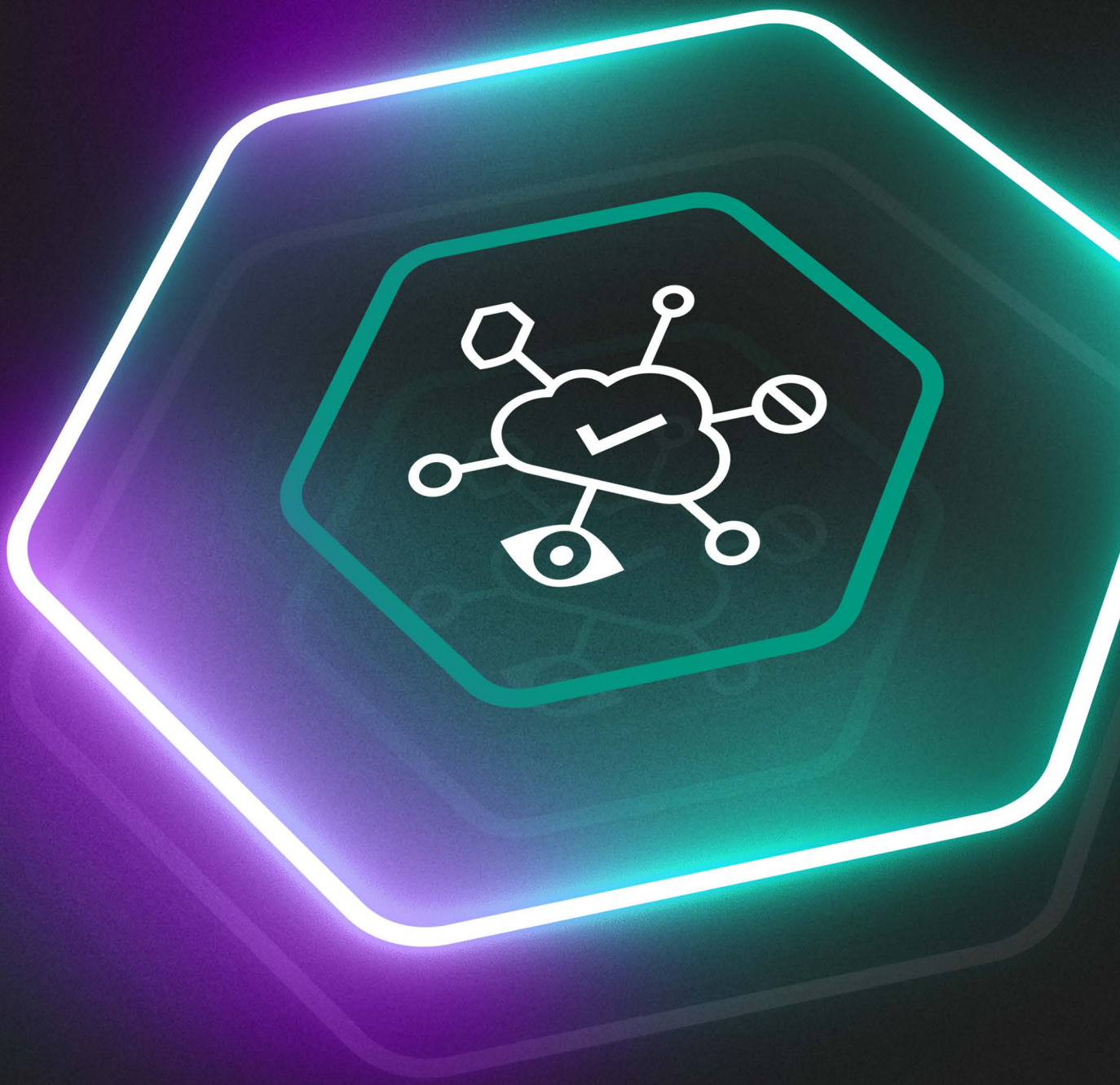

Kaspersky Endpoint Detection and Response

Expert

kaspersky BRING ON THE FUTURE

Eine Lösung für alles

Kaspersky EDR Expert ist eine Einzellösung, die über eine Cloud-basierte zentrale Verwaltungsplattform oder – in komplett isolierten Umgebungen – über eine Offline-Konsole verwaltet werden kann.

Kaspersky Endpoint Detection and Response Expert

Cyberkriminelle werden immer raffinierter und können den bestehenden Schutz erfolgreich umgehen. Jeder Bereich Ihres Unternehmens kann Risiken ausgesetzt sein, die geschäftskritische Prozesse stören, Produktivität beeinträchtigen und die Betriebskosten erhöhen.

