kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Die Bedrohungslandschaft befindet sich im stetigen Wandel. Daher bedarf es leistungsstarker Tools, um sein Unternehmen umfassend zu schützen.

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 Anti-Malware-Technologien zu schützen. Es gilt, Bedrohungen zu identifizieren, zu analysieren und effektiv zu neutralisieren, die darauf ausgelegt sind, herkömmliche Schutzlösungen zu umgehen.

Die Herausforderungen

Geschäftsunterbrechungen

Bei Malware, Ransomware, Spyware und andere Bedrohungen kommen immer ausgeklügeltere Methoden zum Einsatz, um Erkennungstechnologien auszuweichen. Zudem wird die Durchführung von Angriffen stets billiger. Somit ist nicht nur das Risiko eines schwerwiegenden Angriffs größer als je zuvor, sondern auch der dadurch angerichtete Schaden sowie die einhergehende Beeinträchtigung.

Komplexe Infrastrukturen

Heutzutage müssen IT-Manager und IT-Security-Fachkräfte eine Vielzahl verschiedener Endpoints schützen. Dazu zählen Laptops, Server, virtuelle sowie Cloud-Umgebungen und Remote-Workstations. Gleichzeitig wird die IT-Infrastruktur immer komplexer.

Vertrauenswürdige Systemtools werden in etwa **30 % der Fälle verwendet**, um Skripte und Programme auszuführen, Payloads herunterzuladen, Netzwerke zu durchsuchen oder sich per Fernzugriff Zugang zum infizierten Host zu verschaffen.
Incident Response Analyst Report, Kaspersky 2020

Das Gleichgewicht finden

Bei Cybersicherheit geht es größtenteils um das Finden des optimalen Gleichgewichts zwischen Ihren verfügbaren Ressourcen und dem höchsten Schutzniveau, das erzielt werden kann. Und dabei ist die Zeit Ihrer IT-Spezialisten die knappeste Ressourcen von allen.

Was tun?

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.

Optimal aufgestellt

Kaspersky EDR Optimum basiert auf einem fortschrittlichen Erkennungsmechanismus, der maschinelles Lernen und eine umfassende Verhaltensanalyse umfasst. Auf diese Weise profitieren Sie von tiefen Einblicken in Bedrohungen, unkomplizierten Analysen und Untersuchungswerkzeugen sowie automatisierten Reaktionen. So können Bedrohungen effektiv identifiziert und ihr Umfang erkannt werden. Dies ermöglicht eine sofortige Reaktion, sodass eine Störung des Geschäftsablaufes verhindert werden kann.

Eine Lösung für alles

Kaspersky EDR Optimum bietet fortschrittliche Erkennung, Analysen und Reaktionsmöglichkeiten. So können die Verteidigungsmechanismen für eine ganze Bandbreite an Endpoints, wie Laptops, Server, Cloud- und virtuellen Umgebungen, deutlich optimiert werden. Die Lösung kann sowohl On-Prem als auch in der Cloud bereitgestellt und verwaltet werden.

Auch bei erfolgreichen Angriffen fiel der finanzielle Verlust um **32 % geringer** aus, wenn innerhalb einer Woche auf eine Datenschutzverletzung reagiert werden konnte.
Incident Response Analyst Report, Kaspersky 2020

Einfachheit und Effizienz

Kaspersky EDR Optimum wurde für kleinere Cybersicherheitsteams mit begrenzten Ressourcen entwickelt, die ihre Vorfallsreaktion verbessern möchten. Die Leistung wurde optimiert, sodass maximale Effizienz bei minimalem Einsatz von Ressourcen erzielt werden kann. Dank Automatisierung und der zentralen Bündelung aller Verwaltungstätigkeiten sowie der Verbesserung aller Arbeitsprozesse können Sie die Zeit Ihrer Sicherheitsspezialisten bestmöglich nutzen.

