Kaspersky®
Endpoint
Security

The leading multi-layered endpoint protection platform, based on true cybersecurity technologies

The threat environment is advancing exponentially, putting critical business processes, confidential data and financial resources at ever-increasing risk from zero-day attacks. During the past 12 months, over 38% of all businesses have been affected by some form of malware. 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, physical and virtual, static and mobile, you have a strong foundation for your overall security strategy.

Kaspersky Lab technologies and threat intelligence continually evolve to protect your business from even the latest, most sophisticated threats and exploits, including targeted attacks.

This zero-second protection against known and unknown threats is further enhanced by powerful control and data protection tools including Integrated Encryption, Automated Patching and Mobile Endpoint protection – all managed together through a single console – Kaspersky Security Center.

Threat Prevention

Our leading threat prevention engine, harnessing HuMachine™ intelligence, protects you from ransomware, exploits and even the most advanced forms of cyberthreat.

Advanced Endpoint Control

Easy and effective centralized web, device and application controls reduce your attack surface and help keep users safe.
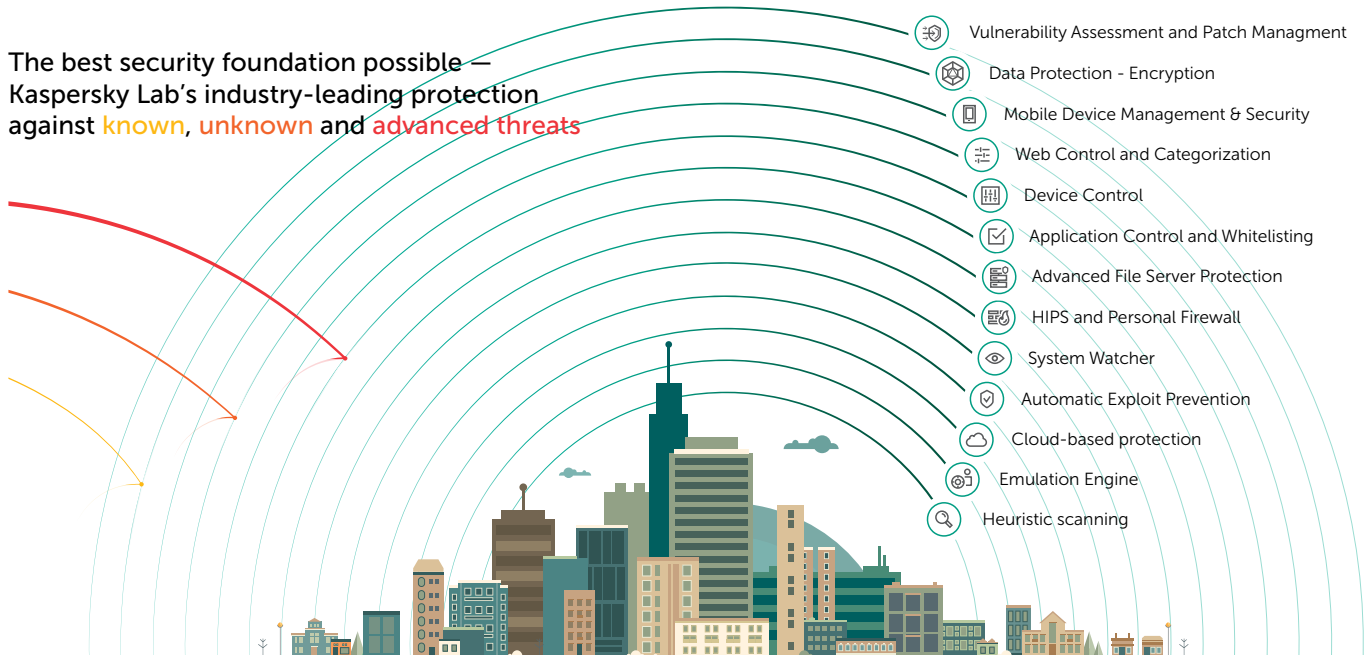
Data Protection

FIPS 140.2 certified full disk encryption helps fully protect confidential data on stationary and mobile devices.

Multi-layered Protection

The best security foundation possible — Kaspersky Lab's industry-leading protection against known, unknown and advanced threats

Vulnerability Assessment and Patch Managment

Data Protection - Encryption

Mobile Device Management & Security

Web Control and Categorization

Device Control

Application Control and Whitelisting

Advanced File Server Protection

HIPS and Personal Firewall

System Watcher

Automatic Exploit Prevention

Cloud-based protection

Emulation Engine

Heuristic scanning

POWERFUL MULTI-LAYERED PROTECTION FROM ALL FORMS OF CYBER-THREAT

Unprecedented Security Based on Machine Learning

Fully securing every endpoint against every form of known and unknown cyber-threat is a major task. Traditional anti-malware 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.

High Performance

Kaspersky Lab's unique integrated security pulses continuously at the heart of your IT infrastructure, applying powerful protection through a single endpoint agent, with minimal impact on speed or resources. Built in-house as a 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.

Unified & Centralized Management

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

Unequalled Next-Generation Threat Prevention and 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], powered by world-leading security intelligence and machine learning technologies.

Layer upon layer of proactive, intelligent protection intermeshes to provide powerful, resilient defenses against the most sophisticated known, unknown and advanced cyber-threats.

- Multi-Algorithm **Heuristic & Threat Emulation Analysis** – detects unknown malware, supplementing traditional **signature-based** technologies.

- **Cloud-Assisted Protection (Kaspersky Security Network)** – 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 behavior patterns, and restores key files should the system be impacted – reliable protection against ransomware.

