Kaspersky EDR Optimum
Kaspersky EDR
Kaspersky MDR

Funktionsvergleich

kaspersky

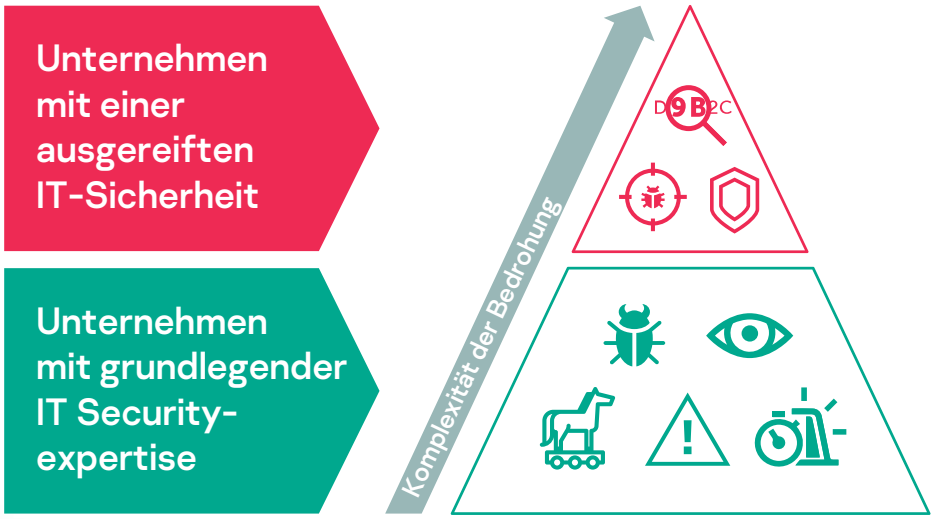
Einleitung

Dieses Dokument thematisiert den ganzheitlichen Security-Ansatz von Kaspersky, der Schutz vor selbst den komplexesten Bedrohungen bietet. Wir beleuchten, wie unsere Produkte und Services Ihre Anforderungen basierend auf Ihrem IT Security-Niveau und verfügbaren Ressourcen erfüllen können.

Heutzutage kann jedes Unternehmen, ungeachtet der Branche oder Größe, Opfer von Cyberkriminellen werden. Dabei sind einige Unternehmen besser vorbereitet als andere. Die Kosten und der Aufwand, die mit einem Angriff verbunden sind, sinken konstant. Deshalb ist das Risiko für Unternehmen umso größer. Die Bedrohungen reichen von unbekannter Malware, Ransomware und dateilosen Bedrohungen bis hin zu APT-ähnlichen Angriffen und gezielten Kampagnen. Sie geben Aufschluss darüber, wie viel Zeit und Aufwand Cyberkriminelle heutzutage bereit sind zu investieren.

Selbst mit knappen Ressourcen und begrenzter Sicherheitsexpertise sollte jedes Unternehmen in der Lage sein, Bedrohungen effektiv abzuwehren. Während einige Unternehmen über gut ausgebildetes IT-Personal verfügen, haben andere vielleicht keine IT-Experten oder stehen erst am Anfang des Aufbaus einer IT-Abteilung.

Unser Portfolio umfasst fortschrittliche Lösungen, die Schutz vor selbst den komplexesten Bedrohungen bieten. So werden die Anforderungen von Unternehmen jeder Größe und Branche erfüllt. Wir möchten Sie dabei unterstützen, die ideale Kombination aus Produkten und Services zu finden. Dabei berücksichtigen wir Unternehmensgröße, Branche, den IT-Reifegrad sowie verfügbare Ressourcen.



Kaspersky EDR Optimum

Kaspersky Managed Detection and Response

Kaspersky Endpoint Detection and Response

Kaspersky EDR Optimum

Ideal für kleine und mittelständische Unternehmen mit begrenzter IT-Sicherheitsexpertise oder mit knappen Ressourcen

Kaspersky EDR Optimum ist ideal für Kunden, die nur über begrenzte IT-Expertise und -Ressourcen verfügen. Dank der Lösung kann auf Bedrohungen reagiert werden, noch bevor sie Schaden anrichten können. Die Lösung ergänzt Kaspersky Endpoint Security for Business, unsere führende Endpoint Protection-Plattform, ideal. Kaspersky EDR Optimum vereint alle Funktionen von Kaspersky Security for Business Advanced mit grundlegenden EDR-Fähigkeiten. Die Verwaltung erfolgt zentral über die Kaspersky Security Center-Konsole.

