Kaspersky Endpoint Detection and Response Optimum

Heben Sie Ihre Endpunktverteidigung auf die nächste Stufe und gehen Sie direkt gegen ausweichende Bedrohungen vor – ganz ohne Aufwand.

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

Mit Kaspersky Endpoint Detection and Response Optimum sind Sie im Kampf gegen versteckte Bedrohungen optimal aufgestellt. Heutzutage reicht es nicht mehr aus, sein Unternehmen nur mit standardmäßigen Anti-Malware-Technologien zu schützen. Es ist sehr wichtig, auch die Bedrohungen zu identifizieren, zu analysieren und effektiv zu neutralisieren, die darauf ausgelegt sind, herkömmliche Schutzlösungen zu umgehen.

Die Herausforderungen

Schwer zu erfassende Bedrohungen

Versteckte Malware, Ransomware, Spyware und andere Bedrohungen gehen bei der Umgehung herkömmlicher Erkennungsmechanismen immer raffinierter vor und nutzen für ihre Angriffe seriöse Systemtools und andere fortschrittliche Techniken.

Ransomware-as-a-Service

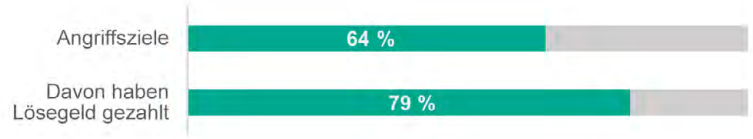
Fertige Tools werden zum kleinen Preis angeboten, sodass Hacker jeden angreifen können. Sie stehlen Daten, schädigen Ihre Infrastruktur und fordern immer höhere Lösegelder.

Begrenzte Ressourcen

Infrastrukturen werden immer komplexer und weitreichender, während Ressourcen wie Zeit, Geld und Aufmerksamkeit immer knapper werden. Da helfen keine Standardtools.

64 % der Unternehmen sind bereits Ransomware-Angriffen zum Opfer gefallen. Davon sind 79 % auf die Lösegeldforderungen der Angreifer eingegangen.

Kaspersky, Mai 2022



"Wir schätzen die umfassenden Lösungen, die Zuverlässigkeit sowie den schnellen Service und Support von Kaspersky. Sie garantieren, dass unsere IT-Umgebung verfügbar bleibt."

Marcelo Mendes CISO, NEO
Fallstudie lesen

So helfen wir

Kaspersky Endpoint Detection and Response (EDR) Optimum unterstützt Sie bei der Identifizierung, Analyse und Neutralisierung versteckter Bedrohungen, indem es benutzerfreundliche, fortschrittliche Erkennung, vereinfachte Untersuchungen sowie automatisierte Reaktionen bietet.

Umfassender Schutz

Unsere fortschrittlichen Erkennungsmechanismen umfassen Technologien wie maschinelles Lernen, Verhaltensanalyse und Cloud-Sandboxing.

Dank einfacher visueller Analysewerkzeuge können Sie die Bedrohung und ihr Ausmaß besser einschätzen. Und schnell eingeleitete Abwehraktionen stoppen den Angriff, bevor er Schaden anrichtet.

Zentrale Lösung

Endpoint-Sicherheit der nächsten Generation wird mit benutzerfreundlichem EDR kombiniert, um den Schutz von Laptops, Workstations, Servern, Cloud-Workloads und virtuellen Umgebungen zu verbessern.

Die gesamte Bereitstellung und Verwaltung erfolgt über eine einzelne zentrale Konsole, die entweder lokal oder in der Cloud bereitgestellt wird.

Einfachheit und Effizienz

Wir haben EDR Optimum speziell für kleinere Cybersicherheitsteams entwickelt, die ihre Verteidigungsmechanismen und ihr Fachwissen ausbauen möchten, dafür aber nicht allzu viel Zeit aufwenden können.

Wir automatisieren und optimieren die meisten Aufgaben, damit Ihnen mehr Zeit für die wirklich wichtigen Dinge bleibt.

