Kaspersky Next
EDR Optimum

Das bietet Kaspersky Next EDR Optimum

Was ist Kaspersky Next EDR Optimum?

Kaspersky Next EDR Optimum bietet starken Endpoint-Schutz, verbesserte Kontrollen, Trainings, Patch-Management und vieles mehr – und zudem noch wichtige EDR-Funktionen.

Transparenz, einfache und schnelle Untersuchung sowie Handlungsempfehlungen stellen sicher, dass Ihre IT und IT-Sicherheitsteams Angriffe schnell und mit minimalem Aufwand an Ressourcen abwehren können.

Warum Kaspersky Next EDR Optimum – und warum gerade jetzt?

Angesichts der sich ständig verändernden Bedrohungslandschaft ist EDR längst keine Option mehr, sondern eine Notwendigkeit.

Jahrelang konnten sich kleine und mittlere Unternehmen (KMUs) sowie Unternehmen mit begrenztem Budget auf Endpoint Protection-Plattformen (EPP) verlassen, wenn es um den Schutz vor gängigen Bedrohungen ging, die in Masse ohne großen Aufwand produziert wurden. Doch die Angreifer von heute nehmen Organisationen jeglicher Größe, Branche und IT-Reife ins Visier – und ihre Angriffe werden immer gefährlicher.

Die fortschreitende Entwicklung der Bedrohungslandschaft hat zur Folge, dass immer raffiniertere Bedrohungen, die bisher nur gegen Großunternehmen eingesetzt wurden, mittlerweile auch KMU und kleinere Großunternehmen betreffen, die nicht über die internen Ressourcen verfügen, um dagegen vorzugehen.

Das gilt vor allem für versteckte Bedrohungen. Diese nutzen für ihre Angriffe legitime Tools aus, enthalten gebrauchsfertige Szenarien zur Umgehung der EPP und sind zudem im Darknet kostengünstig und problemlos erhältlich. Dadurch hat sich das Cybersicherheits-Risiko für Unternehmen, die mit herkömmlichen EPP-Lösungen arbeiten, erheblich erhöht.

Wer bisher nur auf EPP gesetzt hat, empfindet die Einführung von EDR-Funktionen (Endpoint Detection and Response) mit allen dafür erforderlichen Tools und Kompetenzen nicht selten als große Hürde. Das muss aber nicht sein.

Mit passenden EDR-Funktionen zusätzlich zu einer modernen EPP lässt sich eine äußerst effektive Abwehr gegen hochentwickelte und versteckte Bedrohungen aufbauen.

Ein Upgrade auf EDR muss keine Herausforderung sein

Viele Organisationen haben nur begrenzte Zeit und Ressourcen (oder eine kleine IT-Sicherheitsabteilung und keine Pläne, diese zu erweitern). Dennoch ist es für sie wichtig zu wissen, was in ihrer Infrastruktur vor sich geht, und sie müssen in der Lage sein, auf versteckte Bedrohungen zu reagieren, bevor Schaden entsteht.

Die Ergänzung moderner EPP durch geeignete EDR-Funktionen kann einen äußerst wirksamen Schutz gegen fortgeschrittene, ausweichende Bedrohungen bieten. Wenn Sie also noch nicht mit EDR gearbeitet haben, sollten Sie sich für eine Lösung entscheiden, die automatisierte und/oder schnelle, präzise Abwehrmechanismen per Mausklick ermöglicht, um Dateien in Quarantäne zu setzen, den Host zu isolieren, Prozesse anzuhalten, Objekte zu löschen etc.

Mit zunehmender Erfahrung – oder wenn Sie bereits über IT-Sicherheitsexperten und/oder EDR verfügen – brauchen Sie zusätzliche Informationen, Einblicke und effektive Tools für weitere Untersuchungen. Dazu gehören Funktionen für die Ursachenanalyse, eine Importfunktion für Bedrohungsindikatoren (IoCs) sowie die Möglichkeit, eigene IoCs anzulegen und alle Endpoints danach zu scannen.

Das können Sie von einer guten EDR-Lösung erwarten:

- Robuster Schutz gegen immer häufigere und zerstörerischere versteckte Bedrohungen
- Zeit- und Ressourcenersparnis durch ein einfaches, automatisiertes Tool
- Scannen sämtlicher Endpoints nach IoCs, um das Ausmaß eines Angriffs zu ermitteln.
- Klärung der Bedrohungsursache und wie sie zustande gekommen ist
- Abwendung weiteren Schadens durch schnelle automatisierte Gegenmaßnahmen

Ist Ihre EPP der wachsenden Zahl neuer, unbekannter und versteckter Bedrohungen nicht mehr gewachsen? Fehlt Ihnen der Überblick, was auf Ihren Endpoints vor sich geht? Bereiten Ihnen drohende Geldstrafen und eine mögliche Rufschädigung infolge eines größeren Sicherheitsvorfalls Sorge? Dann ist eine moderne EDR-Lösung wie Kaspersky Next EDR Optimum für Sie die perfekte Möglichkeit zum Einstieg oder Ausbau.

