kaspersky BRING ON THE FUTURE

Kaspersky Scan Engine

Kaspersky Scan Engine bietet leistungsstarke Bedrohungserkennung und lässt sich in nahezu jede Anwendung integrieren.

Die Kaspersky Scan Engine (KSE) bietet umfassenden Schutz für Webanwendungen, Proxyserver, Network Attached Storage und E-Mail-Gateways. Die Lösung ist einfach zu verwalten und kann über HTTP und ICAP als eigenständiger Dienst, skalierbarer Cluster oder Docker-Container bereitgestellt werden.
KSE verwendet die neuesten Erkennungsmethoden, um Malware wie Trojaner, Phishing-Bedrohungen, Würmer, Rootkits, Spyware und Adware zu erkennen und zu entfernen.

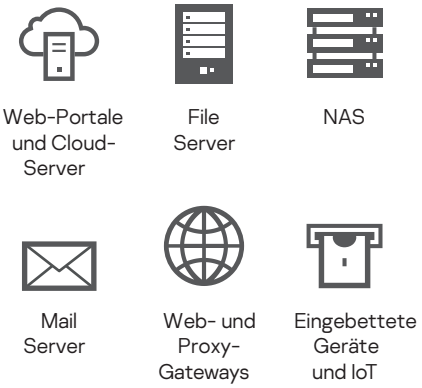
Hauptfunktionen

KSE kann in Windows- und Linux-Umgebungen in einem von zwei Modi betrieben werden:

- **REST-ähnlicher Dienst**, der HTTP-Anfragen von Client-Anwendungen empfängt, die in diesen Anfragen übergebenen Objekte scannt und HTTP-Antworten mit den Scan-Ergebnissen zurücksendet.
- **ICAP Server**, der HTTP-Verkehr scannt, der durch einen Proxy-Server/NAS/ Web Application Firewall/NGFW/jede andere Lösung läuft, die über das ICAP-Protokoll kommuniziert. Dieses Integrationsmodell ermöglicht es auch, die von den Nutzern angeforderten URLs zu scannen und Webseiten mit schädlichen Inhalten, Phishing oder Adware herauszufiltern.

Kaspersky Scan Engine ist auch als Linux-Docker-Container (im HTTP- und ICAP-Modus) verfügbar. Die Lösung kann als einzelner Container, in Docker Swarm, Kubernetes, AWS EKS und ähnlichen Cloud-Umgebungen eingesetzt werden. Kaspersky Scan Engine verfügt über eine webbasierte grafische Benutzeroberfläche, die eine einfache Konfiguration des Produktverhaltens sowie die Überwachung von Service-Ereignissen und Scan-Ergebnissen ermöglicht.

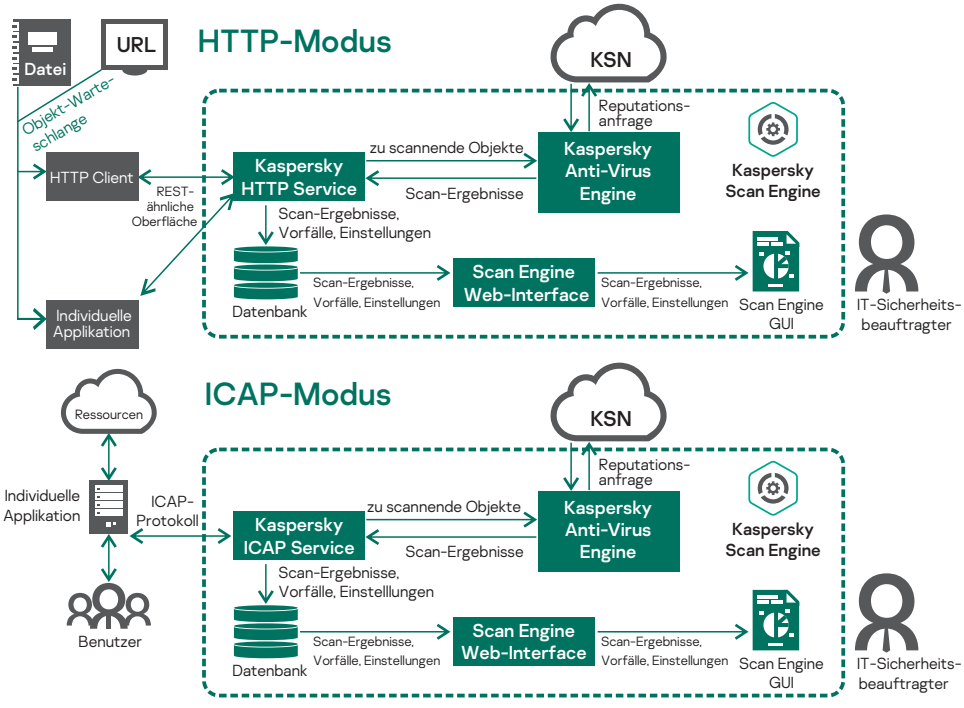
Integrationszenarien



Anwendungsszenarien

Dank einer funktionsreichen REST-ähnlichen API und offenem Quellcode lässt sich Kaspersky Scan Engine problemlos in nahezu jede Lösung in Ihrem Netzwerk integrieren.

