Alles was Sie im Vertrieb über Kaspersky Managed Detection and Response wissen müssen

kaspersky

Sales Pitch

Durch Fernzugriff und die Verbreitung von Methoden für den Informationsaustausch nimmt die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs auf Organisationen jeglicher Art stetig zu.

Gleichzeitig sind die Kosteneines Angriffs deutlich gesunken, weil die komplexen Tools von Cyberkriminellen auf nationaler Ebene zunehmend auch für den breiten Markt verfügbar werden. Mehr als die Hälfte der aktuellen Bedrohungen kommen ohne Malware aus, wobei eine wachsende Zahl von ihnen darauf ausgelegt ist, die vorhandenen automatischen Präventions- und Erkennungsmechanismen zu umgehen.

Zu Bekämpfung dieser Bedrohungen benötigen Unternehmen die entsprechenden Ressourcen und Kenntnisse, damit sie komplexe Anti Targeted Attack-Plattformen wirksam einsetzen können. Die weltweite Knappheit an Spezialisten, die im Umgang mit komplexen Bedrohungen geschult sind, und die Kosten, die für ihre Anstellung anfallen, sind oft die wesentlichen Faktoren, weshalb Unternehmen auf entsprechende Lösungen und Services verzichten.

Kaspersky Managed Detection and Response bietet rund um die Uhr gemanagten Schutz vor der wachsenden Zahl von Bedrohungen, die auf die Umgehung von automatisierten Präventions- und Erkennungssystemen ausgelegt sind. Die Lösung unterstützt und schützt Organisationen, denen das zur Bekämpfung notwendige Fachwissen und Personal fehlt oder deren interne Ressourcen begrenzt sind.

Zielgruppe

Zielgruppe: Primäres Marktsegment sind größere KMUs und mittelständische Unternehmen. Zum sekundären Marktsegment gehören hoch entwickelte Großunternehmen und Security Operations Center.

Branchen: Alle Branchen

Entscheidungsträger: Technische Entscheidungsträger ab 35: CISO, CIO, IT-Techniker, Spezialisten für IT-Sicherheit

Fünf wichtige Fragen an den Kunden

1. Sind Sie mit einem Fachkräftemangel im Bereich der IT-Sicherheit konfrontiert?
2. Welche Strategie verfolgen Sie, um die vorhandenen IT-Sicherheitsfunktionen in Ihrem Unternehmen zu erhöhen? Haben Sie vor, firmenintern in mehr Know-how im Bereich Vorfallmanagement zu investieren?
3. Möchten Sie eine effektives Frühwarnsystem für die Bedrohungserkennung und -reaktion durch eine gesteuerte Überwachung rund um die Uhr einrichten und ausbauen?
4. Mangelt es Ihnen an Kapazitäten, um alle Warnhinweise zeitnah zu verarbeiten?
5. Suchen Sie nach einer Möglichkeit, Ihre Gesamtkosten für IT-Sicherheit zu senken?

