



Kaspersky® Anti Targeted Attack Platform

Minimierung von Cybersicherheitsrisiken im Zeitalter der digitalen Transformation

Cybersecurity muss als Stützpfeiler Ihrer digitalen Unternehmensstrategie Innovationen fördern und zur Erkennung und Minimierung von Risiken beitragen. Dort, wo Cybersicherheit immer noch als reiner Kostenfaktor und potentieller Fortschrittshemmer statt als Motor für Unternehmenswachstum angesehen wird, kann Kaspersky Lab helfen, Erwartungen und Realität in Einklang zu bringen.

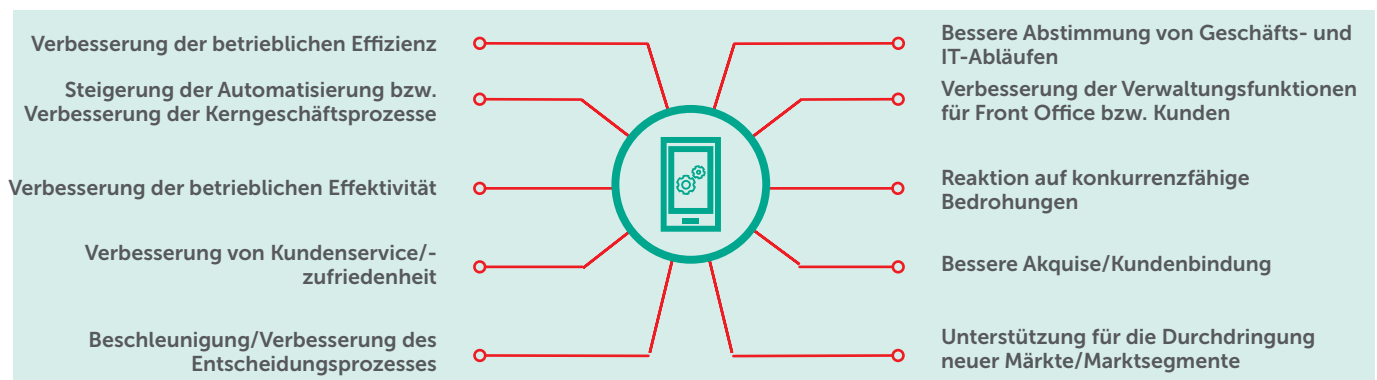
Ein strategischer Ansatz für fortschrittliche Unternehmenssicherheit

Die Kaspersky Anti Targeted Attack Platform bietet einen neuen strategischen Ansatz für die Erkennung gezielter Angriffe. Ergänzt durch unsere mehrstufigen Präventionstechnologien und -lösungen sowie ein umfassendes Portfolio an Cybersecurity Services für die Reaktion und Prognose bietet Kaspersky Lab einen vollständig integrierten, strategischen Ansatz zur Abwehr gezielter Angriffe und zur Erkennung von Bedrohungen und die Reaktion darauf.

Eine unternehmensweite Cybersicherheits-Strategie zur Bewältigung von digitalen Störungen

Der zunehmende Einsatz digitaler Technologien wie Cloud-Dienste, Big Data, Mobiltechnik, IoT und künstlicher Intelligenz – sowohl in Unternehmen als auch in der Gesellschaft im Allgemeinen – hat aufgrund der zunehmenden Konnektivität zahlreiche neue Herausforderungen im Hinblick auf Sicherheit, Compliance und Datenschutz zur Folge.

Geschäftliche Ziele der Digitalisierung



Digitale Transformation – eine neue Rolle für die Cybersicherheit

Cybersicherheit ist neben Compliance und Datennutzung zu einer der wichtigsten strategischen Prioritäten des digitalen Geschäfts geworden. Unternehmen suchen nach Sicherheitsansätzen, die eine klare Fokussierung auf die geschäftlichen Anforderungen ermöglichen.

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 Lösung zur Beschleunigung der Innovation in der digitalen Transformation

- **Integrale Geschäftskontinuität**, die durch die Integration von Sicherheit und Compliance in neue Prozesse von Anfang an erreicht wird.
- **Einblick** in Schatten-IT und versteckte Bedrohungen
- **Maximale Flexibilität** für die Bereitstellung in physischen und virtuellen Umgebungen überall dort, wo Transparenz und Kontrolle erforderlich sind
- **Automatisierung von Untersuchungs- und Reaktionsaufgaben**, 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