Die Lösung blockiert automatisiert gängige Bedrohungen und hilft Ihnen gleichzeitig, auch komplexere Vorfälle zu untersuchen. So sind Sie stets umfassend for komplexen Bedrohungen geschützt, ohne zusätzliche IT-Sicherheitsressourcen einsetzen zu müssen.

Mittels einer Vorfallskarte können Ihre IT-Sicherheitsexperten umfassende Erkennungsdaten für eine detaillierte Untersuchung und Ursachenanalyse nutzen. Sie können auch Indicators of Compromise (IoCs) auf Grundlage vorheriger Entdeckungen erstellen oder IoCs aus Quellen von Drittanbietern importieren. So können Sie im Anschluss Ihre Infrastruktur auf diese Vorfälle untersuchen. Basierend auf den IoC-Ergebnissen können Sie automatisch auf Bedrohungen reagieren oder „one-click"-Reaktionen durchführen, beispielsweise Dateien in Quarantäne verschieben, Hosts isolieren, Prozesse aufheben, Objekte löschen usw.

Kaspersky Sandbox

Sie können Kaspersky EDR Optimum um die automatisierte Kaspersky Sandbox erweitern und so selbst unbekannte Bedrohungen abwehren, die den Endpoint-Schutz umgehen können. Die Lösung führt eine dynamische Analyse unbekannter und komplexer Cyberbedrohungen durch. So nimmt die Anzahl der Bedrohungen, die automatisch blockiert werden können, deutlich zu.

Kaspersky Endpoint Detection and Response

Ideal für mittelständische und große Unternehmen mit sich schnell entwickelnder oder bereits voll entwickelter IT-Sicherheitsexpertise

Kaspersky EDR unterstützt Ihr IT-Sicherheitsteam bei der schnellen, zentralisierten Reaktion auf komplexe mehrschichtige Bedrohungen. Ihre Reaktionszeit wird dabei von Stunden auf Minuten verringert.

Wenn Sie Ihre interne IT-Sicherheitsexpertise weiter ausbauen oder sogar Ihr eigenes SOC entwickeln möchten, dann ist Kaspersky Endpoint Detection and Response (EDR) genau das Richtige für Sie. Die Lösung bietet fortschrittliche Funktionen zur Abwehr von komplexen Bedrohungen für Unternehmen mit gut aufgestellten IT-Sicherheitsteams.

Kaspersky EDR ist ein Tool zur Erkennung, Untersuchung und Reaktion auf komplexe Bedrohungen. Die Lösung ist mit jeder Version von Kaspersky Endpoint Security for Business (mit einem einzelnen Agent) kompatibel. Dazu zählen Kaspersky Security for Windows Server sowie Kaspersky Hybrid Cloud Security, aber auch Endpoint-Schutzlösungen von Drittanbietern.

Mittels fortschrittlicher Erkennungsmechanismen mit Indicators of Attack (IoA), einer integrierten Sandbox und anderen Discovery Engines können Ihre IT-Sicherheitsexperten komplexe Bedrohungen und Angriffe erkennen. Kaspersky EDR sammelt kontinuierlich Telemetrie-Daten und sendet sie zur zentralen Speicherung, damit bei einer Vorfallsuntersuchung schnell auf die Daten zugegriffen werden kann. Dies ist besonders wichtig, wenn gefährdete Endpoints nicht zugänglich sind oder Daten von Cyberkriminellen verschlüsselt wurden.

