E-BOOK

Guia de compras de prevenção contra ameaças

Encontre a melhor solução de proteção contra ameaças baseada em IA para impedir ataques baseados em arquivos.

Índice

Reflexão sobre segurança para o cenário de ameaças atual

A segurança somente do perímetro é muito arriscada para o atual mundo digital

A adoção do trabalho híbrido e dos aplicativos hospedados na nuvem mudou a forma de acessar os recursos das empresas. Os funcionários estão usando dispositivos não gerenciados em redes não seguras, como redes Wi-Fi públicas, para se manterem produtivos remotamente ou em trânsito, efetivamente transformando a internet na nova rede corporativa. Essa expansão de pontos de acesso torna a antiga abordagem de segurança de castelo e fosso inadequada para proteger seus usuários, aplicativos e dados. Depender somente de defesas de perímetro apresenta riscos, pois os controles centrados na rede são ignorados para acesso direto à internet, muitas vezes priorizando a facilidade de uso em detrimento da segurança.

A nova geração de ataques cibernéticos burla os controles de segurança legados com facilidade. É hora de aproximar a segurança dos usuários, migrando da proteção de perímetro para a proteção de usuários, cargas de trabalho e OT/IoT.

Os adversários estão se aproveitando da corrida para a nuvem

Presas entre a cruz e a espada, as equipes de segurança fizeram o possível para adaptar os controles de segurança legados ao atual mundo da mobilidade e da nuvem. Esse descompasso se demonstrou vantajoso para os adversários. Com as dificuldades das organizações em proteger múltiplas bordas de rede, portas acabam sendo deixadas vulneráveis a malwares, como mostram as descobertas feitas pela equipe ThreatLabz, da Zscaler:

- **86%** das ameaças são distribuídas por canais criptografados, com o malware sendo responsável por 78% dos ataques criptografados.[1]
- Os ataques de ransomware aumentaram **40%** em relação ao ano anterior.[2]
- As cargas observadas na Zscaler Sandbox aumentaram **58%**.[2]

Essa rápida evolução das ameaças digitais, agravada pela expansão da superfície de ataque na nuvem, apenas enfatiza a necessidade de as equipes de segurança reavaliarem suas estratégias e reforçarem as defesas contra os riscos cibernéticos modernos.

1. Relatório sobre o estado dos ataques criptografados de 2023 da Zscaler ThreatLabz
2. Relatório de ransomware de 2023 da Zscaler ThreatLabz

É necessária uma evolução na proteção contra malwares de dia zero

Os adversários têm duas vantagens principais: **velocidade** e **proliferação**. Os desenvolvedores de malware estão criando ameaças mais rápido do que os defensores podem defini-las, aproveitando a inteligência artificial (IA) para criar variantes capazes de escapar de medidas de segurança convencionais e métodos de detecção.

O phishing com anexos ou links maliciosos continua sendo um dos mecanismos de distribuição mais comuns atualmente. O uso generalizado de tráfego criptografado complica ainda mais as estratégias de defesa. As ameaças modernas geralmente se escondem no tráfego criptografado, ressaltando a importância de inspecionar todo o tráfego dentro e fora da web; ou você pode, sem saber, permitir que malware entre na sua rede.

Como um recurso crítico da pilha de segurança, as sandboxes são uma medida preventiva contra arquivos e execuções de códigos maliciosos.

Elas foram criadas para serem uma defesa eficaz contra ataques baseados em arquivos desconhecidos que visam escapar do EDR e de outras verificações de malware conhecido. Infelizmente, muitas sandboxes são implantadas fora de banda, dependendo de amostras de malware encaminhadas a elas por NGFWs, produtos de segurança na nuvem ou agentes de terminais.

Isso geralmente significa que a detecção ocorre depois que o malware é baixado no dispositivo do usuário, permitindo infecções por malware ou ransomware de paciente zero, e certamente não respeitando os conceitos de zero trust. Além disso, muitas sandboxes não utilizam análises de IA/ML em grande escala para detectar e colocar automaticamente em quarentena ameaças desconhecidas e arquivos suspeitos, um fator chave na entrega de defesa em linha de paciente zero sem interromper a produtividade.

Por si só, antivírus baseados em assinatura e sistemas de prevenção contra intrusões (IPS) não conseguem evitar as ameaças de dia zero e polimórficas.

