Kaspersky®
Endpoint Security
for Business

Threat Protection

Any security solution is only as effective as the threat prevention engine it's built on. Patch management, encryption, application controls – all these technologies provide valuable additional security, but can't and won't compensate for shortcomings in fundamental threat protection.

Threat protection sits at the heart of every one of our security solutions, products and services. Our multi-layered adaptive approach is based on a spectrum of components, many of them unique, developed to counter different forms of cyberthreat at different levels. The result is an arsenal of next generation defensive and proactive anti-threat technologies, which together enable today's most sophisticated and advanced threats, and even those of tomorrow, to be rapidly detected, mitigated and repelled.

Threat expertise and research

Next generation protection based on our unique HuMachine™ approach – leveraging the combined strengths of Machine Learning, Human Expertise and comprehensive Threat Intelligence. Kaspersky Lab has always led the field in terms of threat intelligence – we have discovered more APTs than any other vendor, and our commitment to investment in future protection technologies is reflected in the size and global reputation of our research teams.

Kaspersky EDR – a true threat hunting tool

Integration with Kaspersky Endpoint Detection & Response delivers automated incident response capabilities. This comprehensive approach to EDR increases visibility across your corporate IT infrastructure, allowing SOC teams make informed decisions about the best strategy to mitigate both low-priority malware and the most advanced threats. EPP and EDR functionality work together through a single agent.

Multi-layered protection powered by advanced technologies

Multi-dimensional protection achieved through a combination of threat prevention technologies powered by Machine Learning algorithms. Advanced endpoint controls and systems hardening, including application control and whitelisting, behavioral detection, automated remediation, exploit prevention and anti-ransomware protection are all incorporated into our endpoint security platform. Protection against PowerShell and fileless attacks is also provided.

Enterprise-grade manageability

The ability to manage hundreds and thousands of endpoints through a single unified console, giving granular control and comprehensive visibility across your whole infrastructure, both on-premises and in the cloud. Enterprise scenarios include automated deployment, health status check, and automated reporting, together with full support for hierarchical and air-gapped environments.

Features

Essential Threat Protection

File Threat Protection

A mandatory component of anti-malware security, deploying a complete spectrum of protection technologies against file-based threats. Includes Windows Subsystem for Linux (WSL) scanning.

Mail Threat Protection

Email is one of the exposure points most exploited by cybercriminals. Mail Threat Protection scans incoming and outgoing email messages for dangerous objects.

Web Threat Protection

To ensure safe and secure working with internet resources, incoming and outgoing data is protected and URLs are checked against lists of malicious or phishing web addresses. Web Threat Protection also scans HTTPS traffic for early interception of the latest threats (botnet agents, droppers, ransomware etc).

Network Threat Protection

Scans inbound network traffic for activity typical of network attacks. Protection against MAC Address Spoofing further hardens your infrastructure by helping identify and block attacks where addresses are changed to compromise endpoints and intercept traffic addressed to other network devices.

Firewall

Restricts network activity associated with the protected node. Preset rules cover the filtration of network packets and data streams, and software-based network interactions.

BadUSB attack prevention

Some viruses modify the firmware of USB devices so the operating system detects the device as a keyboard. BadUSB Attack Prevention implements a keyboard authorization procedure to identify infected USB devices emulating a keyboard. The application allows the use of authorized keyboards and blocks the unauthorized.

AMSI (Anti-Malware Scan Interface) Protection Provider

Enables Kaspersky Endpoint Security to scan objects sent by third-party anti-malware validation apps, Results are forwarded to the requesting application, which can then block/delete the object.

Advanced Threat Protection

Kaspersky Security Network (KSN)

A complex cloud infrastructure collects and analyzes cyber-security-related data from millions of voluntary participants around the world, detecting malware and providing the fastest possible reaction to new threats.

Behavior Detection

Provides proactive defenses, utilizing techniques including Machine Learning to identify and extract suspicious behavior patterns, effectively protecting your system against ransomware. Malicious local file encryption and the remote encryption of shared folders via the network can be identified, halted and mitigated.

Exploit Prevention

Specifically targets malware that exploits software vulnerabilities in popular applications, by recognizing typical or suspicious behavior patterns, halting the exploit in its tracks, and preventing any downloaded malicious code from executing.

Host Intrusion Prevention (HIPS)

Assigns every application to one of four default trust groups based on KSN data. Those from the most trusted group are whitelisted and run with no limitations. The rest will run with limited privileges and limited access to critical system resources.

Remediation Engine

Collects data about suspicious activity, enabling Kaspersky Endpoint Security to roll back actions that have been performed by malware in the operating system.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**
Our unique approach: **www.kaspersky.com/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.com