KASPERSKY ENDPOINT SECURITY FOR ENTERPRISE

Next-generation protection against advanced threats targeting your endpoints and users

The threat environment is advancing exponentially, putting critical business processes, confidential data and financial resources at ever-increasing risk from zero-day attacks. To mitigate the risk to your organization, you need to be smarter, better equipped and better informed than the cyber-professionals targeting you.

But one simple fact is true – the majority of enterprise cyber-attacks are initiated through the endpoint. If you can effectively secure every corporate endpoint, static and mobile, you have a strong foundation for your overall security strategy.

POWERFUL SECURITY

Fully securing every endpoint against every form of known and unknown cyber threat is a major task. Traditional antivirus protection is nowhere near enough. Only through employing a cutting-edge security platform, adopting a multi-layered approach, can you hope to fully protect every single endpoint within and beyond your perimeter.

POWERFUL PERFORMANCE

Endpoint protection should feel as natural and unconscious as breathing. Kaspersky Lab's unique integrated security platform pulses continuously at the heart of your IT infrastructure, applying powerful endpoint protection with minimal impact on speed or resources. Built in-house as a single, fully scalable integrated platform, the solution delivers optimum performance with no software conflicts and no security gaps.

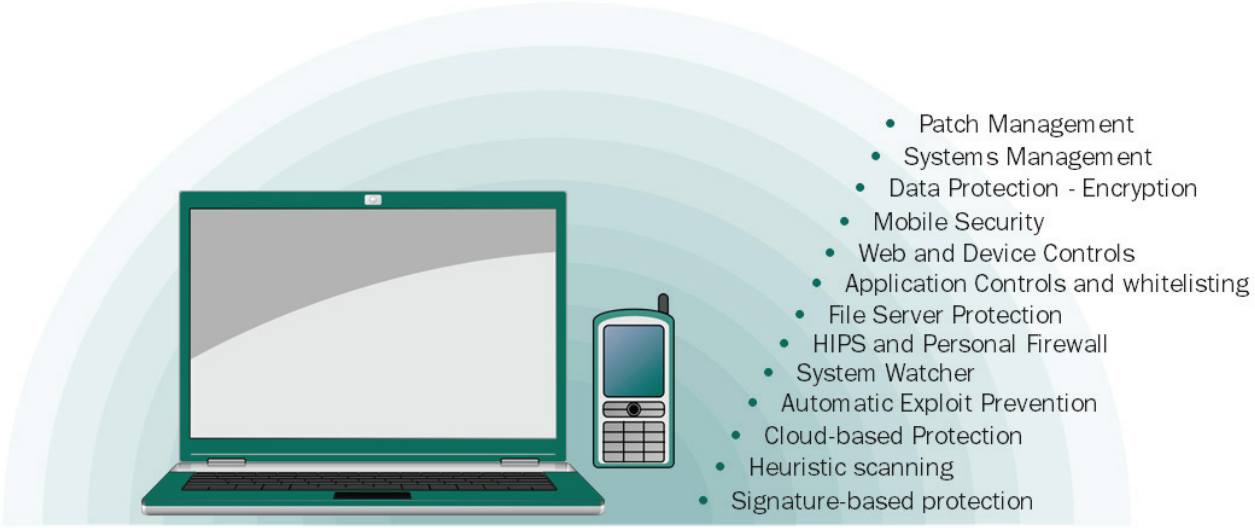
POWERFUL THREAT INTELLIGENCE

Based on unequalled sources of real-time threat intelligence, our technologies continually evolve to protect your business from even the latest, most sophisticated threats, including zero-day exploits. By aligning your security strategy with the world leaders in advanced threat discovery, you are choosing to adopt best of breed endpoint protection, now and in future. There is no better security posture for your organization.

CENTRALIZED MANAGEMENT

Manage multiple platforms and devices from the same console as other endpoints – increase visibility and control without additional effort or technology to manage.

Multi-layered Protection



Unequalled Next-Generation Threat Preventionand Elimination

At the core of your security strategy - the most powerful and effective endpoint protection engine in the industry, as continuously confirmed through independent tests[1].

