Kaspersky®
Endpoint Security
for Business
Select

Kaspersky Endpoint Security for Business Select provides Next Generation, 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 mobile platforms.

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 using the technology is uncomplicated and easy enough for any-sized business to use.

Which tier is right for you?

- **SELECT**
- ADVANCED
- TOTAL

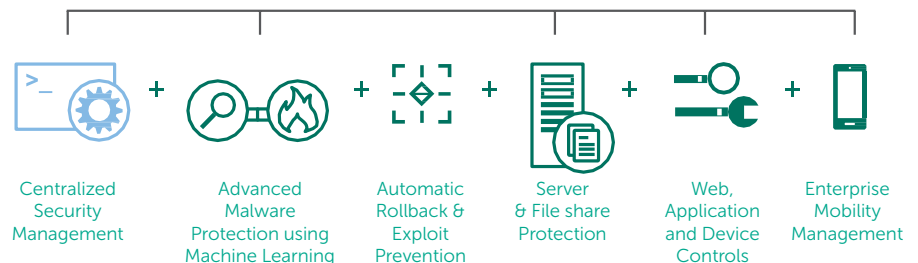### Multiple protection layers for

- 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 *improved*
- Static Machine Learning
- Dynamic Machine Learning *new*
- Process isolation
- Firewall
- OS Firewall management *new*
- Cloud-assisted protection
- Integrated EDR agent *new*
- Application Control *improved*
- Dynamic Whitelisting
- Web Control
- Device Control *improved*
- Server Protection *improved*
- Protection for terminal servers *improved*
- Enterprise Mobility Management *improved*
- Mobile Endpoint Security *improved*
- Reporting *improved*

Centralized Security Management + Advanced Malware Protection using Machine Learning + Automatic Rollback & Exploit Prevention + Server & File share Protection + Web, Application and Device Controls + Enterprise Mobility Management

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 the wide range of preconfigured scenarios.

Agile security

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

A single product – no hidden costs

With multiple security technologies built into a single product, there are no hidden costs. One product means one license – and all you need to protect your endpoints.

Key features

Future-driven threat protection 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. The Behavior Detection blocks attacks, while Automatic Rollback reverses any changes already made.

Protection against encryption for shared folders
Unique anti-cryptor mechanism capable of blocking encryption of files on the shared resources from the malicious process running on another machine on the same network.

Network Threat Protection
Malware using a buffer-overrun 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.

Anti-Rootkit technology
Attackers use rootkits and bootkits to conceal their activities from security solutions. Anti-rootkit technology helps detect even the most deeply hidden infection and neutralizes it.

Mobile security features

Innovative anti-malware technologies
Combined signature-based, proactive and cloud-assisted detection result in real-time protection. A safe browser, on-demand and scheduled scans increase the security.

Deployment Over the Air (OTA) provisioning
This feature 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 provides 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 can use Dynamic Whitelisting Database developed by Kaspersky Lab by systemizing knowledge of legitimate software.

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

Host Intrusion Prevention
Regulates access to sensitive data and recording devices by using local and cloud (Kaspersky Security Network) reputations database, without affecting the performance of authorized applications.

Maintenance and support

Operating in more than 200 countries, from 35 offices worldwide our Professional Services teams are on standby to ensure that you derive maximum benefit from your Kaspersky Lab security installation.

Free trial

Find out why only True Cybersecurity combines ease-of-use agility with HuMachine™ intelligence to protect your business from every type of threat. Visit page and get a free, 30-day trial of the full version of **Kaspersky Endpoint Security for Business**.

Expert analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence