▶ KASPERSKY SECURITY FOR MICROSOFT EXCHANGE SERVERS

Mitigating the risks of confidential data loss through corporate email

One of the biggest email security headaches for IT professionals today is the increasing problem of business-critical or personal data leakage. While email-based malware causes business disruption and expensive downtime, and spam is a constant drain on employee productivity and server resources, confidential data loss can cause irreparable long-term damage to an organization's finances and reputation.

Kaspersky Security for Microsoft Exchange Servers addresses this issue through identifying confidential data and controlling or blocking its distribution by email, supported by smart and reliable anti-spam and anti-malware protection.

- Sensitive data identification and analysis
- Flexible email distribution controls
- Real time anti-spam protection with low 'false positives'
- Anti-phishing protection
- Advanced, cloud-assisted anti-malware security
- Detailed notifications and reports
- Straightforward centralized management
- Separate distribution control and security functionality

DATA LOSS PROTECTION AND CONTROL

By identifying the inclusion of business, financial, personal and other sensitive data in outgoing emails and attachments and controlling the flow of this information, Kaspersky Security for Microsoft Exchange Servers keeps your and your employees' confidential data secure, and in compliance with data protection legislation. Sophisticated analytical techniques, including structured data searches and business-specific glossaries, help identify suspicious emails which can then can be blocked. The system can even alert the sender's Line Manager to the potential data security breach.

SMART SPAM DETECTION AND ANALYSIS

Smart technologies deliver optimum detection rates, effectively blocking spam with minimal false positives. Cloud-based real-time threat notifications support anti-phishing and spam analysis and blocking tools, while flexible controls allow 'grey areas' of unwanted mail to be classified and handled separately.

REAL-TIME ANTI-MALWARE PROTECTION

A full spectrum of malware is detected and eliminated through the real-time traffic scanning of messages and attachments, again supported by the cloud-based Kaspersky Security Network, which even identifies exploits attacking zero-hour vulnerabilities. The scanning of stored messages in background mode minimizes server load.

FLEXIBLE ADMINISTRATION

Centralized management with broad configuration capabilities and a flexible system of reporting and notifications empower the administrator to control the flow of sensitive data through email, as well as securing the IT system against malware threats and resource-wasting spam.

FEATURES

DATA PROTECTION

Detection of Confidential Information. The solution implements modules which detect specific types of data in emails and attachments according to individual categories such as personal details and payment card data (ensuring compliance with data protection legislation). The application also scans against pre-installed themed glossaries: “Finances”, “Administration Documents” and “Offensive and Obscene Vocabulary” which are regularly updated.

Company-Specific Glossaries. Glossaries containing company-specific and even project-specific keywords and phrases can be created to detect the presence of the most sensitive business information in outgoing emails. Glossaries can also be created using Query language.

Deep Level Analysis Using Structured Data. Structured data can also be used as a search object. A combination of specific data types within the same message, or data in complex arrays as would be found in client databases, can be identified as confidential information.

ANTI-SPAM

Smart Spam Recognition Technologies. Elements including sender’s email and IP address, message size and header as well as content and images are analyzed employing smart technologies which use unique visual signatures to detect visual spam. Reputation filtering combats unknown spam by isolating and re-analysing suspicious emails, minimizing the frequency of false positives.

Cloud-Based Real-Time Protection. Reputation filtering and anti-phishing technologies are supported by real-time information about new spam threats through integration with the Kaspersky Security Network (KSN).

Message Classification. Unsolicited messages can be processed by category to ensure that necessary emails are not lost. Obvious spam can be blocked, suspicious messages can be forwarded to an “Unwanted mail” folder, while service messages (for example delivery and receipt notifications) can be sent to the Inbox.

ANTI-MALWARE

Scanning Traffic in Real Time. Detects and deletes all types of viruses, worms, Trojans and other malware in inbound and outgoing messages and attachments. Kaspersky Security Network (KSN) integration provides alerts to new and potential malware threats in real time.

Background Scanning. On-demand and scheduled background-mode scanning of stored files minimizes workload on the server.

Backup Copying. Backup copies of all deleted messages are retained for analysis or restoration in the event of a classification error.

ADMINISTRATION

Centralized Management. A single administration console with centralized reporting is integrated into Microsoft’s Management Console to manage the security of all Microsoft Exchange servers. Security management and confidential information distribution management activities can also be assigned to separate roles and individuals if needed.

Broad Configuration Capabilities. Compliance with corporate IT security policy can be balanced against available resources through, for example, exempting specific file types or message categories from scanning, or applying different levels of anti-spam scanning to different categories. White and black lists of sender and recipient addresses etc can also be created and applied.

Information Distribution Control Policies. Specialized policies can be created to control the distribution of confidential information and set responses to data loss incidents, such as blocking or allowing messages and setting hazard evels.

REPORTING

Flexible Reporting and Notifications. The management console can be used to review security status and activity, including the distribution of confidential information. Report content and frequency can be customized, and event notification management is supported by standard Microsoft Windows® tools.

Analysis of Attempts to Send Confidential Information. Detailed information about each incident allows the administrator to trace the chain of events and identify the sender. An appropriate notification can be forwarded to the sender’s manager.

SYSTEM REQUIREMENTS

Minimum hardware requirements:
See Microsoft Exchange Server system requirements.

Versions of Microsoft Exchange Server:

- 2013
- 2010 x64 SP1

Operating systems:

- Microsoft Small Business Server
- 2011
- 2008 Standard / Premium x64
- Microsoft Essential Business Server
- 2008 Standard / Premium x64
- Microsoft Windows Server®
- 2012 x64
- 2008 x64 R2 Standard / Enterprise Edition SP1
- 2008 x64 Standard / Enterprise Edition SP2

For detailed information, please visit:
www.kaspersky.com/security-microsoft-exchange-servers

KASPERSKY lab