Requisitos de sandbox na nuvem

Até agora, os adversários levaram vantagem ao explorar a alternância de arquiteturas no ambiente de nuvem.

Escolher a sandbox na nuvem correta é essencial para evitar infecções de paciente zero e bloquear o acesso de ameaças persistentes avançadas à sua rede.

A próxima seção destina-se a ajudar você a entender os requisitos específicos que devem ser considerados ao escolher uma sandbox na nuvem.

Descriptografia e inspeção em larga escala

A criptografia se tornou uma tendência de segurança promissora, conferindo proteção e segurança às comunicações privadas e informações sigilosas. Infelizmente, os criminosos cibernéticos estão se aproveitando do tráfego criptografado para ocultar cargas maliciosas.

Descriptografar e inspecionar o tráfego é um processo que exige muita computação e pode transformar dispositivos de sandbox de alto desempenho em dispositivos lentos, interrompendo os negócios com uma latência inaceitável.

Ao avaliar uma solução de sandbox moderna, é importante identificar fornecedores que possam oferecer descriptografia e inspeção integradas ilimitadas e sem latência.

As ameaças por HTTPS cresceram 24,3% ano a ano, representando 30 bilhões de ataques criptografados em 2023.[3]

Lista de verificação de compra:

- ☐ Não requer instalação de hardware ou máquina virtual (VM) adicional para descriptografar o tráfego SSL
- ☐ Inspeciona e analisa os seguintes tipos de arquivo sem latência ou limites de capacidade:

EXE	DOC(X)	TAR
DLL	XLS(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	arquivos de script em arquivos ZIP
SWF	BZ2	

3. Relatório sobre o estado dos ataques criptografados de 2023 da Zscaler ThreatLabz

Lista de verificação de compra:

- ☐ Aplicação imediata de políticas para todos os usuários com proteção idêntica, dentro ou fora da rede corporativa
- ☐ Regras e recursos de quarentena avançados para todos os arquivos de destinos suspeitos
- ☐ Gerenciamento de políticas centralizado que oferece controle granular sobre operações de sandbox, incluindo permissões de tipo de arquivo e retenções automatizadas de destinos suspeitos

Regras e gerenciamento de política centralizados

Evite o gerenciamento incorreto de regras e a configuração manual de sandboxes em cada gateway com gerenciamento de políticas e regras centralizadas fornecidas pela nuvem. Considere soluções com políticas adaptáveis e dinâmicas que sigam os princípios de zero trust descritos pelo **NIST 800-207**. Ao estabelecer políticas de acesso e segurança com base no contexto, incluindo a função e a localização do usuário, a postura do dispositivo e os dados solicitados, o zero trust minimiza as superfícies de ataque. Soluções fornecidas pela nuvem têm benefícios adicionais que podem permitir que você bloqueie ameaças para todos os usuários da organização. Isso significa que não há mais retrospectivas de arquivos (exemplos: inspeções fora de banda e proteções aplicadas após o fato) para uma segurança mais sincronizada. Um aspecto crítico da política de sandbox é que ela oferece a flexibilidade para dar suporte aos negócios, com regras granulares para diferentes conjuntos de usuários, locais, categorias de URL ou ações. Os controles granulares permitem que você alinhe as políticas com a tolerância a riscos e as expectativas de desempenho da sua organização.

Alinhamento das políticas com tolerância a riscos e expectativas de desempenho

Uma solução de sandbox na nuvem deve controlar os riscos e aplicar políticas que estejam de acordo com as necessidades específicas da sua organização. Comece determinando se você tem:

- **Baixa tolerância a arquivos maliciosos:** para organizações que evitam riscos, você pode escolher a Quarentena para ação inicial para arquivos desconhecidos ou suspeitos, o que garantirá que não haja infecções de paciente zero, porque a sandbox analisará o arquivo antes que ele possa ser baixado.
- **Baixa tolerância para arquivos em quarentena:** para organizações tolerantes a riscos que desejam evitar atrasos e interrupções, você pode escolher a Quarentena e isolamento para ação pela primeira vez. Esta ação integra a sandbox com recursos de isolamento do navegador em nuvem, fornecendo aos usuários acesso imediato a um PDF somente leitura sem conteúdo ativo enquanto a sandbox analisa arquivos potencialmente prejudiciais em segundo plano.

