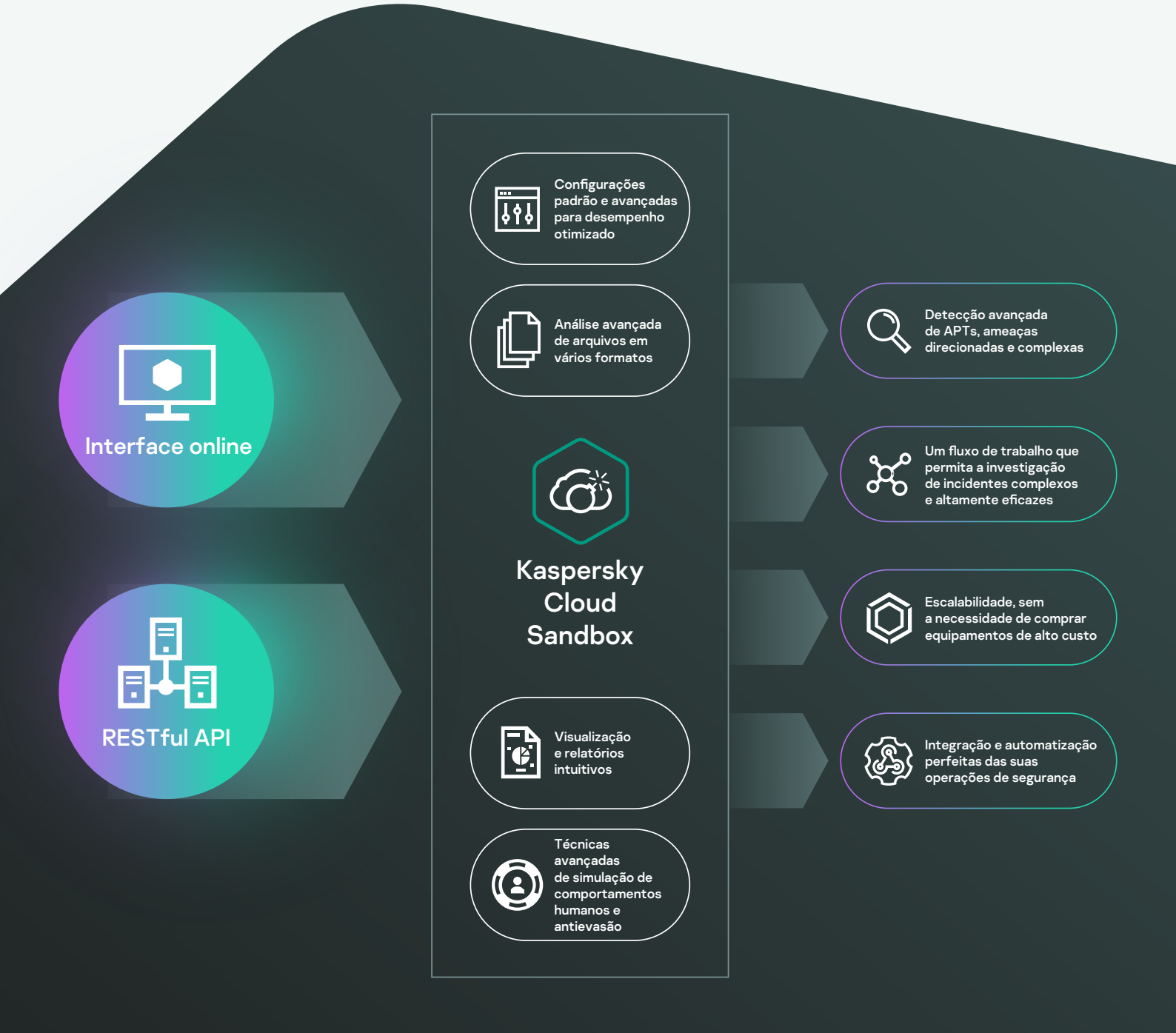
Kaspersky Cloud Sandbox

kaspersky PREPARADOS PARA O FUTURO

Kaspersky Cloud Sandbox

É impossível prevenir os ataques direcionados atuais apenas com ferramentas AV tradicionais. O mecanismo dos antivírus conseguem parar apenas as ameaças conhecidas e suas respetivas variações, ao passo que os agentes de ameaças sofisticados utilizam todos os meios à sua disposição para escapar à detecção automática. As perdas decorrentes de incidentes de segurança da informação continuam aumentando exponencialmente, realçando a importância crescente das capacidades de detecção de ameaças imediata para assegurar uma resposta rápida e combater ameaças antes que ocorram danos significativos.