Vorteile

- **Verhindert verschiedenste Arten** von Bedrohungen
- **Schützt Ihre Systeme und Daten** vor versteckten Bedrohungen
- **Erwischt aktuelle Bedrohungen,** bevor sie sich ausbreiten
- **Erkennt versteckte Bedrohungen** über alle Endpoints hinweg
- **Sorgt für die schnelle Einordnung** und Analyse von Bedrohungen
- **Verhindert Schäden** dank schneller automatisierter Reaktionen
- **Sparen Sie** Zeit und Ressourcen mit einem einzigen, unkomplizierten Tool
- **Umfassende Sicherheit für jeden Endpoint:** Laptops, Server, Cloud-Umgebungen

Hauptfunktionen

- Integrierte **Endpoint-Sicherheit der nächsten Generation**
- **Hochentwickelte Erkennung** auf der Basis lernfähiger Systeme
- **Scannt nach** Gefährdungsindikatoren (Indicator of Compromise, IoC)
- **Visuelle Untersuchung und** Analysetools
- Alle erforderlichen Daten in einer **übersichtlichen Warnkarte dargestellt**
- **Integrierte Anleitung zu** Gegenmaßnahmen und Automatisierung
- **Zentrale Konsole, lokal oder in der Cloud,** und Automatisierung
- Unterstützt **Workstations, virtuelle und physische Server, VDI-Bereitstellungen und Public Cloud-Workloads**

Wichtige Anwendungsfälle

Bin ich gerade Ziel eines Angriffs?

- **Erweiterte Erkennung** – auf Basis lernfähiger Systeme wie Cloud-Sandboxing – erkennt Bedrohungen automatisch.
- **Download und Scan von IoCs** von securelist.com oder anderen Quellen, um hochentwickelte Bedrohungen aufzuspüren

Kann ich Bedrohungen neutralisieren?

- **Mithilfe verschiedener Abwehroptionen** können Sie den Host isolieren, Dateien an der Ausführung hindern oder entfernen.
- **Scannen Sie andere Hosts** auf Anzeichen der analysierten Bedrohung.
- **Wird eine Bedrohung (IoC)** erkannt, kann die automatische Gegenwehr sofort reagieren.

Wo finde ich entsprechende Möglichkeiten zur Weiterbildung?

- **Schauen Sie sich die Anleitung für Gegenmaßnahmen** in der Warnhinweiskarte an.
- **Informieren Sie sich über das Threat Intelligence-Portal** und die neueste TI.
- **Erweitern Sie** bei der Analyse und der Abwehr von Bedrohungen Ihre Kenntnisse.

Wie konnte das passieren?

- Analysieren Sie die Bedrohung in einem **übersichtlichen Prozessbaum.**
- Verfolgen Sie das Ausbreitungsgeschehen in einer **grafischen Detailansicht.**
- **Ermitteln Sie die Ursache und den Eintrittspunkt** in die Infrastruktur.

Wie sorge ich dafür, das sich so etwas nicht wiederholt?

- **Ziehen Sie die richtigen Lehren aus dem Vorfall –** welche IPs und Websites gesperrt, welche Richtlinien geändert und welche Mitarbeiter geschult werden müssen.
- **Erstellen Sie Regeln, mit denen Sie** derartigen Bedrohungen in Zukunft vorbeugen. Z. B. indem die Ausführung von Dateien verhindert wird.

Was ist mit all den Commodity-Bedrohungen?

- **Mit Endpoint Security der nächsten Generation** lassen sich die meisten Bedrohungen sofort stoppen.
- **Verbessern Sie Ihr Patching** mit Vulnerability und Patch Management.
- **Über Endpoint-Kontrollen können Sie die Angriffsfläche reduzieren und** Richtlinien automatisch anpassen lassen.

Funktionsweise

Eine kurze Demo finden Sie in diesem Video.

Woher kommen Sie?

Ihr vorhandener Malware-Schutz reicht einfach nicht aus?

Verstärken Sie Ihren Endpoint-Schutz

Unabhängig davon, ob Sie Kaspersky oder den Endpoint-Schutz eines Drittanbieters verwenden, sollten Sie jetzt über eine EDR-Implementierung nachdenken.

Mit ihr erhalten Sie nicht nur verbesserte Funktionen zur Erkennung und Prävention, sondern sind auch gegen versteckte Bedrohungen gewappnet – sie zu identifizieren, zu analysieren und zu neutralisieren.

In unserem **Käuferleitfaden für ein optimales Sicherheitsniveau** finden Sie ausführliche Informationen, wie Sie sich vor versteckten Bedrohungen schützen können.

Sie nutzen Kaspersky bereits?

Optimieren Sie Ihre Sicherheit

Wir arbeiten kontinuierlich an der Verbesserung unserer Produkte. Mit einem Upgrade können Sie daher sicherstellen, dass Sie unsere Produkte optimal nutzen. Oder Sie wechseln gleich in die Cloud – dann können Sie lästige Routineaufgaben komplett vergessen.

