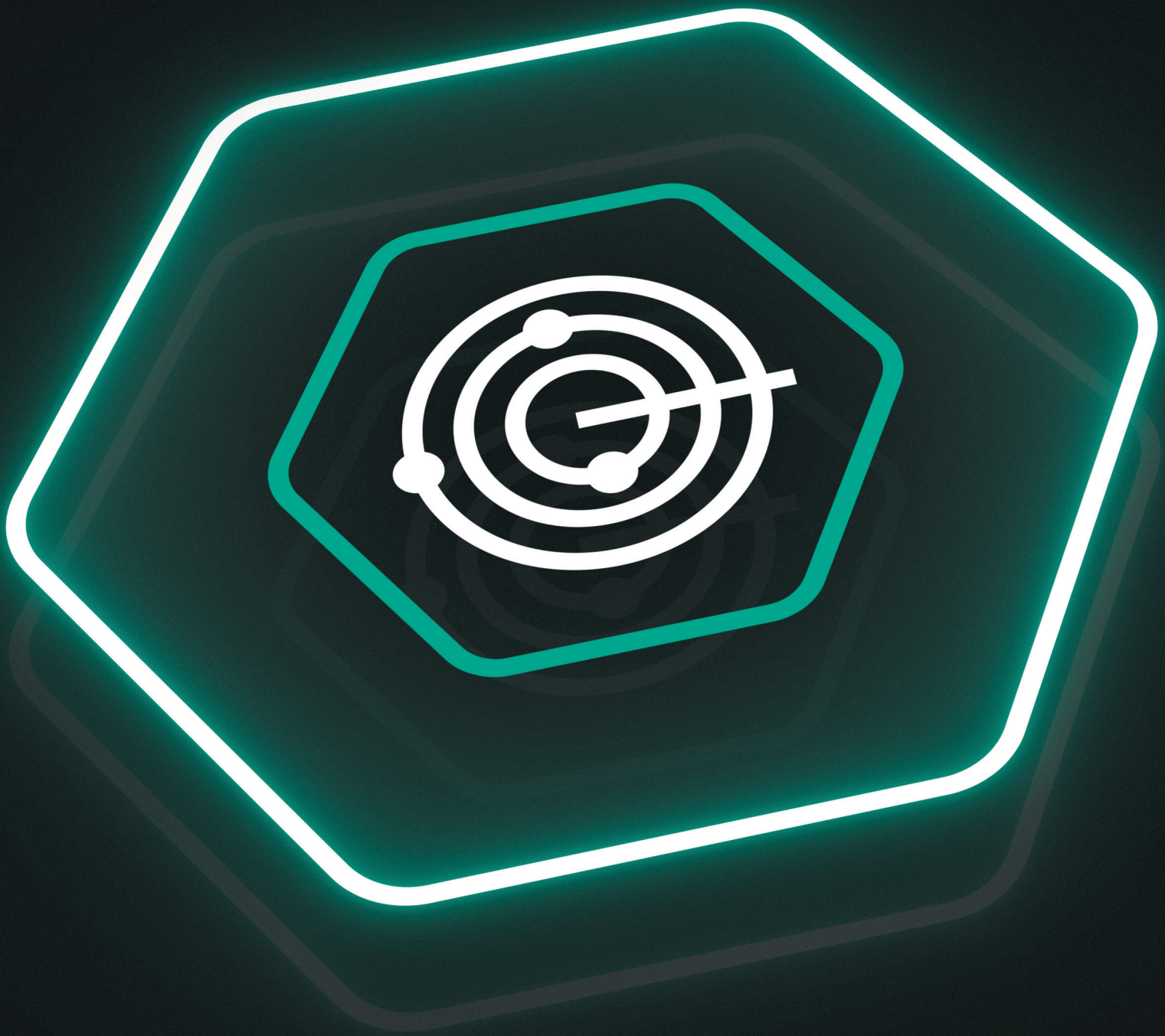


Kaspersky Anti Targeted Attack Platform

kaspersky BRING ON THE FUTURE

Die heutigen Cyberkriminellen sind darauf spezialisiert, einzigartige und innovative Methoden für das Eindringen in Systeme und für die Kompromittierung von Systemen zu entwickeln. Da sich die Bedrohungen ständig weiterentwickeln und immer raffinierter und tiefgreifender werden, sind eine rasche Erkennung und die schnellste und bestgeeignete Reaktion entscheidend geworden.

