Kaspersky Next

Features

Features	For everyone	For small and mid-sized businesses			For enterprises of all sizes	
	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum	Kaspersky Next EDR Expert	Kaspersky Next XDR Expert
• Automated protection from mass threats • System hardening • Cloud discovery	●	●	●	●	●	●
• Endpoint detection and response to complex threats • Patch management • Remote wipe • Encryption management • Advanced MDM • Cybersecurity training for IT administrators		●	●	●	●	●
• Cloud blocking • Data discovery • Security for Microsoft Office 365		●	●	●	●	●
• Alerts aggregation[1] • Active Directory Response from the alert card[1] • Kaspersky Cloud Sandbox[2]			●	●		
• Kaspersky Automated Security Awareness Platform[3]			●	●		●
• 24/7 continuous monitoring, threat hunting and investigation by Kaspersky SOC as well as other MDR features[4]				●		
• Advanced endpoint detection and response to complex and persistent threats • Built-in advanced sandbox • Service management • Forensics (Windows only)					●	●
• Extended detection and response to complex and persistent threats • Cross-correlation engine for data collection, normalization, monitoring and correlation • Email security • Hybrid cloud security • 50 Kaspersky Threat Lookup requests						●

[1] Aggregation and response capabilities in Kaspersky Next XDR Expert are available in more advanced options compared to Kaspersky Next XDR Optimum

[2] Licenses include Kaspersky Threat Intelligence Portal requests for 0.5 users

[3] Licenses include access for 0.2 users to the Kaspersky Automated Security Awareness Platform

[4] For a complete feature breakdown, see the Kaspersky Next Expert and Kaspersky Next Optimum feature lists. Availability may vary depending on the deployment method.

Learn more

Foundations features

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

Optimum features

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

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

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

Expert features[3]

Advanced endpoint detection and response to complex and persistent threats

- Endpoint telemetry collection
- Proactive threat hunting and retrospective analysis
- Advanced detection with Indicators of Attack (IoA)
- YARA rules (Windows only)
- MITRE ATT&CK mapping

Built-in advanced sandbox

- Multi-level assessment and behavior analysis of emulated objects
- Managing virtual machine templates
- Built-in specialized network interface for monitoring interactions of malicious objects with internet resources
- Simulates the actions of ordinary users
- Effectively counteracts modern sandbox bypass techniques used by malware

Service management

- Start / Stop / Delete / Pause / Resume service
- Modify startup service type

Forensics (Windows only)

- Process, file, autorun lists
- Process memory dump
- Memory dump
- Disc image
- NTFS service files
- Registry key

Extended detection and response to complex and persistent threats

- Investigation graph with timeline mode
- Incident response and flexible case management with SLA
- Playbooks: response automation and orchestration
- Deployment toolkit and Open API
- Visual playbook editor

Cross-correlation engine for data collection, normalization, monitoring and correlation

- 250+ third-party connectors
- Dashboards and reporting
- Log management with data lake
- Advanced threat detection and cross-correlation
- Alerts aggregation and asset management
- Active Directory data ingestion and response
- AI-based risk scoring of assets
- AI-enabled detection of DLL hijacking
- Resource dependencies graph
- High availability of SIEM Core with Raft algorithm

Email security

- ML-based malware, spam & phishing detection
- Various deployment options (SEG, cloud, standalone)
- Content filtering
- Email sender authentication using SPF, DKIM and DMARC
- Integration capabilities
- Expanded data export to SIEM

Hybrid cloud security

- System Integrity Monitor
- Log inpection
- Private cloud support: VMware, Red Hat Enterprise Linux, KVM
- Public cloud support: Google Cloud, Microsoft Azure, AWS
- VDI platforms support: VMware, TERMIDESK, Citrix, Hyper-V

50 Kaspersky Threat Lookup requests

[3] Most features from Foundations and Optimum tiers are available at the Expert level too, however there are exceptions such as availability of MXDR features, KASAP and others. Please refer to the Kaspersky Next Expert and Kaspersky Next Optimum feature lists. Availability may vary depending on the deployment method.

www.kaspersky.com

#kaspersky
#bringonthefuture