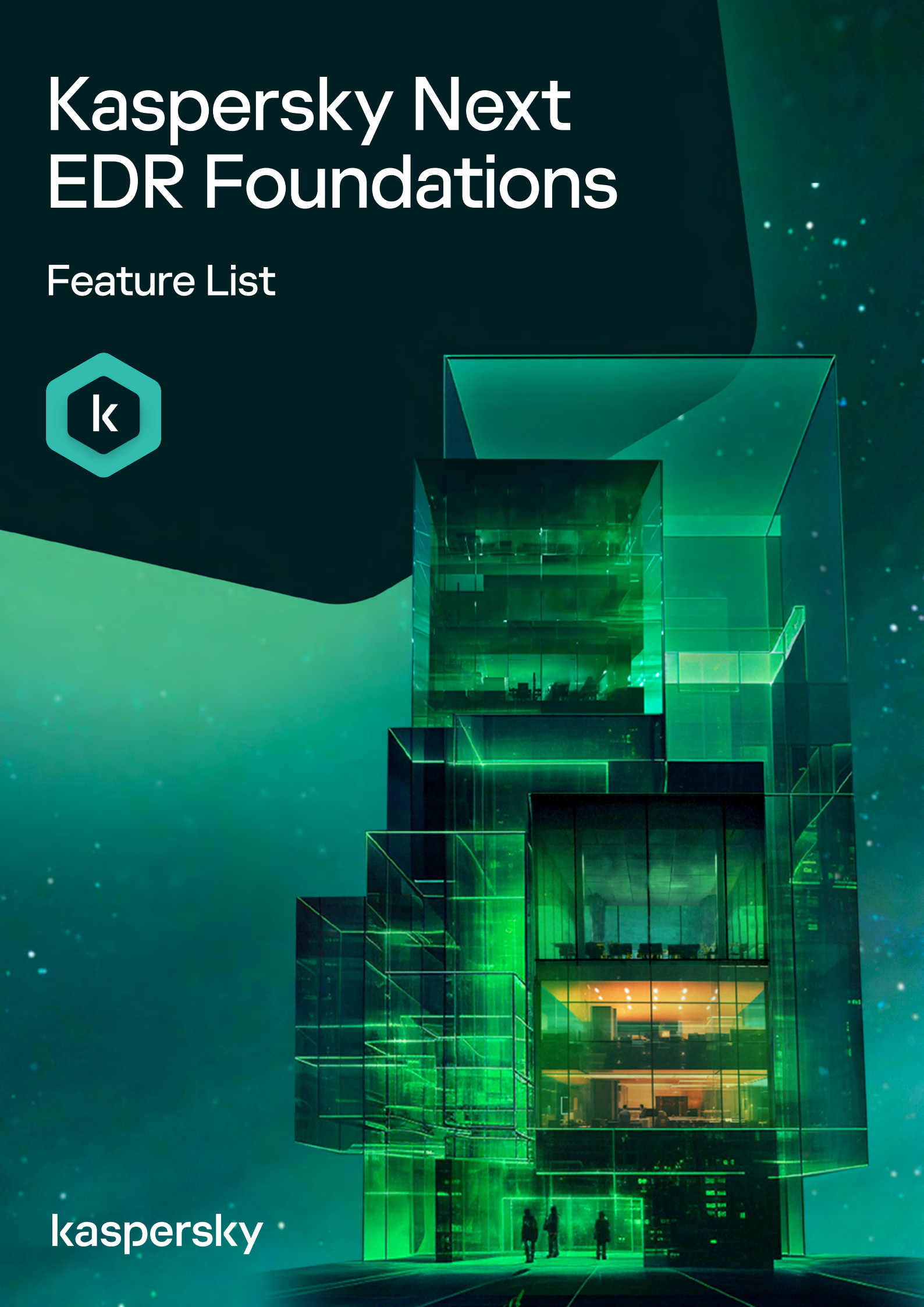
Kaspersky Next EDR Foundations

Feature List



kaspersky

Contents

What is Kaspersky Next?

Kaspersky Next is your new security bedrock. Real-time protection, threat visibility, investigation and response capabilities of EDR and XDR are delivered through progressive tiers, responding to your needs and available resources. This, together with cloud and on-prem deployment options, makes choosing your security easy, and growing your security quick and painless.