Es ist von wesentlicher Bedeutung, dass Unternehmen ihre IT-Sicherheitsabwehr immer wieder neu überdenken,

um den wachsenden Bedrohungsraten im Cyberspace einen Schritt voraus zu sein und die finanziellen Verluste zu begrenzen.

Unübertroffene Cybersicherheit in einer einheitlichen Lösung

Professionelle Cyberkriminelle bevorzugen heutzutage einen Multi-Vektor-Ansatz. Die Kaspersky Anti Targeted Attack Platform kombiniert fortschrittliche Bedrohungserkennung und EDR-Fähigkeiten auf Netzwerkebene und liefert IT-Sicherheitsspezialisten alle nötigen Instrumente, um eine überlegene multidimensionale Bedrohungserkennung zu gewährleisten, Spitzentechnologien anzuwenden, effektive Untersuchungen durchzuführen, proaktiv nach Bedrohungen zu suchen und eine schnelle, zentralisierte Reaktion zu liefern — alles mit einer einzigen Lösung.

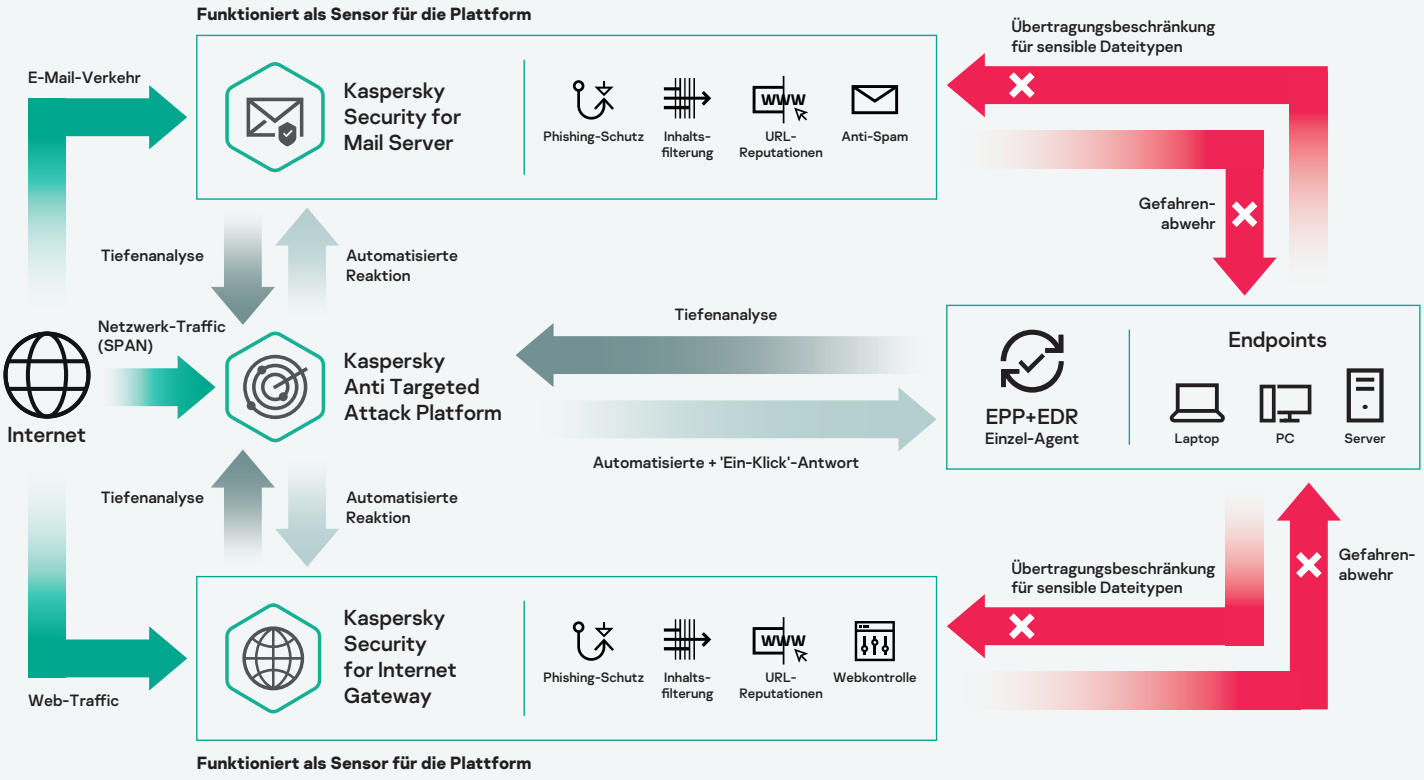
Kaspersky Anti Targeted Attack Platform:

- **VERKÜRZT** die Zeit bis zur Erkennung von und Reaktion auf Bedrohungen
- **VEREINFACHT** die Bedrohungsanalyse und Vorfallsreaktion
- **HILFT**, Sicherheitslücken zu schließen und die „Verweildauer" von Angriffen zu verkürzen
- **AUTOMATISIERT** manuelle Aufgaben – während der Erkennung von und Reaktion auf Bedrohungen
- **ENTLASTET** das IT-Sicherheitspersonal für andere Aufgaben
- **UNTERSTÜTZT** die uneingeschränkte Einhaltung von Rechtsvorschriften

Die raffiniertesten Angriffe in Ihrem Fokus und unter Ihrer Kontrolle

Die Plattform fungiert als eine Extended Detection and Response-Lösung, die einen umfassenden APT-Schutz auf der Grundlage unserer Threat Intelligence bietet und dem MITRE-ATT&CK-System zugeordnet ist. Alle potenziellen Angriffspunkte für Bedrohungen - Netzwerk, Web, E-Mail, PCs, Laptops, Server und virtuelle Maschinen - stehen unter Ihrer Kontrolle.

Die Kaspersky Anti Targeted Attack Platform ist vollständig in **Kaspersky Endpoint Security for Business** integriert und teilt sich einen einzigen Agenten mit Kaspersky EDR. Sie lässt sich außerdem sowohl in **Kaspersky Security for Mail Server** als auch in **Kaspersky Security for Internet Gateway** integrieren, die als Sensoren für die Plattform dienen und eine automatisierte Antwort auf komplexere E-Mail- und Web-Bedrohungen bieten.



Eine vertrauenswürdige Sicherheitslösung, die vollständigen Datenschutz bietet

Alle Objektanalysen werden vor Ort und ohne ausgehenden Datenfluss durchgeführt. Das Kaspersky Private Security Network liefert Reputations-Updates in Echtzeit, wobei die vollständige Isolierung der Unternehmensdaten erhalten bleibt.

Eine einheitliche Plattform zur Beschleunigung der Innovation in der digitalen Transformation durch:

- **Integrale Geschäftskontinuität.** Wir bauen Sicherheit und Compliance von Anfang an in neue Prozesse ein
- **Vollständige Transparenz** bezüglich der IT-Infrastruktur Ihres Unternehmens
- **Maximale Flexibilität** für die Bereitstellung in physischen und virtuellen Umgebungen überall dort, wo Transparenz und Kontrolle erforderlich sind
- **Automatisierung von Aufgaben zur Erkennung und Reaktion auf Bedrohungen**, um die Kosteneffizienz Ihrer Sicherheits-, Vorfallsreaktions- und SOC-Teams zu optimieren
- **Enge, unkomplizierte Integration** in bestehende Sicherheitsprodukte zur Verbesserung des allgemeinen Sicherheitsniveaus und zum Schutz älterer Investitionen in die Sicherheit

Hauptmerkmale:

Mehrschichtige Sensorarchitektur – umfassende Einsicht, erreicht durch eine Kombination von Netzwerk-, Web- und E-Mail-Sensoren sowie Endpoint-Agenten.

Umfassende Engines zur Erkennung von Bedrohungen – arbeiten mit Daten von Netzwerksensoren (Netzwerkverkehrs-analyse) und Endpoint-Agenten (EDR-Funktionen) für schnelle Entscheidungen und weniger Fehlalarme.

Advanced Sandbox – bietet eine sichere Umgebung für die tiefgreifende Analyse von Bedrohungsaktivitäten, unterstützt die Randomisierung von Betriebssystemkomponenten, die Zeitbeschleunigung in virtuellen Maschinen, Anti-Umgehungstechniken, die Simulation von Benutzeraktivitäten und die Ergebniszuordnung zur MITRE ATT&CK-Knowledgebase – all dies trägt zu einer hocheffizienten verhaltensbasierten Erkennung bei.

Retrospektive Analyse – auch in Situationen, in denen kompromittierte Endpoints unzugänglich sind oder wenn Daten verschlüsselt wurden – durch automatisierte Daten-, Objekt- und Entscheidungssammlung und zentralisierte Speicherung.

