



Funktionen

Für jeden

Für kleine und mittelständische Unternehmen

Für Unternehmen jeder Größe



Kaspersky Next
EDR Foundations



Kaspersky Next
EDR Optimum



Kaspersky Next
XDR Optimum



Kaspersky Next
MXDR Optimum



Kaspersky Next
EDR Expert



Kaspersky Next
XDR Expert

- Automatisierter Schutz vor Massenbedrohungen
- System Hardening
- Cloud Discovery



- Endpoint Detection and Response erkennt selbst die komplexesten Bedrohungen
- Patch Management
- Löschen per Fernzugriff
- Verschlüsselungsmanagement
- Secure Mobility Management (integriertes MTM +EMM)
- Cybersicherheitsschulung für IT-Administratoren



- Blockieren von Cloud Services
- Datenerkennung
- Security for Microsoft Office 365



- Aggregation von Warnungen¹
- Active Directory Response von der Alert Karte¹
- Kaspersky Cloud Sandbox²



- Kaspersky Automated Security Awareness Platform³



- Unterbrechungsfreie Überwachung, Threat Hunting und Untersuchung durch Kaspersky SOC sowie weitere MDR-Funktionen⁴



- Hochentwickelte Endpoint-Erkennung und Reaktion auf komplexe und hartnäckige Bedrohungen
- Eingebaute Advanced Sandbox
- Service-Management (nur Windows)
- Forensik



- Erweiterte Erkennung und Reaktion auf komplexe und hartnäckige Bedrohungen
- Kreuzkorrelations-Engine für Datenerfassung, -normalisierung, -überwachung und -korrelation
- E-Mail-Sicherheit
- Hybrid Cloud Security
- 100 kostenlose Kaspersky Threat Lookup-Anfragen



¹ Die Aggregations- und Reaktionsfunktionen in Kaspersky Next XDR Expert sind im Vergleich zu Kaspersky Next XDR Optimum in erweiterten Optionen verfügbar

² Die Lizenzen umfassen Anfragen für das Kaspersky Threat Intelligence Portal für 0,5 Benutzer

³ Die Lizenzen umfassen den Zugriff für 0,2 Benutzer auf die Automated Security Awareness Platform von Kaspersky

⁴ Eine vollständige Übersicht über die Funktionen finden Sie in den Feature Listen von Kaspersky Next Expert und Kaspersky Next Optimum. Die Verfügbarkeit bestimmter Funktionen kann je nach Bereitstellungsmethode und ausgewählter Lizenz variieren.

Weitere
Informationen

Foundations-Funktionen

Automatisierter Schutz vor Massenbedrohungen

- Mehrschichtige Anti-Malware-Lösung
- Verhaltenserkennung
- Exploit Prevention
- Universelles Linux-Kernel-Modul (ULKM)
- Remediation Engine
- Schutz vor Datei-, E-Mail-, Web- und Netzwerkbedrohungen auf Endpoint-Ebene
- Firewall
- Host Intrusion Prevention
- AMSI-Schutz
- Schutz vor BadUSB-Angriffen
- Ursachenanalyse mithilfe der Alert Card
- Globale Threat Intelligence über das Kaspersky Security Network
- Schutz vor mobilen Bedrohungen

System Hardening

- Vulnerability Assessment
- Hardware- und Software-Bestandsaufnahme
- Anwendungs-, Web- und Gerätekontrolle
- Mobile Device Management (MDM)
- Remote Troubleshooting
- Drittanbieter-Apps und OS-Installation

Cloud Security

- Cloud Discovery

Security Awareness

- Simulierte Phishing-Angriffe

Optimum-Funktionen

Endpoint Detection and Response erkennt selbst die komplexesten Bedrohungen

- Gefährdungsindikatoren (IoCs) und Threat Hunting mit automatischer Abwehr über alle Endpoints hinweg
- Adaptive Anomaly Control
- Automatisierte Reaktion per "Single-Click"
- Prüfung auf systemkritische Objekte
- Datei in Quarantäne verschieben/Datei aus Quarantäne wiederherstellen
- Netzwerk isolieren / Isolierung aufheben
- Datei holen / löschen
- Prozess starten / beenden
- Überprüfen (Scannen) wichtiger Bereiche
- Ausführungsverhinderung
- Befehl ausführen

System Hardening

- Patch Management
- Löschen per Fernzugriff
- Verschlüsselungsmanagement
- Secure Mobility Management (integriertes MTM +EMM)

Cloud Security

- Blockieren von Cloud Services
- Datenerkennung
- Sicherheit für Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams

IT-Schulung

- Cybersicherheitsschulung für IT-Administratoren

Extended Detection and Response erkennt selbst die komplexesten Bedrohungen

- Zusammenführen von Warnmeldungen
- Active Directory Response von der Vorfallskarte

Automated Security Awareness Platform

- Flexible Schulungen zum Thema Security Awareness für Mitarbeiter
- Anpassbare Kurse in 25 Sprachen verfügbar
- Dashboards und Berichte zum Sicherheitsbewusstsein
- Video- und Audio-Schulungsformate
- Ableitung von Security Awareness-Maßnahmen auf Basis der Alert Card

