



Zscaler Sandbox

O primeiro mecanismo de detecção, prevenção e quarentena de malware baseado em IA do mundo

A Zscaler Sandbox evita infecções de paciente zero e impede que ameaças persistentes avançadas obtenham acesso à sua rede.

No mundo atual, que prioriza a mobilidade e a nuvem, seus usuários acessam arquivos de qualquer lugar, diretamente da internet e de aplicativos SaaS. Já se foram os dias de lançar clientes de e-mail do escritório corporativo cercados por camadas de segurança. À medida que as demandas por facilidade de uso ultrapassam as defesas centradas na rede, as organizações ficam com uma superfície de ataque expandida em um momento em que os ataques estão se tornando mais tortuosos e os adversários aproveitam as falhas da pilha de segurança legada.

Em um esforço para proteger dados sigilosos corporativos e pessoais, quase todo o tráfego da internet agora é criptografado. Embora isso tenha dissuadido alguns criminosos, a criptografia criou uma falsa sensação de segurança. Sandboxes legadas, com arquitetura de passagem, não oferecem visibilidade e permitem involuntariamente que arquivos maliciosos escapem, escondendo-se no tráfego criptografado, livres de inspeção profunda ou quarentena. Dispositivos de descryptografia de SSL integrados podem ser implantados para ajudar, no entanto, como acontece com a maioria dos hardwares, eles não conseguem ser dimensionados e aumentam as dores de cabeça administrativas e o custo da expansão de dispositivos. Como resultado, as infecções de paciente zero por malware desconhecido continuam a permear as redes e deixam as equipes de TI e de segurança

Benefícios da Zscaler Sandbox:

- **Mecanismo de prevenção contra malware baseado em IA**

Identifique, coloque em quarentena e evite ameaças desconhecidas ou suspeitas de forma inteligente e integrada, utilizando IA/ML avançados sem verificar arquivos benignos novamente.

- **Inspeção completa integrada para descobrir ataques ocultos**

Exponha e evite ameaças evasivas e malwares ocultos no tráfego web criptografado e em protocolos de transferência de arquivo sem limites de capacidade ou latência.

- **Proteção consistente globalmente compartilhada**

Obtenha proteção automatizada contra ameaças previamente desconhecidas com inteligência sobre ameaças integrada compartilhada entre todos os usuários em tempo real.

- **Fluxos de trabalho de SOC aumentados com inteligência sobre ameaças**

Acelere as investigações e as respostas compartilhando informações sobre o comportamento de malwares, inteligência sobre ameaças e relatórios avançados utilizando APIs robustas.

- **Chega de dispositivos físicos e softwares caros**

Implante em segundos, sem a necessidade de comprar hardware ou gerenciar software. Basta configurar e implementar uma política de sandbox para obter valor imediatamente.

- **Proteção disponibilizada na nuvem com presença global na borda**

Obtenha segurança e experiência de usuário totalmente integradas e incomparáveis com o Zscaler Internet Access™, como parte da Zscaler Zero Trust Exchange™.

lutando para impedir a movimentação lateral e a exfiltração de dados, o que deveria ter sido evitado em primeiro lugar.