Layer upon layer of proactive, intelligent protection intermeshes to provide powerful, resilient defences against the most sophisticated known, unknown and advanced cyberthreats.

- Multi-Algorithm **Heuristic Analysis** - detects unknown malware, supplementing traditional **signature-based** technologies.
- **Cloud-Assisted Kaspersky Security Network (KSN)** – facilitates the identification and blocking of new malware threats in real time as they emerge.
- **Automatic Exploit Prevention** - helps proactively stop even the most advanced threats through blocking exploits used by cybercriminals.
- **System Watcher** — Blocks unknown threats by detecting suspicious behaviour patterns, and restores key files should the system be impacted
- **Host-based Intrusion Prevention System (HIPS)** — restricts activities and grants privileges according to the software's trust level
- **Personal Firewall** restricts network activity
- **Network Attack Blocker** stops network-based attacks
- **File servers** are also fully protected

Every Endpoint Under Your Control

Minimize endpoint exposure to risk while increasing productivity. Control individual endpoint access to applications, websites and plug-ins - identifying and blocking the inappropriate, regulating access to the unnecessary, and promoting the valuable and trusted.

All control tools integrate with Active Directory, and simplified, customizable or automated policy creation and enforcement can be centralized or role-based as preferred.

LOWER YOUR EXPOSURE TO ATTACK VIA APPLICATIONS

Powered by **Dynamic Whitelisting, Application Control** significantly reduces your exposure to zero-day attacks by providing total control over the software allowed to run. Blacklisted applications are blocked, while those behaving suspiciously or inappropriately are detected, analyzed and then blocked or restricted with the help of System Watcher and HIPS. Meanwhile, your approved and trustworthy applications continue to run smoothly.

CLOUD-EMPOWERED FLEXIBLE WHITELISTING

from our in-house Whitelisting Lab supports a Default Deny scenario, which can be run in a testbed environment.

ADDRESSING THE DANGERS OF WEB BROWSING

Web Control monitors, filters and controls which websites end-users can access in the workplace, increasing productivity while mitigating your vulnerability to systems penetration and infiltration via websites and social media.

CONTROLLING THE USE OF PORTABLE DEVICES

Device Control guards against the damaging consequences of corporate and customer data loss on unapproved or unencrypted portable devices, and against the upload of infected data from the device.

Protecting Data Through Integrated Encryption

Powerful, user-transparent **encryption** fully secures confidential and sensitive data on the move, on portable devices and in situ. Integrated technology means you can centrally enforce the encryption of corporate data at file, disk or device level, through straightforward security policies addressing groups of endpoints or even individual devices.

---

1 Reference here – Top3.

Eliminating Vulnerabilities Through Intelligent Patching

Exploiting vulnerabilities uncovered in a trusted application is one of the commonest ways to gain access to IT infrastructure through a single endpoint. Prioritizing and managing the timely, efficient patching of vulnerabilities requires a deep understanding of exploits, their behaviors and their current targets. Kaspersky Lab's **automated vulnerability assessment and patch management** system, based on real-time global intelligence into exploit activities, keeps critical patching up to date, without impacting on busy systems and users.

Securing Mobile Endpoints Beyond Your Perimeter

Corporate data has become accessible anywhere, anytime, on smartphones and tablets travelling freely through your IT perimeter. **Mobile device security** guards against threats specifically targeting sensitive data on the move, as well as those attempting to use security weaknesses in corporate or employee owned devices as a 'jumping off point' for systems infiltration.

Features include

- **Powerful multi-layered protection** against malware threats for all leading mobile platforms.
- **Anti-phishing** technology - blocks dangerous links in messages and web pages while calls/sms filters prevents unwanted communication
- **Application wrapping** - allows corporate data to be containerized, encrypted and wiped separately on employee owned devices.
- **Application control and web control** supported by KSN, blocking unauthorized software and website access.
- **Anti-theft** - features including wipe, device lock, locate, SIM watch, 'mugshot' and 'alarm' device detection allowing the swift disablement of devices and erasure of any sensitive data when a device is lost or stolen.
- **Jailbroken or rooted device** detection and reporting, so action can be taken.
- **Centralized management** - including Mobile Device and Applications Management. (MDM/MAM) functionality. Policies can be deployed to heterogeneous devices on all major platforms from a single interface.

