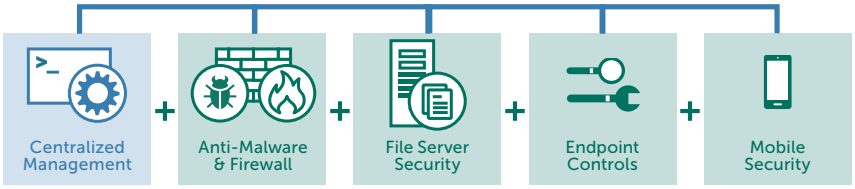
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Powerful multi-layered protection against known, unknown and advanced threats, designed and built by the industry's leading security experts. Kaspersky Endpoint Security for Business, backed by world-renowned threat intelligence, provides unequalled IT security and control.

KASPERSKY lab

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Select



POWERFUL, GRANULAR ENDPOINT CONTROLS COMBINED WITH PROACTIVE SECURITY AND MANAGEMENT FOR MOBILE DEVICES AND DATA

Application, web and device controls, including dynamic whitelisting supported by Kaspersky's unique in-house laboratory, add a further dimension to deep endpoint security. Corporate and employee owned (BYOD) mobile devices are also secured and managed, together with all protected endpoints, though the Kaspersky Security Center console. File server protection ensures that infection cannot spread to secured endpoints through stored data.

PROTECTION FROM KNOWN, UNKNOWN AND ADVANCED THREATS

Best-in-class anti-malware combines with **Automatic Exploit Prevention** and real-time cloud-assisted security intelligence from **Kaspersky Security Network** to provide proactive, targeted protection against the latest threats.

System Watcher provides unique file restoration capabilities while **Host-based Intrusion Prevention System (HIPS) with Personal Firewall** help secure and control application and network activity.

ENDPOINT CONTROLS

Application Control with Dynamic Whitelisting — using real-time file reputations from the Kaspersky Security Network, IT administrators can allow, block or regulate applications, including operating 'Default Deny' whitelisting in a live or test environment. Application Privilege Control and Vulnerability Scanning monitor applications and restrict those performing suspicious.

Web Control — browsing policies can be created around pre-set or customizable categories, ensuring comprehensive oversight and adminstrative efficiency.

Device Control — granular data policies controlling the connection of removable storage and other peripheral devices can be set, scheduled and enforced, using masks for simultaneous deployment to multiple devices.

FILE SERVER SECURITY

Managed together with endpoint security through Kaspersky Security Center.

MOBILE SECURITY

Powerful Security for Mobile Devices — advanced, proactive and cloud-assisted technologies deliver multi-layered real-time mobile endpoint protection.

Web protection, anti-spam and anti-phishing components further increase device security.

Remote Anti-Theft — Lock, Wipe, Locate, SIM Watch, Alarm, Mugshot and Full or Selective Wipe prevent unauthorized access to corporate data if a mobile device is lost or stolen. Administrator and end-user enablement, together with Google Cloud Management support, delivers quick activation if required.

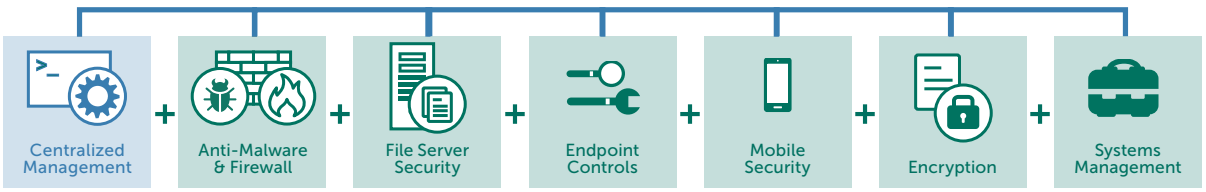
Mobile Application Management (MAM) — controls limit users to running whitelisted applications, preventing the deployment of unwanted or unknown software. '**Application Wrapping**' isolates corporate data on employee owned devices. Additional encryption or 'Selective Wipe' can be remotely enforced.

Mobile Device Management (MDM) — a unified interface for **Microsoft® Exchange ActiveSync** and **iOS MDM** devices with OTA (Over The Air) policy deployment. **Samsung KNOX** for Android™-based devices is also supported.

Self-Service Portal — allows self-registration of employee-owned approved devices onto the network with automatic installation of all required certificates and keys, and user/owner emergency activation of anti-theft features, reducing the IT administrative workload.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Advanced



SYSTEMS MANAGEMENT TOOLS OPTIMIZE IT EFFICIENCY AND SECURITY, WHILE INTEGRATED ENCRYPTION PROTECTS SENSITIVE DATA

Automated patch management and OS image management, remote software distribution and SIEM integration all help to streamline administration, while hardware and software inventories and license management provide visibility and control. Integrated encryption technology adds a powerful layer of data protection.

