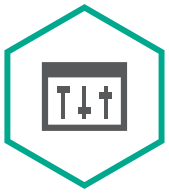

Kaspersky®
Security Center

Manage and protect all your devices – physical, virtual and mobile – from a powerful, single, unified console.

Kaspersky Security Center takes the complexity out of security administration and IT systems management. Fully scalable, the console supports businesses with changing security needs and facilitates comprehensive systems and security management, with easy separation of administrator responsibilities – all from a single, unified management console.

A recognized leader

In 2017, Kaspersky Lab's security products participated in 86 independent reviews, were awarded 72 firsts and achieved 78 top-three finishes. Our endpoint solution's leadership is recognized by leading global analysts.

Kaspersky HuMachine™ approach

Machine learning capabilities, global 'big data' threat intelligence and two decades of human expertise come together to deliver optimum protection with optimum efficiency.

Kaspersky Security Network

Kaspersky Security Network is an intricate distributed infrastructure which delivers a faster-than-ever response to new threats, improving the performance of protection components and minimizing the risk of false positives.

One management console

Because the vast majority of our security technologies can be managed via a single management console – Kaspersky Security Center – it's faster and easier for your security team to apply security policies across all endpoints. Centralized management is complemented by role-based access and integrated dashboards so that each administrator can only access the tools and data relevant to their responsibilities.

Easy scalability

You can scale without changing your initial setup – up to 100,000 physical, virtual and cloud-based endpoints can be managed through a single server installation of Kaspersky Security Center, with optimized backup capabilities.

Expandable architecture

Kaspersky Security Center's extendible architecture includes plug-ins for the management of security products for every platform. If a new security application is purchased or released, the corresponding extension can be installed onto Kaspersky Security Center without console reinstallation or patching.

Benefits

Centralized security management enhances visibility, streamlines costs and optimizes administration efficiency. Kaspersky Security Center includes technologies and tools that, together, deliver an integrated, world-class security platform.

Expedites routine tasks

Endpoint security deployment, configuration and management ensures the up-to-date security of every endpoint and device on the network.

Helps protect all your endpoints and servers

Windows, Linux, Mac, Android, iOS, servers and virtual infrastructure are all protected and managed from the same console.

Reduces exposure to attacks

Centralized web, application and device controls allow you to restrict the use of inappropriate or insecure applications, devices and websites.

Secures mobile working

Supports the centralized administration of protection for leading mobile device platforms, increasing visibility and control without requiring additional resources or technologies.

Streamlines patching

Going beyond the remote deployment of third-party software, automated vulnerability assessment and patch management, based on round-the-clock intelligence into exploited vulnerabilities, keeps potentially vulnerable software up to date and saves your IT administrators' time.

Facilitates inventory and applications deployment

Extended client management tools automate and centralize administrative tasks, including hardware and software inventory, image creation, remote software distribution and troubleshooting.

Empowers Managed Service Providers

Kaspersky Security Center supports B2B subscription-based licensing and multi-tenancy. Unlimited virtual administration servers and remote management via the web console enable the flexible management of multiple clients' IT infrastructures.

Shows the whole picture

Kaspersky Security Center transmits and relays commands, messages and information between the Endpoint Detection and Response (EDR) server, which hunts out evidence of intrusion on every node in real time, and the endpoint agent, thus facilitating increased visibility and security.

Aids GDPR compliance initiatives

The console is used to manage encryption – referred to within the regulation as an additional layer of security to deal with the growing threat of data loss through device theft – and facilitates visibility on an infrastructure-wide scale.

Ensures systems integrity

Kaspersky Security Center enables you to monitor any changes to critically important components of your assets, such as web servers and ATMs, and to respond promptly to breaches in the integrity of these systems.

Plugs proven protection into cloud environments

Native integration between the management console and the Amazon Web Services (AWS) cloud environment provides full visibility and control over Linux and Windows Server based security applications deployed in the cloud.

Simplifies deployment

Enterprise Mobility Management (EMM) management wizards allow for the deployment of protection with Over the Air (OTA) provisioning technology, third-party EMM systems (e.g. VMWare AirWatch), and enrollment consoles (Samsung, KNOX).

Key Features

Out-of-box installation, ready-to-use configuration

Follow best practice out-of-the-box with Kaspersky Lab's preconfigured policies, or create your own. This is particularly useful for smaller organizations with limited IT admin resources available to handle additional configuration tasks.