Dank dieser Lösung kann Ihr IT-Sicherheitsteam detaillierte Vorfallsuntersuchungen durchführen und erhält dabei Zugriff auf das Kaspersky Threat Intelligence Portal und auf erweiterte Erkennungen, die automatisch mit der MITRE ATT&CK-Wissensdatenbank abgeglichen werden. Ihr Team kann auch komplexe Suchanfragen nach untypischem und verdächtigem Verhalten und anderen Anzeichen bösartiger Aktivität starten und dabei die Besonderheiten Ihrer Infrastruktur berücksichtigen. Für spezifische Techniken kann auf MITRE ATT&CK zurückgegriffen werden.

So kann Ihr Team proaktives Threat Hunting durchführen und die entsprechenden Maßnahmen einleiten.

Kaspersky Anti Targeted Attack Platform

Kaspersky EDR kann als Teil der Kaspersky Anti Targeted Attack (KATA) Platform eingerichtet und die EDR-Fähigkeiten mit fortschrittlicher Bedrohungserkennung auf Netzwerkebene kombiniert werden. Somit profitieren Sie von Extended Detection and Response. Ihre IT-Sicherheitsexperten profitieren somit von einem umfassenden Toolkit, mit dem sie eine parallel ablaufende Bedrohungserkennung über Ihr gesamtes Netzwerk, E-Mails, Web und Endpoints hinweg durchführen können.

Kaspersky Managed Detection and Response

Ideal für kleine und mittelständische Unternehmen mit geringer interner IT-Sicherheitsexpertise oder Unternehmen mit ausgereiften IT-Sicherheitsteams, die mit Routineaufgaben überlastet sind

Sie verfügen über kein eigenes IT Security-Team? Kein Problem! Kaspersky Managed Detection and Response bietet sofortigen, erweiterten Schutz gegen komplexe Bedrohungen.
Auch wenn Sie auf ein eigenes IT Security-Team zurückgreifen können, verschafft der Service Ihren Experten mehr Zeit, sich auf die Aktivitäten zu konzentrieren, die wirklich ihre Aufmerksamkeit erfordern.

Wenn Sie über kein internes IT-Sicherheitsteam verfügen oder wenn Ihre IT-Sicherheitsexperten ständig mit Routineaufgaben überlastet sind, ist Kaspersky Managed Detection and Response (MDR) die ideale Lösung. Dieser Service bietet kontinuierlichen Schutz gegen Cyberbedrohungen mit Vorfallsüberwachung rund um die Uhr, sowie Erkennung und Priorisierung mit schnellen und präzisen Reaktionsfähigkeiten.

Mit Kaspersky MDR sind Sie umgehend vor fortschrittlichen Bedrohungen und gezielten Angriffen geschützt.

Wenn Sie über ein ausgereiftes IT-Sicherheitsteam verfügen, können Sie mit Kaspersky MDR interne Ressourcen schonen. Zudem kann auf unsere umfassende Expertise im Bereich Threat Hunting zurückgegriffen werden.

Allgemeine Informationen

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Beschreibung	Endpoint-Schutz, Erkennung und Reaktion	Endpoint Detection and Response	Managed Detection and Response
Ideal für	Kleine und mittelständische Unternehmen mit begrenzter IT-Sicherheitsexpertise oder knappen Ressourcen	Mittelständische und große Unternehmen mit sich entwickelnder oder vollständig entwickelter IT-Sicherheitsexpertise	Kleine und mittelständische Unternehmen mit geringer IT-Sicherheitsexpertise oder Unternehmen mit ausgereiften IT-Sicherheitsteams, die mit ihren Routineaufgaben überlastet sind
Reaktion auf Bedrohungen	Von alltäglichen bis hin zu komplexen Bedrohungen wie Ransomware und dateilosen Bedrohungen usw.	Komplexe Bedrohungen und gezielte, APT-ähnliche Angriffe	Von alltäglichen bis hin zu komplexen Bedrohungen, einschließlich APTs
Unterstützte Betriebssysteme	Windows	Windows Linux (1. Quartal 2021) MacOS (2021)	Windows Linux (3. Quartal 2020) MacOS (1. Quartal 2021)
Anwendung	On-Premise Cloud	On-Premise Cloud (2021)	Cloud
Hardware-Anforderungen	Niedrig	Hoch (Serverinstallation erforderlich)	Niedrig
EPP-Funktionalität	● Beinhaltet Funktionalitäten von Kaspersky Endpoint Security for Business Advanced	● Kann mit Kaspersky Endpoint Security for Business und Kaspersky Hybrid Cloud Security sowie mit EPPs von Drittanbietern genutzt werden	● Kann mit Kaspersky Endpoint Security for Business und Kaspersky Hybrid Cloud Security genutzt werden
Nutzung in Verbindung mit anderen EPP-Anbietern	○	●	●

