Kaspersky Endpoint Detection and Response

Unternehmen arbeiten an der Verbesserung ihrer Sicherheitsstrategie zur Abwehr von hoch entwickelten Bedrohungen und Cyberangriffen. Für Cyberkriminelle sind Endpoints nach wie vor das Hauptziel – doch heutige Bedrohungen umgehen traditionelle Endpoint-Sicherheitsmaßnahmen, stören geschäftskritische Prozesse, beeinträchtigen die Produktivität und erhöhen die Betriebskosten.

Verzögerungen kosten Geld

Laut einer von Kaspersky Lab in Unternehmen durchgeführten Umfrage zu IT-Risiken, kostet die Wiederherstellung eine Woche nach der Entdeckung eines Vorfalls 200% mehr, verglichen mit einer sofortigen Reaktion.

Kaspersky EDR ist ideal für Unternehmen, die Folgendes erreichen möchten:

- Automatisierte Erkennung von und Reaktion auf Bedrohungen – ohne Unterbrechung des Geschäftsbetriebs
- Verbesserung der Endpoint-Transparenz und Erkennung von Bedrohungen durch fortschrittliche Technologien wie ML (maschinelles Lernen), Sandbox, IoC-Scan und Threat Intelligence
- Verbesserung der Sicherheit – mit einer benutzerfreundlichen, unternehmensweiten Lösung für die Vorfallsreaktion
- Aufbau einheitlicher und effektiver Prozesse für Threat Hunting, Incident Management und Vorfallsreaktion

Unterstützung der Compliance:

Threat Intelligence, die über das Kaspersky Private Security Network in Echtzeit und vor Ort bereitgestellt wird

- Keine Abhängigkeit von der Cloud und kein ausgehender Datenfluss über KPSN-Integration
- Alle forensischen Daten werden in Kaspersky EDR zentral in der unternehmenseigenen Umgebung gespeichert.

Aktive Suche nach Bedrohungen:

Durch die Ergänzung einer Kaspersky EDR-Bereitstellung um den rund um die Uhr aktiven Threat Hunting Service – Kaspersky Managed Protection – erhalten Unternehmen Zugriff auf globale Bedrohungsforschung. Darüber hinaus können die Bedrohungsforscher von Kaspersky Lab:

- die in der Unternehmensumgebung gesammelten Daten überprüfen;
- schnell das Sicherheitsteam des Unternehmens informieren, wenn schädliche Aktivitäten entdeckt werden;
- Ratschläge geben, wie Sie reagieren und Abhilfe schaffen können.

Wichtigste Vorteile

Adaptive Threat Response

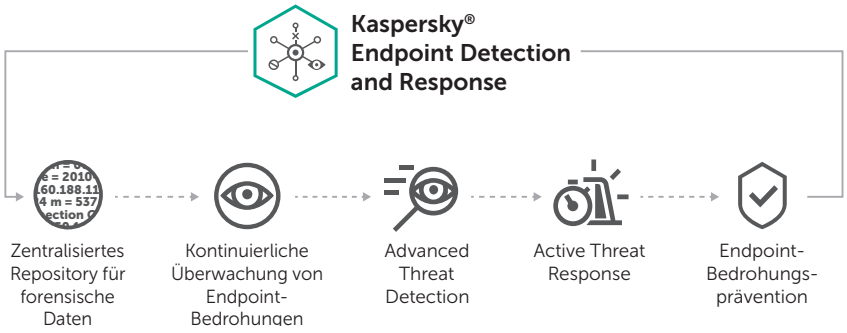
Kaspersky EDR umfasst eine große Anzahl automatisierter Reaktionen, dank derer Unternehmen herkömmliche Beseitigungsmechanismen – wie z. B. Löschen und Re-Imaging – und damit einhergehende kostspielige Ausfallzeiten und Produktivitätsverluste vermeiden können.

Proaktives Threat Hunting

Mit der Schnellsuche unter Verwendung einer zentralen Datenbank sowie einer IoC-Suche (Indicators of Compromise) kann Kaspersky EDR den Sicherheits-Workflow radikal verändern. Statt auf Warnmeldungen warten zu müssen, kann Ihr Sicherheitsteam aktiv nach Bedrohungen suchen und proaktiv Endpoints scannen, um Anomalien und Sicherheitsverletzungen zu erkennen.

