Kaspersky® Endpoint Security Cloud

Strong on protection Easy on management

All businesses are vulnerable to the same expanding range of cyberthreats – but some businesses are more prepared than others.

Cybercriminals know that enterprises and multinationals have invested heavily in IT security. That's why the criminals are launching more attacks against medium-size businesses – that they now regard as 'soft targets'.

Kaspersky Endpoint Security Cloud Up and running in no time

A single attack – against an unprepared business – can result in:

- Loss of sensitive business data – including intellectual property
- Leakage of confidential information about customers and employees
- Damage to employee productivity – which directly affects profitability

Because small-to-medium-size businesses can't afford the extensive, in-house IT teams that larger businesses have, they need security that's easy to set up & run – and even enables remote management by external consultants.

Kaspersky Endpoint Security Cloud covers the specific needs of small-to-medium-size businesses – helping to secure all their Windows and Mac endpoints, Windows file servers and Android & iOS mobile devices. Its industry-leading protection is rapid to implement, roll out and run. There's no need to buy additional hardware – and all security settings can be managed from the cloud, via any online device.

The most tested & most awarded security

For three years in a row, our security technologies have been the most tested and most highly awarded. In a wide range of independent tests, our products consistently achieve more first place awards and more Top 3 ratings than any other vendor's (for details, please see https://www.kaspersky.com/top3).

Centralized management simplifies security

All security functions – across all Windows and Mac desktopts and laptops, Windows file servers plus Android and iOS mobile devices – can be set up and managed via a central management console. You don't need any special IT security skills to operate the console and manage your security – plus it's easy to define security policies that you can apply across all your endpoints.

Cloud-based console – for simple and flexible administration

The ready-to-use, cloud-based console lets administrators use almost any online device to set up and adjust all protection features – for all endpoints. If you choose to subcontract your IT security management, the cloud-based console makes it easy for your external consultant to manage your security remotely. Because the console is hosted in the cloud, you won't need to buy or maintain any additional hardware – and initial set up can be extremely rapid.

Features

Protects all your devices

Award-winning security technologies protect Windows and Mac PCs and Windows file servers against known and unknown IT threats – including cryptors and other types of ransomware attacks. Multiple layers of security include traditional, proactive and cloud-as-sisted anti-malware for files, mail and Web – plus our powerful Firewall, Network Attack Blocker and System Watcher technologies. The solution is delivered with default security policies – developed by our security experts – so all your devices can benefit from immediate protection.

Controls access to devices and the Internet

Device Control tools make it easy to manage which devices are allowed to access your corporate IT network. Web Control tools help you to set up Internet access policies and to monitor Internet usage. Application Privilege Control restricts activities within the endpoint, according to the 'trust level' that has been assigned to the application.

Simplifies management of mobile devices

Our mobile device management (MDM) functionality includes remotely operated features that make it easy to enable smartphones and tablets onto your corporate network, define Wi-Fi network & Bluetooth configuration, control password complexity, manage camera usage and regulate other parameters. Because the iOS MDM server is automatically deployed in the cloud, you won't need any additional hardware to manage your iOS devices.

Protects against mobile threats

Advanced mobile security technologies help to defend your Android and iOS devices against the latest mobile threats – including the growing number of cryptors and other attacks. Anti-phishing protects against websites that try to steal confidential information or identity details. Rooting and jailbreak incidents are automatically detected – so insecure devices can be automatically blocked. Call & text filtering – for Android devices – helps you filter out unwanted calls and texts.

Ready to run – and easy to roll out

Because all functions are managed from the cloud, there's no need to download a management console onto any of your servers. Instead, you just visit the cloud-based console – at cloud.kaspersky.com – and start rolling out the security software to your PCs, file servers and mobile devices.

Safeguards sensitive data – even on lost devices

If a mobile device is lost or stolen, remotely operated security features help to protect your corporate data. Administrators can lock the missing device – and either delete all data or only delete corporate data.

Free trial – running on your desktops, laptops, file servers and mobiles
Visit cloud.kaspersky.com and get a **free**, 30-day trial of the full version of Kaspersky Endpoint Security Cloud. At the end of the trial, if you choose to buy, you just pay the license fees – and, as Kaspersky Endpoint Security Cloud has already been running on your endpoints during the trial, there'll be nothing more for you to set up.

Supported platforms

Windows and Mac OS

Windows file servers

Android and iOS devices

Kaspersky Lab
Kaspersky for Business: **www.kaspersky.com/business**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com