kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Zuverlässige, weitreichende Abwehr mit sofortiger Einleitung von automatisierten Gegenmaßnahmen und einfacher Ursachenanalyse

Das Problem

91 % aller Organisationen sind im Laufe des Jahres 2019 Opfer von Cyberangriffen geworden, wobei **1 von 10** einem gezielten Angriff[1] ausgesetzt war.

Komplexe Bedrohungen bedeuten Verluste

Die Tage simpler Malware sind lange vorbei. Bedrohungen sind heute viel komplizierter, für Unternehmen verlustreicher und entfalten ihre zerstörerische Wirkung längere Zeit unbemerkt.

Der Angreifer hat Sie im Visier

Diese komplexen Bedrohungen sind viel billiger geworden und treten immer häufiger auf, so dass sich Unternehmen, die bislang davon ausgehen konnten, nicht zur Zielgruppe zu gehören, mittlerweile vorsehen müssen.

Effizienz tut Not

Der Mangel an Ressourcen, denen sich Organisationen heute gegenüber sehen, insbesondere an Zeit und ausgebildetem Personal, verschärft die Situation weiter.

So helfen wir

„Eine schwache Endpoint Protection Platform-Lösung macht den Wert eines EDR-Tools zunichte"[2]

„Somit sind Mitarbeiter und Zeit die neuen ROI-Metriken für EDR-Tools"[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum sorgt dafür, dass Sie angesichts von komplexen und hochentwickelten Bedrohungen durch fortschrittliche Erkennung, vereinfachte Untersuchung und automatisch eingeleitete Gegenmaßnahmen sicher bleiben.

Mehr als die Basisfunktionen

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.

Zuverlässige weitreichende Abwehr

In dieser Lösung ist ein benutzerfreundliches, hoch automatisiertes Erkennungs- und Reaktionstoolkit vereint mit den einzigartigen Endpoint Protection-Funktionen sowie der fortschrittlichen Erkennung von Kaspersky Endpoint Security for Business.

Intelligentes Tool sorgt für Effizienz

Mit diesem Tool erhalten Sie mithilfe von einfachen zentralisierten Kontrollen und einem hohen Automatisierungsgrad mehr Zeit für anderes und können Ihre menschlichen Ressourcen gezielter einsetzen. Ein schlanker Workflow aus einer einzigen Konsole, die sowohl lokal als auch in der Cloud implementierbar ist[3].

Hauptvorteile

- Schützen Sie sich selbst vor immer häufiger auftretenden und immer destruktiveren modernen und komplexen Bedrohungen
- Sparen Sie mit einem einfachen und automatisierten Tool Zeit und Ressourcen
- Verschaffen Sie sich einen Überblick über das Ausmaß an komplexen Bedrohungen im gesamten Netzwerk
- Erfahren Sie die Ursache einer Bedrohung und wie sie zustande kommt
- Wenden Sie weiteren Schaden durch schnelle automatisierte Gegenmaßnahmen ab

Anwendungsfälle für EDR

Beantworten Sie die folgenden wichtigen Fragen

- In welchem Kontext tritt die Warnung auf?
- Welche Maßnahmen wurden aufgrund der Warnung bereits eingeleitet?
- Ist die erkannte Bedrohung noch immer aktiv?
- Sind weitere Hosts von dem Angriff betroffen?
- Welchem Pfad ist der Angriff gefolgt?
- Was ist die Kernursache der Bedrohung?

Lernen Sie das komplette Ausmaß der Bedrohung kennen

Sobald Sie erfahren haben, dass Sie eventuell Ziel einer globalen Bedrohung sind – z. B. weil eine Behörde Sie aufgefordert hat, Ihre Systeme auf bestimmte Gefährdungsindikatoren zu scannen – können Sie Folgendes tun:

- Importieren Sie IoCs aus vertrauenswürdigen Quellen, und führen Sie regelmäßig Scans durch, um Anzeichen eines Angriffs zu erkennen.
- Führen Sie nach einer Warnmeldung eine gründliche Untersuchung durch, generieren Sie auf Basis erkannter Bedrohungen entsprechende IoCs und führen Sie Scans im gesamten Netzwerk durch, um herauszufinden, ob andere Hosts betroffen sind.

Reagieren Sie unverzüglich auf sich rasch ausbreitende Bedrohungen.

- Stellen Sie Dateien im Zusammenhang mit komplexen Bedrohungen an allen Endpoints automatisch unter Quarantäne.
- Isolieren Sie betroffene Hosts automatisch, sobald ein Gefährdungsindikator im Zusammenhang mit einer sich schnell ausbreitenden Bedrohung gefunden wird.
- Verhindern Sie, dass die schädliche Datei während der Untersuchung ausgeführt wird und sich im gesamten Netzwerk verbreitet.