Funktionsweise

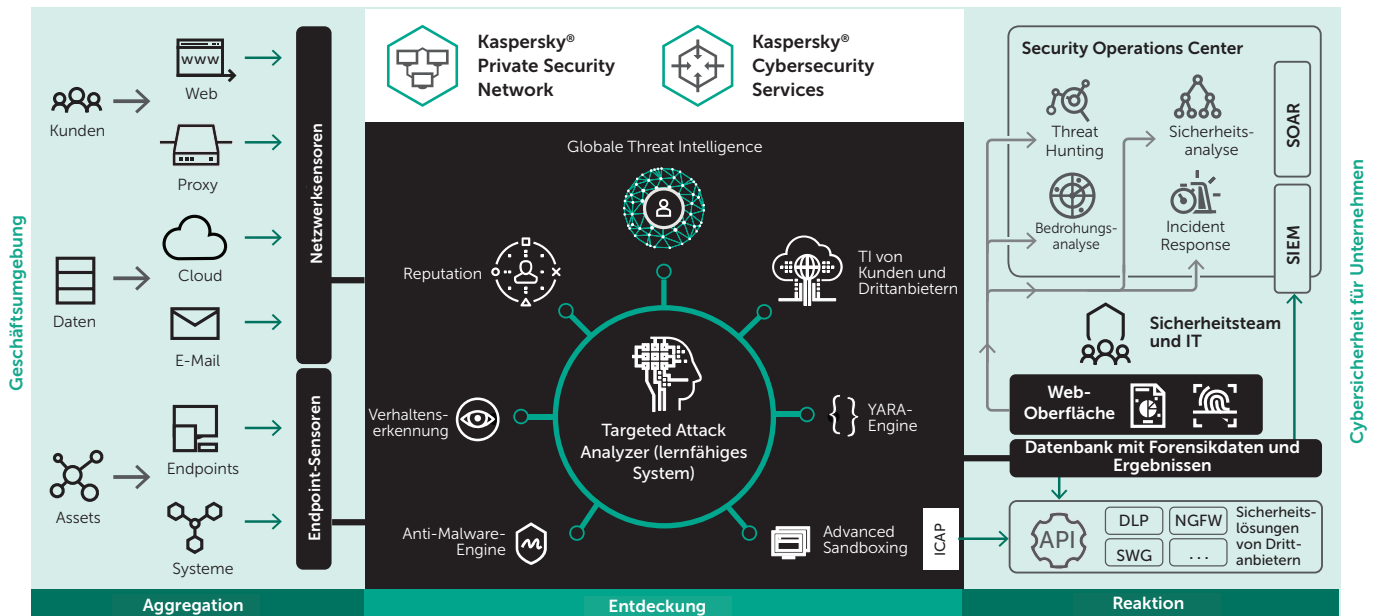


Unabhängige Tests haben ergeben, dass die Kaspersky Anti Targeted Attack Plattform Erkennungsraten von 100 % bei einer Fehlalarmrate von 0 % liefert, sodass keine Zeit mehr für die Reaktion auf Fehlalarme verloren geht. ICSA, 3. Quartal 2017

„Die Kaspersky Anti Targeted Attack Plattform bietet eine hoch entwickelte Bedrohungserkennung auf allen Ebenen eines gezielten Angriffs – von der Erstinfektion über die Befehls- und Steuerungskommunikation bis hin zu horizontaler Infiltrierung Datenexfiltration“ – eine von der Radicati Group 2017 durchgeführte Wettbewerbsanalyse des Advanced Persistent Threat-Schutzes (APT).

Automatisierte Aggregation essentieller Telemetrie und Daten über das gesamte Netzwerk hinweg

Die Plattform nutzt Netzwerk- und Endpoint-Daten, um die vollständige Transparenz verteilter Unternehmensnetzwerke zu gewährleisten und so frühzeitige Bedrohungserkennung und umfassende Reaktion zu ermöglichen. Objekte können über SPAN, ICAP, POP3S oder SMTP gesammelt werden. Verdächtige Objekte können auch aus benutzerdefinierten Konnektoren von Fremdsystemen extrahiert werden.



Integration in vorhandene Sicherheitslösungen

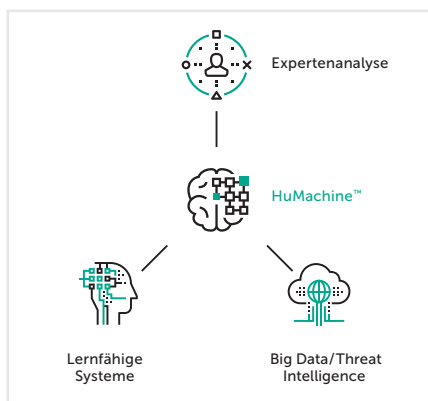
Blockierungsergebnisse und neue Kontexte können in vorhandene Sicherheitslösungen eingespeist werden. Blockierungsregeln können an Next-Generation-Firewalls (NGFWs) gesendet, Daten zu Sicherheitsverletzungen an Ihr SIEM-System (Security Information Event Management) gesendet und eindeutige URL- und Domänen-Insights den Secure Web Gateways (SWG) hinzugefügt werden.

Fortschrittliche, mehrdimensionale Erkennung

Die Kaspersky Anti Targeted Attack Plattform basiert auf führender Security Intelligence sowie fortschrittlichen lernfähigen Technologien und kombiniert Netzwerk- und Endpoint-Daten, Sandboxing und intelligente Analyse, um Vorfälle zu korrelieren, nach Gefährdungsindikatoren zu suchen und auch komplexeste gezielte Angriffe aufzudecken. Die Verknüpfung der verschiedenen Teile eines Vorfalls bietet einen umfassenden Überblick über die gesamte Angriffskette, erhöht das Vertrauen in zugeteilte Bedrohungsbewertungen und reduziert Fehlalarme auf null.

Automatisierte Prävention hoch entwickelter Bedrohungen und umfassende Reaktionsmöglichkeiten

Die Kaspersky Anti Targeted Attack Plattform kann über eine Intelligence-Sharing-Ebene vor Ort, das Kaspersky Private Security Network, automatisch Einschätzungen mit herkömmlichen Sicherheitslösungen von Kaspersky Lab austauschen. Durch diese enge Integration auf globaler, Netzwerk- und Endpoint-Ebene zwischen Kaspersky Anti Targeted Attack Plattform, Kaspersky Security for Mail Gateway, Kaspersky Endpoint Security, Kaspersky Security for Virtualization und Kaspersky Endpoint Detection and Response können bei Auftreten eines Vorfalls sofort fundierte Maßnahmen ergriffen werden.



Kaspersky Lab
 Enterprise Cybersecurity: www.kaspersky.de/enterprise
 Neues über Cyberbedrohungen: de.securelist.com
 IT-Sicherheitsnachrichten: <https://www.kaspersky.de/blog/b2b/>

#truecybersecurity
 #HuMachine

www.kaspersky.de

© 2018 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.