Kaspersky Cloud Sandbox

- Hochladen und Ausführen einer Datei in der Cloud Sandbox
- Eine Datei von einer Webadresse hochladen und anschließend in der Cloud Sandbox ausführen
- Funktionen zur Neutralisierung von Malware, die darauf ausgelegt ist, Sandboxes zu umgehen
- Ausführen der extrahierten Datei aus dem Cloud Sandbox-Bericht
- Exportieren der Analyseberichte
- Automatische Erkennung von Dateitypen
- Verwaltung veralteter Aufgaben zur Ausführung

Managed Protection

- 24x7 Überwachung und Threat Hunting
- Vorfall zur weiteren Untersuchung durch das Kaspersky SOC melden
- Direkte Kommunikation mit dem SOC-Team über Vorfälle
- Benachrichtigungen über Vorfälle per E-Mail/Telegram
- Geführte und automatisierte Reaktionsszenarien
- REST API für die Integration mit IRP / SOAR
- Künstliche Intelligenz-Mechanismen zur Beschleunigung der Untersuchung von Vorfällen
- Asset-Sichtbarkeit mit aktuellem Status
- Kompatibilität mit EPP-Anwendungen von Drittanbietern
- Benutzerfreundliche Dashboards im MDR-Portal
- Regelmäßiges Reporting
- Rohdaten-Telemetriespeicher für 3 Monate
- Erkenntnisse zu kompromittierten Zugangsdaten

Expert-Funktionen³

Erweiterte Detection and Response auf komplexe und hartnäckige Bedrohungen

- Untersuchungsgrafik im Timeline-Modus
- Vorfalldetektion und flexibles Fallmanagement mit SLA
- Playbooks: Automatisierung von Reaktionsmaßnahmen und Orchestrierung
- Deployment Toolkit und Open API
- Visueller Playbook-Editor

Kreuzkorrelations-Engine für Datenerfassung, -normalisierung, -überwachung und -korrelation

- Anbindung an über 300 Drittanbieter
- Dashboards und Berichte
- Protokollverwaltung und Datenspeicher
- Fortschrittliche Threat Detection und Kreuzkorrelation
- Aggregation von Warnungen und Asset Management
- Active Directory: Datenabgleich und Reaktion
- KI-basierte Risikobewertungen für Assets
- KI-gestützte Erkennung von DLL-Hijacking
- KI-gestützte Erkennung von Accountdiebstahl
- KI-gestützte Zusammenfassung von Vorfällen
- GenAI-basierter Assistent für SOC-Analysten
- Diagramm der Ressourcenabhängigkeiten

E-Mail-Sicherheit

- ML-basierte Erkennung von Malware, Spam und Phishing
- Verschiedene Bereitstellungsoptionen (SEG, Cloud, Standalone)
- Inhaltsfilter
- E-Mail-Sender-Authentifizierung mit SPF, DKIM und DMARC
- Integrationsfunktionen
- Erweiterter Datenexport an SIEM
- Attachment-Analyse mit nativer Integration in die Netzwerk-Sandbox von KATA

Hybrid Cloud Security

- Monitoring der Systemintegrität
- Protokollüberprüfung
- Unterstützung für private Cloud: VMware, Red Hat Enterprise Linux, KVM
- Unterstützung für öffentliche Cloud: Google Cloud, Microsoft Azure, AWS

100 kostenlose Kaspersky Threat Lookup-Anfragen

Hochentwickelte Endpoint Detection and Response auf komplexe und hartnäckige Bedrohungen

- Endpoint-Telemetrie-Sammlung
- Proaktives Threat Hunting und nachträgliche Analyse
- Erweiterte Erkennung mit Angriffssindikatoren (IoA)
- YARA-Regeln
- MITRE ATT&CK-Mapping

Eingebaute Advanced Sandbox

- Mehrstufige Bewertung und Verhaltensanalyse von emulierten Objekten
- Vorlagen für virtuelle Maschinen verwalten
- Eingebaute spezialisierte Netzwerkschnittstelle zur Kontrolle der Interaktionen von bössartigen Objekten mit Internet-Ressourcen
- Simulation der Aktionen normaler Benutzer
- Wirksame Bekämpfung moderner Sandbox-Umgehungstechniken, wie sie von Malware verwendet werden

Service-Management (nur Windows)

- Service starten / stoppen / löschen / pausieren / wiederaufnehmen
- Startdiensttyp ändern

Forensik

- Prozess, Datei, Autostart-Listen
- Verarbeitung von Speicherausgüssen
- Speicherausguss
- Datenträgerabbild
- NTFS-Service-dateien
- Registrierungsschlüssel

³ Die meisten Funktionen der Stufen „Foundations“ und „Optimum“ sind auch auf der Stufe „Expert“ verfügbar, es gibt jedoch Ausnahmen wie die Verfügbarkeit von MXDR-Funktionen, KASAP und anderen. Bitte beachten Sie die Feature Listen von Kaspersky Next Expert und Kaspersky Next Optimum. Die Verfügbarkeit bestimmter Funktionen kann je nach Bereitstellungsmethode und ausgewählter Lizenz variieren.