kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Fortschrittliche Erkennungsfunktionen zum Schutz vor unbekannten Bedrohungen – ganz ohne interne IT-Sicherheitsexperten

Heutzutage können Cyberangriffe ganze Unternehmen lahmlegen und sich verheerend auf Finanzen und Ruf der betroffenen Organisation auswirken. Diebstahl von finanziellen Anlagen und Geschäftsgeheimnissen, sinkendes Kundenvertrauen aufgrund von Serviceausfällen sowie zahlreiche andere negative Folgen: Komplexe Bedrohungen stellen eine echte Gefahr für die Stabilität und Rentabilität Ihres Unternehmens dar. Um sich vor den immer raffinierteren Cyberangriffen zu schützen, reichen klassische Tools zum Schutz des Netzwerks (Firewalls, E-Mail-/Web-Gateways, Proxy-Server) sowie zum Schutz der Workstations und Server (Antivirenlösungen und Endpoint-Protection-Plattformen mit grundlegenden Funktionen) allein nicht mehr aus. Zukunftsgerichtete Unternehmen sollten deshalb dringend spezielle Tools für die Erkennung, Untersuchung und Abwehr komplexer Bedrohungen in Erwägung ziehen.

Die Kaspersky Sandbox eignet sich für:

- Unternehmen ohne spezielles Sicherheitsteam, in denen die IT-Abteilung für die IT-Security verantwortlich ist
- Kleine Unternehmen, die keine zusätzlichen IT-Sicherheitsmitarbeiter einstellen möchten
- Große Unternehmen mit geografisch stark verteilter Infrastruktur und ohne lokale IT-Sicherheitsexperten
- Unternehmen, die gewährleisten wollen, dass sich ihre Vollzeit-IT-Sicherheitsanalysten auf einen anderen Bereich konzentrieren können

Seit 20 Jahren entwickelt Kaspersky Sicherheitslösungen für Unternehmen – unabhängig von Größe, Branche und Reifegrad der IT-Sicherheit. Und dank unserer laufenden Forschung und Entwicklung und unserer Fortschritte im Bereich Threat Hunting, Bedrohungsuntersuchung und -abwehr steht Kaspersky im Kampf gegen Cyberkriminalität weiterhin an vorderster Front.

Das Produkt- und Serviceportfolio von Kaspersky zum Schutz vor komplexen Bedrohungen umfasst folgende Lösungen:

- Kaspersky Anti Targeted Attack, eine moderne Lösung zur Erkennung und Untersuchung komplexer Bedrohungen und zielgerichteter Angriffe auf Netzwerkebene
- Kaspersky Endpoint Detection and Response, eine Lösung zur Erkennung, Untersuchung und Abwehr komplexer Cyberbedrohungen, die auf Workstations und Server abzielen
- Kaspersky Threat Intelligence Portal, über das Sie Zugang zur Cloud Sandbox erhalten, einschließlich Analyseberichten zu Advanced Persistent Threats (APT) und anderer Services

Um diese Lösungen und Services jedoch effektiv nutzen zu können, benötigen Unternehmen eine voll ausgestattete IT-Sicherheitsabteilung mit der richtigen Erfahrung und Expertise. Die weltweite Knappheit an Spezialisten, die im Umgang mit komplexen Bedrohungen geschult sind, und die Kosten, die für ihre Anstellung anfallen, sind oft die Hauptgründe dafür, dass Unternehmen auf entsprechende Lösungen und Services verzichten.

Dank patentierter Technologie (Patent Nr. US 10339301B2) kann die Kaspersky Sandbox Unternehmen darin unterstützen, sich vor der steigenden Anzahl immer komplexer werdender Bedrohungen zu schützen, die bestehende Endpoint-Schutzlösungen umgehen können. Die Kaspersky Sandbox ergänzt die Funktionen von Kaspersky Endpoint Security for Business und ermöglicht es Unternehmen, den Schutz ihrer Workstations und Server vor zuvor unbekannter Malware, neuen Viren, neuer Ransomware, Zero-Day-Exploits und anderen Bedrohungen deutlich zu steigern – und dass, ohne hierfür spezielle IT-Sicherheitsanalysten einstellen zu müssen.

