Unpacking Kaspersky Next EDR Foundations

What is Kaspersky Next EDR Foundations?

As the entry level to Kaspersky Next's three product tiers, Kaspersky Next EDR Foundations' powerful ML-based endpoint protection, flexible security controls and EDR root cause analysis equip organizations with the most straightforward way to build a strong core for their cybersecurity.

A simple console, cloud or on-premises deployment, and a variety of quality-of-working-life promoting features reduce complexity and boost efficiency.

Why Kaspersky Next EDR Foundations – and why now?

Taking your EPP for granted is becoming a serious issue

Endpoint protection platforms (EPPs) have become so familiar to IT teams that they're often 'just another part of the furniture'. This is because, alongside defending their perimeters with firewalls and email protection, the vast majority of organizations have focused their efforts on endpoints – including PCs, laptops, servers (physical and virtual) and workstations – as their primary defense against cyberthreats.

As a result, EPPs have become a fundamental step in combating complex attacks. But what's equally important to understand is that the definition of what constitutes an EPP is itself evolving, and bringing new demands in terms of what such a platform must deliver. This is due to the increasing numbers of threats that are bypassing traditional EPP.

The problem with traditional EPP

For years, small-to-medium businesses (SMBs) and low-end enterprises have been able to rely on EPP to defend themselves against an extensive range of commodity threats. But today's attackers are focusing on organizations of all sizes, industries and levels of preparedness.

This evolution of the threat landscape means that over time, increasingly sophisticated threats which previously affected only large organizations are cascading down to impact SMBs and smaller enterprises that do not possess the in-house resources needed to deal with them effectively.

In particular, the advent of evasive threats - which use legitimate tools in attacks, include readymade scenarios to bypass EPP, are low cost and readily available on the dark web – has significantly increased cybersecurity risks for organizations using traditional EPP solutions.

These issues are further compounded by the lack of transparency provided by traditional EPP. In effect these solutions offer only a red light / green light representation that an attack either is or isn't taking place. But what an IT team with even basic security skills requires is visibility into what's happening on individual endpoints, so that this can be analyzed in more detail to increase understanding of the threat.

So how can you tell if it's time to enhance your defenses?

How to tell if your EPP is no longer meeting your needs

Telltale signs that it's time to strengthen your defenses beyond traditional EPP include:

- Your EPP is failing to stop an increasing number of new, unknown and evasive threats.
- You have limited visibility into what's happening on your endpoints. This includes being unable to undertake root cause analysis, investigation and real-time threat response - or having to do this manually, with standard operating system (OS) tools on a case-by-case basis, which is slow, complex and error-prone.
- You don't have the specialist IT security skills or capacity needed to deal with increasingly sophisticated threats.
- You're concerned about potential fines, or the threat to your business's reputation resulting from a major security incident.

If you're experiencing any of these kinds of issues, not only can a modern EPP solution like Kaspersky Next EDR Foundations resolve them, but by incorporating simple endpoint detection and response (EDR) capabilities it can also provide an important steppingstone between traditional EPP and more advanced, fully featured EDR and extended detection and response (XDR) solutions, making it much more than 'just another part of the furniture'.

How Kaspersky Next EDR Foundations can help

What it does

Provides powerful ML-based endpoint protection, flexible security controls and EDR root cause analysis for the most straightforward way to build a strong cybersecurity core

How it works

Ensures effective protection for all endpoints

Incorporates basic EDR capabilities for increased understanding of threats and attacks

Cloud or on-premises console

Business value

Delivers robust endpoint protection together with increased visibility, basic EDR functionality, and IT scenarios including vulnerability assessment and software/hardware inventory

Who it's best for

Businesses with an IT administrator but limited specialist IT security resources

What do you get?