Verstärken Sie zuerst Ihre Endpoint-Abwehr

In Unternehmens-Endpoints laufen alle Daten, Nutzer und Unternehmenssysteme zusammen, um Geschäftsprozesse in Gang zu setzen und zu implementieren. Diese Endpoints bilden nach wie vor das Hauptziel der Cyberkriminellen.

Kaspersky Endpoint Detection and Response (EDR) Expert bietet eine umfassende Übersicht über alle Endpoints in Ihrem Unternehmensnetzwerk und ermöglicht dank fortschrittlicher Abwehrfunktionen die Automatisierung von Routineaufgaben. So können Analysten komplexe und APT-ähnliche Bedrohungen erkennen, priorisieren, untersuchen und neutralisieren.

Aktuelle Herausforderungen

IT-Sicherheitsteams können Endpoints nur dann effektiv überwachen, wenn im System Transparenz herrscht. Die Aufdeckung eines Vorfalls kann Wochen oder sogar Monate länger dauern, als sie sollte. Der Grund: Es kann schwierig sein, genau zu erkennen und zu verstehen, was passiert ist, wie es passiert ist und wie man es beheben kann.

Ineffizienz. Wenn Analysten gezwungen sind, über mehrere dezentrale Konsolen hinweg zu arbeiten, wird der gesamte Prozess ausgebremst; menschliche Fehler werden wahrscheinlicher. Ebenso ergeht es IT-Sicherheitsexperten, wenn sie routinemäßige Erkennungsvorgänge manuell durchführen müssen.

Fehlen relevanter Daten: Wenn Bedrohungsdaten nicht operationalisiert werden können und niemand den Überblick über Taktiken, Techniken und Verfahren des Gegners behält, erschwert das nicht nur die Priorisierung von Warnungen, sondern auch die weitere Untersuchung und Einleitung von Abwehrmaßnahmen.

Vorteile von Kaspersky EDR Expert für Ihre Organisation

1 Effektive Kontrolle und Überwachung sämtlicher Endpoints

Man muss das Gesamtbild betrachten – also wo die Bedrohung herkam, wie sie sich ausgebreitet hat, welche Hosts betroffen sind und was genau zu tun ist, um mögliche Konsequenzen abzuwehren.

2 Arbeitserleichterung für Ihr IT-Sicherheitsteam

Die schnelle, präzise Eindämmung und die Bereinigung von Vorfällen in Umgebungen mit verteilten Infrastrukturen werden durch zentralisierte und automatisierte Maßnahmen unterstützt, die zur Optimierung der Arbeitsabläufe in Ihren Sicherheitsteams beitragen. Und das alles ohne teure zusätzliche Ressourcen und Ausfallzeiten und ohne Produktivitätsverlust.

3 Erfolgreiches Threat Hunting und Bedrohungsabwehr – und zwar schnell

Rohdaten und Risikoeinstufungen werden zentral zusammengefasst und zahlreiche Funktionen erleichtern das Untersuchen von Vorfällen, wie unsere Angriffsindikatoren (Indicators of Attack, IoAs), die Kontextanreicherung durch MITRE ATT&CK, der flexible Abfrage-Generator und der Zugriff auf unsere Wissensdatenbank im Threat Intelligence Portal. Damit wird die Suche nach Bedrohungen effektiver und im Sinne der Schadensbegrenzung und -vermeidung kann schnell auf Vorfälle reagiert werden.

Aktuelle Herausforderungen

Unzulänglichkeiten bei der Reaktion und Untersuchung. Allein die Erkenntnis, dass eine potentielle Bedrohung der Infrastruktur entdeckt wurde, bietet noch keine Garantie, dass die daraufhin ergriffenen Maßnahmen auch wirksam sind. Es kommt in erster Linie darauf an, in Echtzeit auf die Bedrohung zu reagieren und den Vorfall umfassend zu untersuchen. Nur so kann ein erneutes Auftreten verhindert werden.

Verschwendung von teuren Ressourcen. Analysten können sich nicht ausreichend auf komplexe Bedrohungen konzentrieren, wenn sie ihre Zeit mit nebensächlichen Warnhinweisen vergeuden, die eine effektive Endpoint Protection-Lösung automatisch abarbeiten sollte. Abgesehen von der Ressourcenverschwendung kann eine solche Schwemme von Meldungen zum Burnout der Analysten führen, so dass sie die wirklich wichtigen Hinweise übersehen.

Vorteile von Kaspersky EDR Expert für Ihre Organisation

4 Schnellere und effektivere Abwehr

Bei der Abwehr von komplexen und APT-ähnlichen Angriffen leisten Untersuchungen unter Anleitung und schnellere, präzisere Gegenmaßnahmen einen wichtigen Beitrag. Kaspersky EDR Expert bietet einen nahtlosen Workflow mit zentralisiertem Vorfallmanagement und angeleiteter Untersuchung für alle Endpoints im Unternehmensnetzwerk.