Ein Cyberangriff bedroht Ihr Unternehmen: Was tun?

Es ist Ihr erster Arbeitstag als IT-Sicherheitsbeauftragter, Sie sind noch gar nicht richtig angekommen, und schon steht Ihr Unternehmen unter Beschuss.

Was würden Sie tun? Wie würden Sie reagieren?

Erfahren Sie mehr
www.kaspersky.de/response-game

So kann Kaspersky Next EDR Optimum Sie unterstützen

Wirkungsweise

Bietet starken Endpoint-Schutz, überlegene Kontrollmechanismen, Schulungsangebote, Patch-Management und vieles mehr

Essenzielle EDR-Funktionen sorgen für mehr Transparenz über Bedrohungen, eine einfache Untersuchung und verständliche Handlungsempfehlungen, um Angriffe mit minimalen Ressourcen schnell abzuwehren

Funktionen

Verbessert die Sichtbarkeit und Visualisierung von Bedrohungen

Vereinfacht die Ursachenanalyse

Liefert schnelle, automatisierte Gegenmaßnahmen

Konsole lokal oder in der Cloud

Geschäftswert

Eine zentrale Lösung schützt Ihr Unternehmen vor gefährlichen, versteckten Bedrohungen und verbessert Ihre Cybersicherheit

Steigert die Kosteneffizienz. Versetzt die IT bzw. IT-Sicherheitsteams in die Lage, effektiver zu arbeiten, ohne mit mehreren Tools und Konsolen jonglieren zu müssen.

Automatisiert eine Vielzahl von Prozessen und macht dadurch unabhängig von manuellen Eingriffen mit entsprechenden Ausfallzeiten

Vereinfacht die Überwachung, Erkennung und Untersuchung von Bedrohungen sowie die Vorfallreaktion und Prävention

Wer ist die Zielgruppe

Unternehmen mit einem internen IT-Sicherheitsteam (oder auch nur 1 – 3 Sicherheitsexperten), das einen detaillierten Einblick in die Endpunkte und automatische Abwehrmaßnahmen benötigt, um manuelle Aufgaben zu reduzieren

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 Anomaly Control, Überwachung 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

Cloud-Schutz

Erkennen und Blockieren von Cloud-Services, Datenerkennung, Sicherheit für MS O365

Bildung

Cybersicherheits-Training für IT-Administratoren

EDR-Funktionen

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

Kaspersky Next EDR Optimum unterstützt Unternehmen, die ihre Sicherheitssysteme sukzessive an ihre wachsende IT-Umgebung anpassen möchten

Und wenn Sie bereits ein Kaspersky-Sicherheitspaket nutzen?

Wenn ein Unternehmen expandiert und seine IT immer komplexer wird, steigen auch die Anforderungen an die Sicherheit. Kaspersky Next EDR Optimum unterstützt Unternehmen, die ihre Sicherheitssysteme sukzessive an ihre wachsende IT-Umgebung anpassen möchten, indem sie mit der Entwicklung von Prozessen und den notwendigen Kompetenzen zur Vorfallreaktion beginnen. So können sie hochentwickelte Bedrohungen abwehren, die mit einer größer werdenden Angriffsfläche einhergehen. So werden Angriffe schnell und automatisch erkannt, analysiert und abgewehrt. Dies reduziert ihre negativen Folgen erheblich.

Ihre Kaspersky-Lösung	Empfohlene Migration	Im Paket enthaltene zusätzliche Funktionen
Kaspersky Endpoint Security Cloud Pro	Kaspersky Next EDR Optimum	• Monitoring der Dateiintegrität • Protokollüberprüfung • Monitoring der Systemintegrität • Software-/Hardware-Inventarisierung • Installation von Drittanbietersoftware • Lokale Installation des Betriebssystems • Möglichkeit zur Nutzung der Enterprise-Konsole lokal oder in der Cloud (Expert-Ansicht)
Kaspersky Endpoint Security for Business Advanced Kaspersky Total Security for Business	Kaspersky Next EDR Optimum	• Option mit benutzerfreundlicher Cloud Console • Essenzielle EDR-Funktionen, einschließlich Ursachenanalyse, IoC-Untersuchung und automatisierte Reaktionen • Cybersicherheits-Training für IT-Administratoren • Cloud Discovery und Blockierung • Datenerkennung • Sicherheit von MS Office 365
Kaspersky Endpoint Detection and Response Optimum	Kaspersky Next EDR Optimum	• Option mit benutzerfreundlicher Cloud Console • Cybersicherheits-Training für IT-Administratoren • Cloud Discovery und Blockierung • Datenerkennung • Sicherheit von MS Office 365

Weitere Informationen zu Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations — Mehr erfahren

Kaspersky Next XDR Expert — Weitere Informationen

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

Finden Sie mit Hilfe unseres interaktiven Tools heraus, welche Produktstufe am besten zu Ihnen passt: https://go.kaspersky.com/Kaspersky_Next_Tool

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