Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

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.

Mit Kaspersky EDR kann Ihre Organisation:

- Bedrohungen effizient **ÜBERWACHEN** – über Malware hinaus
- Bedrohungen effektiv **ERKENNEN** – unter Verwendung hoch entwickelter Technologien
- Rohdaten und Entscheidungen zentral **ERFASSEN**
- Schnell auf Angriffe **REAGIEREN**
- **Schädliche Aktionen durch entdeckte Bedrohungen** VERHINDERN

... – und das alles über eine intuitive Weboberfläche, die die Untersuchung und Reaktion vereinfacht.

Kaspersky EDR und wichtige Erkenntnisse aus dem IDC-Bericht "Endpoint Security 2020"*

Eine schwache EPP-Lösung macht den Wert eines EDR-Tools zunichte

Kaspersky bietet leistungsstarke vollständige Endpoint-Abwehr (EPP+EDR) über einen einzigen Agenten

Somit sind Mitarbeiter und Zeit die neuen ROI-Metriken für EDRTools

Kaspersky wendet ein hohes Maß an Automatisierung bei komplexen Problemen an und spart Ihren Sicherheitsexperten wertvolle Zeit

EDR muss Daten erschließen, die außerhalb der Endpoints liegen

Kaspersky steigert die EDR-Effektivität durch erweiterte E-Mail- und Web-basierte Erkennung und Sichtbarkeit von Bedrohungen durch ein einziges Tool

Verstärken Sie zuerst Ihre Endpoint-Abwehr

Für Cyberkriminelle bleiben die Endpoints von Unternehmen, an denen Daten, Benutzer und Unternehmenssysteme zusammenkommen, um Geschäftsprozesse zu generieren und zu implementieren, das Hauptziel. Um Ihre Unternehmens-Endpoints zu schützen und zu verhindern, dass sie als Einstiegspunkte in Ihre Infrastruktur verwendet werden, sollte Ihr IT-Sicherheitsteam die vorhandenen Sicherheitsmechanismen verbessern. Um von der automatischen Abwehr gewöhnlicher Bedrohungen bis hin zu schnellen und angemessenen Reaktion auf komplexe Vorfälle einen durchgängigen Endpoint-Schutzzyklus aufzubauen, benötigt man präventive Technologien, unterstützt von fortschrittlichen Abwehrfunktionen.

Kaspersky Endpoint Detection and Response (EDR) bietet eine starke Sicherheitslösung mit einer umfassenden Übersicht über alle Endpoints im Unternehmensnetzwerk und ermöglicht dank fortschrittlicher Abwehrfunktionen die Automatisierung von Routineaufgaben. So können komplexe Bedrohungen erkannt, priorisiert, untersucht und neutralisiert werden.

Wichtigste Vorteile

- Kaspersky EDR erweitert unser meistgetestetes und am häufigsten ausgezeichnetes Flaggschiff, die Endpoint Protection Platform (EPP) – **Kaspersky Endpoint Security for Business** – um leistungsstarke EDR-Funktionen, die Ihr allgemeines Sicherheitsniveau weiter optimieren. Ein einzelner Agent als automatischer Schutz gegen gängige Bedrohungen sowie eine fortschrittliche Abwehr von komplexen Angriffen vereinfacht den Umgang mit Vorfällen und hält den Wartungsaufwand niedrig. Es gibt keine zusätzliche Belastung der Endpoints und keine weiteren Kosten – nur die Gewissheit, dass Ihre Workstations und Server vollständig gegen die raffiniertesten und gezieltesten Bedrohungen geschützt sind.
- Kaspersky EDR verkürzt die Zeit, die für die erste Beweiserfassung benötigt wird, bietet eine vollständige Telemetrieanalyse und maximiert die Automatisierung der EDR-Prozesse, wodurch die Reaktionszeiten bei Vorfällen insgesamt verkürzt werden, ohne dass zusätzliche IT-Sicherheitsressourcen angefordert werden müssen.
- Kaspersky EDR kann in die **Kaspersky Anti Targeted Attack Platform** integriert werden, die EDR-Fähigkeiten und erweiterte Bedrohungserkennung auf Netzwerkebene kombiniert. IT-Sicherheitsexperten erhalten damit alle nötigen Tools, um hochentwickelte, mehrdimensionale Bedrohungen sowohl auf Endpoint- als auch auf Netzwerkebene zu erkennen. Dafür können Sie sich modernster Technologien bedienen, effektive Untersuchungen durchführen und schnelle, zentrale Gegenmaßnahmen ergreifen – alles über eine einzige Lösung.

* IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR

Kaspersky EDR ist ideal, wenn Ihre Organisation dies wünscht:

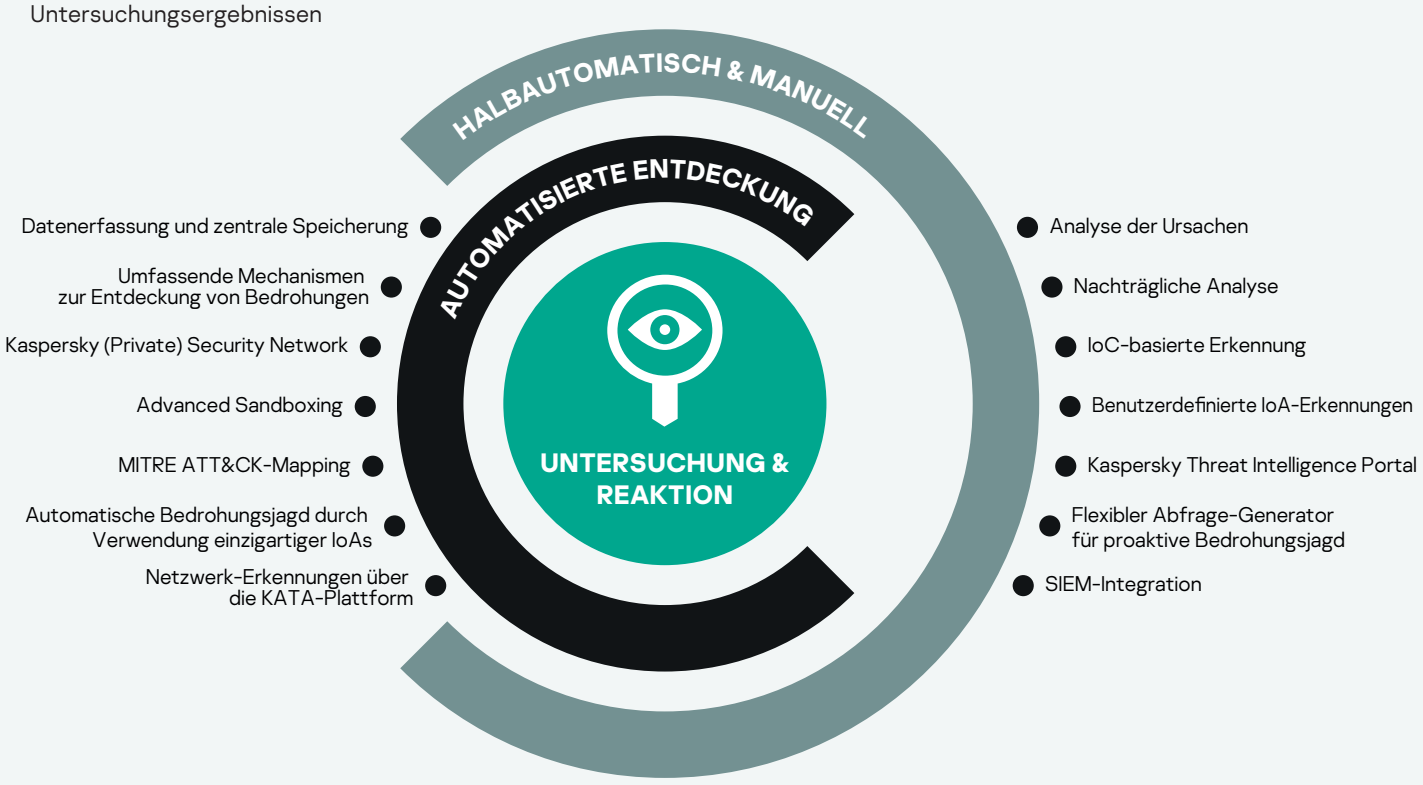
- Verbesserung Ihrer Sicherheit mit einer benutzerfreundlichen, unternehmensweiten Lösung für Vorfallsreaktionen
- Automatisierung von Bedrohungsidentifizierung und -reaktionen – ohne Betriebsunterbrechung während der Untersuchungen
- Verbesserung Ihrer Endpoint-Transparenz und Bedrohungserkennung durch fortschrittliche Technologien
- Verständnis der spezifischen Taktiken, Techniken und Prozeduren (TTPs), die von Angreifern eingesetzt werden, um ihre Ziele zu erreichen, was eine effektivere Verteidigung und Zuweisung von Sicherheitsressourcen ermöglicht
- Aufbau einheitlicher und effektiver Prozesse für Threat Hunting, Incident Management und Vorfallsreaktion
- Steigerung der Effizienz Ihres internen SOC – keine Zeitverschwendung mit der Analyse irrelevanter Endpoint-Protokolle
- Unterstützung der Richtlinienkonformität durch die Durchsetzung von Endpoint-Protokollen, Alarmierungsüberprüfungen und Dokumentation von Untersuchungsergebnissen