Zscaler Sandbox

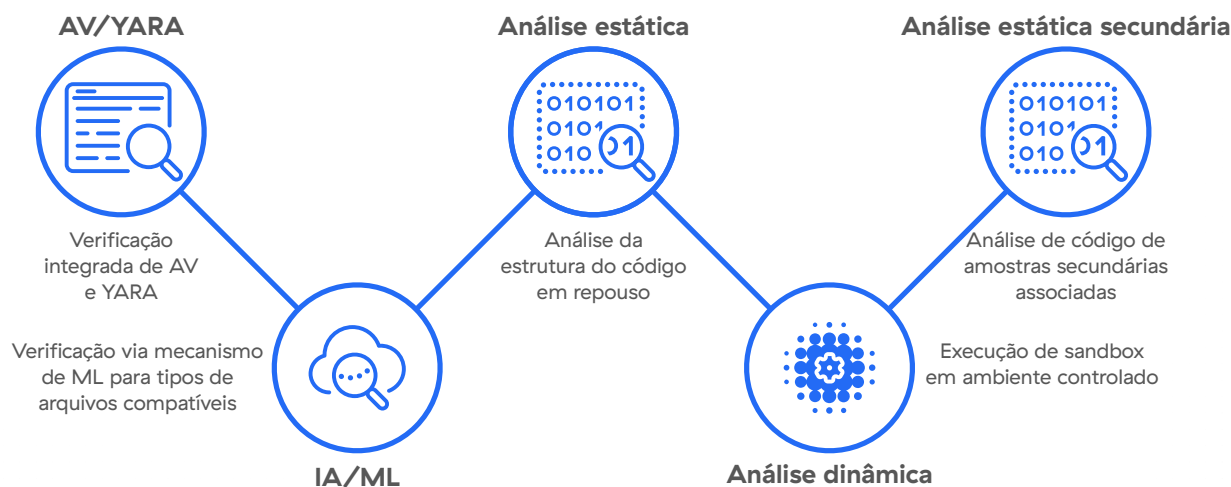
Como um recurso crítico da pilha de segurança, as sandboxes são uma medida preventiva contra execuções de códigos e arquivos maliciosos. Ao contrário das sandboxes fora de banda que fornecem proteção somente após o comprometimento inicial, a Zscaler Sandbox foi desenvolvida especificamente para capturar e impedir ameaças modernas e elusivas que aproveitam técnicas de evasão e exploram os pontos fracos das sandbox tradicionais.

Desenvolvida em uma arquitetura nativa da nuvem baseada em proxy, a Zscaler Cloud Sandbox é o primeiro mecanismo integrado de prevenção contra malwares baseado em IA do mundo que automaticamente detecta, previne e coloca em quarentena de forma inteligente ameaças desconhecidas e arquivos suspeitos. A inspeção ilimitada e sem latência em protocolos web e de transferência de arquivos (FTP), incluindo SSL/TLS, permite que a sandbox de geração de nuvem

realize análises dinâmicas e profundas, garantindo que nenhum arquivo chegue até o usuário como um download de arquivo malicioso.

O arquivo desconhecido ou suspeito é enviado primeiro por meio de um mecanismo de análise de pré-filtragem, que verifica o conteúdo do arquivo em relação a mais de 40 feeds de ameaças, assinaturas de antivírus, regras YARA e modelos de IA/ML para fornecer um veredicto rápido, bloqueando ameaças igualmente conhecidas. Após a triagem inicial, o arquivo passa por análises estáticas, dinâmicas e secundárias robustas que incluem a execução do arquivo em um ambiente controlado e isolado para chegar a um veredicto prático. A etapa final é o pós-processamento, que atualiza o banco de dados de ameaças da Zscaler e a aplicação das políticas do cliente.

Com veredictos baseados em IA, os arquivos benignos são entregues instantaneamente, enquanto os arquivos maliciosos são bloqueados para todos os usuários globais da Zscaler, como resultado da proteção compartilhada do efeito da nuvem. Isso impede infecções e ameaças emergentes para todos os usuários, independentemente do dispositivo ou localização.



Benefícios da sandbox de geração de nuvem

Além de colocar arquivos suspeitos em quarentena, realizar análises baseadas em IA em tempo real e emitir veredictos instantâneos sem atrasos, os relatórios avançados detalhados da Zscaler Sandbox podem fazer com que a sandbox passe da última linha de defesa para o primeiro passo na ação orientada por inteligência. Ao aplicar insights comportamentais de malwares reais direcionados à sua organização, é possível enriquecer os fluxos de trabalho de SecOps para fortalecer suas defesas em toda a pilha de segurança.

Interrompa de forma inteligente ameaças emergentes e infecções de paciente zero Os adversários estão aproveitando a criptografia e os aplicativos na nuvem confiáveis para realizar ataques furtivos. Na verdade, um relatório recente da ThreatLabZ observou malwares sendo entregues pelo Google Drive, AWS e OneDrive.

