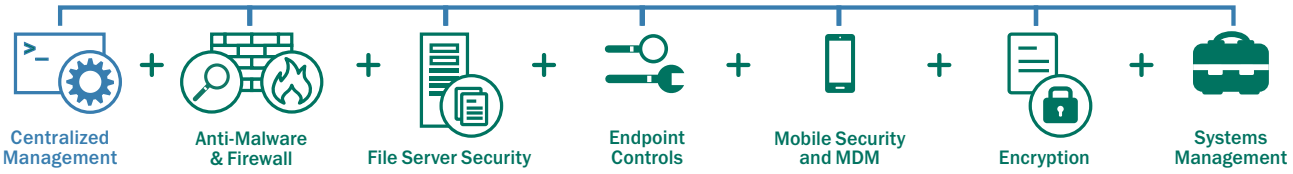
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Endpoint Security for Business offers a complete security solution, designed by the world's leading security experts. The deepest, most forward-looking protection, efficient performance and straightforward management build through progressive tiers to fully secure your business.

All components have been designed and built in-house to mesh together into a single security platform geared to your business needs. The result is a stable, integrated solution with no gaps, no compatibility issues and no additional workload as your system builds.



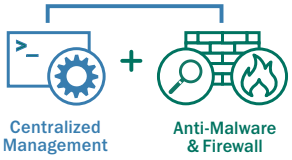
One Comprehensive Management Console — Kaspersky Security Center

At the hub of this unified approach sits Kaspersky Security Center, an intuitive, fully scalable management console that minimizes the total cost of ownership of any Kaspersky Lab security solution.

Simple, seamless security administration for desktop, portable, mobile and virtual endpoints and servers, delivered through a single pane of glass, providing:

- **Combined policy deployment**
- **Separate web console**
- **Scheduled and on-demand reporting**

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — CORE



A layered security model begins with best of breed anti-malware

Kaspersky Security for Business — Core incorporates:

POWERFUL ENDPOINT ANTI-MALWARE SCANNING

Operating at multiple levels in the operating system, rooting out malware using a combination of signature-based, heuristic and cloud-assisted technologies.

KASPERSKY SECURITY NETWORK: CLOUD-ASSISTED PROTECTION

Real-time information from the worldwide Kaspersky Security Network means that new and unknown threats can be identified and eliminated as they emerge.

HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) WITH PERSONAL FIREWALL

Predefined rules for hundreds of the most common applications reduce time spent on firewall configuration.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT

Including File Server Protection, Endpoint Controls and Mobile Security/MDM

Mobile device management and granular endpoint control tools combine with anti-malware protection to provide multi-layered security, even on employee owned mobile devices. File server protection ensures that infection cannot spread to secured endpoints through stored data.

ENDPOINT CONTROLS

Application Control — with 'Dynamic Whitelisting', using real-time file reputations delivered by Kaspersky Security Network, enables IT administrators to allow, block or regulate applications, including operating a 'Default Deny' scenario. Application Privilege Control monitors and restricts applications performing suspiciously.

Web Control — browsing policies can be created around pre-set or customized databases of inappropriate sites, following the user on the corporate network and when roaming.

Device Control — allows users to set, schedule and enforce data policies controlling the connection of removable storage and other peripheral devices to any bus type.

MOBILE SECURITY:

Mobile Anti-Malware — combined signature-based, proactive and cloud-assisted technologies deliver powerful real-time mobile device protection. A safe browser and anti-spam increase security.

Mobile Device Management (MDM) — Kaspersky Security for Mobile supports functionality provided by Microsoft Exchange ActiveSync, Apple MDM and Samsung SAFE.

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

Mobile Controls — administrators can manage and restrict applications usage, while prohibiting the usage of unwanted or grey software. As well as blocking malicious sites, they can also control access to sites, that do not conform to corporate policies.

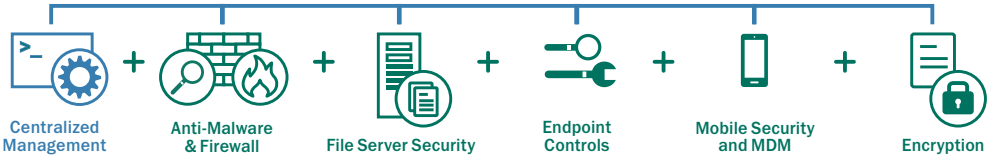
App Containerization for BYOD — corporate data and applications can be isolated from the personal files on the employee device by placing corporate apps in special containers, which can be encrypted and wiped separately from the user's personal data.

