

Ameaças Invisíveis na ERA DA IA

**Blindagem Digital de Modelos LLM e Agentes no MCP
com Kaspersky Scan Engine**

Como proteger a integridade de dados e sistemas na
transição para automação inteligente em ambientes
corporativos e governamentais



Ivan Moulin

Solution Sales Manager, LATAM

ivan.moulin@kaspersky.com

kaspersky cybersecurity
true to business

O Desafio Crítico dos Uploads de Arquivos no B2B e Setor Público



Active Scanning: Securing data flow.

1. Uploads Não Inspeccionados na Web

Portais recebem:

- faturas
- relatórios financeiros
- currículos diariamente.
- uploads de documentos.

E muitos vem com Malwares ocultos infectando os storages

2. Buckets na Nuvem Como Hospedeiros

Repositórios de armazenamento viram repositórios passivos de arquivos infectados., e EDR não inspecionam o que chega diretamente na nuvem,

A Nova Fronteira de Riscos:

Vulnerabilidades em LLM e Agentes de IA



Vulnerabilidades Estruturais de LLM

Arquivos de modelo de IA podem esconder scripts e injeções de backdoors.

E estes pode ser executados diretamente no núcleo do servidor, resultando em **vazamento de dados** e **informações corporativas** sensíveis.

Agentes de IA Hostis

Kaspersky detectou mais de 92.000 ataques cibernéticos disfarçados de serviços de IA no primeiro semestre de 2026.

Kaspersky Scan Engine: A Muralha Ativa Lado Servidor (Server-Side)

O que é e como atua o KSE?

O KSE é integrado à sua infraestrutura de retaguarda (server-side). Atua como um intermediário de alta velocidade que inspeciona todos os tráfegos HTTP, URLs, chaves e uploads que passam pela empresa ou portal público.

HTTP

URLs

chaves

uploads

Principais Vantagens:



Integração nativa e limpa (out-of-the-box).



Desempenho extremo com arquitetura multithread.



Suporte a atualizações de vacina 100% offline (Air-Gapped) para garantir a segurança cibernética de alta confidencialidade e inteligência.



Interface gráfica baseada na web para monitoramento completo, auditoria e geração de relatórios de conformidade (LGPD).



Integração Sem Atrito: REST API vs ICAP Server



Caminho 1: REST API (HTTP) - Sob Demanda

Desenvolvido para desenvolvedores e arquitetos de software de plataformas SaaS, e-commerce, portais e apps customizados.

- Ideal para: Portais de envio de documentos B2B, esteiras DevSecOps, e uploads confidenciais de clientes.



Caminho 2: ICAP Server - Fluxo Contínuo

Projetado para infraestrutura de rede, infraestrutura de armazenamento e administradores de servidores proxy/gateways

- O KSE intercepta URLs, detecta e bloqueia ativamente links de phishing, malwares e adwares antes que cheguem à rede corporativa.
- Ideal para: Gateways de e-mail corporativo, proxies de rede, WAFs e armazenamento NAS central.

REST API (HTTP): **Análise Cirúrgica** sob Demanda para Aplicações

Como funciona o fluxo da REST API nos bastidores?

A REST API atua como um 'Guichê de Triagem de Encomendas' automatizado na sua aplicação:



Passo 1:

O Envio do Pacote

- O usuário final (cliente ou parceiro) faz o upload de um arquivo ou submete uma URL em seu portal web corporativo.



Passo 2:

O Escaneamento no KSE

- O seu portal envia uma requisição HTTP POST segura para o serviço KSE HTTP. O motor de antivírus descompacta, analisa profundamente e higieniza as ameaças.



Passo 3:

O Veredito Inteligente

- O KSE retorna instantaneamente uma resposta JSON contendo o resultado da verificação (Limpou/Infetado/Ameaça), permitindo que seu sistema decida se aceita, bloqueia ou encaminha o arquivo para quarentena.