Tomar uma decisão inteligente com base no comportamento de um arquivo, analisando simultaneamente a memória de processo, a atividade de rede, etc. é a abordagem ideal para compreender as sofisticadas ameaças mais recentes direcionadas e personalizadas. Os dados estatísticos podem ter falta de informação sobre malware modificado, mas as tecnologias de sandbox são ferramentas poderosas que permitem a investigação das origens da amostra de arquivo, a coleta de IOC com base em análise comportamental e a detecção de objetos maliciosos nunca vistos.



Relatórios abrangentes

- DLL carregados e executados
- Ligações externas com nomes de domínio e endereços IP
- Arquivos criados, modificados e eliminados
- Inteligência de ameaças detalhada com contexto acionável para cada indicador de comprometimento (IOC) revelado
- Dumps de memória de processo e dumps de tráfego de rede (PCAP)
- Pedidos e respostas de HTTP e DNS
- Extensões mútuas criadas (mutexes)
- API RESTful
- Chaves de registo modificadas e criadas
- Processos criados pelo arquivo executado
- Capturas de tela
- **e muito mais**

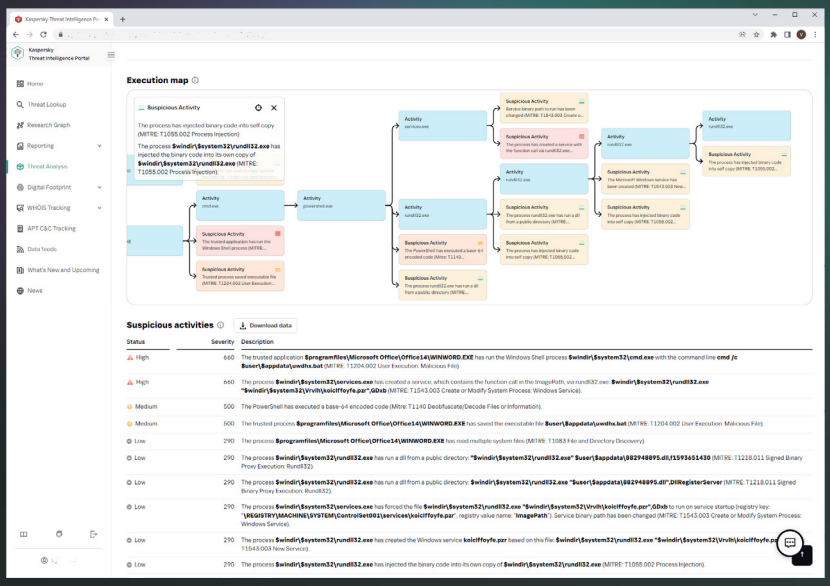
Detecção e mitigação proativa de ameaças

O malware usa diversos métodos para impedir que sua execução seja detectada. Se o sistema não cumprir os parâmetros necessários, o programa malicioso irá muito provavelmente autodestruir-se, sem deixar vestígios. Para o código malicioso ser executado, o ambiente de sandbox tem que conseguir imitar com exatidão o comportamento normal de um usuário final.

O Kaspersky Cloud Sandbox oferece uma abordagem híbrida, que conjuga inteligência de ameaças recolhida a partir de petabytes de dados estatísticos (graças ao Kaspersky Security Network e outros sistemas proprietários), análise comportamental e técnicas antievasão sólidas, com tecnologias que simulam humanos, como clicker automático, percorrer documentos e processos fictícios.

Este produto foi desenvolvido em nosso laboratório de sandbox interno, evoluindo por mais de uma década. A tecnologia incorpora todo nosso conhecimento sobre o comportamento de malware adquirido ao longo de 20 anos de pesquisa contínua de ameaças. Isso nos permite detectar mais de 360 mil novos objetos maliciosos todos os dias para fornecer aos nossos clientes soluções de segurança líderes do setor.

Como parte do nosso Threat Intelligence Portal, o Cloud Sandbox é um importante componente do nosso fluxo de trabalho de inteligência de ameaças. Enquanto a pesquisa de ameaças obtém a mais recente inteligência de ameaças detalhada sobre URLs, domínios, endereços IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS, etc., o Cloud Sandbox vincula esse conhecimento com os IOCs gerados pela amostra analisada.



Agora, você pode executar investigações de incidentes altamente eficazes e complexas, obtendo um entendimento imediato da natureza da ameaça, depois fazer associações à medida que pesquisa para revelar os indicadores de ameaça inter-relacionados.

A inspeção pode exigir muitos recursos, especialmente no que se refere a ataques com várias etapas. O Kaspersky Cloud Research Sandbox aumenta sua resposta a incidentes e atividades forenses, fornecendo a você a escalabilidade para processar arquivos automaticamente sem ter que comprar aparelhos caros ou se preocupar com recursos do sistema.

www.kaspersky.com.br