Intuitive Weboberfläche

Die benutzerfreundliche, browserbasierte Benutzeroberfläche von Kaspersky EDR bietet dem Sicherheitsteam eine durchgehende Transparenz und Kontrolle bei: Erkennung, Untersuchung, Prävention, Warnmeldungen und Berichterstattung. Da zahlreiche Funktionen über eine einzige Oberfläche überwacht und kontrolliert werden können, kann Ihr Sicherheitsteam Sicherheitsaufgaben effizienter ausführen, ohne zwischen verschiedenen Tools und Konsolen wechseln zu müssen.



Komplexe Bedrohungen schnell erkennen und abwehren

Kaspersky Endpoint Detection and Response (Kaspersky EDR) unterstützt Unternehmen bei der Erkennung, Untersuchung und Reaktion:

- verbesserter Einblick in Endpoints
- Automatisieren von manuellen Reaktionsmaßnahmen
- Verbesserung von Untersuchungsfunktionen

... und ist mit traditionellen Endpoint-Sicherheitslösungen kompatibel.

Kaspersky EDR hilft Sicherheitsteams ebenso wie weniger erfahrenen Benutzern dabei, einen Endpoint mit der Präzision eines Cyber-Reaktions-Spezialisten zu testen. Mit Kaspersky EDR kann Ihre Organisation:

- Bedrohungen effizient ÜBERWACHEN – über Malware hinaus
- Bedrohungen wirksam ERKENNEN – unter Verwendung hoch entwickelter Technologien
- Forensische Daten zentral SAMMELN
- Schnell auf Angriffe REAGIEREN
- Schädliche Aktionen durch entdeckte Bedrohungen VERHINDERN

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

Anwendungsfälle:

- Proaktive Echtzeitsuche nach Beweisen für ein Eindringen – einschließlich Gefährdungsindikatoren (IoC) – im gesamten Netzwerk
- Schnelles Erkennen und Abwehr eines Eindringens, bevor der Eindringling größere Schäden und Störungen verursachen kann
- Integration mit SIEM-Produkten – zur Korrelation von Warnungen und Aktivitäten am Endpoint
- Validierung von Warnungen und potentiellen Vorfällen, die von anderen Sicherheitslösungen entdeckt wurden
- Schnelle Untersuchung und zentralisierte Handhabung von Vorfällen – für Tausende von Endpoints – mit nahtlosem Workflow
- Automatisierung von Routineaufgaben, um manuelle Aufgaben zu reduzieren, Ressourcen freizugeben und die Wahrscheinlichkeit einer Überlastung durch zu viele Warnungen zu verringern.

Fortschrittliche Endpoint-Sicherheit

Kaspersky Lab demonstriert unsere anhaltende Führungsposition im Bereich des Endpoint-Schutzes durch die Kombination von fünf entscheidenden Elementen in einer einzigen Lösung:

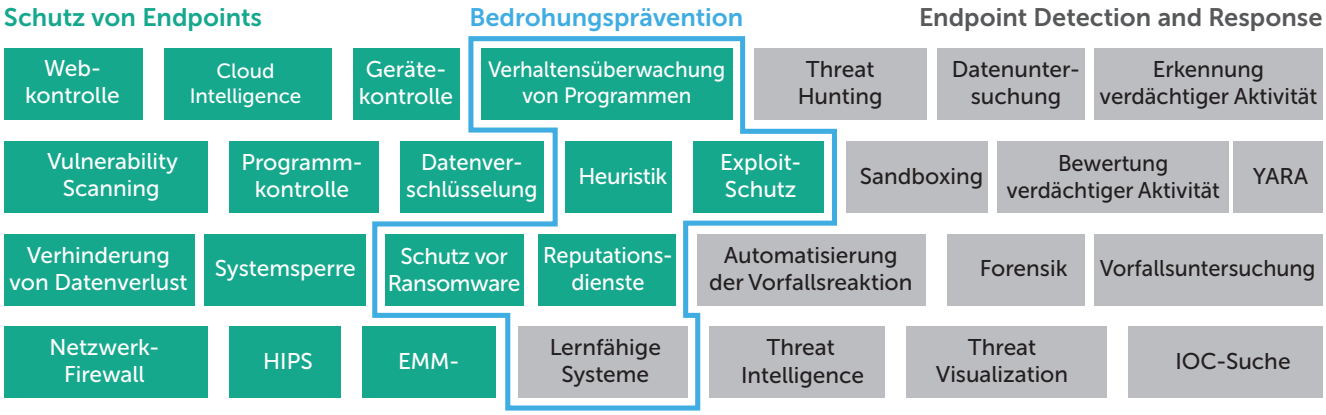
- eine leistungsstarke und lernfähige Next-Generation-Anti-Malware-Engine
- Endpoint Detection and Response (Kaspersky EDR)
- Ein rund um die Uhr aktiver Threat Hunting Service – Kaspersky Managed Protection
- Zugriff auf Bedrohungsanalyse in Echtzeit – über das Kaspersky Security Network
- Fortschrittliche Endpoint-Kontrolle (Gerät/Web/App, Verschlüsselung und mehr)