Kaspersky Next

Kaspersky Next EDR Foundations

Robust security for everyone

Protect all your endpoints

If you need
- Strong endpoint protection
- Basic security controls
- Maximum automation

Kaspersky Next EDR Optimum

Build up your defenses

Boost your security with essential investigation and response

If you need
- Enhanced visibility and response capabilities
- Expanded cloud security
- Enterprise-grade controls

Kaspersky Next XDR Expert

Equip your experts

Protect your business against the most complex and advanced threats

If you need
- Advanced threat detection
- Seamless integration
- Powerful threat-hunting tools

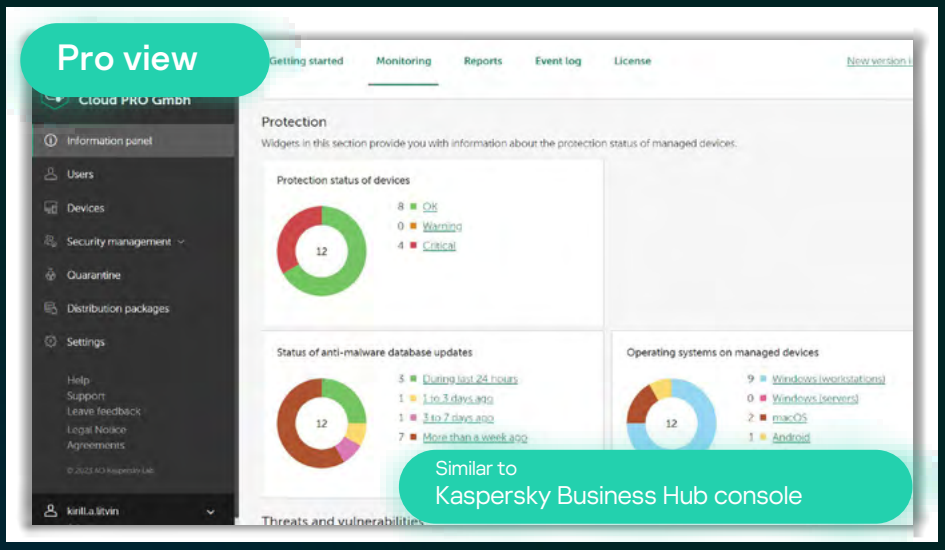
What is Kaspersky Next EDR Foundations?

Kaspersky Next EDR Foundations provides straightforward, affordable protection to keep your business running smoothly while Kaspersky blocks ransomware, file-less malware, zero-day attacks and other emerging threats. With Kaspersky Next EDR Foundations you can perform root-cause analysis with a visualized killchain and drill down into the details for further review.

Features

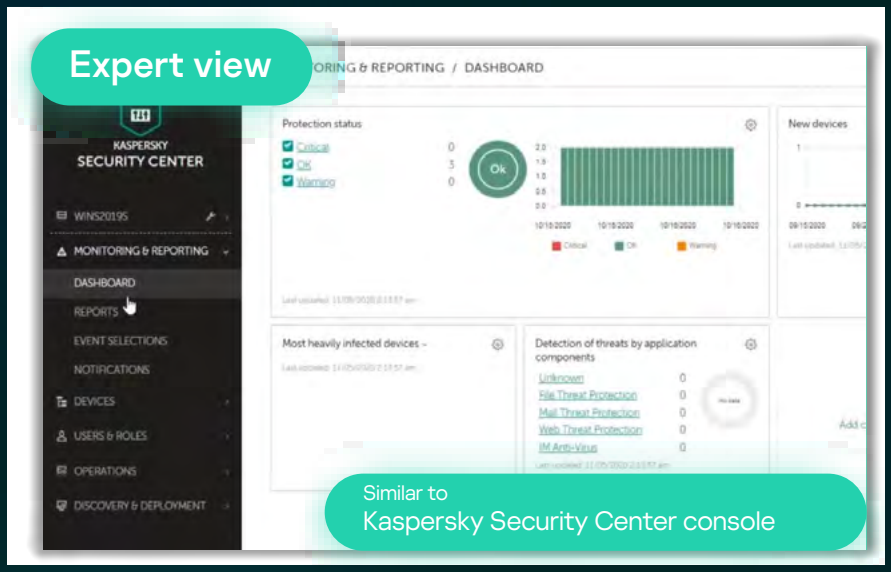
A word about management consoles

There are a number of different ways in which you can choose to manage your Kaspersky Next EDR Foundations:



Pro view: A streamlined, easy-to-manage console hosted in the cloud.

