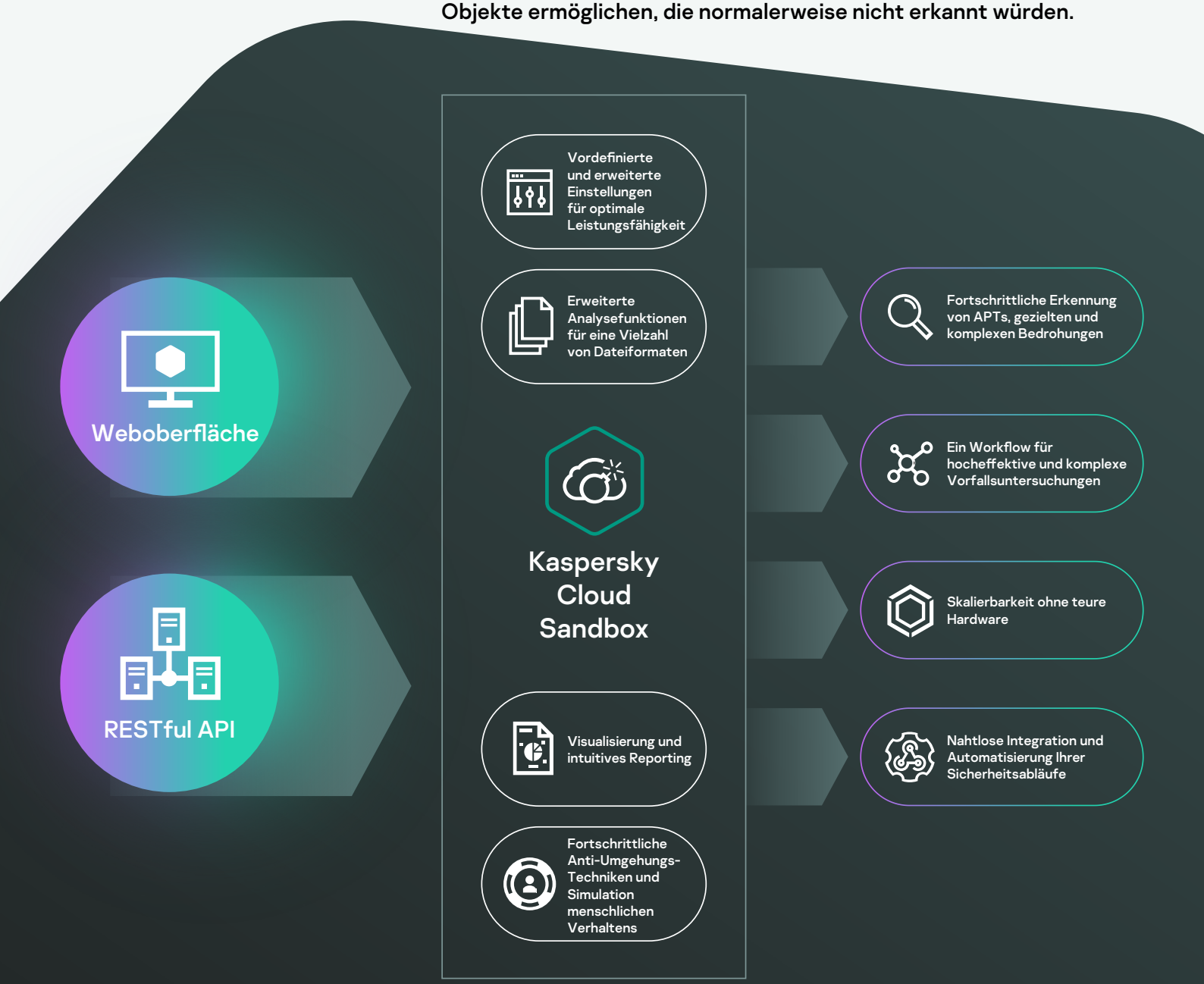
Kaspersky Cloud Sandbox

kaspersky BRING ON THE FUTURE

Kaspersky Cloud Sandbox

Herkömmliche Antiviren-Tools reichen heutzutage nicht mehr aus, um gezielte Angriffe zu verhindern. Virenschutz-Engines können nur bekannte Bedrohungen in verschiedenen Varianten abwehren. Versierte Bedrohungsakteure nutzen jedoch alle ihnen zur Verfügung stehenden Mittel, um eine automatische Erkennung zu umgehen. Verluste durch Zwischenfälle in der IT-Sicherheit steigen weiterhin exponentiell. Dadurch gewinnen Funktionen zur sofortigen Erkennung von Bedrohungen an Bedeutung, um eine schnelle Reaktionsfähigkeit aufzubauen und Bedrohungen entgegenzuwirken, bevor erhebliche Schäden entstehen können.

Intelligente Entscheidungen auf Basis von Dateiverhalten zu treffen und zugleich etwa den Prozess-Arbeitsspeicher, die Netzwerkaktivität usw. zu analysieren, ist der optimale Ansatz, um die neusten ausgeklügelten, gezielten und maßgeschneiderten Bedrohungen zu erfassen. Während es statistischen Daten häufig an Informationen zu kürzlich modifizierter Malware fehlt, bieten Sandboxing-Technologien leistungsstarke Tools, die die Untersuchung der Herkunft von Dateiproben, die Erfassung von IOCs auf Basis von Verhaltensanalysen sowie die Erkennung schädlicher Objekte ermöglichen, die normalerweise nicht erkannt würden.



