become more important and the efficient implementation of those processes is critical. To offer you an example: as we learn about more SPAM tactics and patterns we perform more checks against the sender, recipient, email, attachments, context, filenames, text patterns - and as the size of those checks the delay to the message delivery due to processing can become significant. Exchange Protector employs a comprehensive mail analytic check which runs thousands of message comparisons simultaneously, reducing average message processing time to a fraction of a second.

Message processing development is critical to effectively stopping SPAM, something that is impossible to accomplish with server-installed solutions. Exchange Protector installations process millions of messages each hour and learns from the mail flow patterns in real-time, something that server-software publishers usually lag days or weeks behind. The future of SPAM protection is on identifying threats in real-time and Exchange Protector is designed from the ground up to take advantage of it.

Proactive Mail Identification Systems

Exchange Protector, through proprietary technology, can predict the type of a message it is about to receive by analysing only the SMTP conversation and the IP reputation of the sending host. For example, if the sending server does not even wait for the welcome banner to start the SMTP conversation it is obvious that the message will be SPAM. Furthermore, after the same server has been the origin of 10,000 SPAM messages over the past hour it is pretty clear that the next message will also likely be SPAM. Exchange Protector will not automatically drop these messages but every piece of the SPAM criteria can lead to a score that qualifies it as junk.

Exchange Protector performs hundreds of checks before the SMTP connection is even established. Doing so cuts the volume of unwanted email being downloaded for further checks by a massive amount. Igaware technology enables the Exchange Protector to handle volumes of Spam in the millions, avoiding email delays and protecting bandwidth.

Reliance On RFC And Established Standards

Exchange Protector is proud to be 100% based on established RFC standards. RFC standard compliance is very important to the timely and reliable delivery of legitimate

mail. Reliance on established standards is crucial to timely delivery and ability to effectively troubleshoot mail flow issues with remote servers.

No False Positives

Exchange Protector is one of the few solutions that does not give false positives. This is valuable for a number of reasons, primarily because it results in legitimate emails not being rejected, or consigned to a quarantine that you simply don't have time to wade through. Emails are intelligently scored and if it has a low score (you can control this) it is forwarded to you to be reviewed. It never takes the control out of your hands. This means that you don't have to quarantine Spam email, saving the time that would otherwise have to involve a system administrator or a remote sender resending the message. With our processes you can expect legitimate emails to reach you.

Protection From DoS, Slamming, Botnet Attacks

Exchange Protector is hardened against attacks from hackers and botnets and is able to withstand a large-scale DoS attacks. When a sending server goes from sending a few dozen messages to a few thousand messages a day we can stop them in their tracks.

Adaptive System Advantages

The key to effectively eliminating SPAM and unwanted content is being adaptive to the mail flow - as it happens. One of the most important features of Exchange Protector is its ability to adapt to the changing mail flows, hour to hour, minute to minute, second to second. It is estimated that over 25% of the hosts on the Internet are a part of a botnet or have been compromised in some way. Adapting to those trends and filtering out messages based on topology maps is crucial to eliminating messages because RBLs, honeypot traps and SPAM rules do not work against zero-day SPAM or other threats that are just temporary but still impact your organizations productivity.

Exchange Protector can scale and respond in real-time as well as adapt to the emerging threats long before they reach your inbox.

Accountable To Users and Administrators

Exchange Protector remains accountable to everyone that uses the system through:

- Daily reports come in through email containing past 24 hours of email activity and filtering actions
- Email reports provide statistics, keeping you aware of the SPAM problem and policies in place.
- Full, real-time and secure access to all reports via the web interface..
- Report export option

Protection without accountability is worthless, which is why Exchange Protector excels at reporting its activity. By reporting and interacting with administrators and partners the system learns and becomes more effective.

Convenient Real-Time Email Reports

Exchange Protector provides in-depth reporting of email in real-time and on schedule, showing details on all incoming and outgoing emails and filtering actions. You can obtain rich real-time reports that can be searched, printed or imported into other reporting systems. Reporting is integral because it provides accountability of the system to its users and provides business key performance indicators that show you the true value of Exchange Protector.

Exchange Protector reports are real-time and are the preferred way of interacting with the system.

Legal Disclaimers or Corporate Branding

Exchange Protector features a flexible outbound signature system that can be used for legal disclaimers or corporate branding. For example, UK companies are required to list their business registration numbers on all outbound mail. Many professional lines of business are starting to introduce similar requirements and Exchange Protector allows you to simply attach a signature to all outbound mail.

Signatures also provide an excellent way to include corporate identity markers, such as unique signatures for the entire company. These domain wide policies are quickly configurable and can be easily changed on demand without changing server configuration or installing third party software.

Network Security Options

The following options can be enabled on the Exchange Protector to provide a Unified Threat Management solution for your entire network. With these options enabled you benefit from a Unified Threat Management solution that protects your entire network.

Firewall & VPN

A stateful firewall, with VPN support, using the latest generation of firewall architectures, dynamic packet filtering, or stateful inspection and deep packet inspection. Pre-configured with maximum security settings, it offers immediate and robust protection.

- stateful firewall using the latest generation of firewall architectures, dynamic packet filtering and deep packet inspection.
- supports IPSec (3Des,AES) PPTP and SSL VPN
- complete control over inbound and outbound Internet traffic with definable access policies and Port Forwarding and Port Input options.

Web Filtering

Surfing the web is an important business tool, but without the correct policy enforcement, the business benefits can be negated by significant threats to employee productivity, system downtime, data loss and potential legal liability. Exchange Protector delivers the critical controls need to block access to harmful and inappropriate web content, according to your own Internet use policy.

- access to inappropriate web sites can be blocked according to categories e.g. pornography.
- dangerous files e.g. exe files, can be prevented from being downloaded from the Web.
- Reports show web usage and content filtering.
- ADS Integration enables single sign on authentication.

Installation Options

The Exchange Protector can be installed on your LAN with email forwarded to it from your existing firewall on port 25. This allows SMTP mail to be directly handled by the Exchange Protector before forwarding legitimate email to your exchange server.

The Exchange Protector integrates with Active Directory to gain user lists, which then ensure that only email for legitimate users are passed on. This also allows single sign on for Web filtering if this is enabled.

The Exchange Protector may also be installed as your Internet gateway with firewall and VPN capabilities enabled.