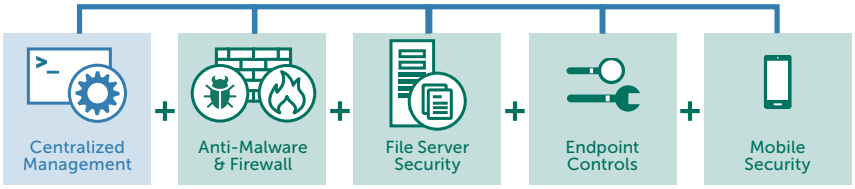
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

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.