5 Optimierter Einsatz Ihrer Lösung – und damit auch Ihrer Experten

Allzu oft werden für den Betrieb einer EDR-Lösung teure Analysten eingestellt, die am Ende nur Warnhinweise abarbeiten, für die sie hoffnungslos überqualifiziert sind, die Ihre EPP ihnen aber nicht abnimmt. Unsere EDR-Lösungen basieren auf unserer häufig getesteten und vielfach ausgezeichneten EPP-Lösung, welche die überwiegende Mehrheit der Warnhinweise automatisch verarbeitet. Ihre Analysten können sich auf die Meldungen konzentrieren, die wirklich ihre Aufmerksamkeit und ihr Fachwissen erfordern. Unsere EPP- und EDR-Produkte bilden eine geschlossene Einheit und arbeiten mit demselben Endpoint-Agent.

Kaspersky EDR Expert ist ideal, wenn Ihre Organisation folgende Ziele verfolgt:

- Verbesserung Ihrer Sicherheit mit einer benutzerfreundlichen, unternehmensweiten Lösung für Vorfallsreaktionen.
- Automatisierung von Bedrohungsidentifizierung und -reaktion, ohne Betriebsunterbrechung während der Untersuchungen.
- Verständnis, welche spezifischen Taktiken, Techniken und Prozeduren (TTPs) Angreifer einsetzen, um ihre Ziele zu erreichen. Dies ermöglicht eine schlagkräftigere Abwehr und die effektive Zuweisung von Sicherheitsressourcen.
- Verbesserung Ihrer Endpoint-Transparenz und Bedrohungserkennung mit fortschrittlichen Technologien.
- Aufbau einheitlicher und effektiver Prozesse für Threat Hunting, Incident Management und Vorfallsreaktion.
- Steigerung der Effizienz Ihres internen SOC, damit keine Zeit mit der Analyse irrelevanter Endpoint-Protokolle und -Warnhinweise vergeudet wird.
- Unterstützung der Richtlinienkonformität dank Durchsetzung von Endpoint-Protokollen, Alarmierungsüberprüfungen und Dokumentation von Untersuchungsergebnissen.

Die Vorteile von Kaspersky EDR Expert für Sie:

- **Die besten und modernsten Methoden zur Bedrohungserkennung Anhand von Profilen potenzieller Bedrohungsakteure lassen sich schädliche Aktivitäten innerhalb einer Infrastruktur sehr effizient und schnell erkennen.**

Mit Kaspersky EDR Expert werden die Gefährdungsindikatoren **(IoCs)** zentral aus Bedrohungsdatenquellen geladen. Außerdem lassen sich automatische IoC-Scans einplanen, was die Arbeit der Analysten erleichtert.

Dank unserer **IoA**-Engine (Indicators of Attack) erkennt Kaspersky EDR Expert verdächtige Aktionen anhand von Kaspersky-eigenen IoAs und unterstützt Sie mit automatisierten Funktionen beim Threat Hunting in Echtzeit.

Um sich ein genaueres Bild zu verschaffen, kann eine Datei oder ein Prozess manuell oder automatisch zur Verhaltensanalyse an die **Sandbox** weitergeleitet werden.

IoAs und Erkennungen in der Sandbox werden zur weiteren Analyse der Taktiken, Techniken und Verfahren des Gegners mit **MITRE ATT&CK** abgeglichen. Einzelne Ereignisse im Vorfallsbaum werden mit Kontext aus der MITRE-Wissensdatenbank angereichert. Dabei werden MITRE definierte Taktiken identifiziert und Ereignisse in einem Vorfallsdiagramm visuell aufbereitet.

Empfehlung für Gegenmaßnahmen

Die automatische Analyse aller Endpoint-Ereignisse, zusammen mit den erfassten TI-Daten, versorgt Sie mit klaren Ereignisbeschreibungen, Beispielen und Empfehlungen für Gegenmaßnahmen.