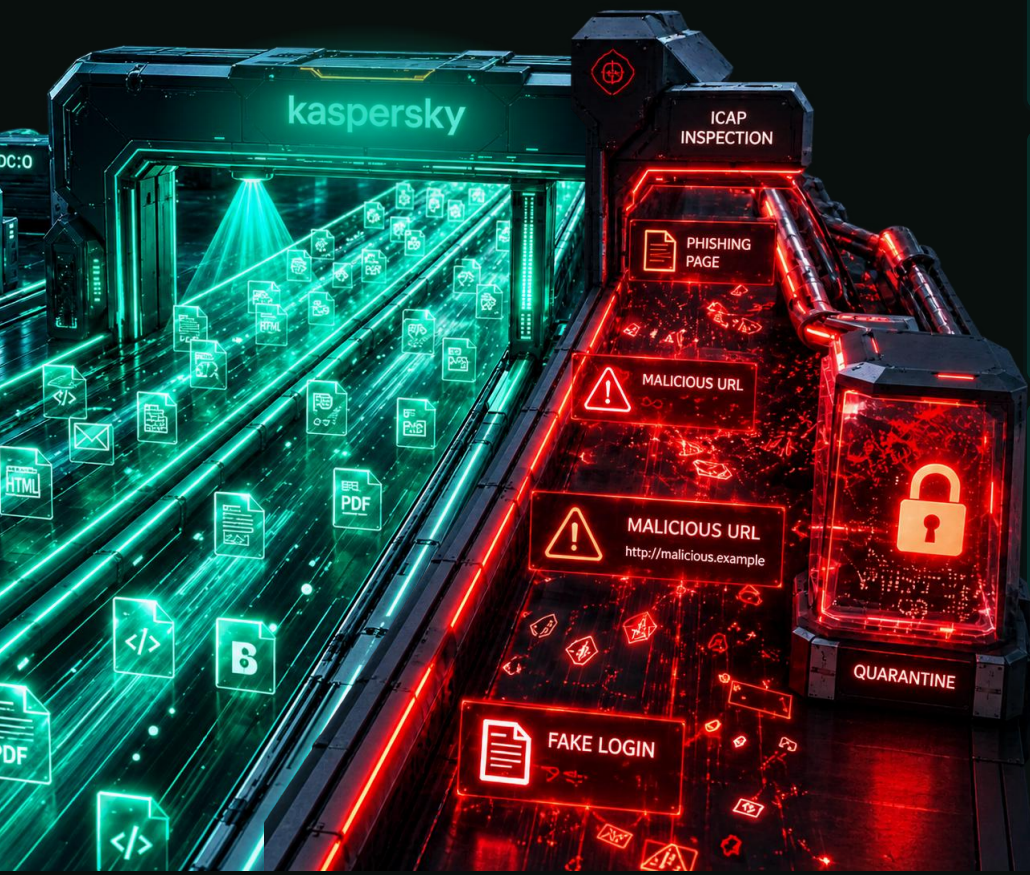


kaspersky

ICAP Server: Filtro de Alta Performance em Fluxo Contínuo de Rede

Como funciona a proteção ICAP transparente?

O ICAP funciona como uma cabine de 'Pedágio Inteligente' em uma rodovia de dados corporativa:



1

Automática Intercepção na Rede

- O tráfego de dados passa continuamente por servidores proxy (ex: Squid), Gateways de Web/Email, F5 ASM ou WAFs.

2

Análise Instantânea sem Bloqueio de Rede

- Os objetos e arquivos são desviados de forma assíncrona ou em tempo real para o KSE ICAP Server.
- O tráfego legítimo passa sem sofrer lentidão ou latência visível.

3

Deteção e Filtragem de Phishing na Raiz

- URLs acessadas por funcionários são verificadas ativamente.
- Páginas falsas de phishing e adwares são barradas imediatamente no gateway de entrada da rede corporativa, protegendo dados confidenciais de serem roubados.

Cinco Diferenciais Tecnológicos Imbatíveis do KSE



A. Desinfecção Cirúrgica de Arquivos

Em vez de deletar um documento da empresa, o KSE limpa cirurgicamente o código malicioso, mantendo a integridade física e utilidade do arquivo corporativo original.

B. Reconhecimento de Formato Real

Detecta tentativas maliciosas de contornar firewalls alterando a extensão do arquivo. O KSE analisa profundamente o cabeçalho binário real do arquivo para desmascarar falsificações.



C. Heurística Avançada de Machine Learning

Combina detecção por assinatura local, algoritmos de heurística preditiva de machine learning e a nuvem Kaspersky Security Network (KSN) para identificar em milissegundos ameaças sofisticadas e inéditas (Zero-Day) de forma local.

D. Controle de Acesso Baseado em Cargos

Perfis independentes de acesso na interface web gráfica do KSE para equipes de TI e segurança (TI, Admin de Redes e Auditores de Conformidade). Permite separar de forma robusta quem configura o sistema de quem audita eventos corporativos.



E. Soberania Digital com Atualização Offline

Oferece suporte total a atualizações de vacinas e assinaturas 100% offline (Air-Gapped) para redes governamentais, militares ou ambientes empresariais ou industriais isolados sem acesso direto à internet pública.



Escalabilidade Sem Limites:

Suporte nativo a Docker Swarm, Kubernetes, AWS EKS e ambientes de nuvem, permitindo escalonamento horizontal sob estresse de alta concorrência.



Implantação Ágil e Blindada via Contêineres Docker

A Metáfora da Caixa Indestrutível

Imagine a complexidade tradicional de instalar um software de segurança empresarial: dependências de bibliotecas, problemas de compatibilidade de sistema operacional Linux/Windows, conflito com outras aplicações...

Com o KSE fornecido como imagem Docker oficial da Kaspersky:



Caixa Blindada Pronta para Uso:

O KSE vem em um contêiner fechado, padronizado, seguro e contendo todo o SO Linux e modos HTTP/ICAP pré-configurados.