- Schutz von Webportalen vor dem Hochladen von Malware
- Schutz von öffentlichen Cloud-Speichern (AWS S3 Bucket, Azure Blob Storage, etc.) vor dem Hochladen von schädlichen Inhalten
- Schutz von Private Cloud Storage (Nextcloud, ownCloud, mehr folgt demnächst) vor dem Hochladen von schädlichen Inhalten
- Schutz des Microsoft SharePoint Servers vor dem Hochladen schädlicher Inhalte
- Scannen von Container-Images auf Malware
- Scannen von Windows-/Linux-Dateispeichern auf Malware
- Anti-Malware-Plugin für Web-/E-Mail-Gateways von Drittanbietern (die Liste der abgeschlossenen Integrationen ist auf Anfrage erhältlich und wird laufend aktualisiert)
- Anti-Malware-Modul für das Dokumentenmanagementsystem des Unternehmens, die Softwareentwicklungspipeline und andere Systeme, die eine Überprüfung von Dateien auf Malware erfordern



Aktuelle Kaspersky-Produktauszeichnungen von unabhängigen Testlabors

Kaspersky

... und viele weitere:
www.kaspersky.de/top3!

Produkt-Features

- Die **preisgekrönte Anti-Malware-Technologie von Kaspersky** bietet hohe Malware-Erkennungsraten und kann sofort auf neue Bedrohungen reagieren.
- Filtern von bösartigen, Phishing- und Adware-URLs
- Erkennung mehrfach gepackter Objekte mit der größten Anzahl unterstützter Packer- und Archivformate
- Fortschrittliche heuristische Analyse und auf maschinellem Lernen basierende Erkennungstechnologien
- Desinfektion infizierter Dateien, Archive und verschlüsselter Objekte: Jede erkannte Bedrohung kann entweder vollständig entfernt werden oder, falls möglich, kann nur die schädliche Nutzlast entfernt werden, während der Rest der Datei sicher bleibt.
- Update-fähige Antiviren-Engine: Erkennungstechnologien und Verarbeitungslogik können durch regelmäßige Updates der Antiviren-Datenbank aktualisiert oder modifiziert werden.
- Basiert auf Big Data: Das Kaspersky Security Network liefert Informationen über die Reputation von Dateien und Webressourcen und ermöglicht so eine schnellere und genauere Erkennung.
- Die Lösung ist nicht nur leistungsstark, sondern auch einfach zu skalieren.
- Kann im Cluster-Modus betrieben werden: Mehrere Instanzen von KSE können im selben Netzwerk eingesetzt und über die Web-Benutzeroberfläche verwaltet werden.
- Die Kommunikation über das TLS-Protokoll wird unterstützt, wenn sie im REST-ähnlichen Service-Modus läuft.
- Eine zusätzliche Filterebene bietet die Komponente Format Recognizer. Mit dieser Komponente können Sie Dateien bestimmter Formate während des Scan-Vorgangs erkennen und überspringen. Dutzende von Formaten werden unterstützt, darunter ausführbare Dateien, Office-Dateien, Mediendateien und Archive.
- **Web-basierte grafische Benutzeroberfläche (GUI) für die Verwaltung und Überwachung:**
  - Hier können Sie die Einstellungen konfigurieren und die Anwendung verwalten.
  - Ermöglicht die Überwachung des Betriebsstatus der Anwendung, des Status der verwendeten Schlüsseldatei oder des Aktivierungscodes sowie der Anzahl der gescannten und erkannten Objekte.
  - Bietet Informationen über alle gescannten Objekte in einem Dashboard. Die Scan-Ergebnisse können im CSV-Format exportiert werden.
- **Reporting-Funktionen:**
  - Wichtige Anwendungsereignisse werden im CEF-Format an ein beliebiges Ziel gesendet, z. B. an Syslog oder eine SIEM-Lösung.
  - Alle Service-Ereignisse sind auf dem GUI-Dashboard sichtbar.
- **Wartungsfunktionen:**
  - Updates der Antiviren-Datenbanken erfolgen automatisch. Kaspersky Scan Engine stellt beschädigte Datenbanken automatisch wieder her.
  - Einfaches Erfassen von Produkt-Traces über die grafische Benutzeroberfläche
  - Flexibles Lizenzmodell, das eine optimale Preisgestaltung für Ihr Integrationsszenario und die Nutzung von Kaspersky Scan Engine gewährleistet.
- Fehlertolerante und robuste Architektur
- Der Quellcode für den HTTP-Dienst/Client und den ICAP-Dienst wird mitgeliefert und kann angepasst werden
- Vollständige Dokumentation und plattformübergreifende API-Unterstützung, ähnliche APIs für Linux/UNIX- und Windows-Versionen
- Option zur Minimierung des externen Datenverkehrs durch Einrichtung eines lokalen Spiegelservers für die Antiviren-Datenbank (zusätzliches Tool erforderlich)

Überzeugen Sie sich selbst – testen Sie jetzt unsere fortschrittliche Lösung unter www.kaspersky.de/partners/technology/contact.

Kaspersky Technology Alliances

Unsere Technologien können in Hardware- und Software-Sicherheitsprodukte und -dienstleistungen von Drittanbietern integriert werden. Alle Lösungen werden durch professionelle Technologiepartnerschaften unterstützt. Erfahren Sie mehr unter www.kaspersky.com/oem.

Cyber Threats News:
www.securelist.com
IT Security News:
www.kaspersky.de/blog/category/business/

www.kaspersky.de