Rasche Aufdeckung und Eindämmung der raffiniertesten Bedrohungen

Kaspersky EDR bietet Endpoint-Schutz auf hohem Niveau und erhöht die SOC-Effizienz, indem es eine fortschrittliche Bedrohungserkennung bereitstellt und den Zugriff auf retrospektive Daten ermöglicht, selbst in Situationen, in denen auf kompromittierte Endpoints nicht zugegriffen werden kann oder wenn Daten während eines Angriffs verschlüsselt wurden. Erhöhte Ermittlungsfähigkeiten durch unsere einzigartigen Angriffsindikatoren (IoAs), die MITRE ATT&CK-Erweiterung und einen flexiblen Abfragegenerator sowie Zugang zu unserer Threat-Intelligence-Portal-Wissensdatenbank - all dies erleichtert eine effektive Bedrohungsjagd und eine schnelle Reaktion auf Zwischenfälle, was zu Schadensbegrenzung und -prävention führt.

Anwendungsfälle:

- **Proaktive Suche nach Beweisen für ein Eindringen in Ihr gesamtes Netzwerk**
- **Schnelles Erkennen und Abwehr eines Eindringens, bevor der Eindringling größere Schäden und Störungen verursachen kann**
- **Schnelle Untersuchung und zentralisierte Handhabung von Vorfällen für Tausende von Endpoints mit nahtlosem Workflow**
- **Validierung von Warnungen und potentiellen Vorfällen, die von anderen Sicherheitslösungen entdeckt wurden**
- **Automatisierung von Routineaufgaben, um manuelle Aufgaben zu reduzieren, Ihre Ressourcen freizugeben und die Wahrscheinlichkeit einer Überlastung durch zu viele Warnungen zu verringern.**



Geschäftsvorteile von Kaspersky EDR im gesamten Unternehmen:

- Hilft, Sicherheitslücken zu schließen und die „Verweildauer“ von Angriffen zu verkürzen
- Automatisiert manuelle Aufgaben während der Erkennung von und Reaktion auf Bedrohungen
- Entlastet das IT- und IT-Sicherheitspersonal für andere wichtige Aufgaben
- Vereinfacht die Bedrohungsanalyse und Vorfallsreaktion
- Verkürzt die Zeit bis zur Erkennung von und Reaktion auf Bedrohungen
- Hilft bei der Erfüllung der vollen Compliance

Und wenn Sie noch mehr wollen ... Kaspersky Managed Detection and Response

Wenn Sie Kaspersky EDR um eine vollständig verwaltete und individuell zugeschnittene Rund-um-die-Uhr-Verteidigung ergänzen, bedeutet dies, dass Ihre IT-Sicherheitsressourcen geschont werden können, indem Sie Aufgaben im Zusammenhang mit der Vorfallsbearbeitung an Kaspersky auslagern oder sich an uns wenden, wenn es Ihrem internen Team an ausreichend qualifizierten Sicherheitsspezialisten für bestimmte Szenarien mangelt.

Gartner peerinsights customers' choice 2020™

Gartner Peer Insights Customer's Choice für EDR-Lösungen 2020 ernennt Kaspersky zum Top-Anbieter

Kaspersky ist einer von nur 6 Anbietern weltweit, die die Gartner Peer Insights "Customer's Choice"-Auszeichnung für die Lösung für Endpoint Detection and Response im Jahr 2020 erhalten haben, mit der höchsten Bewertung aller Anbieter für unseren Service und Kundendienst - das ultimative Kundenkompliment für Kaspersky EDR.

Hinweis zu Gartner

Gartner Peer Insights Customers' Choice umfasst die subjektiven Meinungen individueller Endnutzerrezensionen, -bewertungen und -daten, die mithilfe dokumentierter Methoden untersucht werden. Sie stellen weder die Ansichten noch eine Empfehlung von Gartner oder seinen Tochterunternehmen dar.

MITRE | ATT&CK®

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.

Erfahren Sie mehr unter kaspersky.com/MITRE

Wenn Sie mehr über Kaspersky EDR erfahren möchten, besuchen Sie uns unter:

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Cyber Threats News: https://de.securelist.com/
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

2020 AO Kaspersky Lab.
Eingetragene Marken und Dienstleistungsmarken sind Eigentum der jeweiligen Inhaber.

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven. Transparent. Independent.