



Kaspersky® Endpoint Security for Business

Select



Kaspersky Endpoint Security for Business Select provides HuMachine™-based protection for a wide range of platforms – including Linux servers and endpoints. It delivers multi-layered security that detects suspicious behavior and blocks threats, including ransomware. Cloud-enabled controls reduce your exposure to attacks – and mobile management features help you to protect data on mobile devices.

The protection and management capabilities you need

Kaspersky Lab has built powerful enterprise-class features into the progressive tiers of our offerings. We've made sure that the technology is uncomplicated and flexible enough for any-sized business to use.

Which tier is right for you?

- SELECT
- ADVANCED
- TOTAL

Multiple protection layers for

- Windows, Linux and Mac
- Windows and Linux servers
- Android and other mobile devices
- Removable storage

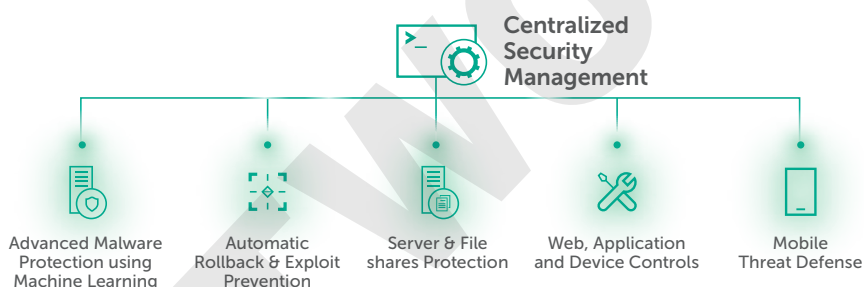
Unparalleled security against

- Software exploits
- Ransomware
- Mobile malware
- Advanced threats
- Fileless threats
- PowerShell & script-based attacks
- Web threats

Features included

- Anti-Malware next level
- Vulnerability Assessment
- Security Policy Adviser
- AI-based learning
- AMSI support new
- Encrypted traffic scanning new
- Process isolation
- Exploit Prevention and Rollback
- Firewall and OS firewall management
- Cloud-assisted protection
- Integrated EDR agent
- SIEM integration via Syslog new
- Application Control
- Web and Device Controls
- Server and containers protection next level
- Windows Linux subsystem support new
- Mobile Threat Defense next level
- Reporting

See our webpages for details [here](#).



Next Generation protection and control for every endpoint

One management console

From the 'single pane of glass' management console, administrators can view and manage the entire security landscape and apply your chosen security policies to every endpoint in your business. This helps deploy security rapidly and with minimum interruption or fuss, using a wide range of preconfigured scenarios.

Agile, adaptive security

The product is designed to work within any IT environment. It employs a full stack of proven and Next Gen technologies to prevent detected attacks; built-in sensors and integration with Endpoint Detection and Response (EDR) enable the capture of large volumes of data to discover even the most obscure, sophisticated cyberattacks.

Customer satisfaction assured

Our strong focus on R&D means that our products deliver the security you need. Decision-makers like you consistently express outstanding levels of satisfaction with the results, as regularly confirmed in independent surveys and reports.

Key features

Core features

Exploit Prevention

Prevents malware executing and exploiting software, delivering an extra layer of protection against unknown, zero-day threats.

Behavioral Detection and Automatic Rollback

Identifies and protects against advanced threats, including ransomware, fileless attacks and admin account takeovers. Behavior Detection blocks attacks, while Automatic Rollback reverses any changes already made.

Protection against encryption for shared folders

A unique anti-cryptor mechanism can block the encryption of files on shared resources conducted by a malicious process running on another machine on the same network.

Network Threat Protection

Malware using a buffer-overflow attack can modify a process already running in the memory and in this way execute malicious code. Network Threat Protection identifies network attacks and stops them in their tracks.

Web console

To improve fault-tolerance you can deploy our web console to centrally manage both physical and virtual machines, not only in Amazon but also in Microsoft Azure cloud environments.

Mobile security features

Innovative anti-malware technologies

Combined ML-based, proactive and cloud-assisted detection result in real-time protection. A Web Protection, on-demand and scheduled scans increase the security.

Deployment Over the Air (OTA) provisioning

Delivers the ability to pre-configure and deploy applications centrally using SMS, email and PC.

Remote anti-theft tools

SIM-Watch, Remote Lock, Wipe and Find - all prevent unauthorized access to corporate data if a mobile device is lost or stolen.

Application Control for mobile devices

Application Control protects data on installed software and enables administrators to enforce the installation and usage of specific applications.

Cloud-enabled endpoint controls

Application Control

Reduces your exposure to attack, giving total control over what software can run when on PCs, powered by Dynamic Whitelisting from our in-house laboratory. Default Allow and Default Deny scenarios are supported.

Dynamic whitelisting

For a better applications categorization, Application Control uses a [Dynamic Whitelisting Database](#) developed by Kaspersky Lab, based on systemizing knowledge of legitimate software.

Device Control

This feature allows users to set, schedule and enforce data policies that control removable storage and other peripheral devices – connected to a USB or any other bus type.

Host Intrusion Prevention (HIPS)

Regulates access to sensitive data and recording devices by using our local and cloud (Kaspersky Security Network) reputation databases, without affecting the performance of authorized applications.

Support and Professional Services

Professional help is available whenever you need it. Operating in more than 200 countries, from 34 offices worldwide, we have you covered 24/7/365. Take advantage of our Premium Support packages (MSA), or call on our Professional Services to ensure that you derive maximum benefit and ROI from your Kaspersky Lab security installation.

See for yourself

Experience True Cybersecurity for yourself! Visit this [page to trial the full version](#) of Kaspersky Endpoint Security for Business.

Kaspersky Lab

Find a partner near you: www.kaspersky.com/buyoffline

Kaspersky for Business: www.kaspersky.com/business

IT Security News: business.kaspersky.com/

Our unique approach: www.kaspersky.com/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.com

© 2019 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

