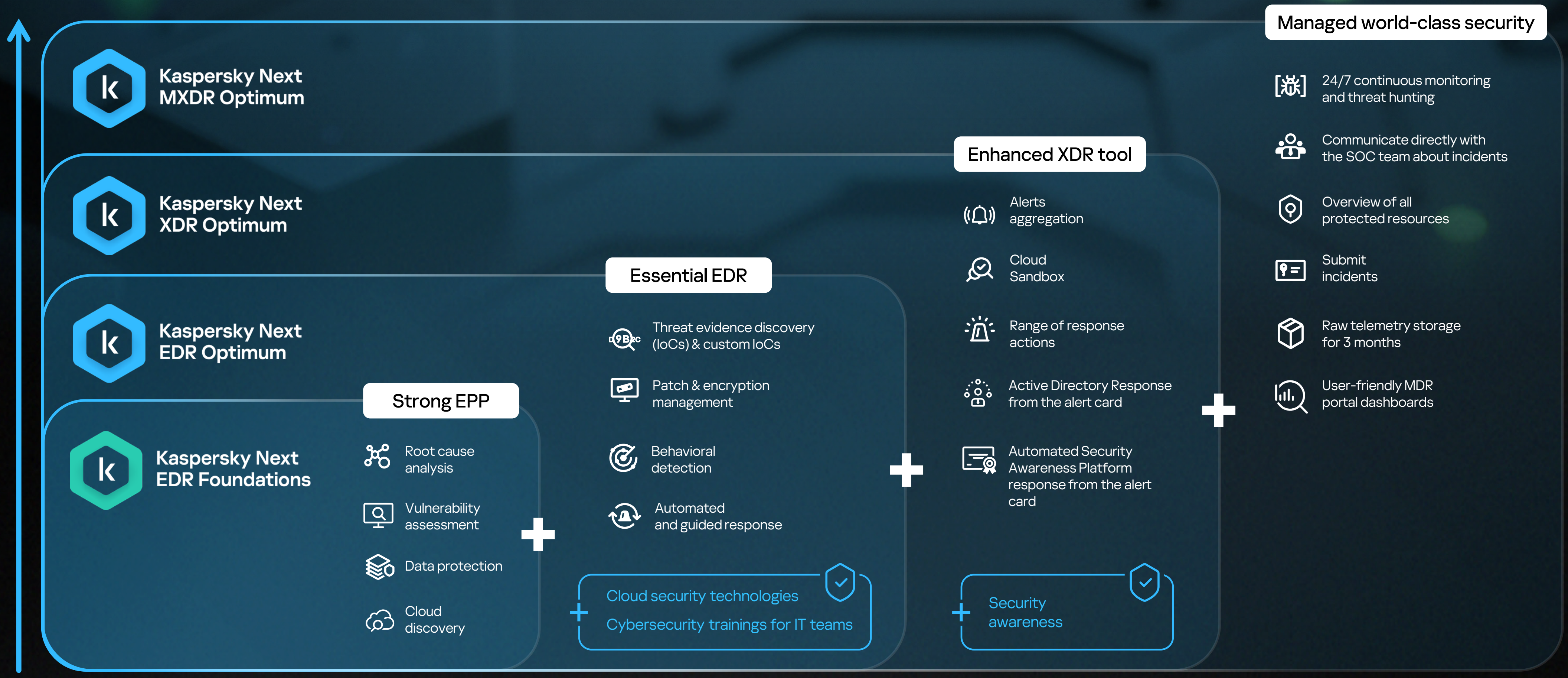
Kaspersky Next Optimum

Feature list



Kaspersky Next MXDR Optimum

Kaspersky Next XDR Optimum

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations

Strong EPP

- Root cause analysis
- Vulnerability assessment
- Data protection
- Cloud discovery

+

Essential EDR

- Threat evidence discovery (IoCs) & custom IoCs
- Patch & encryption management
- Behavioral detection
- Automated and guided response

+ Cloud security technologies
Cybersecurity trainings for IT teams

+

Enhanced XDR tool

- Alerts aggregation
- Cloud Sandbox
- Range of response actions
- Active Directory Response from the alert card
- Automated Security Awareness Platform response from the alert card

+ Security awareness

+

Managed world-class security

- 24/7 continuous monitoring and threat hunting
- Communicate directly with the SOC team about incidents
- Overview of all protected resources
- Submit incidents
- Raw telemetry storage for 3 months
- User-friendly MDR portal dashboards

Kaspersky Next Optimum is for small and mid-sized businesses with lean cybersecurity teams that want to scale protection without added complexity. It starts with strong endpoint protection, enhanced by endpoint detection and response features, and enables a smooth upgrade to essential XDR or MXDR for sophisticated level of cybersecurity.

Kaspersky Next EDR Foundation

Automated protection from mass threats

- Multi-layered anti-malware
- Behavior detection
- Exploit prevention
- Universal Linux Kernel Module (ULKM)
- Remediation engine
- File, email, web and network threat protection on endpoint level
- Firewall
- Host Intrusion Prevention
- AMSI protection
- BadUSB attack prevention
- Root cause analysis with an alert card
- Global threat intelligence via Kaspersky Security Network
- Mobile threat defense

System hardening

- Vulnerability assessment
- Hardware and software inventory
- Application, web and device controls
- Mobile device management (MDM)
- Remote troubleshooting
- Third-party apps & OS installation

Cloud security

- Cloud discovery

+

Kaspersky Next EDR Optimum

Endpoint detection and response to complex threats

- Indicators of compromise (IoC) search with automatic cross-endpoint response
- Adaptive anomaly control
- Single-click and guided response
- System critical object check
- Move file to quarantine / recover file from quarantine
- Network isolation / remove network isolation
- Get / delete file
- Start / terminate process
- Critical areas scan
- Execution prevention
- Execute command

System hardening

- Patch management
- Remote wipe
- Encryption management
- Advanced MDM

Cloud security

- Cloud blocking
- Data discovery
- Security for Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams

IT training

- Cybersecurity training for IT administrators

+

Kaspersky Next XDR Optimum

Extended detection and response to complex threats

- Alerts aggregation
- Active Directory Response from the alert card

Automated Security Awareness Platform

- Flexible security awareness training for employees
- Customizable courses available in 25 languages
- Security awareness dashboards and reports
- Simulated phishing campaigns
- Video and audio training formats
- Automated Security Awareness Platform response from the alert card

Kaspersky Cloud Sandbox

- Uploading and executing a file in Cloud Sandbox
- Uploading a file from a web address and then execute it in Cloud Sandbox
- Anti-evasion features to counter malware designed to avoid sandboxes
- Executing the extracted file from the Cloud Sandbox report
- Exporting the analysis results
- Automatic detection of file types
- Managing obsolete tasks for execution

+

Kaspersky Next MXDR Optimum

Managed protection

- 24/7 continuous monitoring and threat hunting
- Incident submitting for further investigation by Kaspersky SOC
- Direct communication with the SOC team about incidents
- Notifications about incidents via email / Telegram
- Guided and automated response scenarios
- REST API for integration with IRP / SOAR
- Artificial Intelligence mechanisms accelerating incident investigation
- Assets visibility with their current statuses
- Compatibility with third-party EPP applications
- User-friendly MDR portal dashboards
- Regular reports
- Raw telemetry storage for 3 months

www.kaspersky.com

Learn more

#kaspersky
#bringonthefuture