Vorteile

- Zuverlässiger Schutz vor komplexen Bedrohungen
- Umfassende Sicherheit für jeden Endpoint: Laptops, Server, Cloud-Umgebungen
- Überblick über alle Bedrohungen im gesamten Netzwerk
- Bedrohungsursprungsanalyse
- Wenden Sie weiteren Schaden durch schnelle automatisierte Gegenmaßnahmen ab
- Sparen Sie mit einem einfachen und automatisierten Tool Zeit und Ressourcen

Anwendungsfälle für EDR

Hochentwickelte Erkennung

Hochentwickelte Erkennungsfunktionen sind für das Aufdecken versteckter Bedrohungen unabdingbar:

- Verhaltensbasierte Bedrohungserkennung und Exploit Prevention, basierend auf maschinellem Lernen (ML)
- Heuristik, smarte Datensätze, ML-basierte Technologien
- Integrierter Emulator für die Erkennung vor der Ausführung von schädlichem Verhalten
- Sandbox für verbesserte Verhaltensanalyse (verfügbar mit der Kaspersky Sandbox)
- Daten, die im Rahmen der globalen Threat Intelligence gesammelt und von KI-basierten Systemen und Experten analysiert wurden

Antworten auf wichtige Fragen

Versteckte Bedrohungen verbergen sich oft direkt vor unseren Augen und sollten untersucht werden, um sie vollständig zu entfernen. EDR hilft bei der Suche nach Antworten auf diese Fragen:

- Bin ich jetzt in diesem Moment Ziel eines Angriffs?
- Hat dieser branchenweite Angriff meine Infrastruktur erreicht?
- Wo hat die Bedrohung ihren Ursprung?
- Was hat sie mit meinen Hosts angerichtet?
- Gibt es bei dieser Bedrohung verborgene Ebenen?
- Sind andere Endpoints betroffen?

Schnelle Reaktion

Reagieren Sie sofort mit nur einem Klick oder einer automatisierten Reaktion auf Bedrohungen:

- Verhindern Sie, dass die schädliche Datei während oder nach der Untersuchung ausgeführt wird und sich im gesamten Netzwerk verbreitet.
- Stellen Sie Dateien im Zusammenhang mit versteckten Bedrohungen an allen Endpoints automatisch unter Quarantäne.
- Isolieren Sie betroffene Hosts automatisch, sobald ein Gefährdungsindikator (Indicator of Compromise, IoC) im Zusammenhang mit einer sich schnell ausbreitenden Bedrohung gefunden wird.

Sie können jetzt so viel mehr tun

Dank der auf maschinellem Lernen basierenden, erweiterten Erkennung und der Übersicht über erkannte Vorfälle wird der Umfang und der Verlauf der Bedrohung sichtbar. Und Sie können sicherstellen, dass jede Bedrohung vollständig abgearbeitet wurde. Es schlummert nichts mehr noch irgendwo in Ihrem System und kalkuliert, wie viel Schaden es anrichten kann.

Verteidigung von hybriden Infrastrukturen

Hybride Infrastrukturen stellen zwar Herausforderungen für die Sicherheit dar, bringen aber auch erhebliche Vorteile mit sich. Sie können den Schutz für Ihre Daten und Infrastruktur für virtuelle und physische Server, VDI-Bereitstellungen und Public Cloud-Umgebungen um wichtige EDR-Funktionalität erweitern.

Vermeiden Sie Alarmermüdung und profitieren Sie von einer zentralen Verwaltung für all Ihre hybriden Endpoints und Umgebungen sowie einem optimierten EDR-Workflow aus der Cloud oder On-Prem.