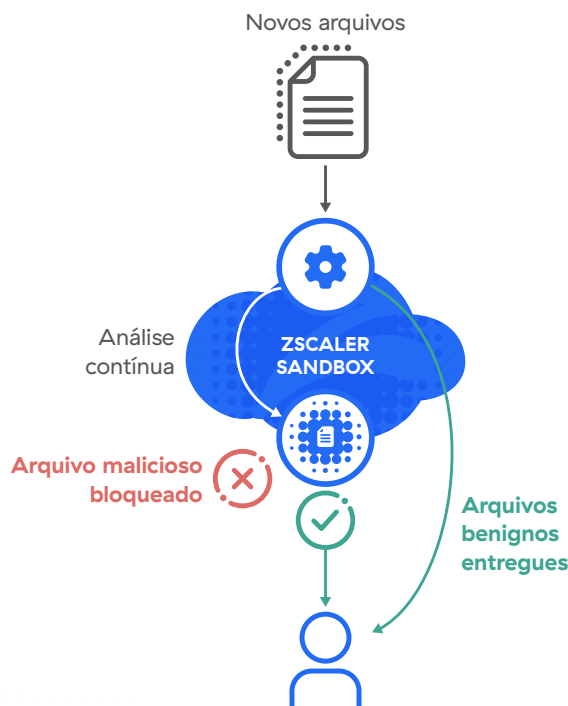
Após uma rápida implantação de vinte minutos da Zscaler Sandbox, a equipe de TI e segurança de um cliente conseguiu entregar de forma segura e instantânea 91% dos arquivos benignos aos usuários após receber um veredicto baseado em IA. Os demais arquivos desconhecidos foram encaminhados para análise dinâmica e aprofundada, que revelou que 5% dos arquivos continham malware ou intenções maliciosas. Os arquivos são bloqueados para os usuários de destino e para todos os usuários e dispositivos globais da Zscaler, independentemente dos locais, para oferecer proteção compartilhada e consistente.

A capacidade de verificar arquivos web e de FTP, principalmente tráfego criptografado, garante visibilidade e impede que invasores obtenham acesso à sua rede.

Antes que um funcionário acidentalmente baixe e abra um novo documento malicioso do Office (Maldocs) com uma macro oculta, a função integrada de quarentena da Zscaler Sandbox, baseada em IA, entra em ação. Quando a análise profunda do arquivo retorna uma classificação de ameaça alta, o arquivo é bloqueado para o funcionário e não pode ser acessado por outros usuários da Zscaler. Os veredictos instantâneos de arquivos sem verificá-los novamente evitam a interrupção da produtividade dos funcionários, enquanto a quarentena e o bloqueio automáticos de arquivos desconhecidos ou maliciosos evitam o que poderia se transformar em diversos incidentes de suporte técnico da TI.

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



Aprimore os fluxos de trabalho do SOC com informações sobre malware e MITRE ATT&CK

Após a análise profunda dos arquivos e a detonação segura de malware desconhecido, a sandbox gera automaticamente um relatório de análise. O ambiente da sandbox, controlado e isolado, captura telas de análise e informa aos analistas sobre polimorfismo e técnicas de evasão de ofuscação, comportamento de retorno de chamada e outras ações. Esse relatório detalha o ciclo de vida do ataque, a cadeia de destruição do evento, o comportamento do malware e a intenção da carga útil, mapeando-os de volta à estrutura do MITRE ATT&CK.

Ao operacionalizar as conclusões contextuais da sandbox com o estrutura do MITRE ATT&CK, as equipes de segurança e de TI podem compartilhar informações em toda a pilha de segurança. Isso permite que a sandbox de geração de nuvem não seja apenas a última linha de defesa contra malware, mas também o primeiro passo na detecção, acelerando a investigação e a resposta, ao mesmo tempo que oferece suporte a exercícios de caça a ameaças.

