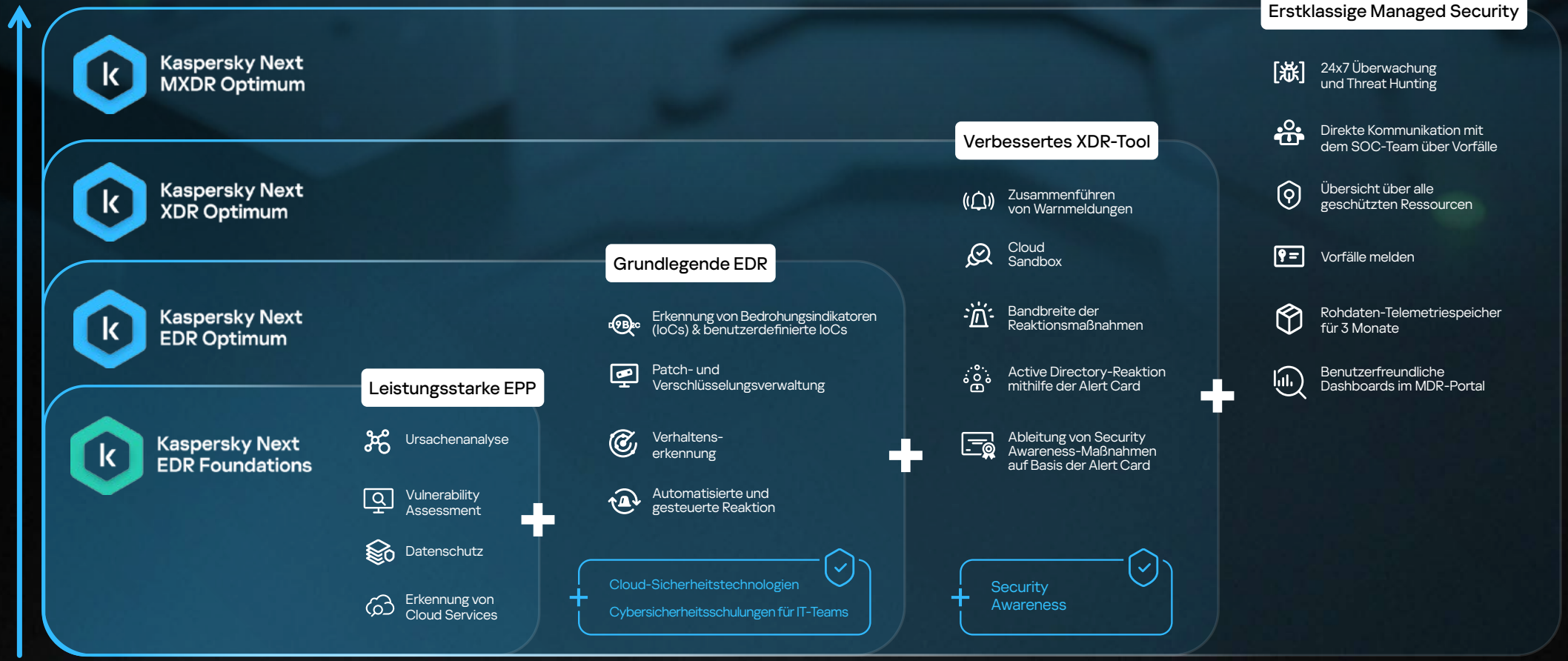
Kaspersky Next Optimum

Features im Überblick



Kaspersky Next Optimum richtet sich an kleine und mittelständische Unternehmen mit schlank aufgestellten Cybersecurity-Teams, die ihren Schutz ohne zusätzliche Komplexität erweitern möchten. Die Stufen reichen von starkem Endpoint-Schutz über erweiterte Endpoint Detection and Response bis hin zu XDR- und MXDR-Funktionen für ein noch höheres Maß an Cyberschutz.

Kaspersky Next EDR Foundation

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

- Erkennung von Cloud Services

+

Kaspersky Next EDR Optimum

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
- Netzwerkisolierung/Netzwerkisolierung aufheben
- Datei abrufen/löschen
- Prozess starten/beenden
- Überprüfen (Scannen) wichtiger Bereiche
- Ausführungsverhinderung
- Befehl ausführen

System Hardening

- Patch Management
- Löschen per Fernzugriff
- Verschlüsselungsmanagement
- Erweitertes MDM

Cloud Security

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

IT-Schulung

- Cybersicherheitsschulung für IT-Administratoren

+

Kaspersky Next XDR Optimum

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
- Simulierte Phishing-Angriffe
- 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, Sandboxen zu umgehen
- Ausführen der extrahierten Datei aus dem Cloud Sandbox-Bericht
- Exportieren der Analyseberichte
- Automatische Erkennung von Dateitypen
- Verwaltung veralteter Aufgaben zur Ausführung

+

Kaspersky Next MXDR Optimum

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 ihrem aktuellem Status
- Kompatibilität mit EPP-Anwendungen von Drittanbietern
- Benutzerfreundliche Dashboards im MDR-Portal
- Regelmäßiges Reporting
- Rohdaten-Telemetriespeicher für 3 Monate

www.kaspersky.de

Mehr erfahren

#kaspersky
#bringonthefuture