Next Generation
endpoint protection
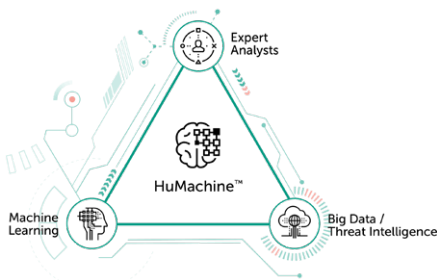
www.kaspersky.com/business
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Protection as part of your business continuity strategy

Technology is a transformative force for business – keep pace or stagnate. But technology also opens the doors to criminals, and it's the endpoint that is the prime target and source of the majority of problems. In the last year alone, over 38% of businesses suffered a cyberattack, while 39% of attacks aimed at protected endpoints succeeded. In this environment, companies need to be smarter than the cybercriminals attacking them.

For as long as there are humans behind cyberattacks, there will be a need for human intellect teamed with innovative technologies to counter them. Kaspersky Lab's protection is based on our global threat intelligence combined with machine learning algorithms, powered by the human expertise of the industry's top specialists. We call this unique combination HuMachine™, and it's in our products' DNA.

In 2017, Kaspersky Lab won the top award from **Gartner Peer Insights for Endpoint Protection Platforms: the Platinum Customer Award**. The award is the highest possible distinction in the competitive Endpoint Protection Platforms market. Our endpoint applications have achieved the highest percentage (90%) of top-three places in independent tests compared to any other vendor.

Invest in the future

The average financial impact of a single data breach for small and medium businesses is $86.5k and for enterprises $992k. Next-generation anti-virus is no longer enough – only a multi-dimensional solution providing security at both multiple technological layers and functional layers of corporate IT infrastructure can deliver the protection you need. True endpoint security combines a variety of smart techniques and technologies to protect businesses against any kind of cyberthreat, on any platform. If you can protect your whole IT network, you ensure your business continuity.

Protect what you value most with HuMachine™-based applications

As your business matures, your IT security budget may not grow at the same rate. Resources must be optimized to meet the challenges of today – and tomorrow. Kaspersky Endpoint Security for Business, harnessing HuMachine™ intelligence, protects against ransomware, exploits and the most advanced cyberthreats. Resource optimized, it's packed with powerful security controls, automated vulnerability and patch management, integrated encryption and can be controlled from a single console across the corporate network.

Agile, adaptive security

The product is designed to work within any IT environment. It employs a full stack of proven and Next Generation technologies. Built-in sensors and integration with Endpoint Detection and Response (EDR) enable the capture and analysis of large volumes of data to ensure discovery of the most obscure, sophisticated cyberattacks.

