Kaspersky Next
EDR Foundations

Das bietet Kaspersky Next EDR Foundations

Was ist Kaspersky Next EDR Foundations?

Kaspersky Next EDR Foundations ist das Einstiegsprodukt innerhalb der drei Produktstufen von Kaspersky Next. Mit ML-gestütztem, leistungsstarkem Endpoint-Schutz, flexiblen Sicherheitskontrollen und EDR-Ursachenanalyse bietet die Lösung Unternehmen alles, was sie brauchen, um ihre Cybersicherheit auf ein solides Fundament zu stellen.

Eine einfache Konsole, die Bereitstellung in der Cloud oder lokal sowie eine Vielzahl an Funktionen, die die Arbeitsqualität verbessern, reduzieren die Komplexität und steigern die Effizienz.

Warum Kaspersky Next EDR Foundations – und warum gerade jetzt?

Verlassen Sie sich nicht ausschließlich auf Ihre EPP-Plattform

Endpoint Protection-Plattformen (EPPs) sind für IT-Teams mittlerweile so selbstverständlich geworden, dass sie sozusagen schon „zum Inventar gehören". Die überwiegende Mehrheit der Unternehmen konzentriert sich neben der Absicherung ihres Perimeters mit Firewalls und E-Mail-Schutz auf ihre Endpoints, also PCs, Laptops, Server (physisch und virtuell) und Workstations, als primären Abwehrmechanismus gegen Cyberbedrohungen.

Daher spielt die EPP eine zentrale Rolle bei der Abwehr komplexer Angriffe. Dabei darf nicht vergessen werden, dass auch die Entwicklung von EPPs nicht stehen bleibt und immer wieder neue Anforderungen auftauchen, denen diese gerecht werden müssen. Traditionelle EPPs sind der wachsenden Vielfalt an Bedrohungen längst nicht mehr gewachsen.

Traditionelle EPP-Plattformen werden zum Problem

Jahrelang konnten kleine und mittlere Unternehmen (KMUs) sowie Unternehmen mit eingeschränktem Budget beim Schutz vor gängigen Bedrohungen auf EPP bauen. Aber die Angreifer von heute nehmen Organisationen jeglicher Größe, Branche und IT-Reife ins Visier.

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

Selbst ein IT-Team mit Basiswissen im Sicherheitsbereich braucht einen Einblick in die Vorgänge auf den einzelnen Endgeräten, um diese detaillierter analysieren und die Bedrohung besser verstehen zu können.

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.

Diese Probleme werden durch den Mangel an Transparenz, den die traditionelle EPP aufweist, noch verschärft. Im Wesentlichen können diese Lösungen nur wie eine Ampel Rot oder Grün zeigen, um zu signalisieren, ob gerade ein Angriff stattfindet oder nicht. Doch selbst ein IT-Team mit Basiswissen im Sicherheitsbereich braucht einen Einblick in die Vorgänge auf den einzelnen Endgeräten, um diese detaillierter analysieren und die Bedrohung besser verstehen zu können.

Woher wissen Sie, dass es Zeit ist, Ihre Abwehr zu verbessern?

Daran erkennen Sie, dass Ihre EPP nicht mehr Ihren Anforderungen entspricht

Die folgenden Anzeichen deuten darauf hin, dass es an der Zeit ist, Ihre Verteidigung über die traditionelle EPP hinaus zu verstärken:

- Ihre EPP kann die wachsende Zahl von neuen, unbekannten und versteckten Bedrohungen nicht mehr stoppen.
- Es fehlt Ihnen an Transparenz, um zu sehen, was auf Ihren Endpoints vor sich geht. Dies bedeutet, dass Sie nicht in der Lage sind, Ursachenanalysen und Untersuchungen durchzuführen und in Echtzeit auf Bedrohungen zu reagieren. Oder Sie müssen dies von Fall zu Fall manuell mit Standardtools des Betriebssystems durchführen, was langsam, komplex und fehleranfällig ist.
- Sie verfügen nicht über die erforderlichen Fachkenntnisse oder Kapazitäten im Bereich IT-Sicherheit, um mit immer raffinierteren Bedrohungen umzugehen.
- Sie sind besorgt aufgrund der drohenden Geldstrafen oder der möglichen Rufschädigung für Ihr Unternehmen als Folge eines größeren Sicherheitsvorfalls.