Gerenciamento simplificado de políticas com controles granulares Como um produto disponibilizado na nuvem, não há hardware para comprar e configurar nem software para gerenciar, reduzindo a complexidade e os recursos. Sem precisar estar no local para configurar e conectar cada dispositivo, você pode começar a usar a Zscaler Sandbox com uma configuração simples em duas etapas:

critérios e ação. Como bônus, as políticas são fáceis de gerenciar, configurar e implantar. Com apenas alguns cliques, os administradores podem implementar políticas, incluindo ordem de regras para execução precisa e outras políticas que seguem usuários ou grupos de usuários, independentemente da localização.



Para controles mais granulares, a sandbox de geração de nuvem pode aprimorar a análise de arquivos estáticos e dinâmicos com a detecção automatizada de impressões digitais JA3 e configurar listas de bloqueio de hash personalizadas e regras YARA. Além disso, as políticas de bloqueio baseadas em pontuação podem agir contra arquivos greyware e adware irritantes ou suspeitos que normalmente não ultrapassam o limite de pontuação de ameaça.

Desenvolvida em uma plataforma zero trust nativa da nuvem, a Zscaler Sandbox é um recurso totalmente integrado do Zscaler Internet Access e faz parte da Zscaler Zero Trust Exchange. A arquitetura exclusiva baseada em proxy protege os usuários de forma integrada, e não após o fato, direcionando o tráfego para a maior pilha de segurança na nuvem do setor para fornecer proteção inteligente e profunda a todos os usuários, independentemente da localização ou da rede. Obtenha proteção global compartilhada com atualizações em tempo real provenientes de 300 trilhões de sinais de ameaças diários, combinadas com proteção de geração de nuvem e princípios de privilégio mínimo do zero trust.

Standard Sandbox vs. Advanced Sandbox

	Standard Sandbox	Advanced Sandbox	
Edições do ZIA	Professional Edition Business Edition	Transformation Edition Edição ELA	A Advanced Sandbox pode ser um complemento do ZIA Professional e Business Edition
Suporte de arquivo	.exe, .dll	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .alcatrão, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, arquivos de script em zips	
Quarentena com IA	—	☑	
Políticas granulares	—	☑	
Relatórios	—	☑	
API	—	☑	

