Functional comparison of Kaspersky Next Tiers

Each tier includes the features and capabilities of the previous tier.
Feature availability depends on the implementation method.

Kaspersky Next EDR Foundations

Automated protection of physical and virtual endpoints

- Multi-layered anti-malware
- Behavior detection
- Exploit prevention
- Remediation engine
- File, mail, web and network threat protection on endpoint level
- Firewall
- Host Intrusion Prevention (HIPS)
- 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 discovery

- Cloud discovery

Supported OSs

- MacOS, Linux, Windows, Android, iOS

+

Kaspersky Next EDR Optimum

Cloud security

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

Advanced detection and response to complex threats

- Indicators of compromise (IoCs) search and 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

IT training

- Cybersecurity training for IT administrators

+

Kaspersky Next EDR Expert

Advanced detection and response to complex and persistent threats

- Endpoint telemetry collection
- Proactive threat hunting and retrospective analysis
- Advanced detection with indicator 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
- Several emulation modes

Service management

- Start / stop / delete / pause / resume service
- Modify startup type of Service

Forensics (Windows only)

- Process lists
- File list
- Autorun list
- Process memory dump
- Memory dump
- Disc image
- NTFS service files
- Registry key

+

Kaspersky Next XDR Expert

Email security

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

Hybrid cloud security

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

Threat Intelligence enrichment (50 Threat Lookups)

Extended detection and response capabilities

- Investigation graph
- Incident response and case management
- Playbooks: Response automation and orchestration
- Deployment toolkit and Open API

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
- Alert aggregation and asset management
- Active Directory data ingestion and response