



用于检测和删除恶意软件的综合性解决方案

卡巴斯基 扫描引擎

简介

卡巴斯基扫描引擎 (KSEn) 为您提供一流的威胁检测解决方案，可以与几乎任何应用程序相集成。

KSEn 可为 Web 门户和应用程序、代理服务器、网络附加存储和邮件网关提供全面保护。

通过 HTTP 和 ICAP, KSEn 可以轻松作为独立服务、可扩展群集或 Docker 容器进行管理和部署。KSEn 使用最新的检测方法进行恶意软件检测和删除，包括木马、网络钓鱼威胁、蠕虫、Rootkit、间谍软件和广告软件。

集成方案



Web 门户和云服务器



文件服务器



网络附加存储



邮件服务器



Web 和代理网关



应用程序商店和市场

关键功能

两种主要模式

类 REST 服务可从客户端应用程序接收 HTTP 请求，扫描在这些请求中传递的对象，并发送带有扫描结果的 HTTP 响应。

ICAP 服务器可扫描通过代理服务器 / NAS / Web 应用程序防火墙 / NGFW / 通过 ICAP 协议进行通信的任何其他解决方案的 HTTP 流量。该集成模式还允许扫描用户请求的 URL；然后含有恶意内容、网络钓鱼内容或广告软件内容的网页会被过滤掉。

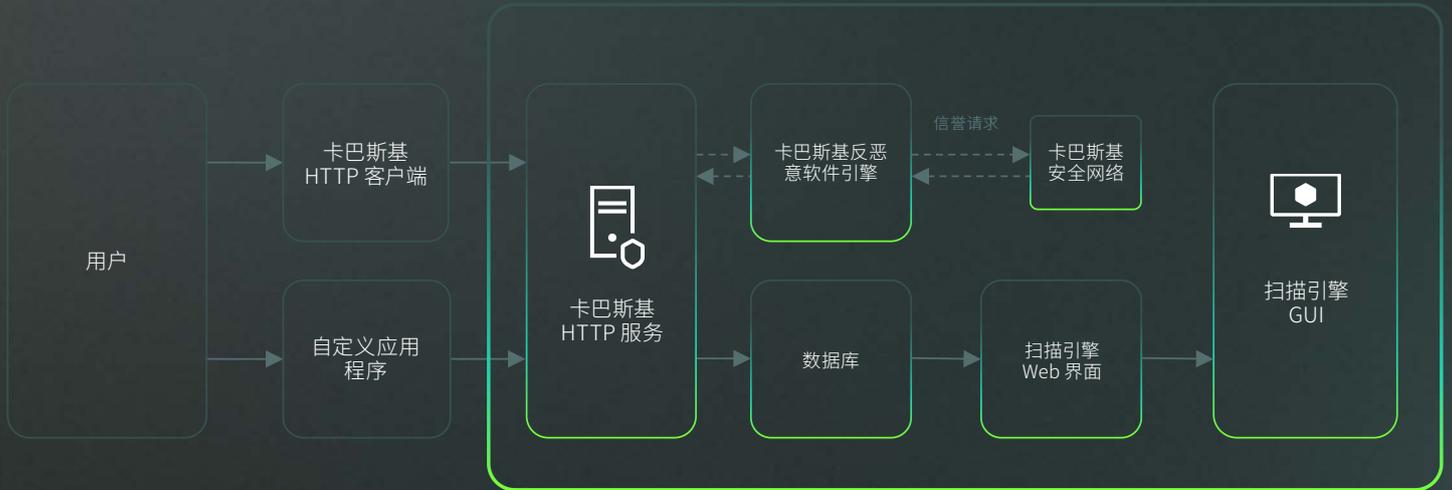
适用于 Linux 的 KSEn

KSEn 也可作为 Linux Docker 容器使用（在 HTTP 和 ICAP 模式中）。它可以作为单独容器部署到 Docker Swarm、Kubernetes、AWS EKS 和任何类似的云端环境中。