Principais recursos da geração de nuvem

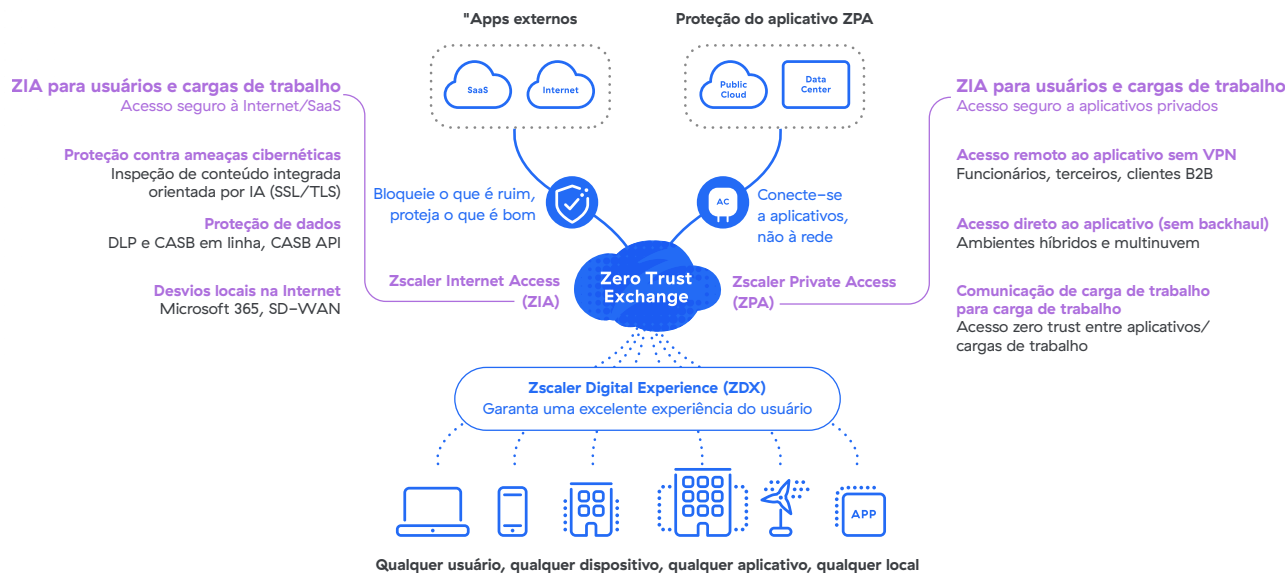
Mecanismo de análise de pré-filtragem	AV, listas de bloqueio de hash, regras YARA, detecções automatizadas de impressões digitais JA3 e modelos de ML/IA
Análise estática, dinâmica e secundária	Análise estática e análise dinâmica, incluindo análise de código e análise de carga útil secundária
Suporte de arquivo	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, arquivos de script em zips
Inspeção SSL	Capacidade ilimitada para inspeção em SSL/TLS
Retenção de arquivos	A Zscaler Cloud Sandbox opera exclusivamente na memória. As informações identificáveis são removidas dos arquivos durante a análise. Após a conclusão da análise, os arquivos benignos são eliminados da memória, enquanto os arquivos maliciosos são criptografados e armazenados por tempo indeterminado, compartilhando informações entre todos os usuários da Zscaler para oferecer proteção contínua.
Sistemas operacionais compatíveis	Windows XP, Windows 10, Android
Suporte de protocolo	HTTP, HTTPS, FTP, FTP sobre HTTP
Arquivos por dia	Ilimitado
Tamanho máximo do arquivo	20 MB para Windows e 50 MB para Android
Método de implantação	Nativo da nuvem
Integração de informações sobre ameaças	Mais de 40 feeds de informações sobre ameaças de parceiros de segurança
Gestão e relatórios	Relatórios completos, incluindo comportamento e intenção de malware, indicadores de comprometimento (IOCs), arquivos descartados, PCAPs
Análise forense	Amostra inicial, cargas secundárias, PCAPs
Suporte de API	Suporte robusto à API, recuperação de relatórios via API no formato JSON
Políticas granulares	Políticas fáceis de usar e configurar para usuários, locais, grupos de locais, tipos de arquivos, grupos de usuários, departamentos, categorias de URL e protocolos
Certificados de privacidade e conformidade	Em conformidade com rigorosas organizações globais de risco, privacidade e conformidade comerciais e governamentais 
Regulamentações do setor e de privacidade de dados	Em conformidade com os regulamentos de privacidade de dados específicos do setor e do país 

A Zscaler Sandbox é totalmente integrada ao Zscaler Internet Access™ e faz parte da Zero Trust Exchange como um todo

A Zscaler Zero Trust Exchange garante conexões rápidas e seguras e permite que seus funcionários trabalhem de qualquer lugar usando a Internet como rede corporativa. Baseada no princípio zero trust de acesso de privilégio mínimo, a plataforma oferece segurança abrangente usando identidade baseada no contexto e aplicação de políticas.

Como a Zscaler fornece a estratégia zero trust a usuários, cargas de trabalho e IloT/TO

Implante em semanas para melhorar a proteção cibernética e a experiência do usuário



Gartner

Zscaler nomeada líder no SSE MQ da Gartner, com a mais alta posição em capacidade de execução.

Saiba mais →



Experience your world, secured.™

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para proporcionar aos seus clientes mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados ao conectar com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers no mundo inteiro, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança integrada na nuvem do mundo. Saiba mais em zscaler.com.br ou siga-nos no Twitter [@zscaler](https://twitter.com/zscaler).

©2023 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIAT™, Zscaler Private Access™, ZPA™ e outras marcas registradas listadas em zscaler.com.br/legal/trademarks são (i) marcas registradas ou marcas de serviço, ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Todas as outras marcas comerciais pertencem aos seus respectivos proprietários.