- Die Ursachen eines Vorfalls werden untersucht und eine Wiederholung verhindert. Kaspersky EDR Expert bietet Endpoint-Schutz auf hohem Niveau und erhöht die Effizienz Ihres SOC. Es stellt eine fortschrittliche Bedrohungserkennung bereit und ermöglicht den Zugriff auf retrospektive Daten auch dann noch, wenn auf kompromittierte Endpoints nicht zugegriffen werden kann oder Daten während eines Angriffs verschlüsselt wurden. Erhöhte Ermittlungsfähigkeiten durch unsere einzigartigen IoAs, die MITRE ATT&CK-Erweiterung und einen flexiblen Abfragegenerator sowie Zugang zu unserer Threat-Intelligence-Portal-Wissensdatenbank – all dies erleichtert die Bedrohungsjagd und eine schnelle Reaktion auf Zwischenfälle. Der Vorteil ist eine effektivere Schadensbegrenzung und -prävention.
- Entscheiden Sie sich für eine bequeme Telemetrie-Speicheroption für forensische Daten. Endpoint-Telemetriedaten werden standardmäßig 30 Tage lang in einer zentralen Datenbank gespeichert, Objekte und Auswertungen ohne Zeitlimit. So lassen sich Endpoint-unabhängig weitere forensische Analysen durchführen. Wenn Sie Ihre Telemetriedaten länger aufbewahren möchten, kann die Dauer auf 60 oder 90 Tage erhöht werden. Bei lokalen Installationen können Sie je nach Hardware-Kapazität und -Eigenschaften die Dauer der Datenspeicherung selbst festlegen.
- Auf den Kunden zugeschnittene Abwehrmöglichkeiten Über die zentrale Verwaltungskonsole können Ihre IT-Sicherheitsexperten Reaktionen per Mausklick auslösen. Dies reduziert die Zahl der manuellen Aufgaben auf ein Minimum und verkürzt Reaktionszeiten von Stunden zu Minuten.
- Arbeiten Sie reibungslos und effizient. Über den Endpoint-Aktivitätsbaum und die integrierten Visualisierungstools können Ihre Ermittler einfach per Mausklick interessante Datenelemente und zusätzliche Informationen im Bedrohungspfad weiterverfolgen. Die Verknüpfung von Ereignissen und Warnhinweisen hilft, das komplette Ausmaß eines Angriffs besser zu erkennen.

Funktionsweise

Auszeichnungen und Anerkennungen

Kaspersky-Produkte werden regelmäßig von weltweit tätigen Forschungsinstituten bewertet. Unsere Fähigkeit, Kunden Hilfe zur Selbsthilfe gegen Cyberangriffe zu leisten, ist weltweit anerkannt. Wir sind der am häufigsten getestete und ausgezeichnete Sicherheitsanbieter.

Kaspersky Endpoint Detection and Response erhält Bestnote im SE Labs-Test

Kaspersky EDR erhielt im Enterprise Advanced Security Test von SE Labs (früher bekannt als Breach Response Test) die höchste Auszeichnung AAA. Die Lösung wurde für ihre Fähigkeit ausgezeichnet, komplexe gezielte Angriffe zu erkennen, schädliches Verhalten von Anfang bis Ende eines Angriffs zu verfolgen und keine Fehlalarme (False Positives) zu generieren. Im Rahmen der Evaluierung wurde das Produkt Tools, Methoden und Verfahren ausgesetzt, wie sie von hochentwickelten Bedrohungsakteuren eingesetzt werden.

IDC MarketScape zeichnet Kaspersky als „Major Player" im Bereich der modernen Endpoint-Sicherheit für Großunternehmen und KMU aus

Damit Unternehmen auch wirklich solche Endpoint Protection-Plattformen und Endpoint Detection and Response-Lösungen (EDR) bewerten, die ihren eigenen Anforderungen entsprechen, hat sich IDC MarketScape die von MES-Anbietern zwischen April und September 2021 eingereichten Daten genau angesehen, um die unterschiedlichen Angebote entsprechend zuzuordnen.

MITRE ATT&CK bestätigt die Qualität der Erkennung

Anerkennung der Bedeutung der Analyse von Taktiken, Techniken und Verfahren (TTPs) bei der Untersuchung komplexer Vorfälle und der Rolle von MITRE ATT&CK auf dem heutigen Sicherheitsmarkt:

- Kaspersky EDR hat an der MITRE Evaluation Round2 (APT29) teilgenommen und ein hohes Leistungsniveau bei der Erkennung wichtiger ATT&CK-Techniken aus dem Bereich von Runde 2 gezeigt, die in entscheidenden Phasen der heutigen gezielten Angriffe angewandt werden.
- Die Entdeckungen von Kaspersky EDR werden mit Daten aus der MITRE ATT&CK-Wissensdatenbank ergänzt, um eine tiefgehende Analyse der TTPs Ihres Gegners zu ermöglichen.

Kaspersky Endpoint Detection and Response Expert

Weitere Informationen

www.kaspersky.de

© 2022 AO Kaspersky Lab.
Eingetragene Marken und Dienstleistungsmarken sind Eigentum der jeweiligen Inhaber.

Wenn Sie mehr darüber erfahren möchten, wie Kaspersky EDR Expert auch Ihr IT-Sicherheitsteam unterstützen kann, nehmen Sie Kontakt mit uns auf!