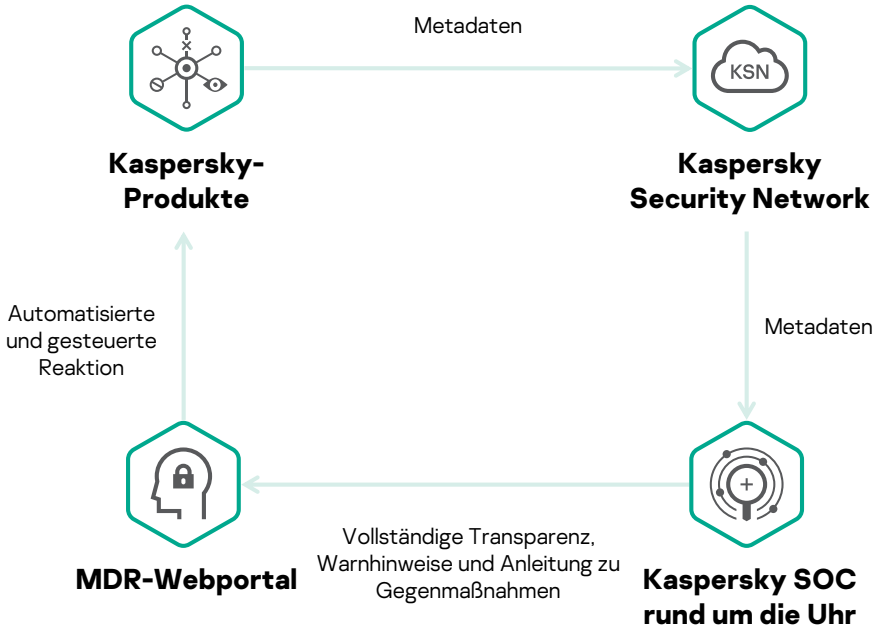
Probleme der Nutzer

1. Erhöhte Gefahr eines erfolgreichen Angriffs
2. Finanzielle Auswirkungen von Angriffen
3. Mangel an Fachwissen, um die neuesten Angriffe abzuwehren
4. Mangel an Kapazitäten, um alle Warnhinweise zeitnah zu verarbeiten

Wie sieht der Vertriebsprozess aus?

Vollständige Unterstützung durch das Kaspersky HQ

Funktionsweise von MDR



Kaspersky-Produkte

Die Module Kaspersky Endpoint Security for Business, Kaspersky Endpoint Detection and Response sowie die Kaspersky Anti Targeted Attack-Plattform senden die Metadaten über die in den unterschiedlichen Regionen vorhandene Kaspersky Security Network-Infrastruktur an die Kaspersky Security Operations Center.

Integrierte EDR

In der Standardversion ist MDR mit EDR Optimum kombiniert. In dieser Version können Kunden infizierte Hosts isolieren, nicht autorisierte Prozesse beenden sowie schädliche Dateien in Quarantäne stellen und löschen – je nach dem, was das Kaspersky SOC als passende Abwehrmaßnahme empfiehlt.

Kaspersky Security Network

Das Kaspersky Security Network ist eine Cloud-basierte Reputationsdatenbank, über die die Kaspersky-Produkte mit Threat Intelligence in Echtzeit versorgt werden. Über die zugehörige Infrastruktur wird die Kundentelemetrie zur weiteren Einordnung und Analyse an das Kaspersky Security Operations Center weitergeleitet.

Kaspersky Security Operations Center (SOC)

Die Mitarbeiter des Kaspersky SOC mit Rechenzentren in Europa und Russland überwachen proaktiv die Telemetrie-Sicherheitsdaten, die sie von den Kaspersky-Produkten erhalten. Mithilfe ständig aktualisierter, selbst entwickelter Angriffsindikatoren, die speziell auf die Umgebung des Kunden zugeschnitten sind, werden so Bedrohungen ausgemacht, die die Sicherheitssysteme der bereitgestellten Lösungen umgehen. Der Analyseprozess läuft mittels patentierter ML-Modelle (maschinelles Lernen) hoch automatisiert ab, so dass Kaspersky sehr wettbewerbsfähige SLAs in Bezug auf die Reaktionszeit anbieten kann.

MDR-Portal

Über das MDR-Portal erhält man einen kompletten Einblick in alle Serviceerkennungen sowie Warnhinweise mit umfassenden Empfehlungen zur Vorfallsabwehr.

Vorfallsreaktion

Kunden von Kaspersky MDR können anhand der Funktionen von EDR Optimum selbst entscheiden, ob sie die empfohlenen Abwehraktionen selbsttätig einleiten wollen, ob sie vorab die Freigabe erteilen wollen, dass zusätzliche Artefakte zur detaillierten Vorfallsanalyse grundsätzlich an Kaspersky weitergeleitet werden, oder ob sie im Einzelfall

Kaspersky zur Einleitung entsprechender Remote-Abwehrmaßnahmen grünes Licht geben möchten[1]. Dabei ist zu beachten, dass die komplette Vorfallsreaktion und digitale Forensik nicht im Paket enthalten sind, sondern bei Bedarf separat zu erwerben sind.

