Solução abrangente
para a detecção
e remoção de malware

Kaspersky Scan Engine

kaspersky BRING ON THE FUTURE

Introdução

O Kaspersky Scan Engine (KSEn) fornece a você a melhor solução de detecção de ameaças da categoria e pode ser integrado à quase todos aplicativos.

O Kaspersky Scan Engine (KSEn) fornece uma proteção completa para portais e aplicativos da Web, servidores proxy, Armazenamento Conectado à Rede (NAS) e gateways de email.

Ele é fácil de gerenciar e implementar através de HTTP e ICAP, podendo ser usado como um serviço autônomo, cluster escalável, ou container Docker. O KSEn utiliza os métodos mais recentes para a detecção e remoção de malware - incluindo Cavalos de Troia, ameaças de phishing, worms, rootkits, spyware e adware.

Cenários de Integração

Portais da Web e servidores na nuvem

Servidores de arquivos

Armazenamento Anexado à Rede (NAS)

Servidores de e-mail

Gateways da Web e Proxy

Lojas de Aplicativos e Marketplaces

Principais Funcionalidades

Dois modos principais

Serviço tipo REST que recebe solicitações HTTP de aplicativos clientes, verifica os objetos transmitidos nessas solicitações, e envia de volta respostas HTTP com os resultados da verificação.

Servidor ICAP que verifica tráfego HTTP transmitido através de um servidor proxy / NAS / Firewall de Aplicativos da Web / NGFW / e qualquer outra solução que se comunica pelo protocolo ICAP. Este modelo de integração também permite escanear as URLs solicitadas pelos usuários; páginas da web com conteúdo malicioso, phishing ou adware que são então filtradas.

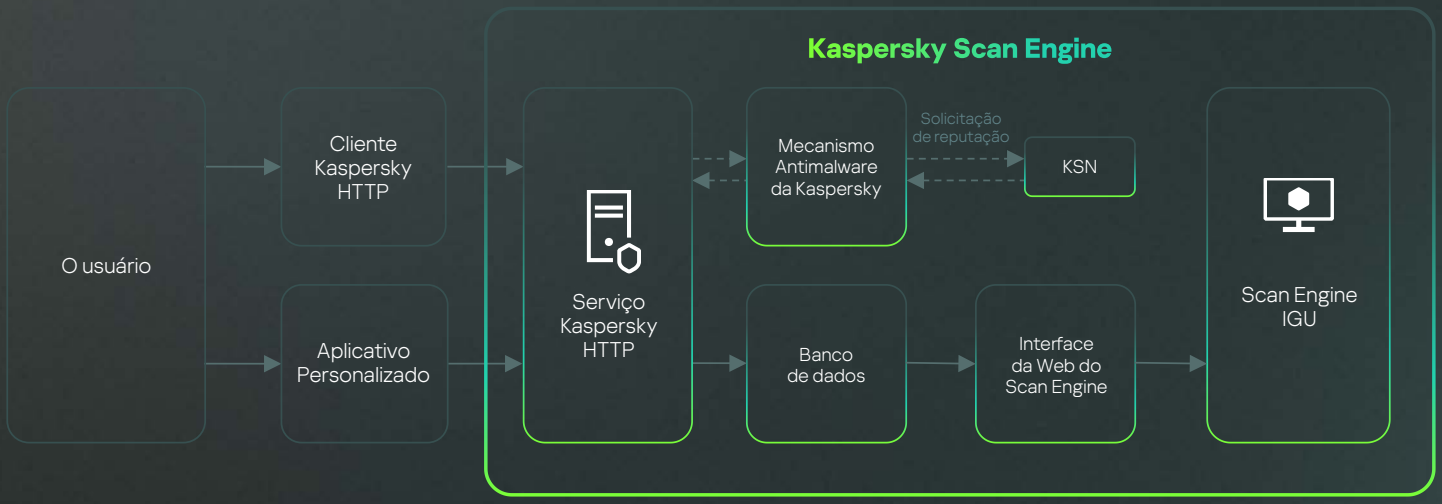
KSEn para Linux

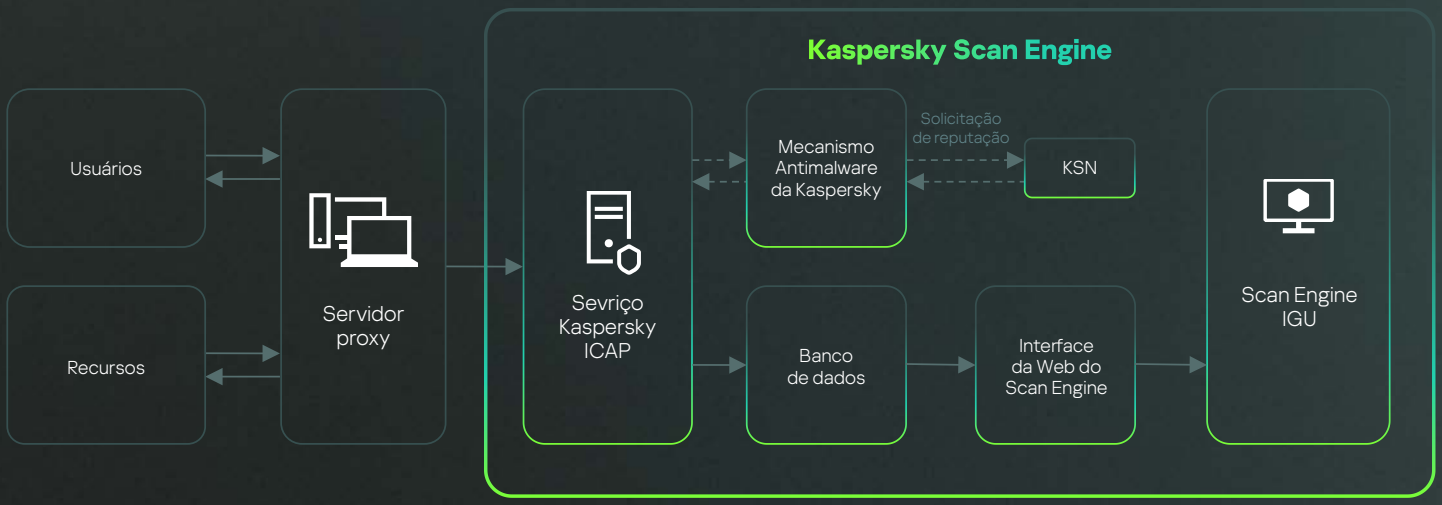
Também disponível como um Linux container Docker (no modo HTTP e ICAP). Ele pode ser implementado como um container individual, para Docker Swarm, Kubernetes, AWS EKS e quaisquer ambientes em nuvem semelhantes.