Maximum number of managed hosts: 2,500



Expert view: A customizable console with granular controls, that provides three options:

- Cloud based. Doesn't make any demands your hardware for management server installation or on your team's time for updating – everything's hosted and supported by Kaspersky.
- Minimum number of managed hosts: 300
- On premises, web console. Provides a web interface for creating and maintaining the protection system
- On premises, MMC. Implemented as a snap-in for Microsoft Management Console (MMC)

Endpoint protection

Feature	Description
Multi-layered anti-malware	Our latest anti-malware engine combines signature-based protection, heuristic and behavioral analysis plus cloud-assisted technologies to protect your Windows workstations from known, unknown and advanced malware threats. Pattern-based detection technology improves detection rates and helps reduce the size of update files, so you benefit from reliable security that consumes less of your communications bandwidth.
Behavior detection	Collects information about the actions of applications on a user's computer and provides this information to other components for more effective protection.
Exploit prevention	Tracks executable files run by vulnerable applications. When there's an attempt that wasn't initiated by the user to run an executable file from a vulnerable application, the component blocks the file from running.
Remediation engine	Lets you roll back actions performed by malware in the operating system, delivering protection against cryptolockers.
File threat protection	Anti-virus detects and eliminates threats on a device in real-time by using the application's anti-virus databases and the Kaspersky Security Network cloud service.
Mail threat protection	This security application component scans incoming and outgoing email messages for threats. It starts when the application starts, resides in the device RAM, and scans all messages sent or received via the POP3, SMTP, IMAP and NNTP protocols.
Web threat protection	This component protects incoming and outgoing data that's sent to and from a device over HTTP, HTTPS and FTP protocols, and prevents dangerous scripts from running on the device.
Firewall	The firewall protects each endpoint against network threats when browsing the internet or using a local network. It blocks unauthorized network connections to the computer, reducing the risk of infection. It monitors the network activity of applications on the device, which reduces the risk of malware propagation in the network. It also restricts actions performed by users who violate the organization's security policy (intentionally or otherwise).
Host Intrusion Prevention (HIPS)	Host Intrusion Prevention prevents applications from performing actions that may be harmful to the operating system, and controls access to operating system resources and personal data.
Network threat protection	This component scans a device's inbound network traffic for activity typical of a network attack, such as the intrusion of a remote device into the operating system. When Network Threat Protection detects an attempted network attack on the device, it blocks network activity from the attacking computer.
BadUSB attack prevention	Prevents infected USB devices that emulate a keyboard from connecting to the computer. When a USB device is connected to the computer and identified as a keyboard by the operating system, the application prompts the user to enter a numerical code generated by the application. This procedure is known as Keyboard Authorization.
AMSI protection	Supports Antimalware Scan Interface (AMSI) from Microsoft. AMSI allows third-party applications with AMSI support to send objects (for example PowerShell scripts) to Kaspersky Endpoint Security for an additional scan, and then to receive the results.
Kaspersky Security Network	Millions of consenting customers and thousands of businesses agree to allow the cloud-based Kaspersky Security Network (KSN) receive anonymized data about malware and suspicious behavior from their computers. This real-time flow of data helps us deliver an extremely rapid response to new malware, while also achieving a lower rate of 'false positives.
Mobile threat defense	A set of protection capabilities to secure Android and iOS devices against viruses and other malware. See details by each OS type below.
SIEM integration	Events can be exported to third party SIEM solution systems that deal with security issues on an organizational and technical level (i.e. SOCs). Syslog and CEF/LEEF protocols are supported. (**On-premises only**)

Security management

Feature	Description
System hardening	
Vulnerability assessment	Provides an overview of applications installed on corporate devices, and a list of patches available to update these applications to the latest versions
Application control	Manages the startup of applications on users' computers and reduces the risk of computer infection by restricting access to applications. This enables you to implement your own corporate security policy when using applications.
Web control	Gives you control of user access to the internet, depending on the site's content or location. Web URL deny listing restricts users from accessing potentially harmful or undesirable websites. Allow listing permits access to safe internet resources only.
Device control	Controls user access to external and removable devices connected to the computer. Administrators can allow or block the use of certain devices by type or create a 'trusted' list.
Mobile Device Management (MDM)	Enables you to manage mobile devices owned by employees in your organization, so you can apply your own corporate security requirements, control compliance, protect devices from threats and prevent any leakage of corporate information.

Mobile threat protection

Feature	Description	Pro view	Expert view
Android			
Anti-virus protection	Detects and neutralizes threats on your device, using the anti-virus databases and the Kaspersky Security Network cloud service. Protects the device against threats, viruses, and other malicious applications in real time, scans new applications and distribution packages in the Downloads folder. Scans all files the user opens, modifies, moves, copies, runs and saves on the device. Blocks adware and applications that can be used by criminals to harm the user's device and data.	✓	✓
Password protection	Protects device access with a screen unlock password.	✓	✓
Anti-theft	Protects information stored on the device against unauthorized access if the device is lost or stolen. Remotely lock and locate the device, sound an alarm, or remotely wipe data from it.	✓	✓
Application control	Manage apps on users' devices using set of rules. You can configure two types of App Control rule: Application Rules and Category Rules.	✓	✓
Compliance control	Checks user device settings for compliance with corporate security requirements. For example, if the device is rooted, have outdated anti-virus databases – protective actions can be configured.	✓	✓
Web control	Blocks access to phishing and malicious websites. Monitors access to websites depending on their contents and location.	✓	✓
Feature control	Enables you to prohibit the use of camera, Bluetooth and Wifi modules on a device in order to minimize the risk of sensitive data leakage, and to configure automatic connection to a corporate wi-fi network on Android.	✓	✓
Wi-Fi configuration	Defines wi-fi network settings when the device connects to the internet.	✓	✓
Synchronization and databases update while roaming	Allows you to run device synchronization with the Administration Server and anti-virus database updates while in the roaming area. The user can also run these manually at any time.	✓	✓