Independentemente das suas necessidades específicas, as políticas devem ser fáceis de aplicar para todos os usuários, grupos, departamentos, locais e grupos de locais a partir de uma única plataforma.

Análise inteligente e inteligência sobre ameaças

Os adversários são conhecidos por reutilizar ataques bem-sucedidos, então é essencial compartilhar proteções com a comunidade de segurança para interromper rapidamente as ameaças. As sandboxes de nuvem desempenham um papel importante nisso ao capturar dados de telemetria e compartilhar insights de ameaças recém-identificadas com feeds de ameaças e a comunidade de segurança.

Mecanismo de prevenção a malwares orientado por IA

As sandboxes disponibilizadas na nuvem são capazes de gerenciar modelos de IA/ML de computação intensiva para gerar uma proteção superior. Procure uma sandbox que identifique, isole e previna ameaças desconhecidas ou suspeitas em linha usando IA/ML avançada, sem exigir análise adicional:

- **Veredictos instantâneos de arquivos:** ao entender instantaneamente quais arquivos provavelmente são maliciosos, os usuários não precisam ficar esperando por um veredicto.
- **Prevenção de dia zero:** embora seja difícil de acreditar, nem toda sandbox previne infecções de paciente zero colocando ameaças desconhecidas em quarentena antes de permitir que sejam baixadas.

Fluxos de trabalho de SOC com inteligência sobre ameaças

Os analistas podem passar muitas horas por dia pesquisando uma única ameaça. Procure uma sandbox na nuvem que reduza esse fardo e acelere a investigação e a resposta ao compartilhar insights comportamentais e inteligência sobre ameaças em cargas maliciosas. As equipes de segurança devem ser capazes de oferecer suporte às investigações com análise direta de arquivos na sandbox por meio de envios de API fora de banda. Certifique-se de que os feeds de ameaças se integrem às suas ferramentas de segurança existentes. Eles devem incluir: contexto atualizado em URLs relatadas, indicadores de comprometimento (IoCs) extraídos e táticas, técnicas e procedimentos (TTPs) que se alinhem a estruturas de segurança cibernética, como MITRE ATT&CK®.

Lista de verificação de compra:

- ☐ Recursos de quarentena baseada em IA que podem utilizar IA/ML para fornecer um veredicto instantâneo sobre arquivos para interromper ameaças sem exigir análise de arquivos
- ☐ Contribuições autônomas a proteções contra ameaças diárias compartilhadas entre usuários e redes, independentemente da localização
- ☐ Integração a um canal de comunicação de ameaças com ferramentas de segurança existentes
- ☐ Envios de arquivos de sandbox fora de banda programáticas, acionadas por API, com fila separada para arquivos enviados por API.

Certifique-se de escolher uma sandbox que possa fornecer mais do que uma pontuação de ameaça. Considere uma sandbox que possa descrever técnicas evasivas utilizadas, como:

- Atrasar a execução do código para evitar a detecção da sandbox
- Capturar e visualizar o tráfego conforme ele passa pela rede
- Abrir portas para permitir a conectividade remota
- Fazer tentativas de movimentação lateral para encontrar alvos de maior valor
- Tentar permitir o controle remoto

Relatórios

Soluções de segurança com relatórios são úteis apenas na medida em que são práticas. O relatório de sandbox na nuvem deve ser:

- Inclusivos de todo o ciclo de vida do ataque malicioso
- Simples de usar e fáceis de navegar
- Fáceis de digerir
- Disponível através de uma interface de programação de aplicativos (API) para que possa ser correlacionado com logs existentes.
- Parte de uma plataforma maior que ofereça suporte a relatórios de conformidade

Melhoria do seu SOC com a estrutura MITRE ATT&CK

Ao avaliar os recursos de relatórios, considere uma inteligência de sandbox que possa ser mapeada à **estrutura MITRE ATT&CK**. Com esse recurso, as equipes de SOC podem aplicar os conhecimentos fornecidos para criar defesas táticas em outras partes da pilha de segurança. Dessa maneira, a sandbox será parte integral dos fluxos de trabalho das operações de segurança.

