



Kaspersky Endpoint Security Cloud

Endpoint protection for agile
businesses

kaspersky

Day-to-day agility

Kaspersky Endpoint Security Cloud is built for agile businesses

Your business is growing. The number of the IT security tasks you need to deal with keeps growing too. But you're not yet ready to hire a dedicated security specialist. So we've created **Kaspersky Endpoint Security Cloud Plus** to help you manage routine security tasks with ease, saving you time and money.

And **Kaspersky Endpoint Security Cloud Pro** goes even further – providing the peace of mind that comes with protection against even evasive threats, as your security matures.

Kaspersky Endpoint Security Cloud is built for agile businesses. From the straightforward user interface through easy deployment and smooth operations, from onboarding new employees to day-to-day maintenance, it's simple to administer, and ready to protect your organization from the latest current and emerging cyberthreats.



Try on a new cybersecurity specialist hat with our EDR capabilities

Start with Root Cause Analysis (included in our Plus license), then move up to Kaspersky Endpoint Security Cloud Pro, adding automated response options like IoC scan and host isolation.

Let's face it, IT admins wear a lot of hats, and cybersecurity is usually just one of many. Although smart admins understand the need for strong cybersecurity solutions, it's just not their area of expertise. Meanwhile, threats keep evolving, and those that used to be seen as rare or only targeting the 'big guys' are becoming commonplace and ubiquitous. So it's important from a budgetary perspective to choose a solution that's regularly upgraded with cutting-edge technologies, so you'll be fully protected well into the future, without the need for further significant investment.

Endpoint Detection and Response gives you access to an enterprise-grade cybersecurity tool and the opportunity to skill-up in evasive threat detection and response. At the same time, our approach promises that your overall EDR user experience will be smooth and straightforward, and won't require any changes to your infrastructure.

Our **Root Cause Analysis** offers advanced threat detection and visibility capabilities, together with access to professional incident investigation tools, without any infrastructure adjustments.

So now you as an IT admin can conduct incident investigations using context and details of the incident. You can perform root cause analysis with attack spread-path visualization, and drill down into the details to review:

- Host data: OS version, network interfaces and users
- File data: name, hash, creation and modification parameters, download parameters, etc.
- Process data: date and time, startup parameters
- Related detects and incidents and more

Automated response options will help you stop threats in their tracks, preventing file execution, using host isolation and IoC (Indicator of Compromise) scan checks. In the event of an attack, the system isolates the host from your network, stopping the attack from spreading to other devices. IoC scan then checks all devices for IoCs similar to that involved in the initial attack, quarantining any that may be affected.

Confidently wearing your security hat, you can now secure and protect the network, answer questions and automatically pull the emergency trigger. Imagine how much happier you could be... and you can look forward to many a better night's sleep from now on.



Stop 'Shadow-IT' chaos and take control of your cloud services

Cloud Discovery lets you block user access to unnecessary, inappropriate and unauthorized cloud resources, keeping your data securely under your control and your colleagues focused and productive.

Look at your fellow-workers – can you tell who's wasting time on Facebook right now, and who's chatting on instant messaging?

And, even more importantly, who's sharing corporate data on cloud storage services you know nothing about? Right – you have no idea. So Cloud Discovery, included in Kaspersky Endpoint Security Cloud, is here to help.

Cloud Discovery lets you see the real picture and develop an action plan. You can block user access to unnecessary, inappropriate and unauthorized cloud resources, keeping your data securely under your control and your colleagues focused and productive. In just a few clicks, you'll have a full picture of cloud usage in your infrastructure – via an interactive widget or exportable report. Armed with these statistics, you can highlight to management the problem of uncontrolled corporate data sharing and disclosure, as well as the time being wasted by employees on social networks and messengers.

In many cases this opens growth opportunities. People don't usually set out to cause harm by using unsanctioned cloud services. Very often, they're just trying to work more efficiently. If, for example, you've implemented a corporate video-conferencing solution or cloud CRM, but your users turn out to be still using public ones or populating google docs tables – it's worth asking why.

