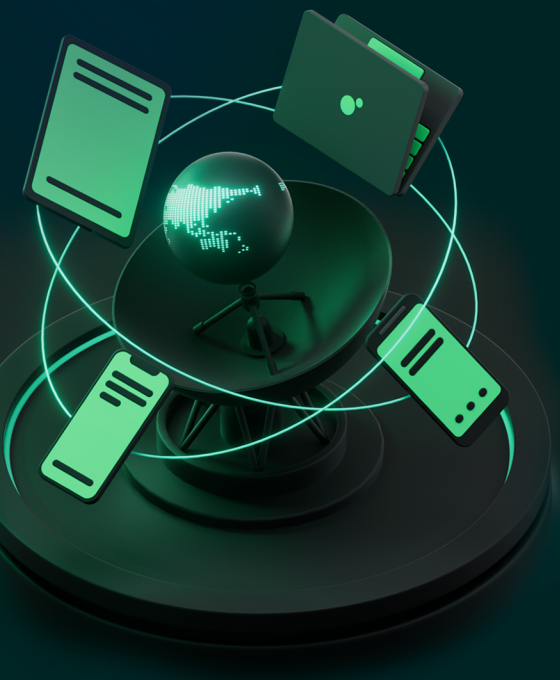
Kaspersky Next XDR Expert

Das bietet Kaspersky Next XDR Expert

Was ist Kaspersky Next XDR Expert?

Kaspersky Next XDR Expert ist die höchste der drei Produktstufen von Kaspersky Next und lässt sich nahtlos in die bestehende Sicherheitsinfrastruktur eines Unternehmens integrieren. Neben Echtzeittransparenz und tiefen Einblicken in sich entwickelnde Cyberbedrohungen bietet die Lösung erweiterte Funktionen zur Bedrohungserkennung, automatisierte Abwehrmaßnahmen sowie eine breite Palette an wichtigen XDR-Funktionen.



Warum Kaspersky Next XDR Expert – und warum gerade jetzt?

Cyberkriminelle verfeinern ständig ihre Taktiken und entwickeln immer raffiniertere Methoden, um die Sicherheitssysteme von Unternehmen zu durchbrechen. Sie nutzen eine breite Palette an unterschiedlichen Taktiken und Techniken sowie einen Multi-Vektor-Ansatz, um verschiedene Schwachstellen für den Einstieg in die Infrastruktur auszuloten.

APTs (Advanced Persistent Threats) umgehen den traditionellen Endpoint-Schutz und bleiben wochen- oder sogar monatelang unerkannt im System versteckt. Die Angreifer nutzen diese Zeit, um sich immer weiter im Netzwerk auszubreiten (lateral movement). Sie verschaffen sich Berechtigungen, greifen Daten ab und sammeln Informationen aus den verschiedenen Schichten der IT-Infrastruktur, um diese für groß angelegte Angriffe oder Datendiebstahl zu nutzen.

Ein wirksamer Schutz vor diesen Bedrohungen erfordert einen umfassenden und proaktiven Ansatz, der fortschrittliche Technologien, robuste Richtlinien, aufmerksame Überwachung, kontinuierliches Training und vieles mehr kombiniert. Genau diesen 360-Grad-Blick auf die Bedrohungslandschaft kann XDR liefern.

XDR macht Schluss mit Silos und isolierten Einzellösungen. Es bietet SOCs und IT-Sicherheitsteams die durchgängige Transparenz und Integration, die sie benötigen, um Bedrohungen schnell zu erkennen, schnell zu reagieren, wirksame Gegenmaßnahmen zu ergreifen und so mögliche Schäden zu begrenzen.

Funktionsweise von XDR

XDR steht für Extended Detection and Response und stellt eine Erweiterung der klassischen EDR-Lösung dar, ergänzt durch und eng verzahnt mit einer ganzen Reihe weiterer Sicherheitstools.

XDR sorgt dafür, dass Sicherheitslösungen, die ursprünglich nicht als kompatible Komponenten entwickelt wurden, bei der Prävention, Erkennung, Untersuchung und Reaktion auf Bedrohungen nahtlos zusammenarbeiten können. Dazu könnten beispielsweise Lösungen für den Schutz von E-Mail, Web, Netzwerk, Cloud-Infrastruktur, Anwendungen, Identitäten usw. gehören, die es ermöglichen, zusätzliche Arten von Angriffsszenarien zu erkennen und zu untersuchen und somit die Abwehr von komplexen Cyberbedrohungen zu stärken.

Durch die Bereitstellung eines zentralen Überwachungsfensters und vollständiger Transparenz zwischen Cybersicherheitstools und -schichten ermöglicht XDR überlasteten Sicherheitsteams, Bedrohungen schneller und effizienter zu erkennen und zu beseitigen. Sie erhalten außerdem umfassende Kontextdaten, um fundierte Sicherheitsentscheidungen zu treffen und künftige Angriffe zu verhindern.

Im Kampf gegen die immer raffinierteren Cyberbedrohungen, brauchen Unternehmen mehr als ein Set an Sicherheitstools von einem einzigen Anbieter.

Finden Sie mit Hilfe unseres interaktiven Tools heraus, welches Kaspersky Next-Produkt am besten zu Ihnen passt: https://go.kaspersky.com/Kaspersky_Next_Tool

Wie profitiert das Unternehmen davon?

Im Kampf gegen die immer raffinierteren Cyberbedrohungen, brauchen Unternehmen mehr als ein Set an Sicherheitstools von einem einzigen Anbieter.

- Angesichts des weltweiten Mangels an Experten für Informationssicherheit bietet XDR einen ganzheitlichen Schutz für eine wachsende und sich verändernde IT-Infrastruktur vor dem Hintergrund der sich rasch entwickelnden Cyberbedrohungs-Landschaft.
- Durch die Automatisierung von Routineaufgaben reduziert XDR den manuellen Aufwand und die Reaktionszeiten, vereinfacht die Arbeit von wertvollen und knappen Arbeitskräften wie IT-Sicherheitsspezialisten und gibt diesen die Möglichkeit, sich mit komplexen Vorfällen zu befassen.
- Mithilfe von Verhaltensanalysen und Telemetriedaten in Echtzeit über mehrere Sicherheitsebenen hinweg können sich Sicherheitsanalysten ein klares Bild von Cyberbedrohungen machen und entscheiden, von welchen die größte Gefahr für die IT-Infrastruktur des Unternehmens ausgeht, um diese zuerst eliminieren.
- XDR hilft die mittlere Zeit bis zur Entdeckung (MTTD) und die mittlere Zeit bis zur Reaktion (MTTR) zu minimieren, was bei der Bekämpfung komplexer Bedrohungen und gezielter Angriffe den entscheidenden Vorteil bringen kann.

Selbst wenn Ihr Unternehmen nur über begrenzte Expertenressourcen verfügt, kann XDR Sie mit Funktionen wie diesen vor komplexen Angriffen schützen:

- Höheres Maß an Prozessautomatisierung
- Zentrale Konsole zur Überwachung
- Playbooks und Automatisierung erlauben eine enge Verzahnung von IT-Sicherheitstools innerhalb von XDR und in gemeinsamen Szenarien
- Eine einzige Data Lake-Umgebung.
- Integrierte Threat Intelligence-Daten zur Anreicherung mit vertrauenswürdigen, relevanten Informationen
- Weniger Fehlalarme und Minimierung der Auswirkung von tatsächlichen Bedrohungen

So kann Kaspersky Next XDR Expert Sie unterstützen

Wirkungsweise

Die offene XDR-Plattform mit komplettem Funktionsumfang lässt sich nahtlos in Ihre bestehenden Sicherheitssysteme, Tools und Anwendungen integrieren

Bietet Transparenz in Echtzeit, tiefe Einblicke in sich entwickelnde Cyberbedrohungen sowie fortschrittliche Funktionen für die Erkennung und automatisierte Abwehr von Bedrohungen

Funktionen

Erkennt komplexe Bedrohungen durch Abgleich multipler Datenquellen

Leistungsstarke EDR-Funktionen mit fortschrittlicher Erkennung und Abwehr

Proaktives Threat Hunting, um gut versteckte komplexe Angriffe aufzuspüren

Geschäftswert

Ökosystem-Ansatz, maximiert im Zusammenspiel mit dem offenen Design die Effizienz der beteiligten Cybersicherheits-Tools, spart Ressourcen und reduziert Risiken.

Vereinfacht die Arbeit von IT-Sicherheitsspezialisten und gibt ihnen den zusätzlichen Kontext, den sie zur Untersuchung von Multi-Vektor-Angriffen benötigen.

Minimiert MTTD und MTTR, welche entscheidend bei der Bekämpfung von komplexen Bedrohungen und gezielten Angriffen sind.

Bietet ganzheitlichen Schutz gegen die sich verändernde Bedrohungslandschaft.

Wer ist die Zielgruppe

Unternehmen mit erheblichen Sicherheitsressourcen, die eine zentrale Plattform mit folgenden Funktionen brauchen:

- Kohärentes Bild der Vorgänge in der gesamten geschützten Infrastruktur
- Integrierte Bedrohungsjagd und Threat Intelligence
- Hervorragende Priorisierung von Vorfällen und weniger falsch-positive Warnmeldungen

Was sind Ihre Vorteile?

Schutz von Endpoints

Datei-, Web- und E-Mail-Virenschutz, Netzwerkschutz, Verhaltenserkennung, Fehlerbehebung, Exploit- und BadUSB-Prävention, HIPS, AMSI, Anti-Cryptor

Security Management

Firewall, Web-, Geräte- und Anwendungskontrollen, adaptive Kontrolle von Anomalien, Erkennen und Blockieren von Cloud-Services, Überwachtung der Dateiintegrität, Protokollprüfung, Überwachung der Systemintegrität

Schutz und Verwaltung mobiler Geräte

Schutz, Kontrollen und Management, iOS MDM

IT-Szenarien

Schwachstellenbewertung (Vulnerability Assessment), Patch-Management, Datenlöschung, Software-/Hardware-Bestandsaufnahme, Drittanbieter-Apps und Betriebssysteminstallation, Remote-Verbindung

Verschlüsselung

Verschlüsselung und Verschlüsselungsmanagement

EDR-Funktionen

Ursachenanalyse, IoC-Scan, One-Click und automatisierte Reaktion, Handlungsempfehlungen

Erweiterte EDR-Funktionalität

Sammeln von Telemetriedaten, Threat Hunting-Funktionen, Erkennung von Angriffsindikatoren (IoA), MITRE ATT&CK-Mapping

XDR-Funktionen

Zusammenführung von Warnmeldungen, Sandboxing, AD-Integration, Threat Intelligence / Kaspersky Security Network Enrichment, Fallmanagement, manuelle und automatisierte Playbooks, Untersuchungs-Grafik, Drittanbieteranbindung, Protokollverwaltung und Datenspeicher, vollautomatische Reaktion, Bedrohungserkennung und Kreuzkorrelation

Und wenn Sie bereits ein Kaspersky-Sicherheitspaket nutzen?

Ihre Kaspersky-Lösung	Empfohlene Migration	Im Paket enthaltene zusätzliche Funktionen
Kaspersky Endpoint Detection and Response Standard / Advanced / Expert*	Kaspersky Next XDR Expert	• Asset-übergreifende Szenarien • Zusammenführen von Warnmeldungen • Incident Workflow • Untersuchungs-Diagramm

* Bitte beachten Sie, dass Sie Kaspersky EDR Expert auch weiterhin als Einzellösung erwerben und einsetzen können oder alternativ ein Upgrade durchführen und die Lösung als Teil von Kaspersky Next XDR Expert nutzen können

Weitere Informationen zu Kaspersky Next XDR Expert

Kaspersky Next XDR Expert

Kaspersky Next EDR Foundations

Mehr erfahren

Kaspersky Next EDR Optimum

Weitere Informationen

Weitere Informationen zu Kaspersky Next finden Sie unter:
https://go.kaspersky.com/next

Cyber Threat News: securelist.com
IT Security News: kaspersky.de/blog/b2b/
IT-Sicherheit für SMB: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

kaspersky.de