[1] Der Kaspersky-Bericht zu globalen IT-Risiken, Kaspersky, 2019

[2] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Dok.-Nr. US45794219, 2020

[3] Es gibt gewisse Einschränkungen bezüglich der Auswahl an Funktionen, die über die Cloud-Konsole verwaltet werden können. Eine vollständige Beschreibung finden Sie unter https://kas.pr/epp-management-options

Ihre Vorteile:

Das ganze Ausmaß der Bedrohung im Überblick

Sicherheitshinweise werden auf Ihren Endpoints angezeigt, wo Sie sie weiter analysieren können, um sich einen Überblick über die komplette Breite und Tiefe der Bedrohung zu verschaffen. So wird sichergestellt, dass Vorfälle vollständig abgehandelt werden und nichts von der Bedrohung auf dem Endpoint übrig bleibt.

Vereinfachen Sie Ihren Workflow

Ein schlanker Workflow aus einer einzelnen Konsole die sowohl lokal als auch in der Cloud implementierbar ist mit einfachen EDR-Szenarien und Gegenmaßnahmen, einschließlich einer umfassenden Übersicht, Scanning nach Gefährdungsindikatoren (IoC) und Abwehroptionen, für die weder Fachwissen in Cybersicherheit noch hoher Zeitaufwand erforderlich ist.

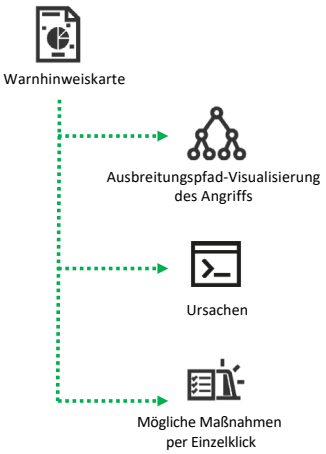
Verstärken Sie Ihre Verteidungsmaßnahmen

Durch Ergänzung mit der Kaspersky Sandbox entsteht eine integrierte Endpoint-Sicherheitslösung mit einfachen, effektiven und hoch automatisierten mehrstufigen Abwehroptionen gegen gängige, komplexe und schwer zu erfassende Bedrohungen.

Analyse von detaillierten Warnhinweisen

Kaspersky EDR Optimum sammelt eine Vielzahl von wichtigen Informationen, damit Sie anhand einer bildlichen Darstellung des Verbreitungspfades eines Angriffs den Zusammenhang zwischen unterschiedlichen Ereignissen verstehen lernen.

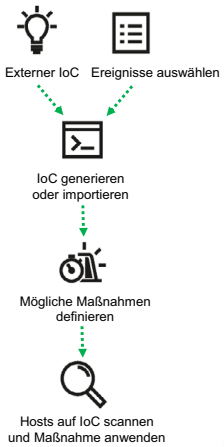
Durch Scannen von importierten oder selbst generierten Gefährdungsindikatoren (IoCs) erhalten Sie einen detaillierten Überblick über sämtliche Hosts im Netzwerk.



Automatische Reaktion

Auf Bedrohungen, die auf der Grundlage von IoC-Scans über alle Endpoints hinweg aufgedeckt werden, können Sie mit automatisierten Gegenmaßnahmen reagieren, oder Sie leiten mit nur einem Mausklick direkt Gegenmaßnahmen ein.

Zu den Gegenmaßnahmen gehören: den Host isolieren, Dateien unter Quarantäne stellen, Host scannen und Datei an der Ausführung hindern.



Weitere EDR-Optionen

Kaspersky Endpoint Detection and Response Optimum ist eine von vielen EDR-Optionen in unserem Portfolio, die auf die jeweiligen Kundenanforderungen zugeschnitten sind. Möglicherweise auch für Sie interessant:

Kaspersky Endpoint Detection and Response

Mit dieser EDR-Expertenlösung, von der Branche und Kunden geschätzt und perfekt geeignet für IT-Organisationen mit erfahrenen IT-Sicherheitsteams, können Sie sehr ausgeklügelten, hochentwickelten und zielgerichteten Angriffen auf den Grund gehen. Bietet verbesserte Bedrohungserkennung, leistungsstarke Untersuchungsfunktionen, vorausschauendes Threat Hunting und zentralisiertes Einleiten von Gegenmaßnahmen.
https://www.kaspersky.de/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

Eine vollständig gemanagte und individuell zugeschnittene Lösung mit Erkennung, Priorisierung, Untersuchung und Reaktion rund um die Uhr – gestützt auf mehr als 20 Jahre erfolgreicher Erforschung von Cyberbedrohungen – gibt Ihnen alle Vorteile eines eigenen Security Operations Center, ohne tatsächlich eines einrichten zu müssen.
https://www.kaspersky.de/enterprise-security/managed-detection-and-response

Weitere Informationen zur Funktionsweise von Kaspersky Endpoint Detection and Response Optimum im Kampf gegen Cyberbedrohungen bei gleichzeitiger Entlastung von Sicherheitsteams und Ressourcen finden Sie unter:
http://www.kaspersky.de/enterprise-security/edr-security-software-solution

Neues über Cyberbedrohungen: https://de.securelist.com/
IT-Sicherheitsnachrichten: business.kaspersky.de/
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 möchten eine sichere Umgebung schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Proven.
Transparent.
Independent.