EBOOK

La guía del comprador de soluciones para la prevención de amenazas

Encuentre la mejor solución de protección contra amenazas impulsada por la IA para detener ataques basados en archivos.

Contenido

Replanteo de la seguridad ante el panorama actual de amenazas

La seguridad exclusivamente perimetral es demasiado arriesgada para el mundo digital de la actualidad

El cambio hacia el trabajo híbrido y las aplicaciones alojadas en la nube han cambiado la manera de acceder a los recursos empresariales. Los empleados están utilizando dispositivos no administrados a través de redes no seguras como Wi-Fi pública para mantener la productividad a distancia o sobre la marcha, y esto convierte a Internet efectivamente en la nueva red corporativa. Esta expansión de los puntos de acceso hace que el antiguo enfoque de la seguridad de castle-and-moat resulte inadecuado para proteger a sus usuarios, aplicaciones y datos. Confiar únicamente en las defensas perimetrales introduce riesgos, ya que se eluden los controles centrados en la red para acceder directamente a Internet, priorizando a menudo la facilidad de uso sobre la seguridad.

La nueva generación de ciberataques evade fácilmente los controles de seguridad heredados. Es hora de acercar la seguridad a los usuarios y pasar de proteger el perímetro a proteger a los usuarios, las cargas de trabajo y OT/IOT.

Los atacantes están aprovechando la migración a la nube

Atrapados entre la espada y la pared, los equipos de seguridad han hecho todo lo posible para introducir los controles de seguridad heredados para el mundo móvil y en la nube de la actualidad. La ineficacia que han demostrado tener significa una victoria para los atacantes. Mientras que las organizaciones luchan por proteger múltiples perímetros de red, inadvertidamente, se dejan puertas abiertas al malware, como lo demuestran los hallazgos de Zscaler ThreatLabz:

- **El 86 %** de las amenazas se transmiten a través de canales cifrados y el malware representa el 78 % de los ataques cifrados.[1]
- Los ataques de ransomware aumentaron un **40 %** interanual.[2]
- Las cargas útiles observadas en el Sandbox de Zscaler aumentaron un **58 %**.[2]

Esta rápida evolución de las amenazas digitales, agravada por la creciente superficie de ataque de la nube, solo enfatiza la necesidad de que los equipos de seguridad reevalúen sus estrategias y refuercen las defensas contra los ciberriesgos modernos.

1. Informe sobre el estado de los ataques cifrados de Zscaler ThreatLabz 2023
2. Informe sobre el ransomware de Zscaler ThreatLabz 2023

Se necesita evolucionar hacia la protección contra malware de día cero

Los adversarios tienen dos ventajas clave: **velocidad** y **proliferación**. Los desarrolladores de malware crean amenazas más rápido de lo que los defensores pueden definirlas, aprovechando la inteligencia artificial (IA) para crear variantes capaces de evadir las medidas de seguridad y los métodos de detección convencionales.

El phishing con archivos adjuntos o enlaces maliciosos sigue siendo uno de los mecanismos de distribución más comunes en la actualidad. El uso generalizado de tráfico cifrado complica aún más las estrategias de defensa. Las amenazas modernas a menudo se esconden en el tráfico cifrado, lo que subraya la importancia de inspeccionar todo el tráfico web y no web, o puede permitir que, sin saberlo, ingrese malware a su red.

Como función crítica en la pila de seguridad, las sandboxes son una medida preventiva contra archivos maliciosos y ejecuciones de código. Pretenden ser una defensa eficaz contra los ataques basados en archivos desconocidos que pretenden eludir el EDR y otros análisis en busca de malware conocido. Lamentablemente, muchas sandboxes se implementan fuera de banda, confiando en que las muestras de malware les sean reenviadas desde los firewalls de próxima generación (NGFW), los productos de seguridad en la nube o los agentes de punto final.

Esto a menudo significa que la detección se produce después de que el malware se haya descargado en un dispositivo de usuario, lo que posibilita las infecciones de paciente cero por malware o ransomware, y desde luego no se ajusta a los conceptos Zero Trust. Además, muchas sandboxes no aprovechan el análisis de IA/ML a gran escala para detectar y poner en cuarentena automáticamente las amenazas desconocidas y los archivos sospechosos, un factor clave para ofrecer una defensa de paciente cero en línea sin interrumpir la productividad.

