kaspersky BRING ON THE FUTURE

# Kaspersky Managed Detection and Response

## für Managed Services-Anbieter

**Die weitgehende Automatisierung von Unternehmensprozessen in allen Bereichen führt zu einer zunehmenden Abhängigkeit der Unternehmen von der Informationstechnologie. Die Kehrseite der Medaille ist: Je mehr die Geschäftstätigkeit eines Unternehmens von der IT abhängt, desto interessanter wird es, die zugehörigen Informationssysteme zu hacken. Unternehmen tun sich oft schwer, an die zur Ermittlung von Bedrohungen erforderliche Expertise zu kommen und angemessen auf Bedrohungen zu reagieren. Oft sind die Sicherheitsteams mit der Verwaltung von Systemen und Tools überfordert, sodass nur wenig Zeit für eine genaue Untersuchung und Analyse bleibt.**

**Auch wenn die Vorteile auf der Hand liegen: Die Einführung von MDR-Praktiken bringt Investitionen in Personal, fachspezifische Schulungen und Technologien mit sich**

## Der Fachkräftemangel im Bereich der IT-Sicherheit hat Krisenniveau erreicht

Mittlerweile gibt es weltweit 4,07 Millionen unbesetzte Stellen in diesem Bereich. 2020 waren es noch 2,93 Millionen. Die wachsende Nachfrage nach Cybersicherheitsexpertise bedeutet auch, dass es nicht mehr nur darum geht, qualifizierte Mitarbeiter zu finden, sondern auch darum, sie durch attraktive Konditionen langfristig zu binden. Wenn ein Unternehmen also nicht bereits über eine Riege von Sicherheitsexperten für Threat Hunting, Untersuchung und Abwehr verfügen, werden sie sich schwer tun, Fachkräfte anzuwerben. Sie werden sich nach anderen Möglichkeiten umsehen müssen.

Die Services von Managed Detection and Response (MDR) sind eine effektive Lösung für Organisationen, die ein Frühwarn- und Abwehrsystem für Bedrohungen auf- und ausbauen möchten, denen aber das interne Fachwissen dafür fehlen. Diese Services gehören in der Cybersicherheit zu den am schnellsten wachsenden Märkten. Gartner geht davon aus, dass 25 % der Unternehmen bis 2024 MDR-Dienste nutzen werden. Aktuell sind es gerade einmal 5 %. Daraus ergeben sich enorme Umsatzchancen für Managed Service Provider (MSPs). Wer sein Portfolio um MDR ergänzt, kann seine Kunden bei der Bewältigung ihrer Sicherheitslücken unterstützten und langfristige Kundenbeziehungen aufbauen.

Auch wenn die Vorteile auf der Hand liegen: Die Einführung von MDR-Praktiken bringt Investitionen in Personal, fachspezifische Schulungen und Technologien mit sich. Viel wichtiger ist aber, dass bei fehlendem Fachwissen im Bereich Threat Hunting und Vorfallsreaktion ein erheblicher Zeitaufwand nötig ist, um das zu ändern. Und in der Zwischenzeit werden sich Ihre Bestands- und potentiellen Neukunden höchstwahrscheinlich beim Wettbewerb nach MDR-Services umschauen. Um die aktuelle Marktdynamik maximal zu nutzen, müssen Sie schnell handeln. Welche Möglichkeiten haben Sie?

Kaspersky MDR für MSPs ist ein Angebot an Sie und Ihre Kunden. Die überlegenen Erkennungs- und Abwehrfunktionen dieser Lösung werden von den erfolgreichsten und erfahrensten Threat Hunting-Teams der Branche unterstützt. Im Gegensatz zu anderen Angeboten nutzt Kaspersky MDR führende Sicherheitstechnologien, patentierte ML-Modelle (maschinelles Lernen), ständig aktualisierte Threat Intelligence und Kasperskys langjährige Erfahrung aus der effektiven Erforschung von zielgerichteten Angriffen. Selbst wenn Sie derzeit nicht über das entsprechende Know-how verfügen, können Sie Ihren Kunden damit vorausschauendes Threat Hunting und Remote-Abwehr mit Anleitung bieten. Und MSPs, die bereits über eigene MDR-Services verfügen, bietet Kaspersky MDR die Möglichkeit, eine wertvolle zweite Meinung von einem spezialisierten und vertrauenswürdigen Partner einzuholen. So können sie die eigenen Erkennung verifizieren und schnell auf die Vorfälle reagieren, die sie eventuell übersehen haben.

[1] https://apt.securelist.com/

# Vorteile von Kaspersky MDR für Managed Service Provider

**Schnelle, skalierbare Komplettbereitstellung ohne große Investitionen in Personal und Technologie**

**Weltweit anerkannte Expertise in Threat Intelligence und Threat Hunting – rund um die Uhr, 7 Tage die Woche, 365 Tage im Jahr.**


**Flexible Zahlungsmodalitäten mit monatlicher verbrauchsabhängiger Abrechnung oder Jahresabonnement**

**Mehrmandanten-Funktionen für mehrere Clients über eine zentrale Verwaltungskonsole**

**Unterstützte Produkte:**

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security für Linux
- Kaspersky Endpoint Security for Mac[1]
- Kaspersky Security for Windows Server
- Kaspersky Security for Virtualization Light Agent[2]
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack

## Funktionsweise

Der Service überwacht die von den Kaspersky-Produkten übermittelte Sicherheitstelemetrie. Die Lösung überprüft die von den Produkten ausgegebenen Warnmeldungen, um die Wirksamkeit der automatisierten Prävention sicherzustellen, und untersucht proaktiv die Metadaten von Systemaktivitäten auf Anzeichen von aktiven oder bevorstehenden Angriffen. Diese Metadaten werden über das Kaspersky Security Network erfasst und in Echtzeit automatisch mit der stets aktuellen Threat Intelligence von Kaspersky abgeglichen, um Taktiken, Techniken und Vorgehensweise von Angreifern zu erkennen.