Endpoint protection
File, web and mail antivirus, network protection, behavior detection, remediation, exploit prevention, HIPS, AMSI, anti-cryptor, BadUSB attack prevention

Security management
Firewall, web, device, application controls, cloud discovery

Mobile protection and management
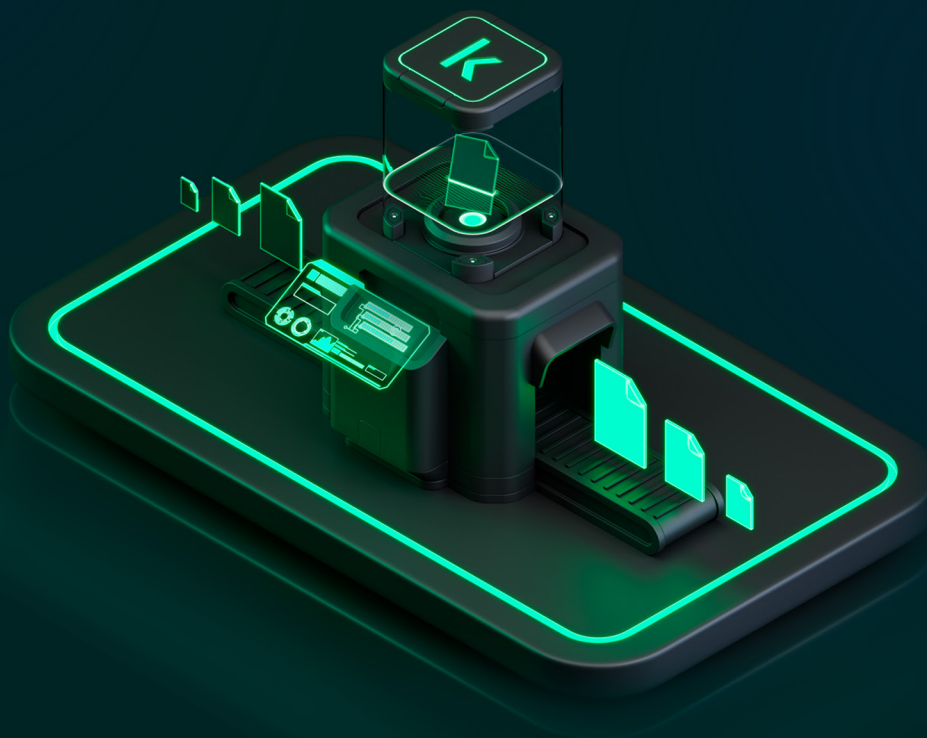Protection, controls and management, iOS MDM

IT scenarios
Vulnerability assessment, software/hardware inventory

EDR capabilities
Root cause analysis

Kaspersky Next EDR Foundations combines the core strengths and capabilities of Kaspersky Endpoint Security Cloud, Cloud Plus and Kaspersky Endpoint Security for Business Select

What if you're already using Kaspersky security?

Kaspersky Next EDR Foundations combines the core strengths and capabilities of Kaspersky Endpoint Security Cloud, Cloud Plus and Kaspersky Endpoint Security for Business Select to create a single strong endpoint protection and control solution requiring little or no effort to install and use. Important controls (particularly applications control, BadUSB, etc.) bring new benefits to Kaspersky Endpoint Security Cloud and Cloud Plus users, while Kaspersky Endpoint Security for Business Select users gain the added value of a cloud console and cloud discovery. And all these users also gain EDR capabilities with root cause analysis functionality.

Your Kaspersky solution	Recommended migration	Additional capabilities you'll get
Kaspersky Endpoint Security Cloud	Kaspersky Next EDR Foundations	• BadUSB attack prevention • Application, web and device control • Root cause analysis
Kaspersky Endpoint Security Cloud **Plus**	Kaspersky Next EDR Foundations	• BadUSB attack prevention • Application control
Kaspersky Endpoint Security for Business **Select**	Kaspersky Next EDR Foundations	• Simple cloud console • Root cause analysis • Cloud discovery

Find out more about Kaspersky Next EDR Foundations

Kaspersky Next EDR Foundations

Kaspersky Next EDR Optimum [Learn more]

Kaspersky Next XDR Expert [Learn more]

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