IGU

O Kaspersky Scan Engine inclui uma interface gráfica do usuário na Web que permite configurar facilmente o comportamento do produto, revisar seus eventos de serviço e resultados do escaneamento.

Casos de uso





Integração com qualquer solução de rede

Graças a uma API do tipo REST rica em recursos e código open source, você pode integrar facilmente o Kaspersky Scan Engine à quase qualquer solução na sua rede.

Proteção para os portais da Web contra upload de malware.

Proteção de armazenamento público em nuvem (AWS S3 bucket e etc.) e privado (Nextcloud, ownCloud, e mais por vir) contra upload de conteúdo malicioso.

Proteção de lojas de aplicativos e marketplaces de software contra o upload de aplicativos maliciosos.

Verificação de armazenamento de arquivo Windows/Linux em busca de malware.

Plugin Anti-malware para gateways da Web/Email de terceiros. A lista de integrações completadas está disponível sob solicitação e recebe atualizações constantemente.

Módulo antimalware para sistema de gerenciamento de documentos corporativos, pipeline de desenvolvimento de software e outros sistemas que exigem que arquivos sejam verificados em busca de malware.

Principais funcionalidades

Solução Premiada Antimalware

A premiada tecnologia antimalware da Kaspersky fornece as melhores taxas de detecção de malware da categoria e pode reagir instantaneamente a ameaças ao longo do caminho.

Filtragem

Filtragem de URLs maliciosas, de phishing e de adware.

Detecção

Detecção de objetos comprimidos (multi-packed). Maior número de empacotadores e formatos de arquivos suportados.

Conectores da plataforma

Suporte para múltiplas plataformas de terceiros, de modo nativo ou através de conectores, tais como Amazon S3, Nextcloud, ownCloud, Kubernetes, e etc.

Desinfecção de Arquivo

Desinfecção de arquivos, objetos codificados e "archives" contaminados. Qualquer ameaça detectada pode ser removida completamente ou, se possível, apenas a carga maliciosa, tornando o restante do arquivo seguro para uso.

Atualização

Mecanismo antivírus atualizável: tecnologias de detecção e lógica de processamento podem ser atualizadas ou modificadas por meio de atualizações regulares do banco de dados do antivírus.

Recursos Avançados

Ferramenta de análise investigativa avançada e tecnologias de detecção baseadas em aprendizado de máquina.

Big Data

Movido a Big Data: o Kaspersky Security Network fornece informações sobre a reputação dos arquivos e recursos da Web, garantindo uma detecção mais rápida e precisa.

Escalabilidade

O Kaspersky Scan Engine fornece o melhor desempenho e é facilmente escalável.

Reconhecedor de formato

É possível adicionar uma camada de filtragem adicional por meio do componente de reconhecimento de formatos. Você pode usar esse componente para reconhecer e ignorar arquivos de formatos específicos durante o processo de verificação. Dezenas de formatos são compatíveis, incluindo arquivos executáveis, compactados, do pacote Office e de mídia.

Suporte TLS

Suporte à comunicação via protocolo TLS durante a execução no modo de serviço tipo REST.

Modo cluster

O Kaspersky Scan Engine pode ser executado no modo de cluster - ou seja, várias instâncias do Kaspersky Scan Engine podem ser implementadas na mesma rede e administradas através da interface de usuário da Web.

Novos recursos do Kaspersky Scan Engine 2.1

Desde Junho de 2022

Segurança e Conformidade

Modo multi-user (múltiplos usuários) e controle de acesso com base na função do usuário, exame das operações, suporte de autenticação de clientes HTTP via tokens de API, proteção contra ataques de força bruta de senha na interface do usuário.

Alterações na arquitetura

O Scan Engine está dividido em dois módulos que podem ser liberados separadamente: (1) Mecanismo AV (KAV SDK), e (2) funcionalidade principal do produto (Scan Engine como um wrapper no KAV SDK).

Aprimoramento da documentação

Manuais para integração com SIEMs (MicroFocus ArcSight, Splunk), Manuais para integração com Oracle Solaris VScan, F5 Application Security Manager, GoAnywhere MFT, Dell Isilon OneFS.

Aprimoramento Operacional

Systemd com suporte completo para trabalhar com os serviços (iniciar/apara/status/reiniciar).

Aprimoramento do modo cluster

Os nós ociosos são removidos automaticamente do cluster e do suporte para clusters heterogêneos (HTTP e ICAP).

Mudanças no syslogging

Múltiplos destinos.
Filtro de eventos a serem enviados.

Prêmios

Prêmios recentes dos produtos da Kaspersky concedidos por laboratórios de testes independentes

Saiba mais

Kaspersky Scan Engine

Avaliação Gratuita por 30 dias, já disponível!
Clique no link abaixo para solicitar uma avaliação do KSEn.

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture