# Zuverlässige Abwehr von Bedrohungen

## Endpoint Detection and Response zum Schutz vor komplexen Angriffen mit automatisierten Massnahmen

### Kaspersky EDR Optimum: die Highlights

- Schutz vor immer raffinierteren und häufigeren Bedrohungen
- Automatisiertes Tool spart Zeit und Ressourcen
- Transparenter Überblick über das Ausmass an komplexen Bedrohungen im gesamten Netzwerk
- Liefert Informationen über die Ursachen von Bedrohungen
- Effektive Schadensminderung durch schnelle, automatisierte Gegenmassnahmen

Kaspersky wurde 1997 in Moskau gegründet. Heute agiert der Sicherheitsspezialist in 200 Ländern, beschäftigt über 4000 hoch qualifizierte Spezialisten und Spezialistinnen und gilt als führender Anbieter von Sicherheitslösungen für Privatanwender, KMU und Grossbetriebe. Kaspersky-Technologien schützen weltweit um die 400 Millionen User und stehen in mehr als 270 000 Unternehmen und Organisationen im Einsatz. Die Cybersecurity-Lösungen und Cybersecurity-Dienste von Kaspersky umfassen cloudbasierte, als Managed Service sowie On-Premises betriebene Endpoint Security, Hybrid Cloud Security und Enterprise Security der nächsten Generation inklusive Lösungen zur Absicherung von IoT- und industriellen Anwendungen. Im Hintergrund stehen dabei stets die langjährige Expertise der Kaspersky-Professionals und die tief greifende Threat Intelligence, die aus den global gewonnenen Cybersicherheitsdaten der eingesetzten Lösungen resultiert. Kaspersky Endpoint Detection and Response (EDR) Optimum vereint benutzerfreundliche, hoch automatisierte Tools zur Erkennung und Abwehr der zunehmend komplexen und öfter auftretenden Bedrohungen aus dem Cyberspace mit den hochwertigen Endpoint-Protection-Funktionen von Kaspersky Endpoint Security for Business. EDR Optimum bietet mit einer zentralen Konsole einen umfassenden Überblick über die Sicherheitslage im gesamten Netzwerk, informiert verständlich über die Ursachen der erkannten Bedrohungen und entlastet das IT- und Security-Team durch automatisch eingeleitete Abwehrmassnahmen von zeitraubenden Routineaufgaben.

# Bedrohungsabwehr mit Kaspersky EDR Optimum

Die Tage simpler Malware sind lange vorbei. Bedrohungen sind heute komplizierter, für Unternehmen verlustreicher und entfalten ihre zerstörerische Wirkung längere Zeit unbemerkt. So wurden 2019 91 Prozent aller Organisationen Opfer eines Cyberangriffs. Kaspersky EDR wehrt auch die fortgeschrittensten Bedrohungen ab und leitet automatisch Gegenmassnahmen ein.

## Endpoint Protection und rasche Reaktion auf Bedrohungen

Kaspersky Endpoint Detection and Response (EDR) Optimum sorgt dafür, dass das Unternehmensnetzwerk angesichts komplexer und hoch entwickelter Bedrohungen durch fortschrittliche Erkennung, vereinfachte Untersuchung und automatisch eingeleitete Gegenmassnahmen sicher bleibt. EDR Optimum umfasst weitreichende Sichtbarkeit, einfache Untersuchungstools und automatisierte Abwehroptionen, damit eine Bedrohung nicht nur erkannt, sondern ihr volles Ausmass und die Ursachen offengelegt werden, um sofort reagieren und Geschäftsunterbrechungen verhindern zu können.

Die Lösung vereint ein benutzerfreundliches, hoch automatisiertes Erkennungs- und Reaktions-Toolkit mit den einzigartigen Endpoint-Protection-Funktionen und der fortschrittlichen Erkennung von Kaspersky Endpoint Security for Business. Einfache zentralisierte Kontrollen und ein hoher Automatisierungsgrad verschaffen den IT- und Security-Teams mehr Zeit für anderes und erlauben den gezielteren Einsatz der Mitarbeitenden – unterstützt durch einen schlanken Workflow aus einer einzigen Konsole, die lokal oder in der Cloud implementiert werden kann.

## Kaspersky Endpoint Detection and Response

### Optimum

## Das Bedrohungsausmass im Überblick

Kaspersky EDR Optimum sammelt eine Vielzahl wichtiger Informationen und verschafft anhand einer bildlichen Darstellung des Verbreitungspfades eines Angriffs unmittelbares Verständnis für den Zusammenhang zwischen unterschiedlichen Ereignissen. Durch Scannen von importierten oder selbst generierten Gefährdungsindikatoren (IoC) erhält man einen detaillierten Überblick über sämtliche Hosts im Netzwerk. Auf Bedrohungen, die auf der Grundlage der IoC-Scans über alle Endpoints hinweg aufgedeckt werden, reagiert EDR Optimum mit automatisierten Gegenmassnahmen – oder das Security-Team leitet mit nur einem Mausklick direkt Gegenmassnahmen ein. Dies kann zum Beispiel die Isolation des betroffenen Hosts, Quarantäne für infizierte Dateien, das Scannen des Hosts oder die Blockierung der Ausführung einer Datei sein.