Dependendo da sua maturidade com a estrutura, você pode usar os relatórios de várias maneiras:

- Reduza o ônus da rotulagem utilizando a taxonomia fornecida
- Verifique técnicas de furtividade que possam estar evitando sua solução de detecção e resposta de terminais (EDR)
- Compare e contraste com outros controles
- Concentre-se nas TTPs mais comuns visando sua organização em vez de tentar impedir todas as táticas e técnicas
- Execute um relatório de engenharia reversa

Perguntas a serem feitas antes da compra

Para ajudar o seu processo de tomada de decisão, a seguir você encontrará um resumo das principais perguntas que devem ser feitas e por que você as deve fazer:

A sandbox permite zero infecções iniciais do paciente, mesmo que apenas uma?

Sandboxes que permitem infecções iniciais de paciente zero enquanto um arquivo está sendo analisado estão falhando em manter a organização segura.

A solução cobre todos os usuários e seus dispositivos, independentemente da localização?

Seus usuários podem estar acessando recursos corporativos em trânsito, em seus próprios dispositivos ou em redes não seguras. É essencial proteger todos os dispositivos que são essenciais para seus trabalhos.[4]

A solução detecta envios de arquivos em linha ou requer envios de arquivo fora de banda?

Soluções que funcionam em linha podem identificar ameaças e bloqueá-las diretamente sem precisar depender de fluxos de rede de NGFW ou implicar software EDR de terminais.

A sandbox examina o tráfego em todos os protocolos HTTP, HTTPS, FTP e FTP sobre HTTP? Existem limitações?

É importante examinar o tráfego para revelar malwares furtivos. Uma sandbox disponibilizada na nuvem pode ser melhor para inspecionar todo o tráfego sem latência.

Ela está em conformidade com as leis e regulamentos relevantes, incluindo os requisitos de zero trust?

Os regulamentos de conformidade podem ter requisitos rígidos sobre como a sandbox trata questões de retenção de arquivos/privacidade. Encontrar uma solução que opere apenas na memória e remova informações identificáveis durante a análise ajuda a atender a esses requisitos. Além disso, considere se as soluções aderem aos princípios de zero trust, conforme estabelecido pelos padrões globais NIST 800-207, e use-os como orientação para reduzir superfícies de ataque e proteger dados.

Com quais outros módulos de segurança a sandbox funciona?

Nenhum produto por si só pode oferecer proteção total contra ameaças persistentes avançadas (APTs). Em vez disso, uma abordagem multicamadas de prevenção, mitigação, detecção e resposta contra ameaças é necessária. A sandbox é uma camada integral e, como tal, deve funcionar em harmonia com outras soluções e módulos.

4. *us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf*

Zscaler Cloud Sandbox e proteção avançada contra ameaças

É hora de obter uma verdadeira sandbox nativa da nuvem

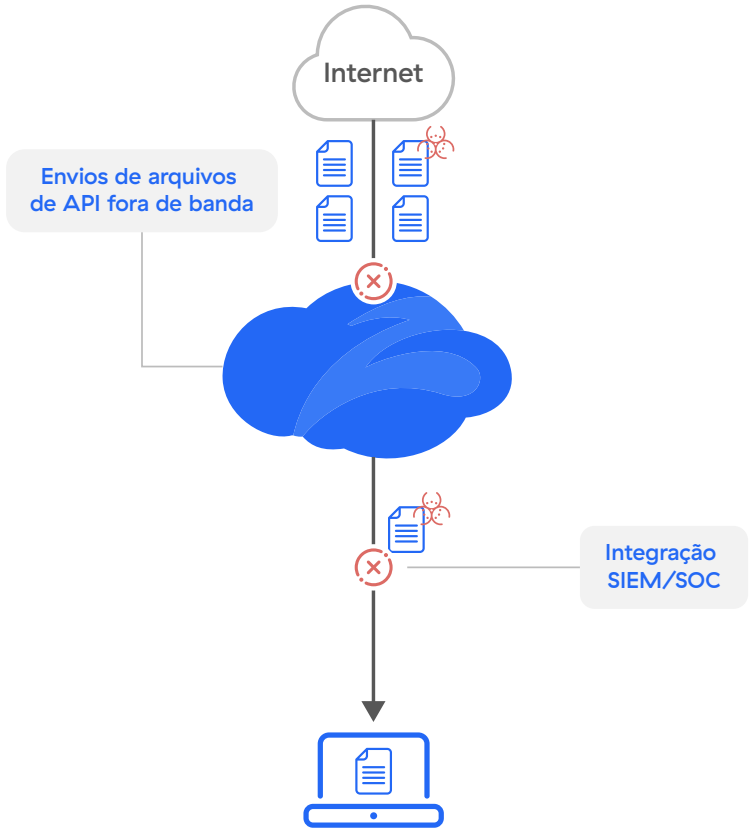
Visto que as organizações estão lidando com superfícies de ataque expandidas e os adversários estão aproveitando as falhas das pilhas de segurança legadas, nunca houve um momento melhor para escolher uma verdadeira sandbox integrada e nativa da nuvem. A Zscaler Cloud Sandbox foi criada com o propósito de capturar e impedir ameaças modernas e ao mesmo tempo garantir proteção contra malwares de dia zero para todos os usuários, em todos os locais.