So sparen sich Unternehmen die Kosten für die Anwerbung und Einstellung solcher hoch spezialisierten Experten. Darüber hinaus können Unternehmen mit stark verteilten Netzwerken so ihre Kosten für den effektiven Schutz ihrer Remote-Standorte optimieren und gleichzeitig den manuellen Aufwand für ihre Sicherheitsmitarbeiter reduzieren.

Bereitstellungs- und Implementierungsoptionen:
Die Kaspersky Sandbox wird als ISO-Image bereitgestellt; CentOS 7 sowie alle erforderlichen Lösungskomponenten sind vorkonfiguriert. Die Lösung kann auf physischen oder virtuellen Servern (mit VMware ESXi) implementiert werden.

Integration:
- SIEM-Systeme können Informationen zu Erkennungen aus der Kaspersky Sandbox abrufen. Hierbei werden die entsprechenden Informationen im Rahmen der allgemeinen Ereignisübertragung über das Kaspersky Security Center gesendet.
- Die Kaspersky Sandbox enthält eine API, die die Integration in andere Lösungen ermöglicht. So können Dateien zur Überprüfung an die Kaspersky Sandbox gesendet und die Ergebnisse von Dateiprüfungen abgerufen werden.

Skalierbarkeit
Mit den bis zu 1000 geschützten Endpoints, die in der Basiskonfiguration unterstützt werden, lässt sich die Lösung einfach skalieren und bietet umfassenden Schutz für umfangreiche Infrastrukturen.

Clustering
Mehrere Server können einem Cluster hinzugefügt werden, um Kapazität und Verfügbarkeit zu steigern.

Lizenzierung
Kaspersky Sandbox wird als Software-Appliance lizenziert. Eine Lizenz umfasst Unterstützung für bis zu 1000 Benutzer von Kaspersky Endpoint Security for Business.

Funktionsweise

Kaspersky Sandbox nutzt die Best Practices unserer Experten für die Abwehr komplexer Bedrohungen und APTs und ist eng in Kaspersky Endpoint Security for Business integriert. Die Lösung wird über das Kaspersky Security Center verwaltet, unsere richtlinienbasierte Management-Konsole.

Der Kaspersky Endpoint Security for Business Agent fordert Daten zu verdächtigen Objekten aus dem gemeinsamen Speicher mit Ergebnissen von Dateiüberprüfungen ab, der sich auf dem Server von Kaspersky Sandbox befindet. Wenn das Objekt bereits gescannt wurde, erhält Kaspersky Endpoint Security for Business das Ergebnis dieses Scans und wendet ein oder mehrere Beseitigungsoptionen an:

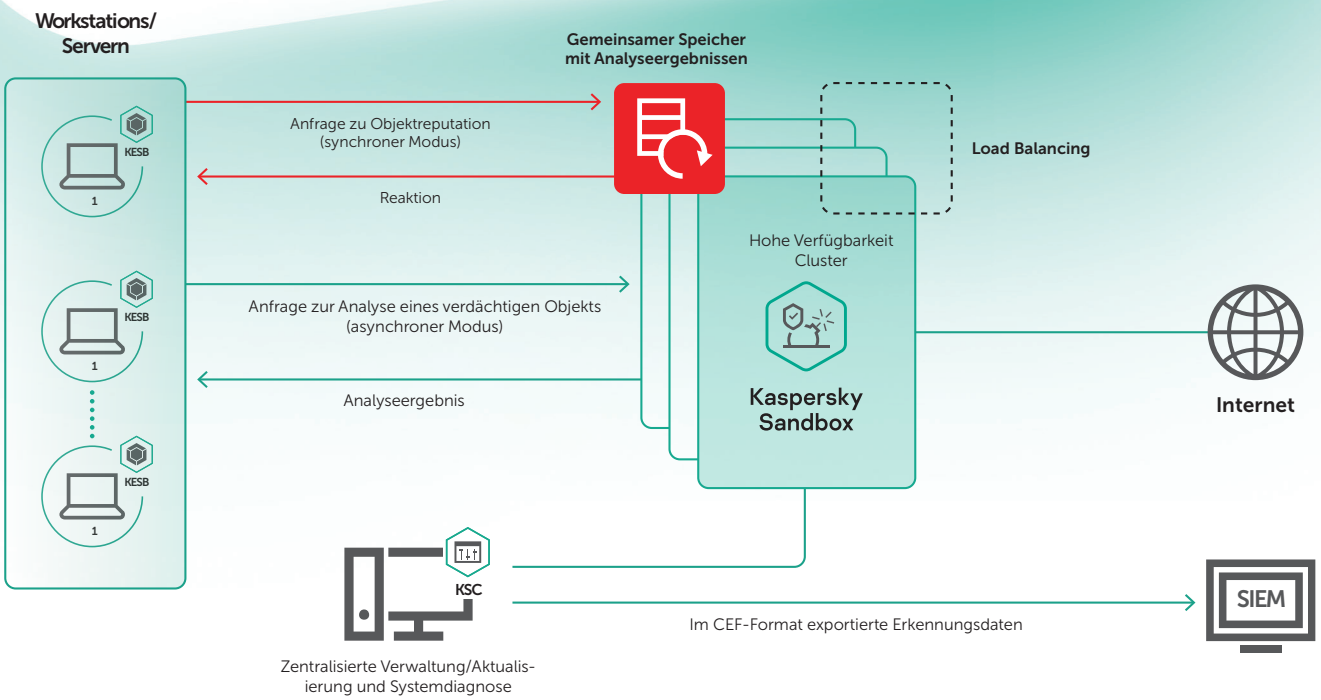
- Entfernen und in Quarantäne verschieben
- Benutzer benachrichtigen
- Scan kritischer Bereiche starten
- Erkanntes Objekt auf anderen Geräten im verwalteten Netzwerk suchen

Wenn das Ergebnis einer Objektprüfung nicht aus dem Speicher abgerufen werden kann, sendet der Kaspersky Endpoint Security for Business Agent die verdächtige Datei an Kaspersky Sandbox und wartet die Antwort der Lösung ab. Sandbox erhält die Anfrage, das Objekt zu scannen, und führt es daraufhin in einer Umgebung aus, die von der echten Infrastruktur isoliert ist.

Der Dateiscan wird auf virtuellen Maschinen ausgeführt, die mit Tools ausgestattet sind, über die sich eine übliche Arbeitsumgebung emulieren lässt (samt Betriebssystem und installierten Programmen). Um etwaige böswillige Absichten des Objekts zu erkennen, führt die Lösung eine Verhaltensanalyse durch und erfasst und analysiert Artefakte. Wenn das Objekt tatsächlich schädliche Aktionen ausführt, erkennt die Sandbox es als Malware. Während der Sandbox-Analyse wird dem Objekt das Ergebnis seiner Überprüfung angehängt.

Nach Abschluss des Emulationsprozesses, wird dieses Ergebnis in Echtzeit an den gemeinsamen Speicher gesendet, damit auch andere Hosts mit Kaspersky Endpoint Security for Business schnell Daten zum gescannten Objekt abrufen können, ohne es erneut analysieren zu müssen. Dieser Ansatz gewährleistet die schnelle Verarbeitung verdächtiger Objekte, reduziert die Belastung der Sandbox-Server und steigert Geschwindigkeit und Effizienz der Bedrohungsabwehr.

Kaspersky Sandbox ist eine effektive Ergänzung zu Kaspersky Endpoint Security for Business. Die Lösung blockiert automatisch fortschrittliche, unbekannte und komplexe Bedrohungen, ohne dass hierfür zusätzliche Ressourcen erforderlich werden. Dies spart Ihren IT-Sicherheitsanalysten viel Zeit, die sie in andere Aufgaben investieren können.



Cyber Threats News: https://de.securelist.com
IT Security News: 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 wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. 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.

Getestet.
Transparent.
Unabhängig.