Die neueste Version von Kaspersky EDR Optimum bietet:

- Anleitung zur Abwehr in der Warnhinweiskarte
- Prüfung systemkritischer Objekte vor Einleiten der Gegenmaßnahmen
- Threat Intelligence Datei-Reputation in Warnkarte
- Unbegrenzte Tiefe der Prozessbaum-Analyse

Weitere Informationen zu den neuen Funktionen finden Sie **hier**.

Neu bei Kaspersky Lab?

Optimieren Sie Ihre Sicherheit

Es gibt zahlreiche Gründe, weshalb sich Tausende von Unternehmen weltweit auf Kaspersky EDR Optimum verlassen:

- Kombination aus leistungsstarker EPP und grundlegendem EDR in einem einzigen Produkt
- Einfach zu verwendende EDR-Funktionen für kleinere Cybersicherheitsteams
- Einfache und flexible Lösung entweder lokal oder in der Cloud

Informieren Sie sich über **Kaspersky Optimum Security** – die perfekte Kombination gegen versteckte Bedrohungen auf der Basis von EDR- und MDR-Technologie

Mehr Schutz durch stufenweisen Ansatz

Die Tools, die Sie einsetzen, sollten perfekt auf Ihre Cybersicherheits- und Geschäftsanforderungen sowie auf Ihr Team und Ihre Ressourcen abgestimmt sein. Wir machen Ihnen die Entscheidung leicht: Wählen Sie unter drei an Ihr Unternehmensprofil angepassten Stufen genau die aus, die Ihre aktuellen Ansprüche an die Cybersicherheit erfüllt.

Kaspersky Security Foundations

Blockiert die überwiegende Mehrheit der Bedrohungen automatisch

- Automatisierte Multi-Vektor-Prävention von Commodity-Bedrohungen – der Großteil aller Cyberangriffe
- Die Grundstufe für Unternehmen jeglicher Größe und Komplexität zum Aufbau einer integrierten Abwehrstrategie
- Zuverlässiger Endpoint-Schutz für Unternehmen mit kleinen IT-Teams, deren Sicherheitsexpertise sich noch im Aufbau befindet

» Mehr Informationen

Kaspersky Optimum Security

Bauen Sie einen Schutz vor versteckten Bedrohungen auf. Ihr Unternehmen hat:

- ein kleines Sicherheitsteam mit grundlegender Erfahrung im Bereich Cybersicherheit.
- eine IT-Umgebung, deren Größe und Komplexität zunimmt und damit auch die Angriffsfläche.
- fehlende Cybersicherheitsressourcen – bei einem gleichzeitig erhöhten Sicherheitsbedarf.
- einen wachsenden Bedarf, die Vorfallsreaktion zu verbessern.

» Mehr Informationen

Kaspersky Expert Security

Einsatzbereitschaft gegen komplexe, APT-ähnliche Angriffe für Organisationen mit:

- komplexen und verteilten IT-Umgebungen.
- einem ausgereiften IT-Sicherheitsteam oder einem Security Operations Center (SOC).
- niedriger Risikobereitschaft aufgrund hoher Kosten durch Sicherheitsvorfälle und Datenschutzverletzungen.
- einem Tätigkeitsbereich, in dem gesetzliche Vorschriften einzuhalten sind.

» Mehr Informationen

Wer wir sind

Wir sind ein globales, privat geführtes Cybersicherheitsunternehmen mit Hunderttausenden von Kunden und Partnern auf der ganzen Welt, das sich **der Transparenz und Unabhängigkeit verpflichtet** hat. Seit 25 Jahren entwickeln wir Tools und Services mit dem Ziel, Ihre Sicherheit zu gewährleisten. Unsere Technologien sind **häufig getestet und vielfach ausgezeichnet**.

IDC

Kundenbewertungen laut IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021

Einer der besten Anbieter

AV-Test

Fortschrittlicher Endpoint-Schutz: Test des Ransomware-Schutzes

100-prozentiger Schutz

Radicati-Gruppe

Advanced Persistent Threat (APT) Market Quadrant

Top-Anbieter

Brauchen Sie noch mehr?

Informieren Sie sich über **Kaspersky EDR Expert**, ein leistungsfähiges EDR-Tool, mit dem Ihre Experten weitreichende Threat Hunting-Funktionen, umfassende Anpassungsmöglichkeiten und hervorragende Erkennungsmechanismen an die Hand bekommen.

Sehen Sie genauer hin

Erfahren Sie mehr über die Funktionsweise von Kaspersky EDR Optimum und finden Sie heraus, wie Sie Ihr Sicherheitsteam und Ihre Ressourcen im Kampf gegen Cyberbedrohungen entlasten:
www.kaspersky.de/enterprise-security/edr-security-software-solution

---

Cyber Threat News: de.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