Zusätzlicher Nutzen für KESB und EDR Optimum

DETECTION
Erkennung über mehrere Endpoints
Erkennung verdächtiger Aktivitäten in legitimen Tools, z. B. die Ausführung von Tools, wie psexec, die für einen Unternehmensprozess ungewöhnlich ist
Erkennung von unbekannten Programmdateien und Skripten mit nicht eindeutigem Verhalten (kann je nach Kontext sowohl schädlich als auch legitim sein), die vom Produkt nicht erkannt wurden, z. B. unbekannte Signup.exe-Datei stellt DNS-Anfragen mit eingebetteten verschlüsselten Daten
TRANSPARENZ
Erläuterungen und Empfehlungen für alle erkannten Phänomene und Warnhinweise: zielgerichtet oder Massen-Malware, ob weitere Untersuchungen oder Abwehr erforderlich sind
RESPONSE
Halbautomatische (zuvor vom Kunden autorisierte) Reaktion, die von Kaspersky remote ausgeführt wird
Anleitung: schrittweise Empfehlungen zu Abwehrmaßnahmen, die bei Vorfällen, die durch Kaspersky SOC aufgedeckt wurden, kundenseitig eingeleitet werden können

Stufen von MDR

KASPERSKY MANAGED DETECTION AND RESPONSE

Optimum

- Proaktive Überwachung rund um die Uhr
- Automatisiertes Threat Hunting und Vorfallsuntersuchung
- Vorfallsreaktion, unter Anleitung und remote[1]
- Überprüfung der IT-Sicherheit u. Überblick über Ressourcen
- MDR-Webportal mit Dashboards u. Berichten
- Verläufe werden 1 Jahr lang gespeichert
- Rohdaten werden 1 Monat lang gespeichert

Expert

- Proaktive Überwachung rund um die Uhr
- Automatisiertes Threat Hunting und Vorfallsuntersuchung
- Vorfallsreaktion, unter Anleitung und remote[2]
- Überprüfung der IT-Sicherheit u. Überblick über Ressourcen
- MDR-Webportal mit Dashboards u. Berichten
- Verläufe werden 1 Jahr lang gespeichert
- Managed Threat Hunting
- Rohdaten werden 3 Monate lang gespeichert
- Zugriff auf Kaspersky SOC-Analyse
- Zugang zum Threat Intelligence-Portal
- API für Datendownload

Weitere Vorteile:

- flexible Optionen für Speicherung und Aufbewahrung entsprechend den gesetzlichen und ermittlungstechnischen/eDiscovery-Anforderungen

Services:

- Gefährdungs-Assessment
- Praktische Schulungen für SOC-Analysten
- Incident Response Retainer

[1]Remote-Antwortszenarien in der Optimum beschränken sich auf die Erfassung der zusätzlichen Systemartefakte
[2]Remote-Antwortszenarien in der Expert umfassen auch invasive Antworten. Sie werden 2021 verfügbar sein.

Zur weiteren Überprüfung, Untersuchungen und Identifizierung neuer Bedrohungen nutzt die Threat Hunting-Funktion eine automatisierte Erkennungsfunktion, die mit eigens ermittelten Angriffsindikatoren arbeitet. Die Managed Threat Hunting-Funktion basiert auf der sorgfältigen Handarbeit unserer erfahrenen Experten, die vorausschauend Bedrohungen aufspüren, die die automatische Erkennung umgehen.

Mit der Stufe MDR Expert erhält der Kunde außerdem über das Kaspersky Threat Intelligence Portal ein freies Kontingent von 1.000 Anfragen an Threat Lookup und 500 an Cloud Sandbox pro Jahr.

1 Vorraussichtlich ab 2021 in der Stufe MDR Expert.

Für kundenspezifische Speicher- und Aufbewahrungsoptionen wenden Sie sich bitte an: intelligence@kaspersky.com. Alle genannten Services sind gemäß dem Standard-Vertriebsprozess separat zu erwerben. Die praktischen Schulungen für SOC-Analysten beinhalten unser Standard-Schulungsprogramm für Malware-Analyse und Reverse Engineering, Digitale Forensik, Vorfallsreaktion und Yara.

Was kostet MDR?