Kaspersky MDR ist in zwei Ausbaustufen erhältlich. **Kaspersky EDR Optimum** steigert unmittelbar Ihre Möglichkeiten zum Threat Hunting und zur Vorfallsreaktion Sicherheitsstatus, ohne dass in zusätzliche Mitarbeiter oder Expertise investiert werden muss, und bietet in einer schnellen, mühelosen Bereitstellung Resilienz gegenüber schwer erkennbaren Angriffen. Der standardmäßig enthaltene EDR-Agent ermöglicht zentralisierte Remote-Aktionen, um infizierte Hosts zu isolieren, nicht autorisierte Prozesse zu beenden sowie schädliche Dateien in Quarantäne zu stellen und zu löschen. All das geschieht remote und ganz einfach per Mausklick.

**Kaspersky MDR Expert** enthält alle Funktionen von Optimum plus einen erweiterten Funktionsumfang und Flexibilität, wie die Direktanforderung von Analysten aus dem Kaspersky SOC, wenn zusätzliche Unterstützung oder Anleitung benötigt wird, drei Monate Speicherung der Rohdaten für rückwirkendes Threat Hunting sowie privilegierten Zugang zu Kaspersky Threat Intelligence.

[1] Wird voraussichtlich ab dem 2. Quartal 2021 unterstützt
[2] Wird voraussichtlich ab dem 1. Quartal 2021 unterstützt

# Vergleich der MDR-Stufen

## Optimum

- Proaktive Überwachung rund um die Uhr
- Automatisiertes Threat Hunting und Vorfallsuntersuchung
- Gesteuerte, nichtinvasive Szenarien der Fernreaktion
- Überprüfung der IT-Sicherheit[1] u. Überblick über Ressourcen
- MDR-Webportal mit Dashboards u. Berichten
- Verläufe werden 1 Jahr lang gespeichert
- Rohdaten werden 1 Monat lang gespeichert
- API für Datendownload[2]

## Expert

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

### 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

**Ein attraktives Angebot an Sie und Ihre Kunden, das viele sofort nutzbare Vorteile bietet:**

- Threat Hunting-Expertise von einem der erfahrensten globalen Teams. Unsere Erfahrung basiert auf 20 Jahren Forschung auf dem Gebiet der gezielten Angriffe
- Einfache Integration von Kaspersky MDR in Ihre vorhandenen Prozesse und Systeme (IRP, SOAR, SIEM) über die Kaspersky MDR-Portal-API
- Kompatibel mit AV-Schutz von Drittanbietern
- Mehrmandanten-Funktionen für mehrere Clients über eine zentrale Verwaltungskonsole

Zur weiteren Überprüfung, Untersuchungen und Identifizierung neuer Bedrohungen nutzt die Threat Hunting-Funktion von MDR Optimum eine automatisierte Erkennungsfunktion, die mit eigens ermittelten Angriffsindikatoren arbeitet. In MDR Expert basiert die Managed Threat Hunting-Funktion auf der sorgfältigen Handarbeit unserer erfahrenen Experten, die proaktiv die Bedrohungen aufspüren, die nicht automatisch erkannt werden.

Im Rahmen dieses Services erhält man über das MDR-Portal einen kompletten Einblick in alle Erkennungen sowie Warnhinweise mit umfassenden Empfehlungen zur Vorfallsabwehr. Dank der Mehrmandanten-Architektur können MSPs alle ihre Kunden zentral verwalten. Über eine API lässt sich das Portal außerdem in Ihre bestehenden Systeme (IRP, SOAR, SIEM) und Workflows integrieren.

Mit einer Reihe von Optionen (separat erhältlich) können Sie die Funktionsweise des Services außerdem ganz flexibel an Ihre eigenen Bedürfnisse anpassen.

[1] Voraussichtlich ab dem 1. Quartal 2021 verfügbar
[2] Voraussichtlich ab dem 1. Quartal 2021 verfügbar
[3] Voraussichtlich ab dem 1. Quartal 2021 verfügbar

# Registrierung zu Kaspersky MDR

Wenn Sie Ihre Managed Services-Portfolios durch die Managed Detection and Response-Lösung von Kaspersky ergänzen, können Sie nur gewinnen:

- Schaffen Sie mit dem aktualisierten MDR-Schutz von Kaspersky für Ihre Kaspersky Endpoint Security for Business-Kunden zusätzliche Anreize für die Verlängerung und sorgen Sie für eine langfristige Kundenbindung.
- Mit dem Upselling einer Lösung, die Schutz rund um die Uhr bietet, gewinnen Sie Großunternehmen als potentielle neue Endpoint Security-Kunden und steigern Ihren Umsatz.

Registrieren Sie sich für Kaspersky MDR und und profitieren Sie von allen Vorteilen des MSP-Programms von Kaspersky – monatliche verbrauchsabhängige Abrechnung oder Jahresabonnement, Mengenrabatte, höhere Gewinnsmargen, Möglichkeiten zum Upselling und Cross-Selling sowie renommierten technischen Support und Vertriebsunterstützung durch Kaspersky.

**Um sich die Chancen** des rapide wachsenden MDR-Marktes zu sichern, sollten Sie noch heute mit uns Kontakt aufnehmen: msp@kaspersky.com

Cyber Threats News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMU: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise
Threat Intelligence Portal: opentip.kaspersky.de

**www.kaspersky.de**



**Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.**

**Erfahren Sie mehr unter kaspersky.de/transparency.**

Proven.
Transparent.
Independent.