Wenn Sie eines dieser Probleme haben, kann eine moderne EPP-Lösung wie Kaspersky Next EDR Foundations nicht nur Abhilfe schaffen. Mit ihren unkomplizierten EDR-Funktionen (Endpoint Detection and Response) ermöglicht sie auch den nahtlosen Übergang von der herkömmlichen EPP zu einer komplett ausgestatteten EDR- und XDR-Lösung (Extended Detection and Response).

So kann Kaspersky Next EDR Foundations Sie unterstützen

Wirkungsweise

Tools für ML-gestützten leistungsstarken Endpoint-Schutz, flexible Sicherheitskontrollen und EDR-Ursachenanalyse sorgen dafür, dass Ihre Cybersicherheit auf einem soliden Fundament steht

Funktionen

Bietet effektiven Ransomware-Schutz für alle Endgeräte

inklusive EDR-Basisfunktionen für einen tieferen Einblick in Bedrohungen und Angriffe

Konsole lokal oder in der Cloud

Geschäftswert

Robuster Endpoint-Schutz gepaart mit zusätzlicher Transparenz, grundlegenden EDR-Funktionen und IT-Szenarien wie Schwachstellenbewertung und Software-/Hardware-Inventarisierung

Wer ist die Zielgruppe

Unternehmen mit eigenem IT-Administrator, aber begrenzten Ressourcen für die IT-Sicherheit

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, Gerät, Anwendungskontrollen, Cloud-Erkennung

Schutz und Verwaltung mobiler Geräte

Schutz, Kontrollen und Management, iOS MDM

IT-Szenarien

Schwachstellenbewertung, Software-/Hardware-Inventarisierung

EDR-Funktionen

Ursachenanalyse

Kaspersky Next EDR Foundations vereint in sich die wesentlichen Vorteile und Funktionen von Kaspersky Endpoint Security Cloud, Cloud Plus und Kaspersky Endpoint Security for Business Select

Und wenn Sie bereits ein Kaspersky-Sicherheitspaket nutzen?

In Kaspersky Next EDR Foundations sind die wesentlichen Stärken und Funktionen von Kaspersky Endpoint Security Cloud, Cloud Plus und Kaspersky Endpoint Security for Business Select in einer einzigen leistungsstarken Lösung vereint. Diese kontrolliert und schützt Ihre Endgeräte und lässt sich ohne großen Aufwand installieren und verwenden. Kunden von Kaspersky Endpoint Security Cloud und Cloud Plus profitieren von wichtigen Kontrollfunktionen (insbesondere Anwendungskontrolle, BadUSB usw.), während Nutzer von Kaspersky Endpoint Security for Business Select zusätzlich die Vorteile der Cloud Console und der Erkennung von Cloud-Services erhalten. Außerdem können sie alle EDR-Funktionen wie die Ursachenanalyse nutzen.

Ihre Kaspersky-Lösung	Empfohlene Migration	Im Paket enthaltene zusätzliche Funktionen
Kaspersky Endpoint Security Cloud	Kaspersky Next EDR Foundations	• Schutz vor BadUSB-Angriffen • Anwendungs-, Web- und Gerätekontrolle • Ursachenanalyse
Kaspersky Endpoint Security Cloud Plus	Kaspersky Next EDR Foundations	• Schutz vor BadUSB-Angriffen • Programmkontrolle
Kaspersky Endpoint Security for Business Select	Kaspersky Next EDR Foundations	• Übersichtliche Cloud Console • Ursachenanalyse • Erkennung von Cloud Services

Weitere Informationen zu Kaspersky Next EDR Foundations

Kaspersky Next EDR Foundations

Kaspersky Next EDR Optimum — Mehr erfahren

Kaspersky Next XDR Expert — Mehr erfahren

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

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