Zwei Modi der Threat-Intelligence-Interaktion – automatisierter Vergleich mit globalen Reputationsdaten aus dem Kaspersky Security Network und manuelle Suche nach Bedrohungen und Ermittlungsabfragen über das Kaspersky Threat Intelligence Portal.

Automatische Bedrohungsjagd in Echtzeit – Ereignisse werden mit einem einzigartigen Satz von Angriffsindikatoren (Indicators of Attack – IoAs) korreliert, die von Kaspersky-Bedrohungsjägern generiert und der MITRE ATT&CK-Matrix zugeordnet werden, die klare Ereignisbeschreibungen, Beispiele und Reaktionsempfehlungen enthält.

Proaktive Bedrohungssuche mit unserem leistungsstarken, flexiblen Abfragegenerator – Analysten können komplexe Abfragen erstellen, um nach atypischem Verhalten und verdächtigen Aktivitäten sowie nach spezifischen Bedrohungen für Ihre Infrastruktur zu suchen.

Fazit

Zuverlässiger Datenschutz, eine abgesicherte IT-Infrastruktur, stabile Abläufe und Compliance sind die Voraussetzungen für nachhaltiges Unternehmenswachstum.

Die Kaspersky Anti Targeted Attack-Plattform hilft Unternehmen mit einer ausgereiften IT-Sicherheit beim Aufbau von zuverlässigen Verteidigungsmechanismen, die Ihre Infrastruktur vor APT-ähnlichen Bedrohungen und zielgerichteten Angriffen schützen und Sie bei der Einhaltung von Compliance-Richtlinien unterstützen, ohne dass Investitionen in zusätzliche IT-Sicherheitsressourcen erforderlich werden. Komplexe Vorfälle werden schnell erkannt, untersucht und abgewehrt. Die Effizienz Ihrer IT-Sicherheit bzw. Ihres SOC-Teams wird gesteigert, indem manuelle Aufgaben von einer vereinheitlichten, weitestgehend automatisierten Lösung übernommen werden, die höchsten Qualitätsanforderungen gerecht wird.

Erwiesenermaßen die wirksamste Lösung der Branche

SE Labs hat die Kaspersky Anti Targeted Attack Platform anhand einer Reihe von Hackerangriffen getestet **und uns ein Triple-A-Rating gegeben**.

In der unabhängigen 'ICSA Labs: Advanced Threat Defense (Q3 2019)' lieferte die Kaspersky Anti Targeted Attack Platform **eine Erkennungsrate von 100 % mit null Fehlalarmen**.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Die Radicati-Gruppe betrachtet Kaspersky als **einen der wichtigsten Akteure in seinem Advanced Persistent Threat (APT) Protection - Market Quadrant 2020**.

Gartner Peer Insights Customer's Choice für EDR-Lösungen 2020 ernennt Kaspersky zum Top-Anbieter

Als einer von nur 6 Anbietern weltweit wurde Kaspersky Anti Targeted Attack Platform mit Kaspersky EDR im Kern als Gartner Peer Insights Customer's Choice für EDR-Lösungen im Jahr 2020 ausgezeichnet - das ultimative Kundenkompliment für unsere Extended-EDR-Lösung.

Hinweis zu Gartner

Gartner Peer Insights Customers' Choice umfasst die subjektiven Meinungen individueller Endnutzerrezensionen, -bewertungen und -daten, die mithilfe dokumentierter Methoden untersucht werden. Sie stellen weder die Ansichten noch eine Empfehlung von Gartner oder seinen Tochterunternehmen dar.

MITRE ATT&CK bestätigt die Qualität der Erkennung

Das Kernelement der Kaspersky Anti Targeted Attack Platform - Kaspersky EDR - beteiligte sich an der MITRE Evaluation Round 2 (APT29) und bewies dabei ein hohes Leistungsniveau bei der Erkennung wichtiger ATT&CK-Techniken, die in entscheidenden Phasen der heutigen gezielten Angriffe angewandt werden.

Mehr erfahren Sie unter kaspersky.com/MITRE

Um mehr über Kaspersky Anti Targeted Attack Platform zu erfahren, besuchen Sie

kaspersky.com/enterprise-security/anti-targeted-attack-platform

Cyber Threats News: https://de.securelist.com/
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sichere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir sie, 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.