

Kaspersky Security Center

Introducing Kaspersky Security Center, our comprehensive, unified management console, providing the administrator with broad, holistic visibility, while at the same time taking IT security controls to a never-before-seen granular level. There's no better way to manage risk in a more pre-emptive fashion. At the intersection of maximum IT flexibility and business productivity - that's where Kaspersky Security Center resides!



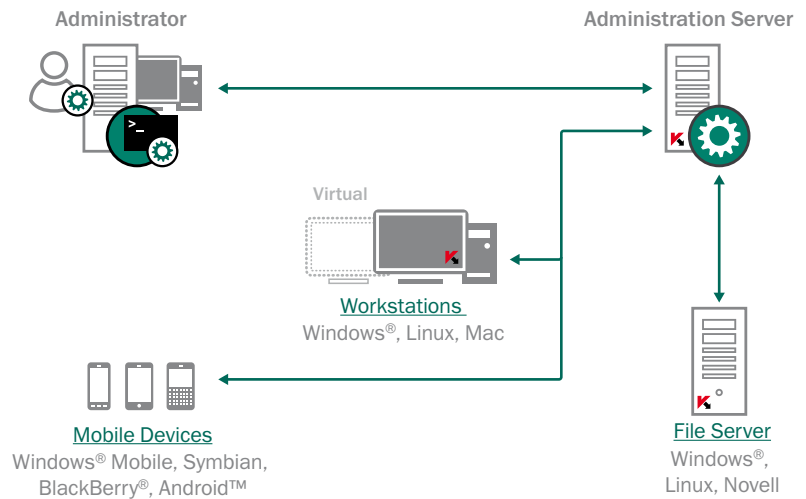
- Remotely deploy Kaspersky on your network endpoints
- Centrally manage your Kaspersky protected devices
- Monitor your security status and report on events and vulnerabilities

Be Ready for What's Next!

DEPLOY	<p>Simple yet very flexible deployment scenarios allow you to secure even the most heterogeneous, highly distributed networks.</p>	<ul style="list-style-type: none"> • Support for any size network – Whatever size infrastructure, Kaspersky Security Center offers deployment and management tools, flexible policy options and robust reporting for small to medium businesses or large enterprises. • Fast deployment system – Distribute fast deployment packages built on your first installation of Kaspersky Security Center using any of several distribution mechanisms, or customize your installation package and add/remove third-party software with the tools provided. • Installation on infected machines – With Kaspersky Security Center you can successfully perform an installation of our endpoint security application even if a machine is infected
MANAGE	<p>Easy and convenient management of the protection system for networks of any complexity. User-friendly scenario-based interface eases the job of system administrators.</p>	<ul style="list-style-type: none"> • Pre-defined policies – Follow best practices with Kaspersky's pre-configured policies, or create your own. • Automated mobile policies – Kaspersky Security Center allows you to set and enforce policies automatically when protected mobile devices leave the corporate network. Perfect for protecting a highly-mobile workforce. • Support for hierarchical management – Organize all protected computers, devices and servers into hierarchical groups with support for task and policy inheritance and control of intermediate administrator privileges.
MONITOR	<p>Stay informed about the state of the protection system, and be the first to know about key events - no matter where you are.</p>	<ul style="list-style-type: none"> • Actionable dashboards – Dedicated dashboards present real-time information on the state of the protection system allowing IT specialists to react promptly to system events. • Powerful reporting system – Prepare and automatically export a wide set of standard reporting templates for all kinds of threat protection activity and administrator actions. Reports can be scheduled or ad-hoc, and are equipped with rich customization capabilities. • Web interface – Remotely monitor protection status and get reports on key events from a flexible and accessible interface.

Multiplatform environment support

- **Support for Virtualized Environments** – Recognition of virtual machines in the corporate administration structure. Also includes automatic load optimization when the product performs intensive operations on virtual hosts.
- **Automated Virtual Lifecycle Processing** – Kaspersky Security Center automatically detects virtual machines, and creates and removes Kaspersky Security Center database records for non-persistent virtual machines.
- **Mixed Environment Support** – Unmatched support for operating systems and virtual platforms, including Windows®, Novell NetWare, Linux®, Mac, VMware, Android™, BlackBerry® and Windows® Mobile.



Windows Endpoint Control Tools*

- **Application Startup Control** – Provides administrators the ability to grant, block and audit application launches.
- **Administrator-Managed Whitelisting** – Provides admin-assigned and cloud-assisted predefined categories of whitelisting rules for application startup control.
- **Application Privilege Control** – Applies restrictions to various actions of applications in the operating system as well as rights to access computer resources.
- **Vulnerability Scanning** – Prevents potential exploits by identifying system weak points, missing patches and neglected application and OS 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.

* For more information, please visit:
<http://www.kaspersky.com/endpoint-security-windows>

How to buy

Kaspersky Security Center provides centralized management of the applications included in the Kaspersky Open Space Security product line as well as Kaspersky Security for File Servers. It is distributed free of charge with these applications.

Administration Server Requirements:

Software Requirements

Microsoft® Data Access Components (MDAC) 2.8+ Microsoft® Windows® DAC 6.0
 Windows Installer 4.5 for Windows Server 2008/ Windows Vista

Database management system:

Microsoft® SQL Server Express 2005, 2008
 Microsoft® SQL Server® 2005, 2008, 2008 R2
 MySQL Enterprise.

32-bit:

Microsoft® Windows Server® 2003+,
 2008 including Core mode
 Microsoft® Windows® XP Professional SP2+,
 Vista® SP1+, 7 SP1

Hardware

1 GHz or higher
 512 MB RAM
 1 GB of available disk space

64-bit:

Microsoft® Windows Server® 2003+ , 2008 SP1,
 2008 R2 including Core mode
 Microsoft® Windows® XP Professional+,
 Vista® SP1, 7 SP1

1.4 GHz CPU
 512 MB RAM
 1GB of available disk space

Administration Console Requirements:

Software Requirements

Microsoft® Management Console 2.0 or later
 Microsoft® Internet Explorer® 8.0

32-bit:

Microsoft® Windows Server® 2003+,
 2008 including Core mode
 Microsoft® Windows® XP Professional SP2+,
 Vista® SP1+, 7 SP1

Hardware

1 GHz CPU
 512 MB RAM
 1GB of available disk space

64-bit:

Microsoft® Windows Server® 2003+,
 2008 SP1, 2008 R2 including Core mode
 Microsoft® Windows® XP Professional +,
 Vista® SP1, 7 SP1

1.4 GHz CPU
 512 MB RAM
 1GB of available disk space

Network Agent & Update Agent Requirements:

Software Requirements

Microsoft® Windows® operating system

Linux

Mac OS

Hardware

1.4 GHz or higher
 512 MB RAM
 32 MB of available disk space for Network Agent
 500 MB of available disk space for Update Agent