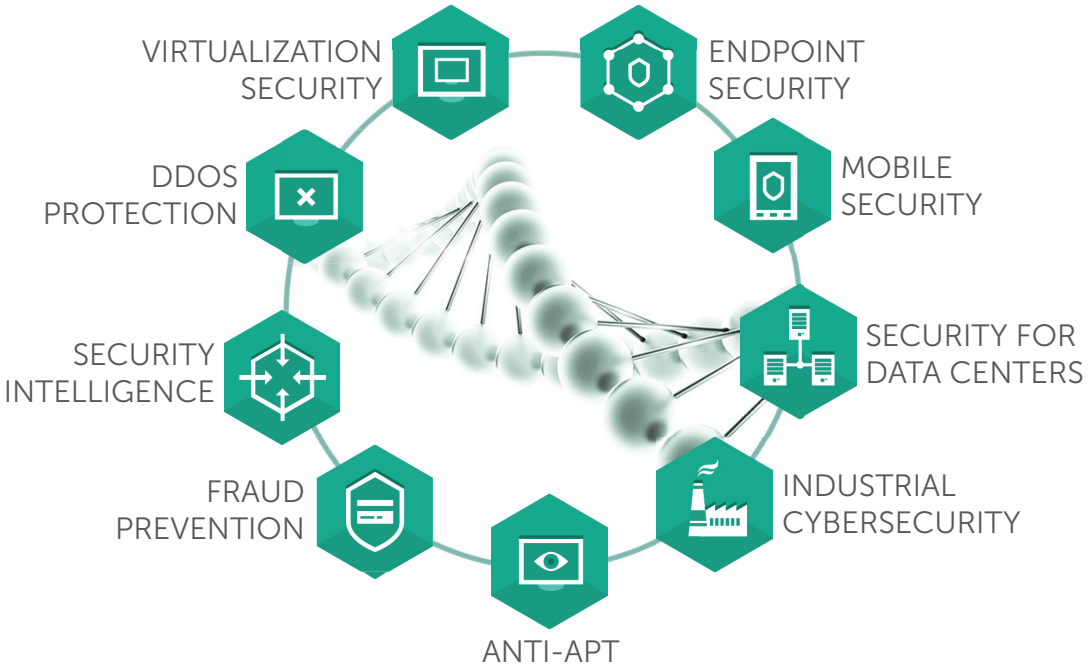
Optimised Efficiency – Integrated Management

Kaspersky Endpoint Security for Enterprise provides your security teams with full visibility and control over every endpoint, static or mobile, under your jurisdiction, wherever it sits and whatever it's doing. Almost infinitely scalable, the solution provides access to inventories, licensing, remote trouble-shooting and network controls, all accessible from one console - the **Kaspersky Security Center**.

Centralized, single-console management is complemented by role-based management functionality, so access rights and responsibilities can be allocated to individual security professionals as required.

The Bigger Picture - Kaspersky Enterprise Security Solutions

Endpoint protection, though critical, is just the beginning. Whether you operate a best-of-breed or single-source security strategy, Kaspersky Lab offers **a range of enterprise solutions** that interlock or work independently, so you can pick and choose without sacrificing performance efficiency or freedom of choice. Solutions covering **virtual** as well as **physical systems, servers and infrastructures** are complemented by those targeting **specific industry issues**, like financial fraud and Denial of Service (DDoS) attacks, and by our range of **Security Intelligence Services**.



Maintenance and Support

Operating in more than 200 countries, from 34 offices worldwide, our 24/7/365 commitment to global support is reflected in our **Maintenance Service Agreement (MSA)** support packages. Our **Professional Services** teams are on standby to ensure that you derive maximum benefit from your Kaspersky lab security installation.

To learn more about securing your endpoints more effectively, please contact the Kaspersky Lab Enterprise Sales Team.

Kaspersky Enterprise Security for Endpoints/V 1.0/Nov 15/Global