Los antivirus basados en firmas y los sistemas de prevención de intrusiones (IPS) por sí solos no pueden prevenir las amenazas polimórficas y de día cero.

Requisitos de sandbox en la nube

Hasta ahora, los atacantes han tenido las mejores cartas al aprovecharse de la arquitectura cambiante en el entorno de la nube.

Elegir la sandbox adecuada en la nube es esencial para evitar que las infecciones de paciente cero y evitar que las amenazas persistentes avanzadas se infiltren en su red.

La siguiente sección tiene como objetivo ayudarle a comprender los requisitos específicos que debe considerar al seleccionar una sandbox en la nube.

Descifrado e inspección a escala

El cifrado se ha convertido en una tendencia prometedora de seguridad que permite proteger y asegurar la comunicación privada y la información confidencial. Lamentablemente, los ciberdelincuentes están aprovechando el tráfico cifrado para ocultar cargas útiles maliciosas.

Descifrar e inspeccionar el tráfico es un proceso que consume muchos recursos informáticos y puede convertir los dispositivos sandbox de alto rendimiento en verdaderos obstáculos que interrumpen la actividad con una latencia inaceptable.

Al evaluar una solución moderna de sandboxing, es importante identificar proveedores que puedan proporcionar servicios ilimitados en línea y sin latencia de descifrado e inspección.

Las amenazas a través de HTTPS crecieron un 24.3 % interanual, lo que representa 30 mil millones de ataques cifrados en 2023.[3]

Lista de comprobación de compras:

- ☐ No requiere instalación adicional de hardware o máquina virtual (VM) para descifrar el tráfico SSL
- ☐ Inspecciona y analiza los siguientes tipos de archivos sin límites de latencia o capacidad:

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	archivos script en archivos ZIP
SWF	BZ2	

3. Informe sobre el estado de los ataques cifrados de Zscaler ThreatLabz 2023

Lista de comprobación de compras:

- Aplicación inmediata de políticas a todos los usuarios con una protección idéntica, ya sea dentro o fuera de la red corporativa
- Reglas y capacidades avanzadas de cuarentena para todos los archivos que provengan de destinos sospechosos
- Gestión centralizada de políticas que permite un control granular sobre las operaciones de sandbox, incluidas las asignaciones de tipos de archivos y las retenciones automáticas de destinos sospechosos

Reglas y administración de políticas centralizadas

Evite la gestión incorrecta de las reglas y la configuración manual de las sandboxes en cada puerta de enlace con la gestión centralizada de políticas y reglas en la nube. Considere soluciones con políticas adaptables y dinámicas que sigan los principios Zero Trust descritos por el **NIST 800-207**.
Al establecer políticas de acceso y seguridad basadas en el contexto (incluidos el papel y la ubicación del usuario, la postura del dispositivo y los datos solicitados) Zero Trust minimiza las superficies de ataque. Las soluciones que se ofrecen en la nube tienen ventajas adicionales que pueden permitirle bloquear las amenazas en todos los usuarios de la organización. Esto se traduce en el fin de las retrospectivas de archivos (ejemplos: inspecciones fuera de banda y protecciones aplicadas a posteriori) para una seguridad más sincronizada. Un aspecto crítico de la política de sandbox es que ofrece la flexibilidad necesaria para respaldar la actividad, con reglas granulares para diferentes conjuntos de usuarios, ubicaciones, categorías de URL o acciones. Los controles granulares le permiten alinear las políticas con la tolerancia al riesgo y las expectativas de rendimiento de su organización.

Alineación de políticas con tolerancia al riesgo y expectativas de rendimiento

Una solución de sandbox en la nube debe controlar los riesgos y aplicar políticas que se ajusten a las necesidades únicas de su organización. Comience por determinar si tiene:

- **Baja tolerancia a los archivos maliciosos:** Para las organizaciones que busquen eludir los riesgos, puede elegir Cuarentena como Primera Acción para los archivos desconocidos o sospechosos, lo que garantizará que no se produzcan infecciones del paciente cero, ya que el sandbox analizará el archivo antes de que pueda descargarse.
- **Baja tolerancia para la puesta en cuarentena de archivos:** Para las organizaciones tolerantes al riesgo que desean evitar retrasos e interrupciones, puede elegir Cuarentena y Aislamiento como Primera Acción. Esta acción integra la sandbox con capacidades de aislamiento del navegador en la nube, proporcionando a los usuarios acceso inmediato a un PDF de solo lectura sin contenido activo mientras la sandbox analiza los archivos potencialmente dañinos en segundo plano.