- **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.

[1] www.kaspersky.com/top3

Anti-Ransomware & Anti-Exploit Protection

Keep your data safe and avoid funding cybercriminals through ransom payments with Kaspersky System Watcher. Protect shared folders from advanced crypto-lockers with Kaspersky Security for Windows Server. And protect your endpoints from the latest exploits with our Automatic Exploit Prevention technologies.

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 what software is 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.

Leverage Cloud-Empowered Flexible Whitelisting

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

Address the Dangers of Web Browsing

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

Control 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.

Apply Advanced Protection to Your Corporate Servers

Application Launch Control on servers providing unprecedented security by using configured rules to allow or block the startup of executable files, scripts, and MSI packages, or the loading of DLL modules onto servers.

Every Endpoint Under Your Control

Minimize endpoint exposure to risk while increasing productivity. Control individual endpoint access to applications, websites and devices – 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.

Protecting Data through Integrated FIPS 140-2 Certified 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. All this through the same single console used to manage all your Kaspersky Lab endpoint security, together with native OS encryption including Microsoft BitLocker.

Eliminating Vulnerabilities through Automated 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 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.
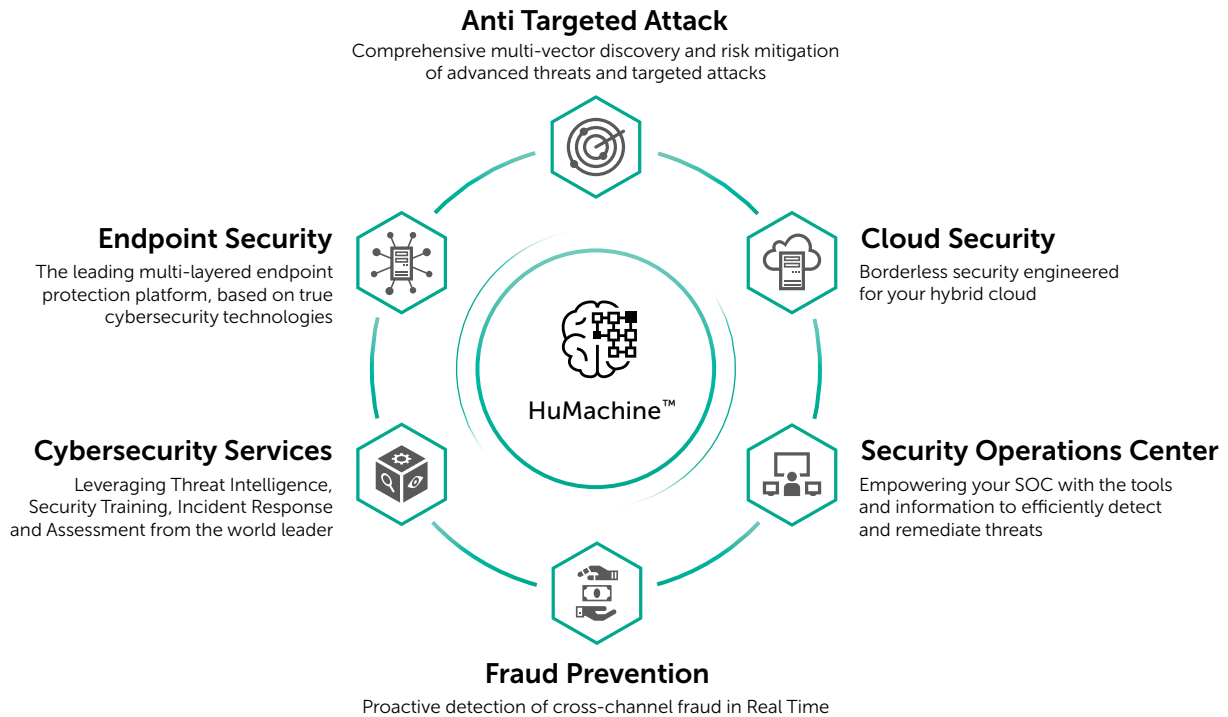
Optimized Efficiency – Integrated Management

Kaspersky Endpoint Security provides your security teams with full visibility and control over every workstation, server or mobile device, 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. Our solutions protect **virtual and cloud-based systems** as well as **physical endpoints, servers and infrastructures**, and also address cybersecurity issues in specific **industry verticals**, such as financial services, healthcare, and government establishments.

Anti Targeted Attack
Comprehensive multi-vector discovery and risk mitigation of advanced threats and targeted attacks

Endpoint Security
The leading multi-layered endpoint protection platform, based on true cybersecurity technologies

Cloud Security
Borderless security engineered for your hybrid cloud

Cybersecurity Services
Leveraging Threat Intelligence, Security Training, Incident Response and Assessment from the world leader

Security Operations Center
Empowering your SOC with the tools and information to efficiently detect and remediate threats

HuMachine™

Fraud Prevention
Proactive detection of cross-channel fraud in Real Time

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.

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence
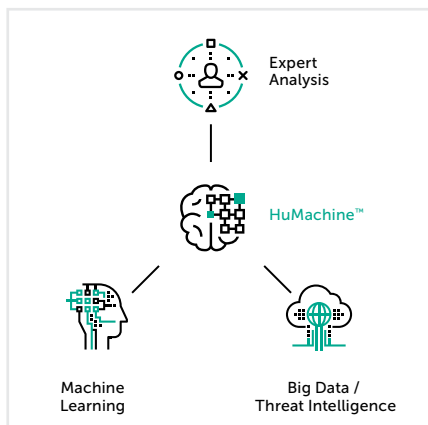
Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com