Die Preisliste ist den Kunden nicht zugänglich. Die Lizenzierung erfolgt pro geschütztem Node und Jahr. Um den Preis zu berechnen, brauchen Sie die Anzahl der geschützten Nodes und die gewählte Produktstufe (Optimum oder Expert), die Sie dann auf Ihre lokale Preisliste anwenden.
Die Preisspanne für Kaspersky MDR Optimum beginnt bei 60 US-Dollar pro Node/Jahr für bis zu 1.000 Nodes und reicht bis 15 US-Dollar pro Node/Jahr für mehr als 10.000 Nodes.
Die Preisspanne für Kaspersky MDR Expert beginnt bei 120 US-Dollar pro Node/Jahr für bis zu 1.000 Nodes und reicht bis 30 US-Dollar pro Node/Jahr bei mehr als 10.000 Nodes.

Welche Kaspersky-Produkte werden von MDR unterstützt?

Zur Freischaltung des Services ist Kaspersky Endpoint Security for Business erforderlich.

MDR unterstützt die folgenden Kaspersky-Produkte:

- KESB for Windows V11.4+ mit komplettem Support: Telemetrie-Sammlung, Analyse und Abwehr
- KESB for Windows V10 SP1 mit eingeschränktem Support: nur Telemetrie-Sammlung und Analyse
- KESB for Mac (2. Quartal 2021)
- KSWS V10+
- KESB for Linux V11 SP1 +
- KATA\KEDR 3.7 Patch 1

Wie funktioniert das Upgrade von Kaspersky Managed Protection-Kunden auf MDR?

Wie funktioniert das Upgrade von Kaspersky Managed Protection-Bestandskunden auf das neue MDR?

- Bestandskunden von Kaspersky Managed Protection mit aktivem Service-Abonnement erhalten für die verbleibende Laufzeit ihres Abonnements ein kostenloses Upgrade auf MDR.
- Kunden mit Support zu regulären Bürozeiten (5x8) erhalten ein Upgrade auf MDR Optimum, solche mit Rund-um-die-Uhr-Support (24/7) ein Upgrade auf MDR Expert.
- KMP for KATA-Kunden erhalten ein Upgrade auf MDR Expert. Aufgrund der Einstellung der Zusatzservices zu KATA, wird Kunden empfohlen, nach Ablauf des bestehenden Abos ein Upgrade auf MDR Expert für KESB und KATA vorzunehmen. Alle Ausnahmefälle bedürfen der Überprüfung und Genehmigung. Bitte senden Sie derartige Anfragen direkt an: intelligence@kaspersky.com.
- Wenn die Verlängerung von KMP bereits bezahlt ist, ändert sich der Preis nicht. Sofern noch keine Zusagen gemacht wurden, lautet die dringende Empfehlung:
  - Erläutern Sie die neuen MDR-Funktionen, die KMP nicht bietet (umfassende Transparenz über das MDR-Portal, zentraler Abwehr-Agent zur Einleitung der Abwehrmaßnahme, Empfehlungen per Service-Richtlinien sowie Szenarien für die Remote-Abwehr, die ab 2021 unterstützt werden).
  - Machen Sie ein Angebot auf der Grundlage der neuen Preisgestaltung für die entsprechende MDR-Stufe.

Jegliche Ausnahmen und Sonderrabatte bedürfen der Überprüfung und Genehmigung. Bitte senden Sie derartige Anfragen direkt an: intelligence@kaspersky.com.

Verweise auf sämtliche Vertriebs- und Marketingmaterialien

- Webseite
- Vertriebsschulungen
- Präsentationen:
  - Allgemeine Produktpräsentation
- Produktdatenblätter und Whitepapers
  - KASPERSKY MANAGED DETECTION AND RESPONSE
  - Hunting the Hunters
- MITRE-Bewertung
- Fallstudien:
  - Broschüre „Donau Chemie"
  - Broschüre „Bank mit Sitz in Texas"
- Deman Gen Banner
- Infografik
- Infografik 2
- E-Mails an Kunden
- Teleskript für Kunden
- Grafik

Neues über Cyberbedrohungen: https://de.securelist.com/
IT Security News: business.kaspersky.de/
Threat Intelligence-Portal: opentip.kaspersky.de

www.kaspersky.de

kaspersky BRING ON THE FUTURE