Independientemente de sus necesidades específicas, las políticas deben ser fáciles de aplicar a todos los usuarios, grupos, departamentos, ubicaciones y grupos de ubicación desde una sola plataforma.

Análisis inteligente e información sobre amenazas

Se sabe que los adversarios repiten los ataques exitosos, por lo que es esencial compartir las protecciones con la comunidad de seguridad para detener rápidamente las amenazas. Los entornos aislados en la nube desempeñan un papel importante en la captura datos de telemetría y compartir información de las amenazas recientemente identificadas con los canales de amenazas y la comunidad de seguridad.

Motor de prevención de malware con IA

Las sandboxes distribuidas en la nube pueden administrar modelos de IA y ML con una capacidad de computación intensiva para impulsar una protección superior.

Busque una solución de sandbox que identifique, ponga en cuarentena y evite de manera inteligente amenazas desconocidas o sospechosas en línea mediante IA/ML avanzados sin necesidad de análisis adicionales:

- **Veredictos de archivos instantáneos:** Al comprender instantáneamente qué archivos son muy probablemente maliciosos, los usuarios no tienen que esperar un veredicto.
- **Prevención del día cero:** Aunque parezca difícil de creer, no todos los entornos sandbox evitan las infecciones de paciente cero poniendo en cuarentena las amenazas desconocidas antes de permitir su descarga.

Flujos de trabajo SOC con inteligencia de amenazas

Los analistas pueden pasar muchas horas al día investigando una sola amenaza. Busque una sandbox en la nube que reduzca esta carga y acelere la investigación y la respuesta al compartir información sobre el comportamiento y la inteligencia de amenazas sobre cargas útiles maliciosas. Los equipos de seguridad deben poder respaldar las investigaciones con análisis directo de archivos en la sandbox a través de envíos de API fuera de banda. Asegúrese de que los feeds de amenazas se integren con sus herramientas de seguridad existentes. Deben incluir: contexto actualizado sobre las URL informadas, indicadores extraídos de compromiso (IoC) y tácticas, técnicas y procedimientos (TTP) que se alineen con marcos de ciberseguridad como MITRE ATT&CK®.

Lista de comprobación de compras:

- ☐ Capacidades de cuarentena basadas en IA que pueden aprovechar la IA/ML para emitir un veredicto instantáneo sobre los archivos con el fin de detener las amenazas sin necesidad de analizarlos.
- ☐ Contribución autónoma a las protecciones diarias contra amenazas compartidas entre usuarios y redes independientemente de la ubicación
- ☐ Integración de la fuente de amenazas con las herramientas de seguridad existentes
- ☐ Envíos de archivos “fuera de banda” programáticos e impulsados por la API con una cola separada para los archivos enviados a través de la API

Asegúrese de elegir un sandbox que pueda proporcionar más que una puntuación de las amenazas. Considere un sandbox que pueda delinear las técnicas evasivas utilizadas, tales como:

- Retrasar la ejecución de código para evitar la detección del sandbox
- Capturar y visualizar el tráfico a medida que pasa por la red
- Abrir puertos para permitir la conectividad remota
- Intentar el movimiento lateral para encontrar objetivos de mayor valor
- Tratar de permitir el control remoto

Informes

Las soluciones de seguridad con informes son tan útiles como procesables. Los informes de la sandbox en la nube deberían estar:

- Incluir todo el ciclo de vida de los ataques maliciosos
- Ser fáciles de usar y de navegar
- Ser fáciles de incorporar
- Disponibles a través de una interfaz de programación de aplicaciones (API) para que puedan correlacionarse con los registros existentes
- Ser parte de una plataforma más grande que también admita informes de cumplimiento

Mejora de su SOC con el Marco MITRE ATT&CK

Cuando evalúe las capacidades de generación de informes, considere la inteligencia sandbox que pueda asignarse al marco **MITRE ATT&CK**. Con esta capacidad, los equipos SOC pueden aplicar los conocimientos aportados a la construcción de defensas tácticas en otras partes de la pila de seguridad. De este modo, el sandbox es una parte integral de los flujos de trabajo de las operaciones de seguridad.