SYSTEMS MANAGEMENT

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

Operating System Deployment — easy creation, storage and deployment of OS golden images from a central location, including UEFI support.

Software Distribution and Troubleshooting — remote software deployment and application and OS update available on-demand or scheduled, including Wake-on-LAN support. Time-saving remote troubleshooting and efficient software distribution is supported through Multicast technology.

Hardware and Software Inventories and Licensing Management — identification, visibility and control (including blocking), together with license usage management, provides insight into all software and hardware deployed across the environment, including removable devices. Software and hardware license management, guest device detection, privilege controls and access provisioning are also available.

Remote Desktop Tools — instant connection to client computers managed in Kaspersky Security Center for easy diagnostics and troubleshooting. For reduced response times, increased efficiency and streamlined support for remote sites, Kaspersky Security Center uses RDP and Windows Desktop Sharing technology (as used in Windows Remote Assistance). Remote connection to client computers through the Network Agent allows full administrator access to the data and applications installed on the client, even if the client TCP and UDP ports are closed.

SIEM Integration — support for IBM® QRadar and HP ArcSight SIEM systems.

Role Based Access Control (RBAC) — administrative responsibilities can be assigned across complex networks, with console views customized according to assigned roles and rights.

ENCRYPTION

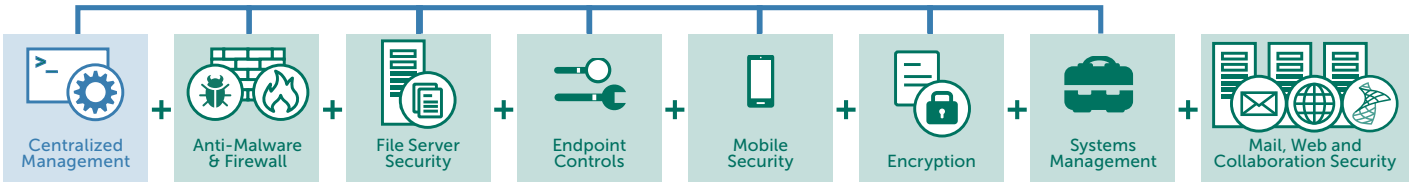
Powerful Data Protection — file/folder (FLE) and Full Disk (FDE) encryption can be applied to endpoints. Support for "portable mode" ensures encryption administration across devices leaving administrative domains.

Flexible User Login — pre-boot authentication (PBA) for added security includes optional 'single sign-on' for user transparency. 2-factor or token based authentication is also available.

Integrated Policy Creation — unique integration of encryption with application and device controls provides an additional layer of security and administrative ease.

Kaspersky Endpoint Security for Business — ADVANCED also includes all components of the SELECT tier.

KASPERSKY TOTAL SECURITY FOR BUSINESS



ORGANIZATIONS THAT DEMAND COMPREHENSIVE SECURITY FOR THEIR ENTIRE IT ENVIRONMENT CHOOSE KASPERSKY TOTAL SECURITY FOR BUSINESS

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 users are productive and free from the threat of malware, regardless of device or location.

MAIL SERVER SECURITY

Effective prevention of email based malware, phishing attacks and spam using cloud-based, real-time updates for exceptional capture rates and minimal false positives a includes Anti-malware protection for IBM® Domino®. DLP functionality for Microsoft Exchange is available separately.

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. DLP functionality for Sharepoint, available separately, provides content and file filtering capabilities, identifies confidential data and protects against data leakage.

Kaspersky Total Security for Business also includes all components of the ADVANCED and SELECT tiers.

Security with a difference

Kaspersky Lab delivers the most powerful anti-malware on the market by harnessing the world-leading Security Intelligence that is built into our DNA and influences everything we do — and how we do it.

- **We're a technology-driven company** — from top to bottom, starting with our CEO, Eugene Kaspersky.
- **Our Global Research & Analysis Team (GReAT)**, an elite group of IT security experts, has been the first to uncover many of the world's most dangerous malware threats and targeted attacks.
- **Many of the world's most respected security organizations** and law enforcement agencies have actively sought our assistance.
- Because Kaspersky Lab develops and perfects all of its own core technologies in-house, our products are naturally more stable and more efficient.
- **Each year, Kaspersky Lab participates in more independent tests than any other vendor** — and comes top in a much higher percentage of them than any other vendor.
- **The most widely respected industry analysts** – including Gartner, Inc, Forrester Research and International Data Corporation (IDC) — rate us as a Leader within many key IT security categories
- **Over 130 OEMs** — including Microsoft, Cisco Meraki, Juniper Networks, Alcatel Lucent and more — use our technologies within their own products and services.

For more information about Kaspersky Endpoint Security for Business, please contact your reseller.

KASPERSKY lab