kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Funcionalidades avançadas de detecção para proteger de ameaças desconhecidas e ambíguas sem a necessidade de contratar profissionais de segurança de TI

Os ataques cibernéticos atuais são capazes de paralisar empresas e devastar sua integridade financeira e sua reputação. Roubo de recursos financeiros e segredos comerciais, perda da confiança do cliente por causa de serviços inativos e inúmeros outros efeitos negativos de ameaças complexas têm um impacto enorme sobre a estabilidade e a prosperidade dos negócios. Para evitar os ataques cibernéticos em rápida evolução, as ferramentas tradicionais criadas para proteger o perímetro da rede (firewalls, gateways de e-mail/da Web, servidores proxy) e também estações de trabalho e servidores (proteção antivírus e soluções do tipo plataforma de proteção de endpoints com funcionalidade básica) isoladas não são mais suficientes. Por isso, as empresas com pensamento inovador precisam considerar seriamente ferramentas especializadas para detectar, investigar e responder a incidentes complexos.

A solução Kaspersky Sandbox é adequada para:

- Empresas que não têm uma equipe de segurança dedicada, onde a responsabilidade pela segurança de TI é do departamento de TI.
- Pequenas empresas que não querem agregar recursos adicionais de segurança de TI.
- Grandes organizações com uma infraestrutura geograficamente distribuída que não contam com especialistas em segurança de TI no local.
- Empresas que precisam garantir que seus analistas de segurança de TI em tempo integral foquem tarefas críticas.

Há mais de 20 anos, a Kaspersky desenvolve ferramentas de proteção para empresas de todos os tamanhos, setores e níveis de maturidade da segurança de TI. Com as pesquisas e o desenvolvimento contínuos, além dos avanços que fizemos na busca, investigação e resposta a ameaças, a Kaspersky continua na vanguarda do combate ao crime cibernético.

O portfólio de produtos e serviços da Kaspersky para deter ameaças complexas inclui:

- Kaspersky Anti Targeted Attack, uma solução de ponta para detectar e investigar ameaças complexas e ataques direcionados no nível de rede.
- Kaspersky Endpoint Detection and Response, uma solução para detectar, investigar e responder a ameaças cibernéticas complexas em estações de trabalho e servidores.
- Kaspersky Threat Intelligence Portal, que oferece acesso à Cloud Sandbox, com relatórios analíticos sobre ameaças de APTs e outros serviços

No entanto, para utilizar essas soluções e serviços com eficiência, as empresas precisam ter um departamento de segurança de TI completo com experiência e conhecimento apropriados. A escassez global de especialistas treinados para lidar com ameaças complexas e o custo de contratá-los muitas vezes é o principal fator que impede as empresas de adquirir esse tipo de soluções e serviços.

Baseada em uma tecnologia patenteada (patente nº US 10339301B2), a Kaspersky Sandbox ajuda as organizações a combater as ameaças modernas, que crescem em número e complexidade, capazes de burlar a proteção de endpoints existente. Complementando as funcionalidades do Kaspersky Endpoint Security for Business, a Kaspersky Sandbox permite que as organizações aumentem significativamente o nível de proteção de suas estações de trabalho e servidores contra malware previamente desconhecido, novos vírus e ransomware, exploits de "dia zero" e outras ameaças sem a necessidade de analistas de segurança de informações altamente especializados.

Isso poupa às pequenas empresas as despesas de recrutamento e contratação desses profissionais tão valiosos. E, no caso de grandes corporações com redes distribuídas, é possível otimizar custos para proteger seus escritórios remotos eficientemente e, ao mesmo tempo, aliviar a carga de trabalho manual dos analistas de segurança.

Opções de fornecimento e implementação
A Kaspersky Sandbox é fornecida como uma imagem ISO que inclui o CentOS 7 pré-configurado e todos os componentes necessários da solução. Ela pode ser implementada em um servidor físico ou em servidores virtuais baseados no VMware ESXi.

Integração
- Sistemas de SIEM podem receber informações sobre as detecções feitas pela Kaspersky Sandbox. Essas informações são enviadas via Kaspersky Security Center, no fluxo de eventos gerais.
- Uma API é implementada na Kaspersky Sandbox para integração com outras soluções, permitindo enviar arquivos para a Kaspersky Sandbox para verificação e solicitar reputações de arquivos.

Escalabilidade
A configuração básica dá suporte a até 1.000 endpoints protegidos, o que facilita o dimensionamento da solução, que oferece proteção contínua para grandes infraestruturas.

Clusterização
É possível clusterizar vários servidores para expandir sua capacidade e disponibilidade.

Licenciamento
A Kaspersky Sandbox é licenciada como um dispositivo de software. Uma licença inclui suporte para até 1.000 usuários do Kaspersky Endpoint Security for Business.

Como funciona
A Kaspersky Sandbox aproveita as práticas recomendadas de nossos especialistas para combater ameaças complexas e ataques em nível de APT, e está fortemente integrada ao Kaspersky Endpoint Security for Business. Ela é gerenciada pelo Kaspersky Security Center, nosso console de gerenciamento unificado baseado em políticas.

