Unterstützen Sie Ihr wachsendes Unternehmen mit erweiterter Sicherheit, die effektiv, benutzerfreundlich und kosteneffizient ist

Kaspersky Next XDR Optimum

kaspersky bring on the future

Für kleine und mittelständische Unternehmen

Kaspersky Next XDR Optimum richtet sich an kleine und mittelständische Unternehmen mit einer etablierten IT-Infrastruktur. Unabhängig davon, ob die Sicherheit vom gesamten IT-Team oder von dedizierten Mitarbeitern verwaltet wird, bietet die Lösung einfach zu verwaltende Tools, die starken, umfassenden Schutz bieten, ohne die vorhandenen Ressourcen zu überlasten.

Nutzen Sie Ihre Ressourcen optimal und steigern Sie die Wirksamkeit Ihrer Reaktion auf Vorfälle

Cyberbedrohungen, die auf kleine und mittlere Unternehmen abzielen, werden immer komplexer. Die Angreifer nutzen zunehmend legitime Systemtools und fortgeschrittene Techniken, um nicht entdeckt zu werden. Mitarbeiter, die sich der Cybersicherheitsrisiken nicht bewusst sind, sind außerdem anfällig für Phishing- und Social-Engineering-Angriffe. Diese können finanzielle und rufschädigende Folgen haben.

Gleichzeitig erschweren begrenzte Ressourcen, darunter knappe Budgets und ein Mangel an qualifiziertem Personal, die Abwehr dieser Bedrohungen zusätzlich. Deshalb sind fortschrittliche und dennoch benutzerfreundliche Tools, die das richtige Maß an Schutz für Ihr Unternehmen bieten, so wichtig.

Steigern Sie Ihre Sicherheit mit Kaspersky Next XDR Optimum

Die Lösung wurde für kleinere Sicherheitsteams entwickelt, um die Reaktionsfähigkeit bei Vorfällen zu verbessern und Fachwissen aufzubauen – und das ganz ohne zusätzliche Belastung durch zeitaufwändige Routineaufgaben. Da mehrere Prozesse automatisiert sind, kann sich Ihr Team auf das Wesentliche konzentrieren.

Kaspersky Next XDR Optimum lässt sich problemlos in Ihre bestehende Infrastruktur integrieren, ohne dass Sie neue Systemkomponenten hinzufügen müssen.

Erkennung, Analyse und Reaktion

- Verhaltens-erkennung
- Aggregation von Warnungen
- Cloud Sandbox
- Erkennung von Bedro-hungsindikatoren (IoCs) & benutzerdefinierte IoCs
- Ursachenanalyse
- Bandbreite der Reaktionsmaß-nahmen

Endpoint-Schutzfunktionen

- Optimierte Anti-Malware
- Erweitertes Hardening
- Vulnerability Assessment
- Endpoint-Kontrolle
- Datenschutz
- Patch Management

Vom fortschrittlichen Endpoint-Schutz und Cloud-Sicherheit bis hin zur Automatisierung von IT-Aufgaben und wichtigen XDR-Funktionen:

Zukunftssicherer Endpoint-Schutz für Ihr Unternehmen

Vermeiden Sie Geschäftsunterbrechungen mit automatischem Schutz durch branchenbewährte, ML-basierte Anti-Ransomware- und Anti-Malware-Tools, die Infektionen durch bekannte und unbekannte Bedrohungen verhindern.

Behebung von Schwachstellen durch System Hardening und Awareness-Schulungen

Verringern Sie Ihre Angriffsfläche mit einem auf dem Benutzerverhalten basierenden System Hardening, und sparen Sie Zeit mit einem zentralisierten Schwachstellen-, Patch- und Verschlüsselungsverwaltung. Außerdem bieten wir alle Schulungen an, die Ihr Team benötigt, um die neuen Sicherheitsfunktionen optimal zu nutzen.

Erweitern Sie Ihre **Detection and Response-Fähigkeiten**

Erhalten Sie Einblicke in Bedrohungen und wie sie sich innerhalb und außerhalb von Endpoints bewegen. Nutzen Sie Automatisierung und geführte Reaktionsmaßnahmen, um Angriffen entgegenzuwirken, sowie Untersuchungstools, um deren Aktivitäten nachzuverfolgen.

Schulen Sie Ihr gesamtes Team so, dass es eine aktive Rolle bei der Sicherheit spielen kann

Statten Sie Ihre IT-Mitarbeiter und nicht-technischen Mitarbeiter mit dem Wissen und den Fähigkeiten aus, die sie benötigen, um sicher zu bleiben. Stärken Sie Ihr IT-Sicherheitsteam und schaffen Sie gleichzeitig eine starke, sicherheitsbewusste Kultur in Ihrer gesamten Belegschaft.

Nutzen Sie unser Cloud-basiertes System für die **Dateiverarbeitung**

Untersuchen Sie bösartige Dateien ganz einfach und erhalten Sie mehr Kontext und Details mit unserer Cloud Sandbox-Integration – laden Sie potenziell schädlicher Proben hoch, um ihre Reputation innerhalb von Sekunden direkt über die Produktschnittstelle zu überprüfen, und nutzen Sie die generierten Daten für zukünftige IoC-Scans.

Kontrolle der Schatten-IT mit Cloud-Sicherheit, auf die Sie sich verlassen können

Verringern Sie Ihre Anfälligkeit und schützen Sie Ihre Daten und Mitarbeiter durch Kontrolle der Schatten-IT. Behalten Sie im Auge, welche Cloud-Services genutzt werden, und unterbinden Sie unbefugte Zugriffe. Finden Sie heraus, welche sensiblen Daten in Microsoft-365-Anwendungen gespeichert sind.

Profitieren Sie von **verschiedenen Bereitstellungsoptionen**

Reduzieren Sie die Gesamtbetriebskosten, indem Sie Cloud-basierte Bereitstellungs- und Automatisierungstools nutzen, oder installieren Sie On-Prem, um die volle Kontrolle zu behalten[1].

[1] Die lokale Verwaltungskonsole ist Linux-basiert. Kaspersky Next XDR Optimum unterstützt alle Betriebssysteme über seine Endpoint-Agenten und die Cloud-Konsole. Eine Cloud-basierte Bereitstellungsoption wird ab dem 4. Quartal 2025 verfügbar sein.

Kaspersky Next XDR Optimum – Teil unserer Kaspersky Next-Produktlinie

Kaspersky Next ist eine mehrstufige Produktlinie für Unternehmen jeder Größe. Kaspersky Next Optimum richtet sich an kleine und mittelständische Unternehmen mit schlank aufgestellten Cybersicherheitsteams, 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.

Warum Kaspersky Next Optimum?

Basiert auf unserer branchenführenden Endpoint-Lösung

Seit über einem Jahrzehnt belegen Kaspersky-Produkte in unabhängigen Tests und Bewertungen stets Spitzenplätze. Unser bewährter automatisierter Endpoint-Schutz reduziert die Anzahl der Warnmeldungen, die Sicherheitsteams analysieren müssen, und verbessert so ihre Effizienz.

Basierend auf umfassendem Wissen und Expertise

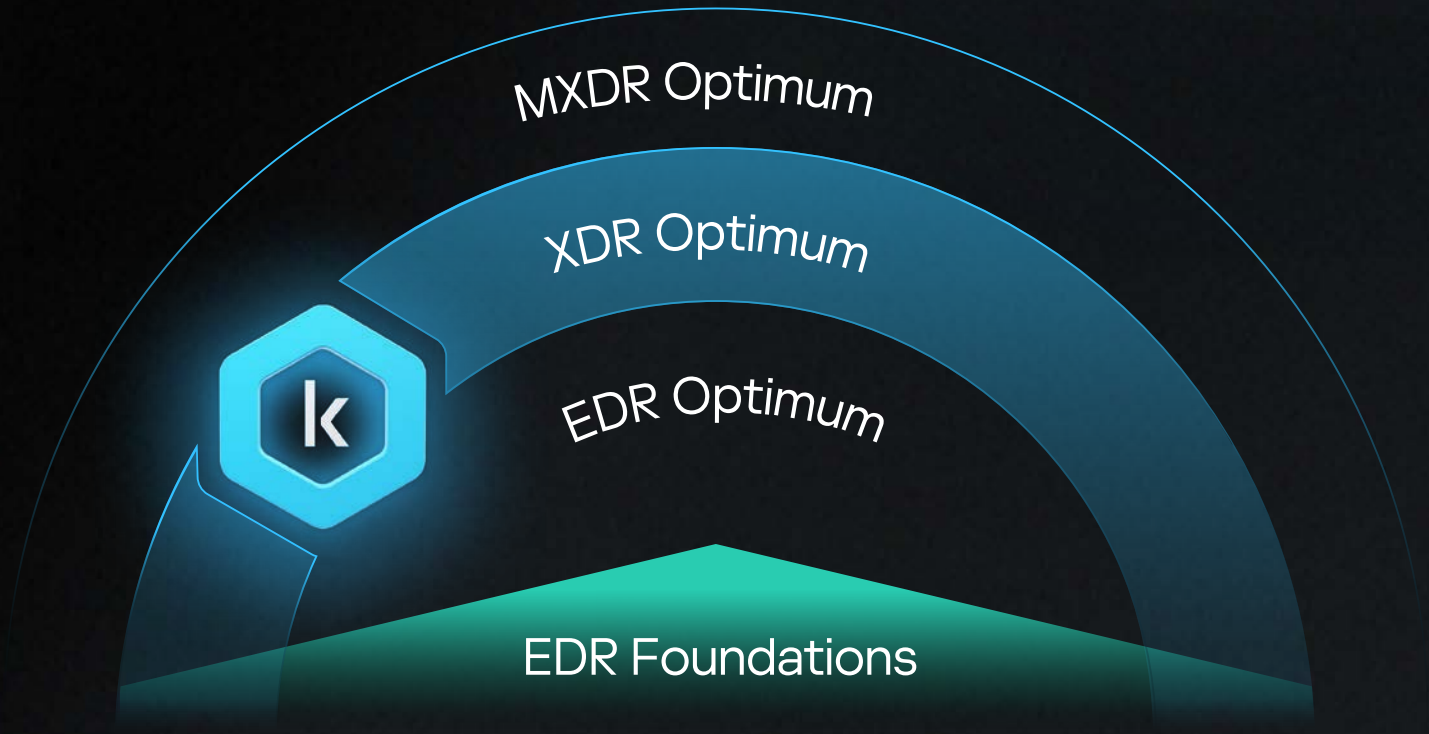
Kaspersky Next basiert auf der jahrzehntelangen Erfahrung und dem umfassenden Fachwissen unserer globalen Sicherheitsteams. Unsere Spezialisten arbeiten gemeinsam an der Bewältigung komplexer Cyberbedrohungen und entwickeln die Technologien, die unseren Produkten zugrunde liegen, kontinuierlich weiter. Dieser Ansatz gewährleistet, dass unsere Lösungen zuverlässig, innovativ und auf die realen Sicherheitsanforderungen abgestimmt sind.

Mehrschichtige Prävention auf der Grundlage von KI-Technologie

Kaspersky verwendet prädiktive Algorithmen, Clustering, neuronale Netze, statistische Modelle und Experten-Algorithmen, um die Erkennungsgeschwindigkeit und -genauigkeit zu erhöhen.

Flexibler Cyberschutz

Kaspersky Next schützt Unternehmen jeder Größe. Wenn Ihre Anforderungen wachsen, können Sie problemlos von grundlegendem Endpoint-Schutz zu erweiterten Lösungen skalieren, die in höheren Stufen verfügbar sind.



www.kaspersky.de

Mehr erfahren

#kaspersky
#bringonthefuture