Feature	Description	Pro view	Expert view
Root detection	System files are unprotected on a hacked device and can be modified. Moreover 3rd party apps from unknown sources could be installed on hacked devices. Upon detection of a root attempt, we recommend that you immediately restore normal operation of the device.	✓	✓
Mail configuration	Allows you to set up an Exchange mailbox to work with corporate mail, contacts, and the calendar on the mobile device.		✓
KNOX/ Exchange ActiveSync (EAS) support	The Kaspersky Endpoint Security for Android app can be deployed through the Samsung KNOX Mobile Enrollment console. Exchange ActiveSync protocol can be used to configure restrictions to device features, in order to keep an EAS device secure.		✓
Android Work Profile support	Allows you to set up the separate container (by using Android Work Profile) for your corporate apps and data.		✓
PKI integration	Enables you to set up the connection to your MS CA and transfer the certificates for mail, VPN, wi-fi authentication to the connected mobile devices		✓
iOS			
Web control	Monitors access to websites depending on their contents and location. Settings are only applied to supervised devices.	✓	✓
Web anti-phishing, anti-malware	Secures the iOS device against anyphishing and malware resources that your employees may be facing.		✓
Password protection	Protects device access with a screen unlock password.	✓	✓
Proxy settings	Protects traffic when connecting the device to the internet through a global HTTP proxy. Settings are only applied to supervised devices.	✓	✓
Anti-theft functionality	Remote lock and wipe functions can be applied to a stolen device to protect data loss.	✓	✓
Feature control	Restricts user access to native iOS device features including camera control, apps installation, screenshots, AirDrop, iCloud, etc. A total of up to 40 various features are supported. Please note that some features can be managed only for supervised devices.	✓	✓
Access Point Name configuration	Configures Access Point Name (APN) when connecting to data services in a mobile network.	✓	✓
AirPrint configuration	Configures AirPrint for printing documents from the device.	✓	✓
Wi-Fi configuration	Defines wi-fi network settings when the device connects to the internet.	✓	✓
Email setup	Configures email accounts belonging to the device user.	✓	✓
CalDAV setup	Configures CalDAV accounts belonging to the device user for handling the calendar.	✓	✓
Calendar subscriptions	Configures subscription to third-party calendars for adding events to the device.	✓	✓
Jailbreak detection	System files are unprotected on a hacked device and can be modified. Upon detection of a jailbreak, we recommend that you immediately restore normal operation of the device.		✓

Cloud security

Feature	Description
Cloud Discovery	Enables the discovery and restriction of inappropriate or unauthorized cloud resources usage, as well as the time wasted on social networks and messengers. Monitor 2,700+ cloud services. Every detected cloud service now has a rating that indicates how dangerous using the service is. This means that IT admin can easily assess potential risks and decide to allow or block a particular service.

Essential EDR capabilities

Feature	Description
Root cause analysis	A threat propagation graph shows key processes. network connections. DLLs, registry hives affected or involved in the alert. All detections are highlighted on the graph, providing the analyst with full context for the incident and facilitating the process of revealing the affected components. The graph provides drill-down capabilities with additional information on processes, etc.

Multitenancy

Multitenancy is an operational mode which applies when the solution is used to protect infrastructure of several organizations at the same time. Kaspersky Next EDR Foundations multi-tenancy supports MSPs in offering Managed Endpoint Protection as a Service. The easy-to-operate multi-tenant console enables multiple client management using just one account. Up to 300 users can be split into independent isolated workspaces with their own best practice security profiles.

Find out more about Kaspersky Next EDR Foundations

Kaspersky Next
EDR Foundations

Kaspersky Next
EDR Optimum

Learn more

Kaspersky Next
XDR Expert

Learn more

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

kaspersky.com

Learn more about Kaspersky Next at:
https://go.kaspersky.com/next

Choose the tier that suits you best by taking a short survey in our interactive tool:
https://go.kaspersky.com/Kaspersky_Next_Tool