Future-driven security for outsourced IT

Built-in multitenancy, together with threat prevention, mobile security, data encryption and vulnerability and patch management, empower Managed Service Providers (MSPs) to add IT security to their offerings.
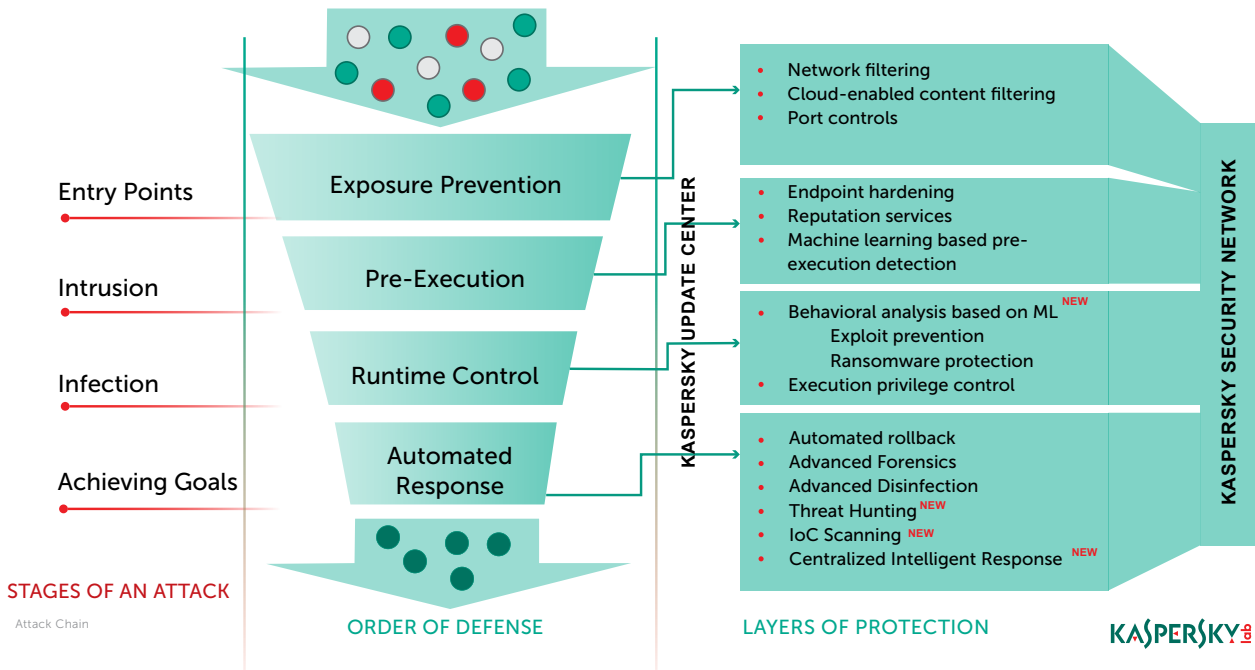
Low footprint; high performance

Our most tested, most awarded HuMachine-based security delivers optimum protection with minimal impact on PC resources. Signature-less components ensure threats are detected even without frequent updates.

Comprehensive protection

Kaspersky Endpoint Security for Business uses several Next Generation technologies (such as endpoint hardening, behaviour analysis based on machine learning, exploit prevention, etc.) to neutralize the majority of threats before they hit the advanced protection layers. Suspicious files that make it as far as the endpoint are detected and blocked.

STAGES OF AN ATTACK
Attack Chain

Entry Points

Intrusion

Infection

Achieving Goals

Exposure Prevention

Pre-Execution

Runtime Control

Automated Response

ORDER OF DEFENSE

KASPERSKY UPDATE CENTER

- Network filtering
- Cloud-enabled content filtering
- Port controls

- Endpoint hardening
- Reputation services
- Machine learning based pre-execution detection

- Behavioral analysis based on ML ^{NEW}
    Exploit prevention
    Ransomware protection
- Execution privilege control

- Automated rollback
- Advanced Forensics
- Advanced Disinfection
- Threat Hunting ^{NEW}
- IoC Scanning ^{NEW}
- Centralized Intelligent Response ^{NEW}

LAYERS OF PROTECTION

KASPERSKY SECURITY NETWORK

This combination of advanced technologies with our multi-layered approach achieves the perfect balance between performance and efficient protection. It plays a critical role in our products achieving one of the highest detection rates in the industry, as continuously demonstrated through independent tests.

Multiple protection layers for

- Windows, Linux or Mac
- Android and other mobile devices
- Removable storage
- Windows and Linux Servers
- Mail servers
- Web gateways
- Collaboration servers

Unparalleled defense against

- Software exploits
- Ransomware
- Mobile malware
- Unknown threats
- Fileless threats
- PowerShell and other script-based attacks
- Web threats
- Email-distributed threats
- Phishing attacks
- Spam

Anti-Ransomware and Anti-Exploit protection
Based on unparalleled sources of real-time threat intelligence and machine learning, our technologies continually evolve. Protect your endpoints from the latest exploits and keep your data and shared folders safe and secure from advanced threats and ransomware.

Block account takeovers
Behavior Detection implements a Memory Protection mechanism, which guards system-critical processes and prevents leaking user and administrator credentials.

Lower your exposure to attack through 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 on desktops and servers. Application Control intercepts the launch of executable files, DLLs and controls scripts executed by a variety of interpreters. Behavior Detection and Exploit Prevention monitor the application's behavior, block potentially malicious activity and protect legitimate applications from being exploited and used by malware. Your approved and trusted applications continue to run smoothly.

Neutralize rootkit
Attackers use rootkits and bootkits to hide their activities from security solutions. Anti-rootkit technology, part of Kaspersky Lab's multi-layered, Next Generation protection, helps detect even the most deeply hidden infection and neutralizes it.

Spot more attacks and intrusions – even the most obscure
Built-in sensors and integration with Kaspersky Endpoint Detection and Response enable the capture and analysis of large volumes of data onshore without impacting on user productivity. It delivers advanced threat hunting for evidence of intrusion – such as indicators of compromise (IoC).

Prevent exposure via network
Malware using a buffer-overrun attack can modify a process already running in the memory and in this way execute the malicious code. The Network Threat Protection identifies network attacks and exploits and stops them in their tracks.

Beyond endpoint protection – now and in the future

Simplify inventory and patching

Discovering hardware and software inventory details and managing the timely patching of vulnerabilities is tedious and time-consuming. Exploiting unpatched vulnerabilities is one of the most common ways cybercriminals attack IT infrastructure through a single endpoint. Going beyond just remote deployment of new third-party software, automated vulnerability assessment and patch management, based on round-the-clock intelligence into exploited vulnerabilities, keeps potentially vulnerable software up to date saving your IT administrators time to spend on other tasks.

Secure data sharing through encryption

User-transparent FIPS 140-2 certified encryption fully secures confidential data on portable devices and on-site. Integrated technology means you can centrally enforce the encryption of corporate data at file, disk or device level and enable secure sharing of data across your network.

Support for remote and mobile scenarios

Data has become accessible anytime, travelling freely through the perimeter. Mobile security protects against threats specifically targeting data on the move, as well as attempts at using weaknesses in devices as springboards for subsequent infrastructure infiltration. Device Control guards against the consequences of data loss on unapproved or unencrypted portable devices and the uploading of infected data from the device.

Optimize efficiency with management for all platforms

A single console gives you full visibility and control over every workstation, server and mobile device, wherever it's located and whatever it's doing. Almost infinitely scalable, the solution provides access to licensing, remote trouble-shooting and network controls. Centralized management is complemented by Active Directory integration, role-based model and integrated dashboards.

Regulate access to sensitive data and recording devices

Our solution restricts application privileges according to assigned trust levels, limiting access to resources like encrypted data. Working in step with local and cloud (KSN) reputations database, Host Intrusion Prevention System (HIPS) controls applications and restricts access to critical system resources, audio and video recording devices.

Stop Web threats before they reach your endpoints

By stopping the majority of incoming threats at the gateway level, we significantly reduce the impact of the human factor and workstation security specifics by not letting them reach the endpoints.

A secure gateway remains the first line defense for the majority of corporate security scenarios, despite the penetration of mobility into the working processes. Our security technologies filter traffic flowing through the gateways, automatically blocking incoming threats before they reach your endpoints and servers. This significantly reduces the risk of vulnerability exploitation and considerably reduces operational overheads for IT security staff.

Increase productivity and reduce threats

Kaspersky Lab's cloud-assisted, Next Generation anti-spam detects even the most sophisticated, unknown spam with minimal loss of valuable communication due to false positives. Reducing the time wasted, resources and risks associated with spam by stopping it in its tracks saves system and human resources. The protection incorporates multiple proactive security layers, including machine learning and cloud-assisted threat intelligence, to filter out malicious attachments, known and previously unknown malware in incoming mail.

Enable secure collaboration

Our security for Microsoft SharePoint® includes anti-malware, content filtering and file filtering, to help your business enforce its collaboration policies and prevent inappropriate content from being stored on your corporate network.

Kaspersky Endpoint Security for Business lets administrators see, monitor, control and protect their IT environment. The Next Generation tools and technologies are intelligently balanced across the progressive tiers to meet your evolving security and IT needs at every point in your business journey.