Stärkung traditioneller Endpoint-Sicherheit

Da Kaspersky EDR mit einer breiten Palette traditioneller Sicherheitsprodukte verschiedener Anbieter kompatibel ist, kann Kaspersky EDR auch gemeinsam mit der vorhandenen Endpoint-Sicherheitslösung eines Unternehmens eingesetzt werden und bietet dann zusätzlich:

- Next-Generation-Funktionalität – für hoch entwickelte Erkennung und Prävention;
- zentral gesteuerte Untersuchungs- und Reaktionsprozesse.

... ohne dass das Unternehmen seine bisherige Sicherheitslösung ersetzen muss.



Objektanalyse in einer isolierten virtuellen Umgebung

Kaspersky EDR beinhaltet eine vor Ort installierte Advanced Sandbox, die eine automatisierte Extraktion beliebiger Dateien zur gründlichen Analyse ermöglicht – an jedem Endpoint. Damit steht dem Unternehmen ein hauseigenes Virenlabor zur Verfügung, ohne dass Daten außerhalb des Netzwerks gesendet werden müssen.

Hoch entwickelte, lernfähige Erkennung

Die lernfähige Engine von Kaspersky EDR – Targeted Attack Analyzer (TAA) – erstellt eine Baseline für Endpoint-Verhalten. Dies ermöglicht es, einen Verlauf zu erstellen, anhand dessen festgestellt werden kann, wie ein Verstoß erfolgte. Darüber hinaus können – durch Korrelation forensischer Daten, von Threat Intelligence und Beurteilungen der Sicherheits-Engine – Anomalien aufgedeckt werden.

Geschäftliche Vorteile für das Unternehmen:

Senkt die Kosten

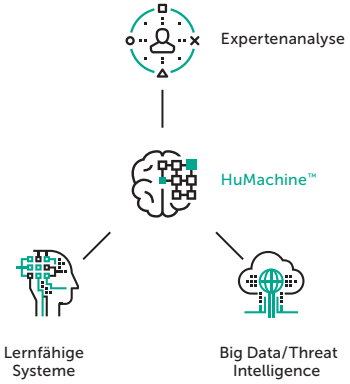
- Automatisiert manuelle Aufgaben – während der Erkennung von und Reaktion auf Bedrohungen
- Beschleunigt die Eindämmung von Bedrohungen, um Geld und Ressourcen zu sparen
- Entlastet das IT- und Sicherheitspersonal für andere Aufgaben
- Hilft, Betriebsstörungen während der Untersuchungen zu minimieren

Beschleunigt den ROI

- Ermöglicht einen effizienten Workflow
- verkürzt die Zeit bis zur Erkennung von und Reaktion auf Bedrohungen
- Unterstützt die Einhaltung der Compliance (PCI DSS und mehr) durch die Durchsetzung von Endpoint-Protokollen, der Überprüfung von Warnmeldungen und der Dokumentation von Untersuchungsergebnissen

Verringert Angriffsrisiken

- Hilft, Sicherheitslücken zu schließen und die „Verweildauer" von Angriffen zu verkürzen
- Vereinfacht die Bedrohungsanalyse und Vorfallsreaktion
- Stärkt die vorhandene Sicherheit durch Bedrohungsvalidierung



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de