O agente do Kaspersky Endpoint Security for Business solicita dados sobre um objeto suspeito do cache operacional compartilhado de vereditos, localizado no servidor da Kaspersky Sandbox. Se o objeto já foi verificado, o Kaspersky Endpoint Security for Business recebe o veredito e aplica uma ou mais opções de neutralização:

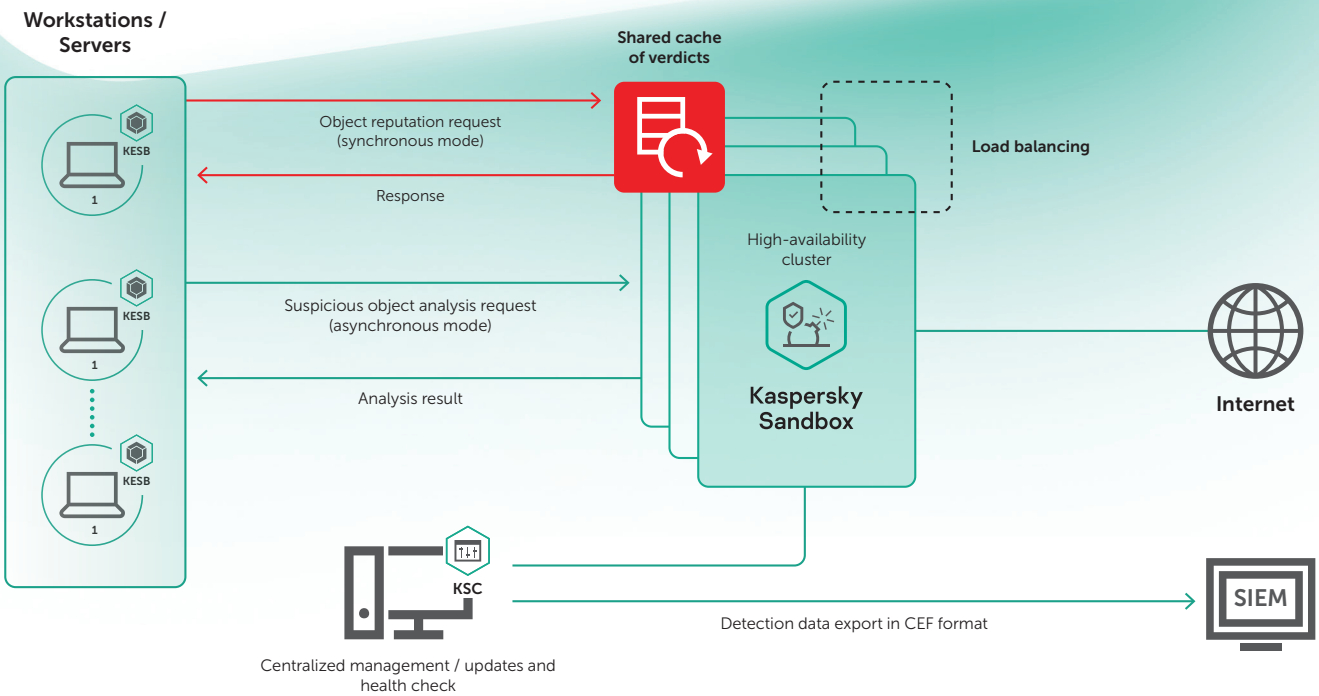
- Remover e colocar em quarentena
- Notificar o usuário
- Iniciar uma verificação de áreas críticas
- Pesquisar o objeto detectado em outras máquinas da rede gerenciada.

Se não for possível obter o veredito sobre a reputação de um objeto do cache, o agente do Kaspersky Endpoint Security for Business enviará o arquivo suspeito para a Sandbox e aguardará a resposta. A Sandbox recebe a solicitação para verificar o objeto, e o objeto de teste é executado em um ambiente isolado da infraestrutura real.

A verificação do arquivo é executada em máquinas virtuais equipadas com ferramentas que simulam um ambiente de trabalho típico (sistemas operacionais/aplicativos instalados). Para determinar a intenção maliciosa de um objeto, é realizada a análise de comportamento, artefatos são coletados e analisados e, se o objeto executar ações maliciosas, a Sandbox o reconhecerá como malware. Durante a análise da Sandbox, um veredito é atribuído ao objeto.

Quando o processo de simulação do objeto é concluído, o veredito resultante é enviado em tempo real para o cache operacional compartilhado de vereditos, permitindo que outros hosts que têm o Kaspersky Endpoint Security for Business instalado obtenham rapidamente dados sobre a reputação do objeto verificado sem precisar analisar o mesmo arquivo novamente. Essa abordagem garante o rápido processamento de objetos suspeitos, reduz a carga sobre os servidores da Kaspersky Sandbox e melhora a velocidade e a eficiência da resposta a ameaças.

A **Kaspersky Sandbox** é um complemento essencial do Kaspersky Endpoint Security for Business. Ela bloqueia automaticamente ameaças avançadas, desconhecidas e complexas sem a necessidade de recursos adicionais, e libera os analistas de segurança de TI para outras tarefas.



Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/
Segurança de TI para PMEs: kaspersky.com/business
Segurança de TI para grandes empresas: kaspersky.com/enterprise

www.kaspersky.com

Nós somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de construir um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos possam aproveitar as infinitas oportunidades que ela proporciona. Garanta a cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com/transparency

Proven. Transparent. Independent.