kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Security Cloud

How to build managed IT security services with Kaspersky Endpoint Security Cloud Tips and tricks

There's a massive market opportunity out there for anyone ready to reach out and take it. So what's your excuse for not selling managed IT security services? No security experience? Not an issue. Don't have time to skill up? You don't need to. With Kaspersky Endpoint Security Cloud, you can be up and running your own IT security services practice in minutes, with no setup, implementation or maintenance costs, and no special skills needed. It really is that easy.

So get out there!

More and more SMBs prefer peace of mind to running the risk of economizing on cybersecurity. They're looking to MSPs like you to give them that peace of mind, by providing them with security as a service. And they're prepared to pay for it.

Kaspersky Endpoint Security Cloud is a simple-to-use product that can set you on the path to providing a number of cybersecurity services, based on our portfolio. It's delivered totally from the cloud, takes only minutes to sign up to, and comes with predefined security policies and web-based management – the ultimate combination for remote services providers. You'll love how agile it is to use, and just how effortless.

Here's a suggested service plan, split into three easy 'offer and upsell' levels. Each contains an anchor feature, helping lead your client to considering an upgrade to the next level.

Must Have	File Threat Protection aka antivirus	Anti-ransomware	Vulnerability assessment
	Web threat protection	Firewall	Mail Treat protection
			upsell
Wise Decision Includes Must Have plus	Device control	Encryption management	Patch management
	Web control		
		upsell	
Confident Enough Includes Wise Decision plus	Office 365 threat protection		

- 'Must Have' capabilities can be delivered with the Kaspersky Endpoint Security Cloud license.
- Web and Device controls, Patch management and Encryption management require the purchase of Kaspersky Endpoint Security Cloud Plus License.
- Office 365 threat protection requires the purchase of a Kaspersky Security for Microsoft Office 365 license.

No travel costs for your technicians – everything can be done remotely.

No on-premises deployment - we host your management console for you in the cloud

No customer site visits – endpoint agent distributives can be emailed to any user

Corporate device protection

File Threat Protection. Prevents computer file systems from becoming infected. Files opened or run on an endpoint or any attached drives are continuously scanned for viruses and other threats.

Anti-ransomware. Protects against ransomware, screen lockers, and exploits, as well as rolling back any changes made to the operating system by malicious or infected applications.

Firewall. Protects corporate data stored on the user's computer, blocking threats to the operating system as long as the computer's connected to the internet or a local area network. The firewall can detect and block different network connections - so you can, for example, increase the security of an endpoint by blocking all remote connections.

Vulnerability assessment. Identifies vulnerabilities in operating systems, Microsoft and other applications, and offers update recommendations. A vulnerability is a flaw in an OS or application that can be exploited by malware makers to penetrate the IT system and introduce threats.

Patch management. Enables the timely and automated patching of detected vulnerabilities in Windows, Microsoft and a number of third-party applications.

Corporate Data protection

Device control. Ensures the security of confidential data by blocking or restricting the connection to endpoints of devices, such as USB sticks, that could enable the downloading of sensitive corporate data or the uploading of an infection.

Encryption management. Prevents other users from gaining unauthorized access to data stored on the user's device. Encryption is an essential way to prevent data exposure if a device is stolen or lost.

User protection on the Internet

Web threat protection. Every time someone goes online, information stored on the system is exposed to viruses and other malware. These can infiltrate the computer while the user is downloading free software or browsing websites that have been compromised by criminals. Network worms can find a way onto a computer as soon as the user establishes an internet connection - even before they open a web page or download a file.

Web control. Can be used to block or restrict access to unnecessary, time-wasting or inappropriate websites, reducing traffic and helping users become more productive. Blocking file sharing services also prevents employees from sharing corporate data to their own accounts in applications like Box or Dropbox.

Communications protection

Mail threat protection. Ensures that files received via email are safe, by scanning both incoming and outgoing messages for viruses and other threats.

Office 365 protection and management. Provides extended protection against viruses, phishing and other threats in MS Office. Available for Exchange Online and OneDrive. A dedicated license is required.

How to upsell

Vulnerability Assessment → **Patch Management**

Offer your customer a test drive by installing and running vulnerability assessment. This should generate a long list of recommendations on updates needed. Then offer regular patching to deal with these recommendations, and to strengthen the customer's system against cyberattacks. The automated patch management included in Kaspersky Endpoint Security Cloud Plus makes delivering a remote patching service quick and easy.