Desenvolvida em uma arquitetura nativa da nuvem baseada em proxy, a Zscaler Cloud Sandbox é o primeiro mecanismo integrado de prevenção contra malwares orientado por IA do mundo que automaticamente detecta, previne e coloca em quarentena de forma inteligente ameaças desconhecidas e arquivos duvidosos. A inspeção ilimitada e sem latência em protocolos da web e de transferência de arquivos (FTP), incluindo SSL/TLS, permite que a sandbox na nuvem realize análises dinâmicas e profundas, garantindo que nenhum arquivo chegue até o usuário como um download de arquivo malicioso.

Vantagem da IA da Zscaler Sandbox: treinada com mais de 500 milhões de amostras, com atualizações de segurança em tempo real provenientes de 300 trilhões de sinais diários.

A quarentena orientada por IA impede malwares nunca antes vistos

Proteção integrada com entrega instantânea de arquivos benignos, defesa de paciente zero e controles granulares de política



Complexidade e custo reduzidos

- Fácil de implementar, sem hardware ou software para gerenciar
- Remova produtos pontuais redundantes e desconexos
- Elimine o backhauling do tráfego de internet sobre MPLS ou VPN

Proteção imediata e adaptativa para todos os usuários e locais

- Defina políticas globais em um único console centralizado
- Aplique alterações de política imediatamente
- Identifique as ameaças uma vez e bloqueie-as imediatamente para todos os clientes

Revele ameaças ocultas

- Impeça infecções de paciente zero de ameaças conhecidas e emergentes com a quarentena orientada por IA
- Faça upload de arquivos para análise (portal de verificação de arquivos)

Serviço de plataforma integrada

- Pré-filtragem de todas as ameaças conhecidas utilizando antivírus, listas de bloqueio de hash, regras de classificação de malwares YARA, detecções automatizadas de impressão digital JA3 e modelos de ML/IA
- A Collective Intelligence Framework (CIF) permite que a Zscaler integre mais de 60 fontes de ameaça, além da própria fonte de ameaças da Zscaler, alimentada por bilhões de transações em sua base de clientes.
- Integre uma sandbox na nuvem à uma solução de EDR para aumentar a eficácia da segurança e mitigar o acesso inicial, a execução e as táticas persistentes

Um estudo de validação econômica do ESG descobriu que a Zscaler Zero Trust Exchange gerou uma redução de 90% nos dispositivos de segurança.[5]

- Análise estática, dinâmica e secundária, incluindo análise de código e análise de carga secundária
- Inspeção de SSL ilimitada e sem latência
- Proteção para o tráfego de entrada e saída
- Aprimore a investigação e resposta de segurança com envios de arquivos de API repletos de informações forenses, incluindo usuário, origem da localização, táticas evasivas e mais

A Zscaler Cloud Sandbox™ é um recurso totalmente integrado do Zscaler Internet Access™ e parte da Zscaler Zero Trust Exchange™.

Para mais informações, visite
zscaler.com/br/technology/cloud-sandbox

5. info.zscaler.com/resources-industry-report-esg-economic-validation

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que os clientes tenham mais agilidade, eficiência, resiliência e proteção. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança integrada na nuvem do mundo. Para saber mais, visite **www.zscaler.com/br**.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com/br