Ativação em Minutos:

Uma única linha de comando Docker ativa o serviço do motor de antivírus de forma imediata.



Isolamento Físico de Aplicação:

Se houver qualquer atualização ou mudança no portal do cliente, as dependências do KSE permanecem perfeitamente isoladas no contêiner, garantindo estabilidade sistêmica.



Escalabilidade sem Fronteiras: Orquestração e Alta Escala



Processamento Elástico de Milhões de Arquivos

O KSE foi arquitetado nativamente em cluster de alta disponibilidade para absorver e processar volumes maciços de requisições sem criar gargalos na infraestrutura de grandes corporações e governos:

✓ Docker Swarm & Kubernetes:

Orquestração nativa que escala instâncias do KSE de forma horizontal de acordo com os picos de acessos de cidadãos ou transações de clientes.

✓ Ambientes Multicloud e Nuvem Híbrida:

Integração automática e escalável em plataformas de contêineres na nuvem (como AWS EKS, Microsoft Azure AKS ou Google GKE).

✓ Balanceamento Inteligente de Recursos:

O cluster do KSE distribui as tarefas de varredura entre as instâncias ativas de forma automatizada e resiliente, removendo nós ociosos e garantindo performance estável.



Nós de Processamento do KSE Cluster

[Docker Container KSE 01 - Ativo]

- Status: Varrendo uploads da REST API (Portal B2B)
- Latência de varredura: 12ms

LATÊNCIA
12ms

[Docker Container KSE 02 - Ativo]

- Status: Monitorando ICAP Server (Storage AWS S3)
- Latência de varredura: 8ms

LATÊNCIA
8ms

[Docker Container KSE 03 - Ativo]

- Status: Auditando arquivos de Modelos LLM e IA
- Latência de varredura: 42ms

LATÊNCIA
42ms



- **Tolerância total a falhas:** se uma instância cair, as demais absorvem o tráfego de maneira 100% imperceptível para a operação do cliente.

Onde Aplicamos o KSE: Casos Reais no B2B e Setor Público



A. Bancos & Fintechs

- **Cenário:**
Clientes de bancos enviam comprovantes de residência, fotos e PDFs de demonstrativos financeiros via app mobile ou portal web.
- **O que o KSE protege:**
Bloqueia malwares direcionados e ransomwares que tentam penetrar o banco de dados interno da instituição antes de serem salvos.

B. SaaS, Cloud & Storages

- **Cenário:**
Proteção ativa de repositórios centrais de nuvens híbridas e buckets públicos de armazenamento.
- **O que o KSE protege:**
Varredura em tempo de upload de arquivos no AWS S3, Azure Blob, Nextcloud ou ownCloud, prevenindo que a empresa hospede involuntariamente arquivos maliciosos.



C. E-commerce & Portais

- **Cenário:**
Plataformas recebem notas fiscais, faturas de fornecedores e contratos PDF constantemente de milhares de parceiros.
- **O que o KSE protege:**
Varredura local cirúrgica que impede fraudes de faturamento baseadas em injeções de macros em faturas e anexos suspeitos de ERPs.

D. Portais Governamentais

- **Cenário:**
Secretarias de saúde, fazenda ou educação que coletam dados e processos eletrônicos de cidadãos.
- **O que o KSE protege:**
Garante a segurança nacional da infraestrutura pública e das informações confidenciais da população de ponta a ponta.



Como Iniciar a Proteção Hoje: Comece Sua PoC Sem Custo

Prova de Conceito (PoC) Simples de 30 Dias

A Kaspersky oferece **um período completo de avaliação** sem custos do Kaspersky Scan Engine para que você valide a facilidade de integração no ambiente de produção do seu cliente ou no seu próprio órgão público:

- ✓ Licença de Avaliação Completa de 30 Dias.
- ✓ Acesso imediato à Imagem Docker Oficial do KSE.
- ✓ Exemplos práticos de código aberto e SDKs em GitHub para integração REST API super ágil.
- ✓ Suporte técnico especializado do time de engenharia de segurança cibernética OEM da Kaspersky durante o período de validação.



Como Solicitar a Sua Licença de Teste

Siga um dos caminhos rápidos para habilitar o KSE em seu cliente:

1

Contato Comercial Direto na América Latina:

- Responsável: Ivan Moulin
- Cargo: Solution Sales Manager LATAM
- Email: ivan.moulin@kaspersky.com

2

Portal de Tecnologia Oficial da Kaspersky OEM:

- Acesse: www.kaspersky.com/partners/technology/contact

3

Documentação de Inteligência e Ameaças:

- Notícias de Segurança de TI: securelist.com
- Blog Corporativo Business: business.kaspersky.com

OBRIGADO!

OBRIGADO!

OBRIGADO!

kaspersky

