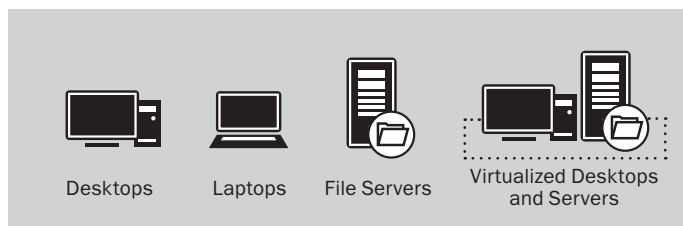# Kaspersky
Endpoint Security 8 for Windows®

Cyber threats targeting your business have become extremely dynamic and exponentially more complex.

Kaspersky delivers comprehensive anti-malware solutions that are powerful, efficient and easy to administer.

Desktops   Laptops   File Servers   Virtualized Desktops and Servers

Kaspersky Endpoint Security 8 for Windows® is a powerhouse of protection, bringing layer upon layer of superior, intelligent protection against emerging and increasingly sophisticated threats — all backed by the relentless anti-malware expertise of Kaspersky Lab's specialists. Kaspersky Lab ensures the security of your business so you can stay focused on running it.

PROTECTION	CONTROL

Kaspersky provides centralized protection of endpoints in a corporate network and beyond from all kinds of malware, potentially dangerous programs and network attacks.

The solution provides effective tools to control compliance with policies on application, device and web usage. Comprehensive control of your corporate endpoints enhances security posture and improves employee productivity.

Deeper Protection:

- **Enhanced Signature Detection and Heuristics** — Vastly improved malware detection and reduced false positives in file, mail and web traffic.

- **Kaspersky Security Network (KSN)** — Integration with the cloud-based file and URL reputation database provides rapid protection from emerging threats based on analysis of real-time activity from the global Kaspersky user community.

- **System Watcher and Behavior Stream Signatures Technology** — Proactively monitors and analyzes systems operations for suspicious activity and identifies dangerous application patterns within a user's system.

- **Rollback of Malicious Activity** — Automatically returns a system to a point before malicious activity occurred.

- **Advanced Firewall and Intrusion Detection System** — flexibly managed Firewall and Intrusion Detection System align with your application control policies.

Powerful Control Tools:

- **Application Startup Control** — Provides administrators with the ability to grant, block and audit application launches.

- **Administrator-Managed Whitelisting** — Provides administratively assigned and cloud-managed, predefined categories of whitelisting rules for application startup control.

- **Application Privilege Control** — Applies restrictions to the actions of applications in the operating system as well as rights to access computer resources.

- **Vulnerability Scanning** — Prevents potential attacks by identifying system weak points, missing patches and neglected exploitable updates.

- **Device Control** — Allows granular control of external device operations — enforces usage policies and reduces the risk of data loss.

- **Web Control and Content Filtering** — Monitoring and filtering users' browser activities by category, content and data type, regardless of workstation location.
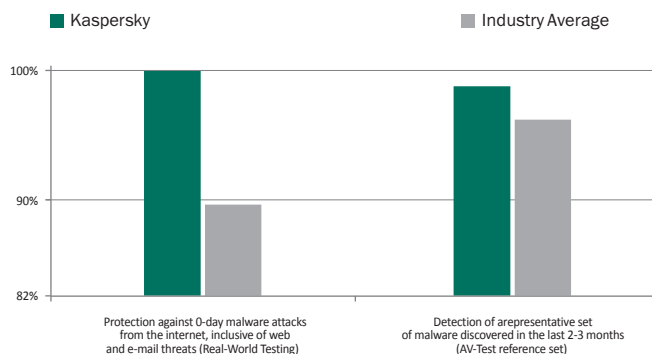
Independent Tests Results

Source: AV-TEST Institute (www.av-test.org)

REPAIR: Cleaning and repair of a malware-infected computer
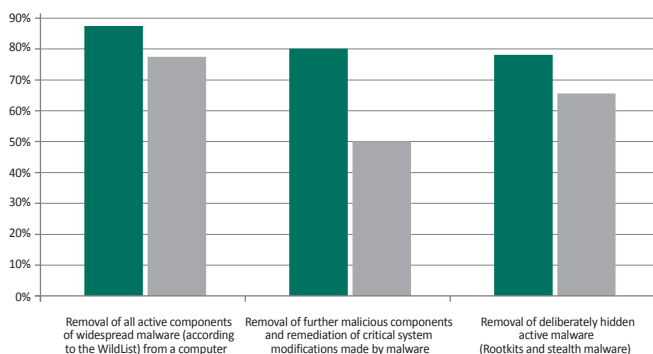
PROTECTION: Protection against malware infections (such as viruses, worms and Trojan horses)

■ Kaspersky   ■ Industry Average

(bar chart: REPAIR)

- Removal of all active components of widespread malware (according to the WildList) from a computer
- Removal of further malicious components and remediation of critical system modifications made by malware
- Removal of deliberately hidden active malware (Rootkits and stealth malware)

(bar chart: PROTECTION)

- Protection against 0-day malware attacks from the internet, inclusive of web and e-mail threats (Real-World Testing)
- Detection of arepresentative set of malware discovered in the last 2-3 months (AV-Test reference set)

Integrated Protection

At Kaspersky, we build our own software from the ground up, rather than 'buying in' other technologies and trying to force them into our solutions.

This results is a homogeneous solution with a light resource footprint — agile, efficient and easy to deploy. Full-scale integration of all program components ensures that protection does not give rise to system conflicts or slow computers down.

Centralized Management

Installing the solution on endpoints, configuring protection and control parameters, managing updates and responding effectively to potentially threatening events — all these as well as other administrative tasks can be carried out centrally and remotely using Kaspersky Security Center.

Learn more about Kaspersky Security Center by visiting http://www.kaspersky.com/security-center

General Requirements

- 1 GB of available disk space on the hard drive

PC Requirements

Software requirements	Hardware
Windows® 7 (x32 / x64 Professional / Enterprise / Ultimate SP0 or higher)	2.0 GHz or higher 512 MB of free RAM
Windows Vista® (x32 / x64 SP2)	2.0 GHz or higher 512 MB of free RAM
Windows® XP Professional (x32 SP3 / x64 SP2)	2.0 GHz or higher 256 MB of free RAM
Windows® Embedded Standard 7 (x32 / x64 SP1)	800 MHz or higher 256 MB of free RAM
Windows® Embedded POSReady 2009 latest SP	

Server Requirements

Software requirements	Hardware
Windows Server® • x32/x64 2003 Standard SP2 • x32 2003 R2 Standard / Enterprise SP2 • x32/x64 2008 Standard / Enterprise SP2 • x64 2008 R2 Standard / Enterprise	2.0 GHz or higher 512 MB of free RAM
Small Business Server 2008 (x64 Standard) Small Business Server 2011 (x64 Essentials / Standard)	2.0 GHz or higher 512 MB of free RAM

How to buy

Kaspersky Endpoint Security 8 for Windows® can be purchased as part of the Kaspersky Open Space Security product line. To help you choose the most suitable product we recommend that you consult a sales manager with one of Kaspersky Lab's partners.

Compatible with Windows® 7

AV TEST CERTIFIED No. 120554

AV TEST AWARD BEST REPAIR Kaspersky Endpoint Security

Enhanced for intel inside™ CORE™

AV comparatives APPROVED Corporate Product 2011

vmware READY

Works with Windows Server® 2008 R2

KASPERSKY lab