Bedrohungserkennung

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Erkennung	◒	●	●
Häufige sowie einige komplexe Bedrohungen	● Verwendet Erkennungskomponenten von Kaspersky Endpoint Security for Business	● Kann Erkennungskomponenten von Kaspersky Endpoint Security for Business und anderen EPP-Anbietern verwenden	● Verwendet Erkennungskomponenten von Kaspersky Endpoint Security for Business
Fortschrittliche und zielgerichtete Angriffe	○	●	● Von Kaspersky-Analysten erkannt
Fähigkeit, benutzerdefinierte, auf TTPs basierte Erkennungslogik hinzuzufügen	○	● Benutzerdefinierte IoA-Regeln	● Auf Grundlage der kundenspezifischen Bedürfnisse von Kaspersky-Analysten aktualisiert
Tiefgreifende Analyse verdächtiger Dateien	● Durch Integration der Kaspersky Sandbox	● Integrierte Sandbox-Komponente mit MITRE ATT&CK-Mapping	● Dateianalyse durch Kaspersky-Analysten während der Untersuchung oder auf Anfrage des Kunden
Threat Hunting	○	●	● Ausgeführt von Kaspersky-Analysten

Vorfallsuntersuchung

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Untersuchung	◒	●	● Ausgeführt von Kaspersky Analysten
Detaillierte Erkennungsinformation	●	●	●
IoC-basierte Analyse	●	●	●
IoC-Erstellungsoption	◒ Von Erkennungen durch Kaspersky Endpoint Security for Business	●	● Von Kaspersky-Analysten und mit Erkennungen von Kaspersky Endpoint Security for Business
Ereigniskontext zur Ursachenanalyse	◒ Erweiterte Erkennungen durch Kaspersky Endpoint Security for Business	●	●
Zugang zum Threat Intelligence Portal	◒ Open TIP	● Kaspersky TIP	● Kaspersky TIP
MITRE ATT&CK-Mapping	○	●	●
Manuelle Dateieinreichung zur Analyse an die Sandbox	○	●	● Von Kaspersky-Analysten oder auf Kundenwunsch
Detaillierte Informationen zu verdächtigen Dateien	○	●	●
Zugriff auf „Rohdaten“ zur Analyse	◒ Daten aus Erkennungen (ausschließlich durch Kaspersky Endpoint Security for Business)	●	● Von Kaspersky-Analysten als Teil der Untersuchung durchgeführt
Nachträgliche Analyse	○	●	● Von Kaspersky-Analysten
Grundlegende digitale Forensik	○	●	● Von Kaspersky-Analysten

Reaktion

	Kaspersky EDR Optimum	Kaspersky EDR	Kaspersky MDR
Reaktionstools gegen komplexe Bedrohungen	●	●	● Automatisierte Ausführung, basiert auf Reaktionsempfehlungen
Automatisierte Reaktion	Basiert auf Erkennungsergebnissen durch Kaspersky Endpoint Security for Business und erstellten IoC-Erkennungen	Automatische Vorbeugung auf Grundlage von Sandbox-Erkennungsergebnissen	Von Kaspersky-Analysten erstellte Reaktionsregeln
Teilweise automatisierte Reaktion	●	●	●
Ausführung einer EXE-Datei stoppen	●	●	●
Host-Isolation	●	●	●
Zusätzliche Reaktionen (Datei/Skript ausführen, Prozess stoppen, Datei in Quarantäne verschieben, Datei löschen)	●	●	●
Gesteuerte Untersuchung und Reaktion	○	●	● Bereitgestellt durch Kaspersky Analysten

www.kaspersky.de