The answers may surprise you. They could include problems using corporate software, old usage habits, a lack of knowledge, or just a missed email about new company policies. Issues like these can slow digital transformation and overall business growth. Cloud Discovery analytics can point the way to better user education and security hygiene improvement.

A simple, cost-effective alternative to purchasing an expensive and complicated **CASB (Cloud Access Security Broker)** solution, Cloud Discovery will help you detect and block the use of unauthorized cloud services and shadow IT as part of your standard cyber-defenses, with no special skills needed.





Security for Microsoft Office 365 included

Even with Cloud Discovery on board you may, like many businesses, have security concerns about Microsoft Office 365. To further help you take your cloud under your control, we include Office 365 protection with **Kaspersky Endpoint Security Cloud Plus** and **Pro** tiers. With every 10 licenses, we provide Kaspersky Security for Microsoft Office 365 protection for 15 mailboxes/users. **Our Office 365 security solution offers advanced**, all-in-one threat protection for Microsoft Office 365 communication and collaboration services including:

- **Microsoft Exchange Online, OneDrive, SharePoint Online and Teams**
- **Advanced threat protection: anti-phishing, anti-malware, anti-spam, unwanted attachment removal and protection on demand**



GDPR compliance with minimum hassle

GDPR compliance is non-negotiable, no matter what size your operation. Data Discovery, also included in **Kaspersky Endpoint Security Cloud Plus** and **Pro** tiers, gives you the visibility and control you need to prevent data leaks and stay compliant. Now you can see exactly where and why every piece of data you're responsible for is being stored and processed in the cloud, check whether personal data could be accessible by external parties, spot data that's being stored longer than it should, and much more. Keeping fully compliant suddenly becomes so much simpler.

Patch management for the laid-back

Nobody enjoys manually patching devices, but it's something that has to be done regularly for cyber-hygiene reasons: like brushing your teeth, it's boring but effective. So why not relieve yourself of the hassle, and leave everything to the automatic scheduled patch management? It's included in both **Kaspersky Endpoint Security Cloud Plus** and **Kaspersky Endpoint Security Cloud Pro**

Effortless device encryption

FileVault (macOS) and BitLocker (Windows) based disk drive encryption can also be managed through the Kaspersky Endpoint Security Cloud console, and encryption can be applied remotely if needed.

Almost every organization collects and stores different forms of personally identifiable information, financial data, confidential documents and other sensitive data in their IT systems. Disclosure or loss of this data can lead to fines and prosecution, and can have a highly negative impact on the business overall. Data Encryption helps ensure this data won't be compromised should your system be breached or a device stolen.

Efficient endpoint agent deployment - AD (Active Directory) or not AD?

Download your Kaspersky Endpoint Security client, then add the simple logon script provided to your AD domain policy

With just a handful of computers to look after, it's easy enough to install endpoint protection using just a flashdrive. Once you're up to 50-100 devices, things become less straightforward – but deployment should still be rapid and hassle free.

Kaspersky Endpoint Security Cloud offers two installation modes, depending on what works best for you:

1. Remote deployment via email

A link is emailed to each device via the **Kaspersky Endpoint Security Cloud console**. The user clicks on the link to activate application download and installation on the endpoint, after which the endpoint will be visible in the list of protected devices on your console.

2. Automatic deployment with AD (Active Directory)

Download your **Kaspersky Endpoint Security client**, then add the simple logon script provided to your AD domain policy. The application will automatically deploy onto your endpoints, and you'll see them listed as protected devices in the **Kaspersky Endpoint Security Cloud console**. Check out the instructions [here](#).

Go ahead and see for yourself!

For more about how Kaspersky Endpoint Security Cloud can help your clients protect their businesses the easy way, and to try us out for yourself, please visit <https://cloud.kaspersky.com/>

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

2022 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.



We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/about/transparency



Proven.
Transparent.
Independent.