Umfassendes Reporting

- Geladene und ausgeführte DLLs
- Externe Verbindungen mit Domainnamen und IP-Adressen
- Erstellte, geänderte und gelöschte Dateien
- Detaillierte Bedrohungsinformationen mit umsetzbarem Kontext für jeden aufgedeckten Gefährdungsindikator (IOC)
- Verarbeitete Speicherauszüge und Netzwerkverkehr-Dumps (PCAP)
- HTTP- und DNS-Anfragen und -Antworten
- Erstellte gemeinsame Erweiterungen (Mutexes)
- RESTful-API
- Geänderte und erstellte Registrierungsschlüssel
- Von der ausgeführten Datei erstellte Prozesse
- Screenshots
- **Und vieles mehr**

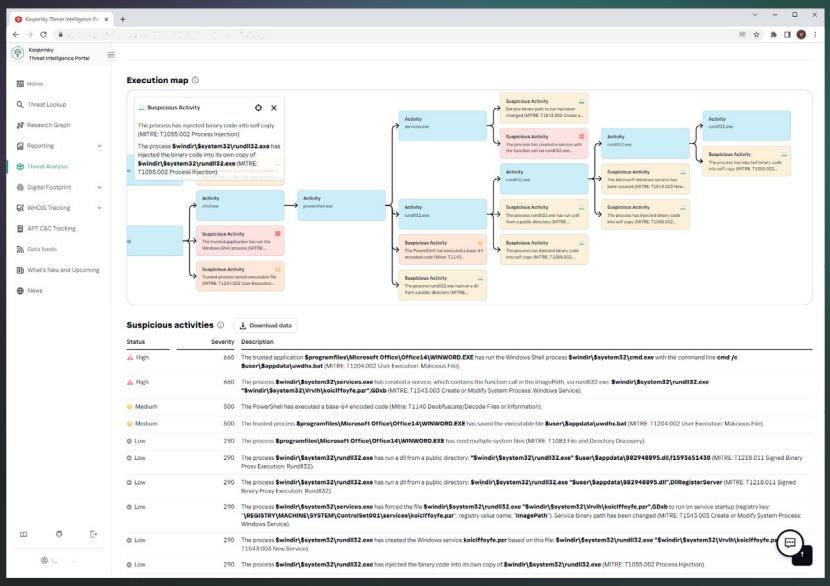
Proaktive Bedrohungserkennung und Risikominimierung

Malware verwendet eine Vielzahl von Methoden zur Verschleierung, damit sie nicht entdeckt wird. Wenn das System die erforderlichen Parameter nicht erfüllt, zerstört sich das schädliche Programm selbst, ohne Spuren zu hinterlassen. Damit der Schadcode ausgeführt werden kann, muss die Sandboxing-Umgebung daher in der Lage sein, ein normales Nutzerverhalten genau nachzuahmen.

Kaspersky Cloud Sandbox bietet einen hybriden Ansatz und kombiniert dabei Bedrohungsinformationen aus statistischen Daten im Petabyte-Bereich (dank des Kaspersky Security Network und anderen unternehmenseigenen Systemen), Verhaltensanalysen und besonders robuste Anti-Umgehungs-Techniken mit menschlichen Simulationstechnologien wie Auto-Clickern, Dokumentscrolling und Dummy-Prozessen.

Das Produkt wird bereits seit über 10 Jahren intern in unserem Sandbox Lab weiterentwickelt. Die Technologie vereint unser gesamtes Wissen hinsichtlich des Verhaltens von Malware, das wir uns in über 20 Jahren Bedrohungsforschung angeeignet haben. So können wir jeden Tag über 360.000 neue schädliche Objekte erkennen und unseren Kunden branchenführende Lösungen zur Verfügung stellen.

Cloud Sandbox ist Teil des Threat Intelligence Portals und ein wichtiger Bestandteil Ihres Threat Intelligence Workflows. Während Threat Lookup die neuesten detaillierten Bedrohungsdaten zu URLs, Domänen, IP-Adressen, Hash-Werten, Bedrohungsnamen, statistischen/Verhaltensdaten, WHOIS/DNS-Daten etc. abruft, können mit Cloud Sandbox diese Kenntnisse mit den von der analysierten Probe erzeugten IOCs verknüpft werden.



Jetzt können Sie hochwirksame und komplexe Vorfalluntersuchungen durchführen, um ein sofortiges Verständnis der Art der Bedrohung zu gewinnen und zusammenhängende Bedrohungsindikatoren aufzudecken.

Untersuchungen können äußerst ressourcenintensiv sein, insbesondere bei mehrstufigen Angriffen. Kaspersky Cloud Sandbox beschleunigt die Vorfallsreaktion sowie forensische Aktivitäten. So profitieren Sie von Skalierbarkeit für die automatische Verarbeitung von Dateien, ohne kostspielige Hardware erwerben oder sich Gedanken über Systemressourcen machen zu müssen.

www.kaspersky.de