KASPERSKY SECURITY FOR COLLABORATION

Data protection and control for collaboration platforms, including SharePoint farms.

The platform you use to share files and information also provides an ideal rapid transit system for dangerous malware and other IT threats.

To provide a secure and smooth shared working environment, Kaspersky Lab has developed a solution combining ease of management with premium real-time protection against malware attacks and confidential data leaks.

- Award-winning anti-malware engine
- Confidential data "search and protect"
- Data access controls
- Cloud-based real-time protection – Kaspersky Security Network
- File and content filtering
- Anti-phishing protection
- Back-up and storage
- Centralized, flexible management
- Intuitive administration console

Highlights

FULLY SECURING YOUR SHAREPOINT PLATFORM

If you are running Microsoft SharePoint Server, you'll know that, as all content is stored in an SQL database, traditional endpoint solutions can't do the job. Kaspersky Security for Collaboration applies award-winning advanced anti-malware protection throughout the SharePoint farm and to all its users. Powerful protection against known, unknown and advanced threats is provided through the cloud-supported Kaspersky Security Network, while anti-phishing technology protects against web-based threats to collaborative data.

PREVENTING CONFIDENTIAL DATA LEAKAGE

To control and protect the circulation of confidential data, that data must first be identified. Using pre-installed or custom dictionaries and data categories, Kaspersky Security for Collaboration checks every document placed on SharePoint servers for sensitive information, word by word and phrase by phrase. Personal and payment card data is specifically targeted for protection and control, while structure-based searches hunt out sensitive documents such as customer databases.

ENFORCING COMMUNICATION POLICIES

Content and filtering features help enforce your communication policies and standards, identifying and blocking inappropriate content while preventing the wasteful storage of inappropriate files and file formats.

EASY TO MANAGE

Security for the entire server farm can be administered centrally from a single, intuitive dashboard. Administration is fast and straightforward, with no special training needed.

ANTIVIRUS PROTECTION

- **On-access scan** - files are scanned in real time, while uploading or downloading.
- **Background scan** - files stored on the server are regularly checked using the latest malware signatures.
- **Integration with Kaspersky Security Network** - providing real-time cloud-assisted protection against even zero-day threats.

SUPPORTS YOUR ORGANIZATION'S COMMUNICATION POLICIES

- **File filtering** - helps enforce document storage policies and reduce the demands placed on storage devices. By analyzing real file formats, regardless of the extension name, the application ensures that users cannot use a banned file type in violation of the security policy.
- **Protection for wikis/blogs** - protects all SharePoint repositories, including wikis and blogs.
- **Content filtering** - prevents the storage of files that include inappropriate content, regardless of file type. The content of each file is analyzed based on key words. Customers can also create their own custom dictionaries for content filtering.

CONFIDENTIAL DATA LEAKAGE PREVENTION

- **Document scanning for confidential information** - Kaspersky Security for Collaboration scans all the documents downloaded on SharePoint servers for confidential information.

  The solution integrates modules that identify specific types of data, confirming that it meets relevant legal standards - for example, personal data (defined by regulatory compliances, such as HIPAA or EU Directive 95/46/EC) or PCI DSS standard data (Payment Card Industry Data Security Standard).

  Data is scanned against built-in, regularly updated thematic dictionaries covering categories including: "Finance", "Administrative documents" and "Humiliating and abusive language", and against customized dictionaries.
- **Structured data search** - if information presented in specific structures is found in a message, it will be treated as potentially confidential, ensuring control over sensitive data, such as customer databases, held in complex arrays.

FLEXIBLE MANAGEMENT

- **Ease of management** - an entire server farm can be centrally managed from a single console. An intuitive interface includes all the most commonly used administrative scenarios.
- **Single dashboard** - a clearly laid out dashboard provides real-time access to the current product status, database version and license status of all protected servers.
- **Backup of modified files** - in the event of any incident, the original files can be restored if required, and detailed back-up information about modified files can be used to support investigations.
- **Integration with Active Directory®** - enables the authentication of Active Directory users.

SYSTEM REQUIREMENTS

SharePoint servers:
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016

Operating System (to install the solution)
For SharePoint Server 2010:
- Windows Server 2008 x64/ 2008 R2 / 2012 R2

For SharePoint Server 2013:
- Windows Server 2008 R2 x64 SP1 / 2012 x64 / 2012 R2

For SharePoint Server 2016:
- Windows Server 2012 R2 x64

The full list of system requirements is available at kaspersky.com

How to buy

Kaspersky Security for Collaboration can be purchased as part of Kaspersky Total Security for Business, or as a standalone Targeted Solution

Note! When purchasing this product, the option to prevent confidential information leakage is sold separately.

Kaspersky Security for Collaboration/Version 0.4/Apr 16/Global

KASPERSKY lab