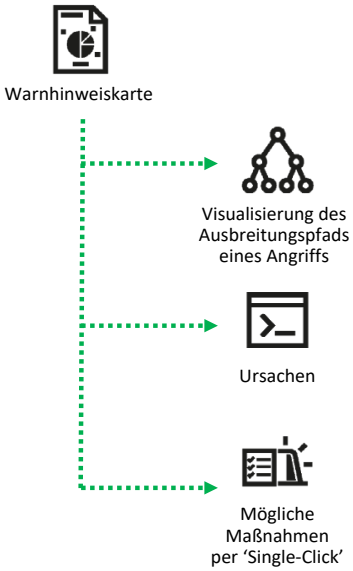
Endpoint-Schutz auf mehreren Ebenen

EDR-Technologien existieren nicht in einem Vakuum – sie erfordern eine solide Basis mit starken Endpoint-Schutz, um effektiv zu funktionieren. Unser mehrstufiger Endpoint-Schutz stellt sicher, dass Sie nicht abgelenkt werden: Sei es durch die Abwicklung von Commodity-Bedrohungen oder durch Vorfälle, die eigentlich schon von einer automatisierten Anti-Malwaresoftware hätten erledigt werden sollen. Darum funktioniert Kaspersky EDR Optimum in Verbindung mit unserer vielfach getesteten und ausgezeichneten Endpoint Protection Platform[1]: Kaspersky Endpoint Security for Business und Kaspersky Hybrid Cloud Security.

Bedrohungen analysieren

Für die Durchführung von schnellen Analysen sind in einer einzelnen Vorfallskarte erweiterte Daten zur Erkennung sowie ein detailliertes Ausbreitungsgeschehen gesammelt. So lassen sich fundierte Entscheidungen treffen, die entweder zu einer Reaktion per Mausklick oder einer automatisierten Reaktion führen.

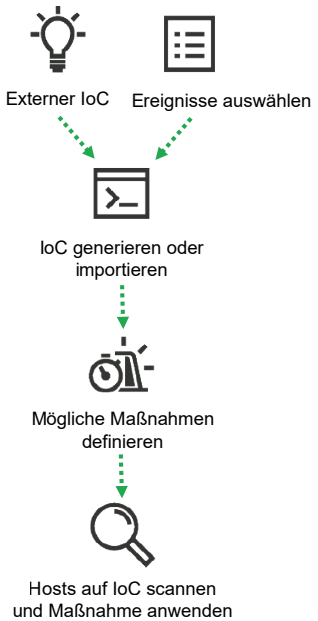
IoCs können von vertrauenswürdigen Quellen importiert oder auf Basis der Untersuchung generiert werden. Ziel ist die Aufdeckung versteckter Bedrohungen, die in Endpoints entlang Ihrer Infrastruktur lauern.



Ihre Reaktion automatisieren

Reagieren Sie mithilfe der „Single click"-Optionen, die in der Vorfallskarte verfügbar sind, sofort auf Bedrohungen während der Untersuchung. Oder richten Sie im Fall von Entdeckungen, die auf IoC-Scans basieren, automatisierte Reaktionen ein. Abwehraktionen umfassen:

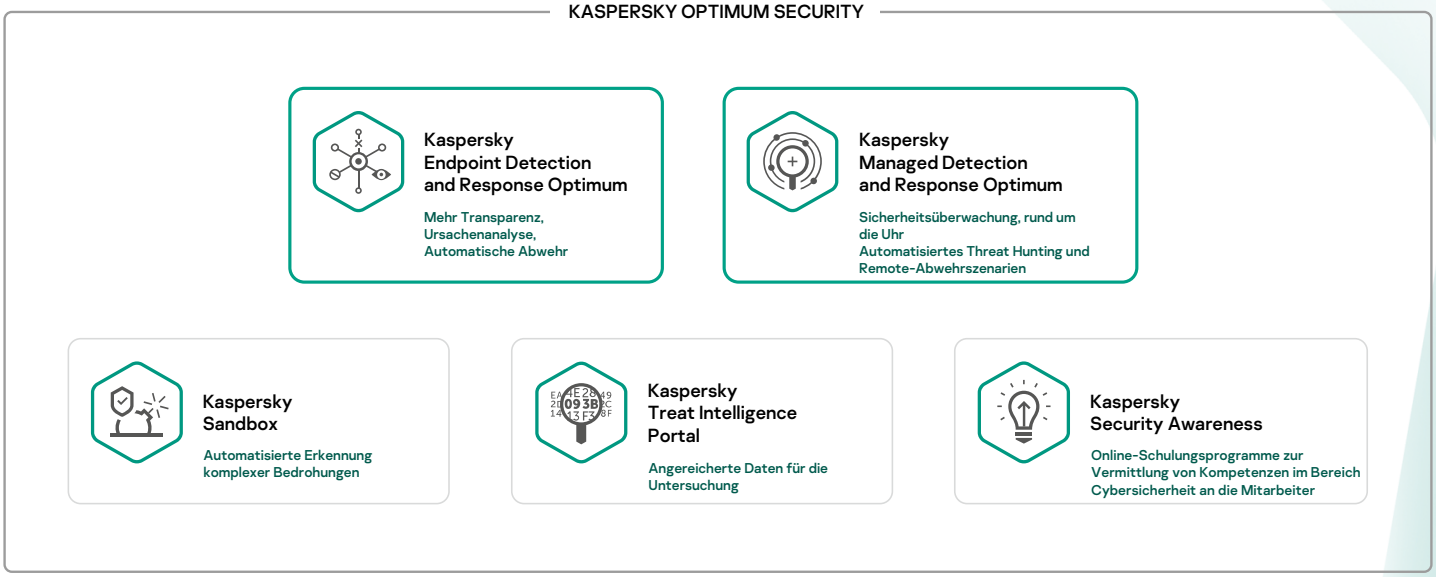
- Trennen des Hosts
- Datei in Quarantäne setzen
- Ausführung verhindern
- Scan für kritische Bereiche starten



[1] https://www.kaspersky.de/top3

Ihre Kaspersky Optimum Security-Plattform

EDR ist Teil eines umfassenden Ökosystems, das mehrere Technologien, Tools und Services umfasst: Kaspersky EDR Optimum ist die Hauptkomponente von Kaspersky Optimum Security, eine fortschrittliche Lösung, die zuverlässig vor komplexen Bedrohungen schützt und gleichzeitig Ihre Ressourcen schont.



Ein ganzheitlicher Sicherheitsansatz

Kaspersky Optimum Security baut auf Kaspersky Security Foundations auf. Kaspersky Expert Security bietet noch leistungsstärkere Tools, die fortschrittlichen Schutz vor selbst den komplexesten Bedrohungen bieten.

Kaspersky Security Foundations

Blockiert automatisch den Großteil der Bedrohungen.

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

Kaspersky Optimum Security

Zuverlässiger Schutz vor komplexen Bedrohungen. Ideal für:

- Unternehmen mit einem kleinen Sicherheitsteam mit grundlegender Erfahrung im Bereich Cybersicherheit
- Unternehmen mit einer IT-Umgebung, deren Größe und Komplexität zunimmt und damit auch die Angriffsfläche
- Unternehmen, denen es an Cybersicherheitsressourcen mangelt – bei gleichzeitigem erhöhten Sicherheitsbedarf
- Unternehmen, die ihre Vorfallsreaktion verbessern möchten

Kaspersky Expert Security

Vorbereitung auf komplexe, APT-ähnliche Angriffe. Für Unternehmen 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
- Und wo die Einhaltung gesetzlicher Vorschriften eine Rolle spielt

Weitere Informationen rund um die Funktionsweise von Kaspersky Endpoint Detection and Response Optimum finden Sie unter: https://www.kaspersky.de/enterprise-security/edr-security-software-solution.

Cyber Threats News: de.securelist.com
IT Security News: www.kaspersky.de/blog/b2b

www.kaspersky.de