Kaspersky® Total Security for Business

Businesses that have mature IT environments – with a mix of recent and legacy systems – need to fine-tune their security for different systems. Our most comprehensive security solution for endpoints, infrastructure and collaboration servers lets you do just that – so you get rigorous security that you can tailor to your IT estate.

Kaspersky® Endpoint Security for Business Advanced

For security that works harder to protect your business, choose **Kaspersky Endpoint Security for Business Advanced**. As well as securing all your endpoints and servers, it delivers extra security layers to protect sensitive data and eliminate vulnerabilities – and it helps simplify systems management tasks too.
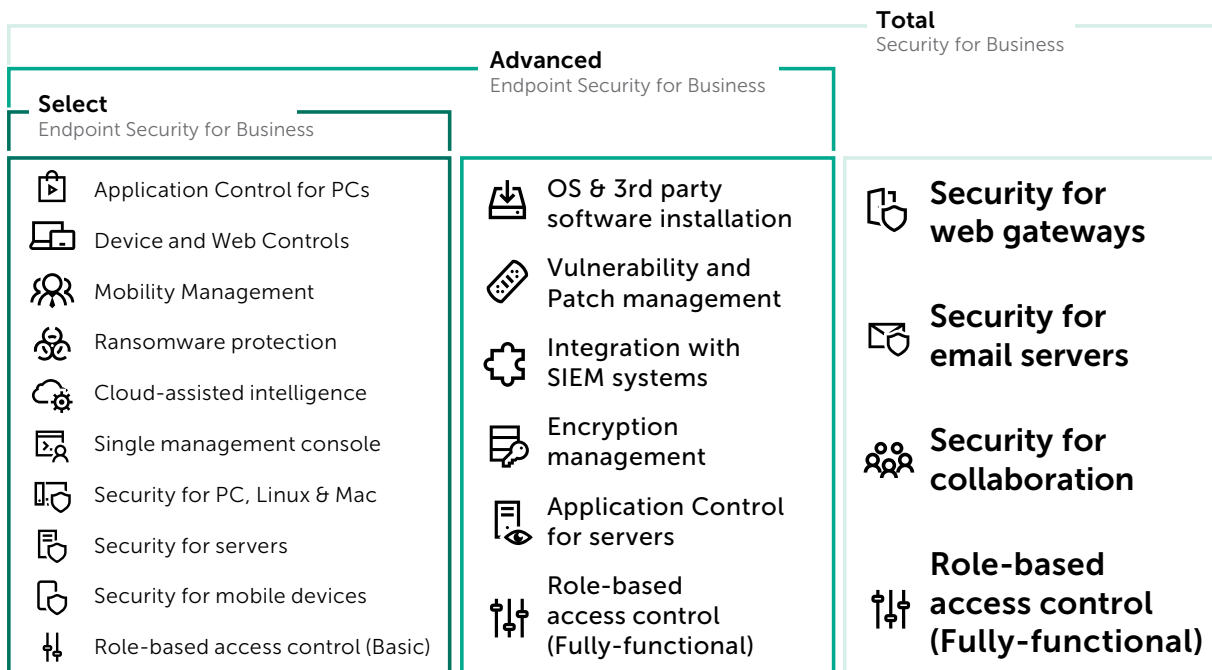
Kaspersky® Endpoint Security for Business Select

With more of your business operations going digital, you need to protect every server, laptop and mobile device. We deliver Next Generation security that helps you protect every endpoint your business runs, in a single solution with one flexible management console.

Which tier is right for you?

Whatever your unique, evolving IT needs, **Kaspersky Endpoint Security for Business** has the ideal solution for you.