Dependiendo de su madurez con el marco, puede utilizar los informes de distintas maneras:

- Reducir la carga del etiquetado mediante el uso de la taxonomía proporcionada
- Ver las técnicas sigilosas que pueden estar evadiendo su solución de detección y respuesta de los puntos finales (EDR)
- Hacer comparaciones y contrastes de otros controles
- Concentrarse en los TTP más comunes dirigidos a su organización en lugar de evitar todas las tácticas y técnicas sin un objetivo definido
- Realizar un informe de ingeniería inversa

Preguntas a formular antes de comprar

Para ayudarle a guiar su proceso de decisión, le presentamos un conjunto de las preguntas clave que debe formular y por qué hacerlo:

¿La sandbox permite infecciones iniciales de paciente cero, aunque sea solo una?

Las sandbox que permiten una infección inicial de paciente cero mientras se analiza un archivo no logran mantener la seguridad de la organización.

¿La solución abarca a todos los usuarios y sus dispositivos, independientemente de su ubicación?

Es posible que sus usuarios accedan a los recursos corporativos desde cualquier lugar, en sus propios dispositivos o a través de redes no seguras. Es fundamental proteger todos los dispositivos que son esenciales para sus trabajos.[4]

¿La solución detecta el envío de archivos en línea o requiere envíos fuera de banda?

Las soluciones que funcionan en línea pueden identificar amenazas y bloquearlas directamente sin tener que depender de flujos de red de NGFW o incluir software EDR de punto final.

¿La sandbox examina el tráfico en todos los protocolos HTTP, HTTPS, FTP y FTP a través de HTTP? ¿Existen limitaciones?

Es importante examinar el tráfico para descubrir malware sigiloso. Una sandbox distribuida en la nube puede ser mejor para inspeccionar todo el tráfico sin latencia.

¿Cumple las leyes y normativas pertinentes, incluidos los requisitos Zero Trust?

Las normativas de cumplimiento pueden tener requisitos estrictos sobre cómo se gestiona el sandboxing y sobre cuestiones de retención de archivos/privacidad. Encontrar una solución que funcione solo en la memoria y elimine la información identificable durante el análisis le ayudará a cumplir estos requisitos. Además, considere si las soluciones se adhieren a los principios Zero Trust según lo establecido por las normas globales NIST 800-207 y utilícelas como guía para reducir las superficies de ataque y proteger los datos.

¿Con qué otros módulos de seguridad funciona la sandbox?

Ningún producto puede proteger completamente contra las amenazas persistentes avanzadas (APT). En cambio, se requiere un enfoque multicapa de prevención de amenazas, mitigación, detección y respuesta. Sandboxing es una capa integral y, como tal, debe funcionar bien con otras soluciones y módulos.

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

Zscaler Cloud Sandbox y Advanced Threat Protection

Es hora de una verdadera sandbox en línea nativa en la nube

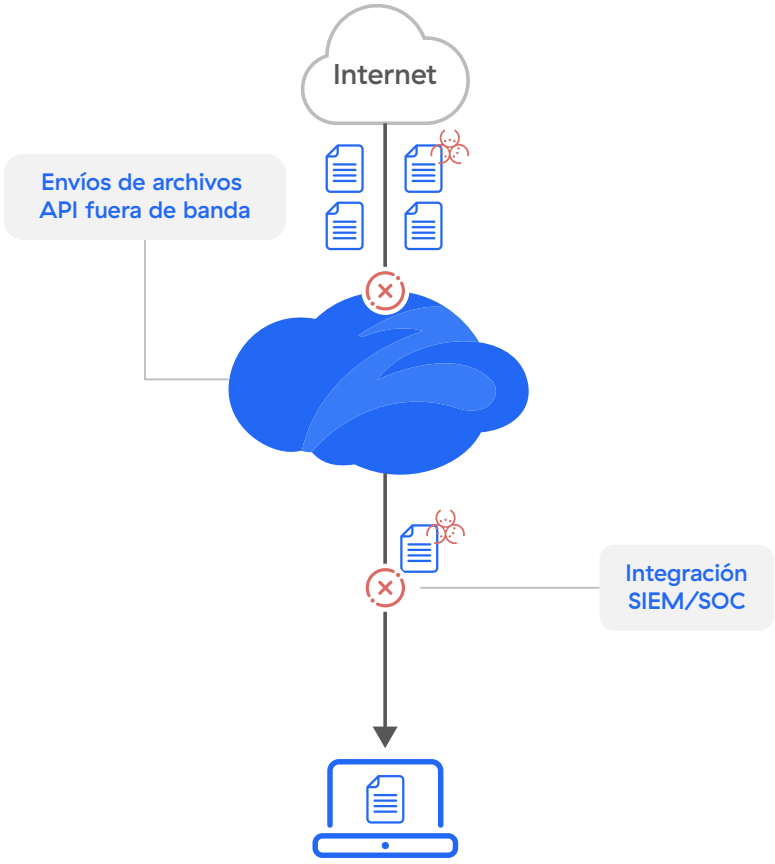
Mientras que las organizaciones se ocupan de las superficies de ataque más grandes y los atacantes aprovechan las brechas de la pila de seguridad heredada, nunca ha habido un mejor momento para elegir una verdadera sandbox nativa en la nube en línea. Zscaler Cloud Sandbox está diseñada específicamente para capturar y detener las amenazas modernas al tiempo que garantiza una protección contra malware de día cero para todos los usuarios, en todas las ubicaciones.