Beyond threat protection management

Manage physical, virtual and cloud-based endpoints together through one console, improve efficiency, reduce your TCO and more:

- Set up and manage security policies across Windows, Linux and Mac devices.
- Manage cloud-assisted protection, provided by Kaspersky Security Network.
- Centrally manage Application Control, Device Control and Web Control for enhanced protection.
- Manage the Host-Based Intrusion Prevention System (HIPS).
- Configure and manage firewall settings in Linux and Windows operation systems.
- Configure Kaspersky Encryption, Microsoft BitLocker and FileVault encryption to protect data if devices are lost or stolen. Align encryption policies with application and device controls.

Convenient mobile security management

Manage mobile devices – including Android, iOS – in the same way as you manage other endpoints. Administrators can:

- Control how employees access the web on their mobile devices, block malicious websites, and protect users from phishing websites that can steal information and identity details.
- Prevent rooted devices from accessing corporate applications or data.
- Lock, locate or wipe stolen mobile devices, using anti-theft features which can be activated by an administrator or by the user via the Self-Service Portal.
- Roll out unified mobile security policies by enabling access to different platforms' MDM functions via a single interface.

Virtualized environment support

Avoid performance-sapping threat protection 'storms' by recognizing virtual machines and facilitating load balancing during intensive operations – all from the same management console. Whether you're using agentless protection or light agent to protect your virtual environment, you can fully manage these security applications via Kaspersky Security Center.

Cloud environment support

Enjoy complete visibility and control over Kaspersky Endpoint Security for Linux and Kaspersky Security for Windows Server instances deployed in the cloud, provided through tight integration between the management console and the AWS cloud environment.

Integration with targeted solutions

Leverage integration with various targeted solutions, enabling you to monitor security for embedded systems, gateways, email systems and collaboration platforms. You can view connectivity and health status, and access consolidated statistics for all servers, together with the other security components your organization uses, all through a single console.

Enhanced reporting

Review a wide range of built-in and customizable reports, apply dynamic filtering and sort reports by any field.

Web management console

Enable the remote management of endpoints and mobile devices from the web console.

Role-based model

Assign different endpoint groups or management tasks to different administrators via Role-Based Access Control, customizing the management console so that each administrator can only access the tools and data relevant to their responsibilities.

World-class vulnerability and patch management

Identify possible entry points for malicious programs into your network by detecting vulnerabilities in your applications or operating system, and eliminating them before malware can cause disruption, through the Vulnerability and Patch Management capabilities included in Kaspersky Security Center. Plus:

- Prioritize vulnerabilities and automatically distribute patches and updates for Microsoft and non-Microsoft software.
- Remotely resolve update issues for any physical, virtual or Amazon EC2 machine.
- Reduce update traffic to remote offices by using a remote endpoint as an update agent.
- Monitor patch installation status through successful patch application reporting.

Streamlined IT asset management

Relying on a wide range of IT systems management features which streamline IT asset management tasks in heterogeneous networks, you can:

- Automatically identify hardware and software on the network, giving total visibility of all assets that need to be managed and secured.
- Minimize the effort needed to set up new devices or roll out new applications with automatic software provisioning.
- Deploy software at your command, or schedule it for after-hours, and specify additional parameters to customize software package installation
- Employ remote troubleshooting – including authorization mechanisms, plus remote session logs.
- Control the creation, storage and cloning of secured system images to help optimize OS deployment, while reducing the time taken to deploy. UEFI is supported.

Built-in audit best practices

Kaspersky Security Center logs and stores all changes in settings, policies, tasks and managed applications, for version comparison and roll-back if required. Audit capabilities allow administrators to compare two policies – after which a report is generated reflecting which settings match and which differ.

System requirements

For the most complete, up-to-date requirements, please refer to the Knowledge Base.

General requirements

- CPU with operating frequency of 1,4 GHz or higher
- 4 GB of memory (RAM)
- 10 GB free disk space

Operating systems

- Microsoft Windows 10, 8.1, 8, 7
- Microsoft Windows Server 2016, 2012 R2, 2012
- Microsoft Small Business Server 2011
- Microsoft Windows Server 2008 R2, 2008 SP1, 2008

Version requirements for subscription

Please check with your local partner about subscription availability in your country – and see the relevant system requirements here.

How to buy

Kaspersky Security Center is included in:

- Kaspersky Total Security for Business
- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Security for Business Select
- Kaspersky Vulnerability & Patch Management
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Storage
- Kaspersky Security for Mobile
- Kaspersky Security for Mail Server
- Kaspersky Security for File Server

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

#truecybersecurity
#HuMachine

www.kaspersky.com