Select Endpoint Security for Business	**Advanced** Endpoint Security for Business	**Total** Security for Business
Application Control for PCs	OS & 3rd party software installation	Security for web gateways
Device and Web Controls	Vulnerability and Patch management	Security for email servers
Mobility Management	Integration with SIEM systems	Security for collaboration
Ransomware protection	Encryption management	Role-based access control (Fully-functional)
Cloud-assisted intelligence	Application Control for servers	
Single management console	Role-based access control (Fully-functional)	
Security for PC, Linux & Mac		
Security for servers		
Security for mobile devices		
Role-based access control (Basic)		

Adding more security as you need it

Automating and centralizing the discovery of software vulnerabilities and patch management helps protect against the more dangerous threats, including ransomware. For **Kaspersky Endpoint Security for Business Select** customers, this automation is available with the **Kaspersky Vulnerability and Patch Management Add-on**.

Also for Select customers, the **Kaspersky Encryption Add-on** enables Full Disk, File Level Encryption, utilizing strong encryption algorithms and featuring support for Single Sign-On for immediate access to encrypted files, as well as for smartcards/tokens for two-factor authentication. It lets you encrypt files and folders that are stored on local and removable drives.

For even more security without any additional complexity, just activate the required feature set from within Kaspersky Security Center.

Why upgrade your current endpoint protection?

Always have the latest technologies – quick and easy: one server, one console, single agent

Support any business process via deeper integration – single code base, built in-house

Avoid hidden cost and separate licensing – all the functionality you need in a single purchase

Enhanced audit and control capability; unified management with role-based access

At Kaspersky Lab, we develop and perfect all our own technologies in-house, which makes all our applications more stable and more efficient. We are committed to our own R&D and incorporate many technological innovations into our products. Just some examples:

- Multi-layered Machine Learning: using Machine Learning methods at different stages of the killchain on endpoints and in the cloud.
- Active hunting for threats as a result of the integration between endpoint protection and Endpoint Detection & Response or Anti Targeted Attack solutions.
- Unique cloud mode for protecting components delivers optimum protection with minimal impact on PC resources and Internet bandwidth usage.
- Support for Microsoft Windows Server containers, external traffic security and firewall management.
- Enhanced Device Control and Anti-Bridging functionality.
- Enhanced Application Control with Trusted Certificates category and Test Mode for policies.
- The new clean user interface visualizes the multi-layered protection, showing the status of protection and the effectiveness of Kaspersky Lab's latest technologies in action.

True Cybersecurity: It's In Our DNA

Kaspersky Lab delivers powerful cybersecurity solutions using the world-leading threat intelligence that's built into our DNA and influences everything we do. As an independent company we are more agile, think differently and act faster.
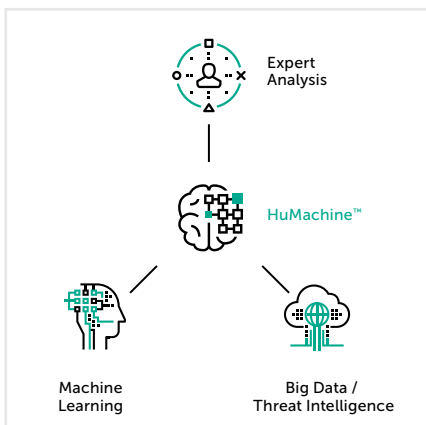
- **Our expertise is from the top down** – starting with our CEO, Eugene Kaspersky.
- **Our Global Research & Analysis Team (GReAT)** – elite group of security experts has discovered many of the world's most dangerous malware threats and targeted attacks.
- Our groundbreaking **Global Transparency Initiative** is further evidence of our commitment to protecting customers from cyberthreats, regardless of their origin or purpose.

Build up your GDPR compliance with True Cybersecurity
Kaspersky Lab raises awareness about the cybersecurity-related aspects of GDPR. Our solutions help customers reduce the risks of a data breach and prevent security incidents. We also help our customers' DPOs with enhanced visibility of the monitored infrastructure.

The Bigger Picture – Kaspersky IT Security Solutions for Business

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 products that interlock or work independently, so you can pick and choose without sacrificing performance efficiency or freedom of choice. Learn more on our website.

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence

Kaspersky Lab
Find a partner near you: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
True Cybersecurity: **www.kaspersky.com/true-cybersecurity**
IT Security News: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com