ESET is a Wholesale Success at Gardners Books

After a history of positive experience Gardners Books turned to ESET once again to protect their Mail Servers.

CUSTOMER

Gardners Books is one of the UK's leading independent wholesalers specialising in the sale of books, DVDs, CDs, eBooks and other media. They have been a key organisation in the book supply industry for over 25 years and have a strong customer base of retail companies, local bookshops and many internet based shops and resellers. Gardners Books are constantly investing in innovative technology which has helped them to build up a strong, reliable company supporting a global network of retailers.

The organisation has a heavy reliance on the reliability of their IT network and in particular Virtual infrastructure. In order to maintain the daily running of the company Gardners Books requires a good quality network infrastructure that is capable of processing large amounts of data. Having a consistent and fast connection to the outside world is a major priority.

CHALLENGE

Gardners Books had previously relied on external mail scanners to protect their mail servers but chose to review this after experiencing issues with this solution. The IT team noticed an increase in the amount of items slipping onto their client PC's when using the external mail scanner, being very conscious of potential security issues they decided it would be best to look at other solutions.

"We were looking for an Email security package for our Exchange 2013 environments in a DAG setup to give us an extra layer of security for our mail data bases and incoming mail." Gardners Books already relied on ESET for File Server security and Endpoint security solutions and had been an ESET customer for some time. When looking into mail server security solutions they once again turned to ESET's range of business security solutions.

SOLUTION

ESET Mail Security for Microsoft Exchange Server integrates powerful antivirus and antispam detection capabilities that ensure all harmful email-borne content is filtered away at the server level, while ESET's light footprint means the system can continue to run at full speed. Mail Security allows the application of policies for specific content based on real file type, and monitors security status or enables fine-tuned configuration easily via the ESET Remote Administrator tool.

According to Tom Wright, I.T. Service Officer at Gardners Books. "We chose ESET for several reasons. 1) Easy and clear licensing model 2) Over head on the server was minimal and hasn't impacted performance. 3) A good catch rate on items that had slipped through the external mail scanner. 4) As we have had previous dealings with ESET we know they offer a fast and reliable service."

MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

ESET Mail Security for Microsoft Exchange Server integrates powerful antivirus and antispam detection capabilities that ensure all harmful email-borne content is filtered away at the server level, while ESET's light footprint means your system can continue to run at full speed.

With our solution, you get complete server protection – including the server's own file system. You can apply policies for specific content based on real file type, and monitor security status or fine-tune configuration easily via our user-friendly ESET Remote Administrator tool.

Antivirus and Antispyware	Eliminates all types of threats, including viruses, rootkits, worms and spyware with optional cloud-powered scanning for even better performance and detection. Optional cloud-powered scanning: Whitelisting of safe files based on file reputation database in the cloud for better detection and faster scanning. Only information about executable and archive files is sent to the cloud – such data is not personally attributable.
Antispam and Anti-Phishing	Stops spam and phishing attempts, and delivers high interception rates without the need to manually set a Spam Confidence Level (SCL) Threshold. After installation, the antispam module is ready to run without the need to manually tune settings or thresholds.
Local Quarantine Management	Each mailbox owner can directly interact, via a standalone browser, with spam or suspected-malware messages that have been denied delivery to the mailbox. Based on privileges set by the admin, the user can sort quarantined messages, search among them and execute allowed actions – message-by-message, or by group – all via web browser. Actions vary based on the reason a message was quarantined. A regular email report summarizing quarantined messages with embedded links to execute actions can be sent to the user.
Database On-Demand Scan	Administrators can choose which databases and, in particular, which mailboxes will be scanned. These scans can be further limited by using the modification time-stamp of each message to choose which should be inspected, thereby reducing to a minimum the server resources devoted to the task.
Message Processing Rules	Message processing rules offer a wide range of combinations by which every single message can be handled. The evaluated parameters include standard fields like subject, sender, body and specific message header, but also allow further conditional processing depending on previous anti-spam filtering or antivirus scanner results. Corrupted or password-protected archives are detected and attachments are screened internally to determine real file type, not only purported extension. Rules can be changed according to the desired actions.
Exploit Blocker	Strengthens the security of applications such as web browsers, PDF readers, email clients and MS office components, which are commonly exploited. Monitors process behaviors and looks for suspicious activities typical of exploits. Strengthens protection against targeted attacks and previously unknown exploits, i.e. zero-day attacks.
Advanced Memory Scanner	Monitors the behavior of malicious processes and scans them once they decloak in the memory. This allows for effective infection prevention, even from heavily obfuscated malware.
Host-Based Intrusion Prevention System (HIPS)	Enables you to define rules for system registry, processes, applications and files. Provides anti-tamper protection and detects threats based on system behavior.
Device Control	Blocks unauthorized portable devices from connecting to the server. Enables you to create rules for user groups to comply with your company policies. Allows soft blocking, which notifies the end user that his device is blocked and gives him the option to access it, with activity logged.

ENJOY SAFER TECHNOLOGY™