FILE SERVER SECURITY

Managed together with endpoint security through Kaspersky Security Center, file server protection ensures that malware cannot spread to secured endpoints through stored, infected data.

Kaspersky Endpoint Security for Business — Select also includes all components of the Core tier.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



Including Encryption and Systems Management

Kaspersky Endpoint Security for Business — Advanced promotes IT administrative efficiency and compliance. Prioritized patching, OS image management and remote troubleshooting combine to streamline everyday administration, while infrastructure, guest users and inventories all sit firmly under IT control. Comprehensive, transparent encryption adds a further layer of security, and all components are managed through a single uncluttered console — Kaspersky Security Center.

SYSTEMS MANAGEMENT

Vulnerability and Patch Management — automated OS and application vulnerability detection and prioritization, combined with the automated distribution of patches and updates.

Operating System Deployment — easy creation, storage and deployment of OS images from a central location, as well as OS migration.

Remote Software Distribution And Troubleshooting — remote deployment and update from a single console, automated for over 100 applications, can be on-demand or scheduled for quieter periods. Time-saving remote troubleshooting is fully supported and a single 'agent' at branch offices can accept updates for local rollout, using Multicast technology.

Network Access Control (NAC) — automatically recognizes and checks new devices on the network against inventories and IT security policies, denies access to compromised devices and redirects guest devices to a captive portal.

Hardware and Software Inventories — full visibility and control (including blocking) of all software deployed across the network, together with the automatic identification, registration and tracking of all hardware, including removable devices.

ENCRYPTION

Comprehensive File/Folder and Full Disk — choose from full-disk or file level that is transparent to the user and is backed by Advanced Encryption Standard (AES) 256 bit encryption to secure critical business information in the event of device theft or accidental loss. Includes support for removable devices.

Secure Data Sharing — allows Users to easily create encrypted and self-extracting packages to ensure data is protected when sharing via removable devices, email, network or web.

Kaspersky Endpoint Security for Business — Advanced also includes all components of the Select and Core tiers.

▶ KASPERSKY TOTAL SECURITY FOR BUSINESS

Including periphery security for servers and gateways

Kaspersky Total Security for Business delivers the most complete platform of protection and management offered in the industry today. Kaspersky Total Security for Business secures every layer of your network and includes powerful configuration tools to ensure your users are productive and free from the threat of malware, regardless of device or location.

MAIL SERVER SECURITY

Effectively prevents email based malware threats, phishing attacks and spam using cloud-based, real time updates for exceptional capture rates and minimal false positives. Anti-malware protection for IBM Domino is also included.

SECURITY FOR INTERNET GATEWAYS

Ensures secure Internet access across the organization by automatically removing malicious and potentially hostile programs in HTTP(S) / FTP / SMTP and POP3 traffic.

COLLABORATION SECURITY

Defends SharePoint® servers and farms against all forms of malware, while content and file filtering capabilities help prevent the storage of inappropriate content.

Kaspersky Total Security for Business also includes all components of the Advanced, Select and Core tiers.

ONE PLATFORM. ONE SERVER. ONE CONSOLE.

Complexity is the enemy of security. Here are some of the benefits that only a genuinely deeply integrated platform solution can bring:

- **Keeping it simple.** Kaspersky Solutions are designed together from first principles to work smoothly and efficiently as a single entity — with no security gaps.
- **Hassle-free installation.** Just one installation process, with no re-boots or application add-ons.
- **Single policy deployment.** Different protection and control parameters can be managed together through just one policy.
- **Working together.** Integrated solution components can share information (hardware inventory informing device controls, for example) for more efficient, targeted activity.
- **A clearer, deeper view.** The administrator can see, control and generate integrated reporting across the whole IT environment from a single console.
- **Unified rights management.** All aspects of user activity can be overseen and controlled from a single point of information.
- **One license, one purchase.** All the functionality you need brought together in a single package.

KESB/Version 0.2/July 14/Global

KASPERSKY lab