Construida sobre una arquitectura nativa de la nube basada en proxy, la solución Zscaler Cloud Sandbox es el primer motor de prevención de malware impulsado por la IA del mundo que detecta, previene y pone en cuarentena de manera inteligente amenazas desconocidas y archivos sospechosos en línea. La inspección ilimitada y sin latencia de los protocolos de transferencia web y de archivos (FTP), incluido SSL/TLS, permite que la sandbox en la nube realice análisis dinámicos en profundidad y en tiempo real, asegurando que ningún archivo desconocido llegue al usuario como una descarga maliciosa de archivos.

La ventaja de Zscaler Sandbox AI: Entrenada con más de 500 millones de muestras, con actualizaciones de seguridad en tiempo real procedentes de 300 billones de señales diarias.

La cuarentena impulsada por la IA detiene el malware nunca antes visto

Protección en línea con distribución instantánea de archivos benignos, defensa de paciente cero y controles de políticas granulares



Reducción de la complejidad y los costos

- Fácil de implementar, sin hardware ni software que administrar
- Elimine los productos puntuales redundantes e inarticulados
- Elimine el tráfico de retorno de Internet a través de MPLS o VPN

Protección inmediata y adaptativa para todos los usuarios y ubicaciones

- Defina políticas globales en una única consola centralizada
- Aplique los cambios de política inmediatamente
- Identifique las amenazas una vez y bloquee inmediatamente para todos los clientes

Detecte amenazas ocultas

- Detenga las infecciones de paciente cero por amenazas conocidas y emergentes con la cuarentena que utiliza la IA
- Cargue archivos para análisis (portal de comprobación de archivos)

Plataforma integrada distribuida como servicio

- Filtrado previo de todas las amenazas maliciosas conocidas mediante antivirus, listas de bloqueo hash, reglas de clasificación de malware YARA, detecciones automatizadas de individualización (fingerprinting) JA3 y modelos de ML/AI
- Los feeds del Marco de Inteligencia Colectiva (CIF) permiten a Zscaler integrarse con más de 60 feeds de amenazas además del propio feed de hilos de Zscaler, alimentado por miles de millones de transacciones a través de su base de clientes.
- Agregue una solución de EDR sobre un sandbox en la nube para aumentar la eficacia de la seguridad y mitigar el acceso inicial, la ejecución y las tácticas persistentes

Un estudio de validación económica de ESG descubrió que Zscaler Zero Trust Exchange generaba una reducción del 90 % en dispositivos de seguridad.[5]

- Análisis estático, dinámico y secundario, incluido el análisis de código y el análisis de carga útil secundaria
- Inspección SSL limitada y sin latencia
- Protección del tráfico entrante y saliente
- Mejore la investigación y la respuesta de seguridad con análisis forenses enriquecidos de envíos de archivos API, incluidos el usuario, el origen de la ubicación, las tácticas evasivas, etc.

La solución Zscaler Cloud Sandbox™ está totalmente integrada con Zscaler Internet Access™ y forma parte del intercambio holístico Zscaler Zero Trust Exchange.

Para obtener más información, visite
zscaler.com/mx/technology/cloud-sandbox

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

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zero Trust Exchange™ protege a miles de clientes contra ciberataques y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange, basado en SASE, es la plataforma de seguridad en la nube en línea más grande del mundo. Para obtener más información, visite **www.zscaler.com/mx**.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134