kaspersky BRING ON THE FUTURE

# Kaspersky Endpoint Security Cloud EDR Preview 2021 oder Kaspersky Endpoint Detection and Response Optimum – welches davon ist das richtige Tool für Sie?

Endpoint Detection and Response umfasst ein breites Spektrum unterschiedlicher Methoden, Technologien und Tools.
Innerhalb des Kaspersky-Portfolios haben Sie die Wahl zwischen zwei EDR-basierten Einsteigerlösungen:

- Kaspersky Endpoint Security Cloud EDR Preview 2021
- Kaspersky Endpoint Detection and Response Optimum

Dieses Dokument soll Ihnen eine Entscheidungshilfe bieten, welches der beiden EDR-Tools für sie das richtige ist.

## Kaspersky Endpoint Security Cloud EDR Preview 2021

Dieses Modul bietet fortschrittliche Funktionen zur Erkennung und Visibilität sowie den Zugang zu einer professionellen Vorfallsuntersuchung. Für Sie bedeutet das weder zusätzlichen Aufwand noch zusätzliche Kosten, denn all das ist in Ihrer Kaspersky Endpoint Security PLUS-Lizenz bereits enthalten.

Sie können Warnhinweise anhand von Vorfallskontexten und -details untersuchen und die Ursachen über eine Visualisierung des Angriffspfads analysieren. Folgende Daten stehen zur Überprüfung zur Verfügung:

- Hostdaten: Version des Betriebssystems, Netzwerkschnittstellen und Benutzer
- Dateidaten: Name, Hash, Download-, Erstellungs- und Änderungsparameter etc.
- Prozessdaten: Datum und Uhrzeit, Startparameter
- Zugehörige Erkennungen

Und mehr.

Alle diese Informationen sind über die gesamte Kaspersky Endpoint Security Cloud-Installation verfügbar, die Sie unabhängig von Ort und Zeit über Ihre Cloud-basierte Konsole verwalten können.

Und was die Vorfallsreaktion betrifft, kümmert sich unsere Remediation Engine automatisch um die Eindämmung der Bedrohung.

## Kaspersky Endpoint Detection and Response Optimum

Dieses Modul unterstützt Sie und Ihre IT-Sicherheitsexperten mit einem benutzerfreundlichen EDR-Toolkit beim Aufbau und der Optimierung von Prozessen zur Vorfallsreaktion. Neben der zuverlässigen Erkennung und vollständigen Analyse von Bedrohungen durch das Tool behalten Sie die volle Kontrolle über die Art Ihrer Gegenmaßnahmen.

Fortschrittliche Erkennung, mehr Transparenz, einfache Ursachenanalyse, vorausschauendes Scannen nach Gefährdungsindikatoren (Indicator of Compromise, IoC) sowie automatisierte und manuelle Abwehroptionen werden entweder Cloud-basiert oder lokal über die zentrale Kaspersky Security Center-Konsole verwaltet

Mit Kaspersky EDR Optimum übernehmen Sie die volle Kontrolle und heben Ihre Abwehrmaßnahmen gegen versteckte Bedrohungen mit geringem zusätzlichen Ressourcenaufwand auf ein völlig neues Niveau.

# Detaillierter Vergleich.

| | Kaspersky Endpoint Security Cloud EDR Preview 2021 | Kaspersky Endpoint Detection and Response Optimum |
|---|---|---|
| **Erkennung** | ML-basierte fortschrittliche Erkennung | ML-basierte fortschrittliche Erkennung |
| IoC-Scans über mehrere Endpoints | ✗ | ✓ |
| **Transparenz** | | |
| Eine Karte mit Kontext und Details zum Warnhinweis | ✓ | ✓ |
| Ursachenanalyse (Visualisierung des Angriffspfads) | ✓ | ✓ |
| Threat Intelligence-Daten | ✓ | ✓ |
| **Response** | EPP Remediation Engine | EPP Remediation Engine sowie per Mausklick oder voll automatisch eingeleitete Abwehrmaßnahmen, die bei Erkennungen aus den IoC-Scans sofort eingeleitet werden:<br>· Isolieren des Hosts<br>· Datei entfernen<br>· Dateiausführung verhindern<br>· Kritische Host-Bereiche scannen |
| **Management** | Online-Konsole Kaspersky Endpoint Security Cloud | Kaspersky Security Center, Cloud-basiert oder On-Premise |

**Cyber Threats News:** de.securelist.com
**IT Security News:** www.kaspersky.de/blog/b2b
**IT-Sicherheit für KMU:** kaspersky.de/business
**IT-Sicherheit für Großunternehmen:** kaspersky.de/enterprise

**www.kaspersky.de**