

# Kaspersky Next EDR Expert

Leistungsstarker Schutz  
für Ihre Endpoint-Infrastruktur





## Kaspersky Next EDR Expert

Kaspersky Next EDR Expert bildet eine zentrale Komponente innerhalb von Kaspersky Next. Mit proaktivem Schutz für die gesamte Infrastruktur bietet Kaspersky Next EDR Expert umfassende Cybersicherheit gegenüber komplexen Bedrohungen.

# Kaspersky Next EDR Expert

Daten, Benutzer und Unternehmenssysteme sind miteinander verbunden. Hinzu kommt, dass Endpoints nach wie vor das Hauptziel von Cyberkriminellen darstellen. Deshalb bedarf es einer leistungsstarken Kombination aus präventiven Bedrohungstechnologien und fortschrittlichen Sicherheitsmechanismen.

**Kaspersky Next EDR Expert** ist eine fortschrittliche Endpoint Detection and Response-Lösung, die im Zusammenspiel mit der Endpoint Protection Plattform (EPP) Cyberangriffe wirksam blockiert. Darüber hinaus untersucht die Lösung Ihre Systeme automatisch auf komplexere Cyberbedrohungen, geht proaktiv Vorfällen nach und gibt IT-Spezialisten ein umfassendes Portfolio von Reaktionstools an die Hand, mit denen sie effektiv arbeiten können.

Kaspersky Next EDR Expert dämmt Bedrohungen schnell ein und bereinigt Vorfälle in verteilten Infrastrukturen. Die Lösung unterstützt Ihre IT-Sicherheitsabteilung und ermöglicht effektiveres Arbeiten, indem sie umfassenden Endpoint-Schutz über einen zentralen Agenten bereitstellt und den Wartungs- und Supportaufwand für installierte Produkte reduziert, ohne dabei die Leistung zu beeinträchtigen.



## Auszeichnungen

Unsere Technologien werden regelmäßig von unabhängigen Prüflabors getestet und die Qualität unserer Produkte wird immer wieder von führenden Analyse-Agenturen bestätigt. Wir haben zahlreiche internationale Auszeichnungen erhalten.



## Das kann Kaspersky Next EDR Expert für Ihr Unternehmen leisten:

- Effizienzsteigerung für Ihre Sicherheitssysteme dank vielfach ausgezeichnete EPP und leistungsstarker EDR-Funktionalität
- Verstärkte Kontrolle Ihrer Endpoint-Infrastruktur
- Verbesserte Erkennung und Eindämmung hochentwickelter Bedrohungen
- Unterstützung bei der Einrichtung von Prozessen zur Bedrohungserkennung, zum Umgang mit Vorfällen und zur Vorfallsreaktion durch optimierte Zuweisung von Ressourcen
- Unterstützung bei der Einhaltung gesetzlicher Vorgaben und Standards

# EDR



### 2 Erkennung

Bedrohungserkennung auf der Grundlage von Indikatoren wie IoC und IoA sowie benutzerdefinierten Regeln

Anreicherung der Erkenntnisse durch globale Threat Intelligence-Daten

Proaktives Threat Hunting und nachträgliche Analyse



### 3 Untersuchung

Detaillierte Untersuchung und Ursachenanalyse

Toolkit für die digitale Forensik



### 4 Response

Unterstützung bei einer Vielzahl von Abwehraktionen

# EPP



### 1 Schutz

Leistungsstarke Antiviren-Engine

Mehrfache Sicherheitskontrollen und Datenschutz

Vulnerability Scanning und Patch Management

Verhaltensanalyse und adaptive Kontrolle von Anomalien

# Hauptfunktionen

Kaspersky Next EDR Expert bietet umfassende Einblicke in sämtliche Endpoints innerhalb der Unternehmensinfrastruktur sowie eine visuelle Darstellung der einzelnen Phasen der Bedrohungsuntersuchung. Leistungsfähige Erkennungsmodule und Werkzeuge zur Ursachenanalyse stellen eine effiziente Erkennung und Untersuchung von Bedrohungen sicher.

Anschließende Analysen und die Zuordnung von erkannten Bedrohungen zur MITRE ATT&CK-Wissensdatenbank ermöglichen die Einordnung der von den Angreifern verwendeten Taktiken und Techniken. Das Produkt bietet außerdem proaktives Threat Hunting und Zugriff auf das Kaspersky Threat Intelligence-Portal, mit dem Experten die einzelnen Schritte eines Angriffs rekonstruieren und selbst besonders raffinierte Angriffe abwehren können.

## EPP



### Führende Präventionstechnologien, einschließlich ML-basierter Technologien

- Automatisierte Bedrohungsabwehr
- Automatisierte Wiederherstellung
- Schutz vor Phishing-Versuchen
- Schutz vor der Ausnutzung von Schwachstellen
- Schutz vor Diebstahl von Anmeldedaten



### Sicherheit und Datenkontrollen

- Programmkontrolle
- Webkontrolle
- Gerätekontrolle
- Adaptive Anomaly Control
- Verschlüsselungsmanagement und Richtlinienverwaltung
- Verschlüsselung tragbarer Geräte



### Schwachstellenbewertung und Patch-Management

- Fortschrittliches Patch-Management
- Vulnerability Assessment
- Lizenzverwaltung
- Zentrale Bereitstellung von Anwendungen und Betriebssystemen
- Remote-Management-Tools
- Bestandsaufnahme aller Assets

## EDR



### Automatisierte Erkennung von hochentwickelten Bedrohungen

- Datenerfassung und -speicherung
- Erweiterte Erkennungsmechanismen anhand von IoA-Regeln
- Automatischer Zugang zu Bedrohungsdaten (KSN)
- Retrospektive Analyse
- MITRE ATT&CK-Mapping



### IoC-Suche und Threat Hunting

- Vollständige Transparenz und Kontrolle
- Priorisierung des Vorfalls
- IoC-Untersuchung
- YARA-Regeln
- Zugang zu Threat Lookup
- Flexibler Abfrage-Generator für proaktive Bedrohungsjagd



### Response

- Tool zur Vorfallsreaktion
- Einrichtung automatisierter Reaktionsaufgaben
- Empfohlene reaktive Maßnahmen
- Eindämmung von Bedrohungen
- Zentralisierte Ortung von Vorfällen



# Kaspersky Next EDR Expert

Mehr erfahren

[www.kaspersky.de](http://www.kaspersky.de)

© 2024 AO Kaspersky Lab.  
Eingetragene Markenzeichen und Handelsmarken  
sind das Eigentum ihrer Besitzer.

#kaspersky  
#bringonthefuture