图形用户界面 (GUI)

KSEn 包括一个基于 Web 的图形用户界面，可让您轻松完成产品配置、查看其服务事件和扫描结果。

用例



与任何网络解决方案集成

得益于功能丰富的类 REST 的 API 和开源代码,您可以轻松将 KSEn 与网络中的几乎任何解决方案相集成。

保护 Web 门户,防止恶意软件上传。

为公共 (AWS S3 bucket 等) 和私有 (Nextcloud、ownCloud 等) 云存储提供防止恶意内容上传的保护。

为应用程序商店和软件市场提供防止恶意应用程序上传的保护。

扫描 Windows/Linux 文件存储中的恶意软件。

用于第三方 Web/邮件网关的反恶意软件插件。我们按照您的要求可以为您提供现有集成方案列表,该列表会不断更新。

反恶意软件模块可用于检测公司文档管理系统、软件开发管线是否存在恶意软件,亦可用于其他需要检查文件是否存在恶意软件的系统。

主要功能

屡获殊荣的反恶意软件技术

卡巴斯基屡获殊荣的反恶意软件技术提供了同类最佳的恶意软件检测率，并可以立即对新出现的威胁做出响应。

平台连接器

直接或通过连接器接入多个第三方平台，如 Amazon S3、Nextcloud、ownCloud 和 Kubernetes 等。

高级功能

高级启发式分析器和基于机器学习的检测技术。

格式识别器

格式识别器组件支持添加更多过滤层。在扫描过程中，您可以使用此组件来识别和跳过某些格式的文件。支持可执行文件、Office 文件、媒体文件和存档等多种格式。

过滤

过滤出恶意、网络钓鱼和广告软件的 URL。

文件杀毒

对受感染的文件、存档和编码对象进行杀毒处理。可以完全删除任何检测出的威胁，或者（如果可能的话）只删除恶意负载，保持剩余文件的安全。

大数据

由大数据提供技术支持：卡巴斯基安全网络提供有关文件和 Web 资源的信誉信息，从而确保检测更快、更准确。

TLS 支持

当在类 REST 服务模式中运行时，支持通过 TLS 协议进行通信。

检测

检测多次打包对象。支持各种打包程序和存档格式。

更新

可更新的反病毒引擎：通过定期更新反病毒数据库，可以升级或修改检测技术和处理逻辑。

可扩展性

KSEn 具备一流的性能，并且可以轻松扩展。

群集模式

KSEn 可以在群集模式中运行：多个 KSEn 实例可以部署在同一个网络中并通过 Web UI 进行管理。

卡斯基扫描引擎 2.1 的新功能

2022 年 6 月推出



安全性和合规性

多用户模式和基于角色的访问控制；操作审核；支持通过 API 令牌进行 HTTP 客户端身份验证；防止暴力破解密码，保护 Web UI 安全。



架构更改

KSEn 分成两个模块，可以单独发布：(1) AV 引擎 (KAV SDK) 和 (2) 主要产品功能 (KSEn 用作 KAV SDK 的包装程序)。



文件改进

SIEM 集成手册 (MicroFocus ArcSight、Splunk)；Oracle Solaris VScan、F5 Application Security Manager、GoAnywhere MFT、Dell Isilon OneFS 集成手册。



运营改善

Systemd 与相关服务 (启动/停止/状态/重启) 完全兼容



群集模式改进

自动删除群集中的空闲节点，并支持异构 (HTTP 和 ICAP) 群集。



系统日志记录更改

多个目标位置。过滤要发送的事件。

奖项

卡斯基最近获得的由独立测试实验室颁发的产品奖项



阅读更多



Kaspersky Scan Engine

提供 30 天免费试用版!

请点击下方链接，提交 KSEn 试用请求。

[阅读更多](#)

www.kaspersky.com.cn

© 2023 AO Kaspersky Lab。
注册商标和服务商标归其各自所有者所有。

#kaspersky
#bringonthefuture