Web control → **Office 365 protection**

Demonstrate how web control blocks web applications that the customer's employees may well be using to store valuable corporate data on - without anyone in IT agreeing, or even knowing. This is a great solution to stop a really big problem - uncontrolled data exfiltration. While talking about file sharing, check whether your client is using Microsoft Office 365. As more companies are adopting this cloud collaboration platform and moving their email to Exchange Online and file sharing to OneDrive, those services should also be secured to avoid a data breach. Kaspersky Security for Microsoft Office 365 effectively secures Exchange Online based mail traffic, and files shared on OneDrive, at a fraction of a cost of Microsoft's security offerings.

Mobile Security as a bonus or marginal extra service

Secure mobile working

Your customers need to know their corporate data is fully protected on their employees' mobile devices. With mobile protection, you can remotely manage antivirus on all these devices, enforcing password management policies and taking all the actions needed if a device is lost or stolen.

Enables you to provide a mobile device protection service with unlimited margins, on your terms. Each user license already includes protection for 2 mobile devices without any additional cost to you. You can push mobile antivirus agents to mobile devices remotely, enforce password management policies, restrict features and of course locate, lock or wipe lost or stolen devices. All these functions are very straightforward to manage remotely from the cloud console, no matter where you or your customers are located.

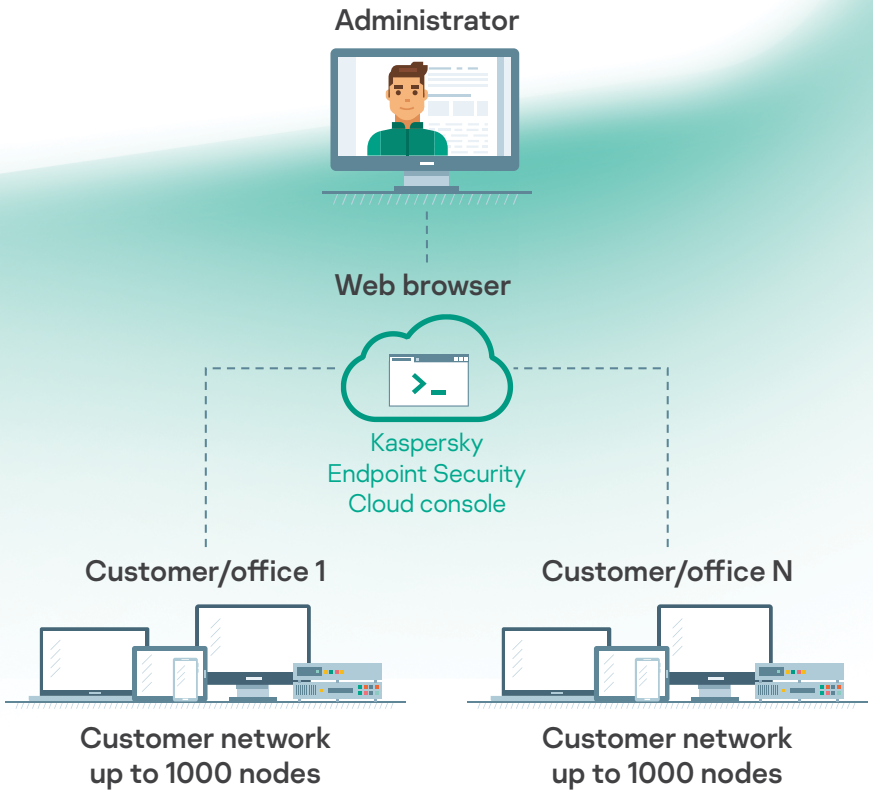
Benefits for MSPs

Multi-tenant management console – multiple client management from a single console, using just one account.

Integration - with popular Remote Monitoring and Management (RMM) and Professional Services Automation (PSA) tools for optimum efficiency

Multiple administrator capability – share security management roles with your customers if required

Flexible monthly billing – change the number of protected nodes, connect new customers, and pay only for the maximum number of nodes supported in any one month.



Want to talk?
Contact us at
kaspersky.com/msp

Ready to enroll?
Register now at
partners.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

2019 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/transparency

Proven.
Transparent.
Independent.