LIBRO ELECTRÓNICO

La guía del comprador para la prevención de amenazas

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

Índice

Replantearse la seguridad para el panorama de amenazas actual

La seguridad que sólo protege el perímetro es demasiado arriesgada para el mundo digital actual

El paso al trabajo híbrido y a las aplicaciones alojadas en la nube han cambiado la manera en que se accede a los recursos empresariales. Los usuarios emplean dispositivos no gestionados a través de redes desprotegidas, como las redes wifi públicas, para seguir siendo productivos en otros lugares o mientras viajan, lo que convierte a Internet en la nueva red corporativa. Esta expansión de puntos de acceso hace que el antiguo enfoque de seguridad de castillo y foso sea inadecuado para proteger a sus usuarios, aplicaciones y datos. Depender únicamente de las defensas perimetrales introduce riesgos, ya que se pasan por alto los controles centrados en la red en favor del acceso directo a Internet, priorizando a menudo la facilidad de uso por sobre la seguridad.

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

Los adversarios se están aprovechando de la prisa para adaptarse a la nube

Los equipos de seguridad se encuentran entre la espada y la pared y han hecho todo lo posible para forzar la introducción de los controles de seguridad heredados en el mundo de la nube y móvil actual. Esa incompatibilidad ha supuesto una ventaja para los adversarios. Mientras las organizaciones intentan proteger múltiples perímetros de red, dejan sin saberlo puertas abiertas al malware, como prueban los descubrimientos del equipo ThreatLabz de Zscaler:

- **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 frente a los riesgos cibernéticos modernos.

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

Es preciso que la protección contra el malware de día cero evolucione

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 el método de entrega más común en la actualidad. El uso generalizado de tráfico cifrado complica aún más las estrategias de defensa. Las amenazas modernas a menudo se ocultan en el tráfico cifrado, lo que subraya la importancia de inspeccionar todo el tráfico web y no web, o de lo contrario puede permitir que, sin usted saberlo, entre malware a su red.

Como función esencial de la pila de seguridad, los sandboxes son medidas preventivas frente a los archivos maliciosos y la ejecución de código. Están pensados para ser una defensa eficaz frente a ataques desconocidos basados en archivos que buscan evadir EDR y otros análisis en busca de malware conocido. Lamentablemente, muchos entornos sandbox se implementan fuera de banda y dependen de que se les envíen muestras de malware desde NGFW, productos de seguridad en la nube o agentes de terminales.

Esto a menudo significa que la detección ocurre después de que el malware se ha descargado en el dispositivo del usuario, lo que permite infecciones de malware o ransomware en el paciente cero, y ciertamente no cumple con los conceptos de zero trust. Además, muchos entornos sandbox no aprovechan el análisis de IA/ML a gran escala para detectar y poner en cuarentena automáticamente amenazas desconocidas y archivos sospechosos, un factor clave para brindar defensa del paciente cero en línea sin interrumpir la productividad.

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

Requisitos de sandbox en la nube

Hasta ahora, los adversarios tenían la ventaja de poder explotar la arquitectura cambiante en el entorno en la nube.

Elegir el sandbox en la nube adecuado es esencial para evitar las infecciones de paciente cero y hacer que las amenazas persistentes avanzadas no puedan acceder a su red.

La siguiente sección pretende ayudarle a comprender los requisitos que debería tener en cuenta al seleccionar un sandbox en la nube.

Descifrado e inspección a escala

El cifrado se ha convertido en una tendencia de seguridad prometedora, dado que permite realizar comunicaciones privadas y proteger los datos confidenciales. Por desgracia, los cibercriminales se aprovechan del tráfico cifrado para ocultar cargas útiles maliciosas.

Descifrar e inspeccionar el tráfico es un proceso que requiere un uso intensivo de recursos informáticos y puede convertir a los dispositivos sandbox de alto rendimiento en lentos bloqueos, interrumpiendo con ello el negocio con una latencia inaceptable.

Al evaluar una solución de sandbox moderna, es importante encontrar proveedores que puedan descifrar sin latencia, carezcan de limitaciones y puedan inspeccionar en línea.

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 los elementos a comprar:

- ☐ No es preciso instalar hardware o máquinas virtuales (VM) adicionales para descifrar el tráfico SSL
- ☐ Inspección y análisis de los siguientes tipos de archivos sin latencia ni límites de capacidad:

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

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

Lista de los elementos a comprar:

- Aplicación inmediata de las políticas para todos los usuarios (protección idéntica para todos), ya estén dentro o fuera de la red corporativa.
- Reglas y capacidades de cuarentena avanzada para todos los archivos de procedencia sospechosa.
- 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

Gestión y reglas de política centralizadas

Evite la mala gestión de las reglas y la configuración manual de los entornos aislados en cada puerta de enlace con la gestión de políticas y las reglas centralizadas entregadas en la nube. Considere soluciones con políticas adaptables y dinámicas que sigan los principios de zero trust descritos por **NIST 800-207**. Al establecer políticas de acceso y seguridad basadas en el contexto (incluido el rol y la ubicación del usuario, la postura del dispositivo y los datos solicitados), zero trust minimiza las superficies de ataque. Las soluciones entregadas en la nube tienen ventajas adicionales que pueden permitirle bloquear amenazas en todos los usuarios de la organización. Hacerlo significa que ya no hay más retrospectivas de archivos (ejemplos: inspecciones fuera de banda y protecciones aplicadas después del hecho) para una seguridad que está más sincronizada. Un aspecto fundamental de la política de entornos aislados es que ofrece la flexibilidad para respaldar el negocio, 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 las políticas con la tolerancia al riesgo y las expectativas de rendimiento

Una solución de sandbox en la nube debería controlar los riesgos y aplicar políticas que se ajusten a las necesidades exclusivas de su organización. Empiece determinando si tiene:

- **Baja tolerancia a archivos maliciosos:** para las organizaciones que evitan los riesgos, puede elegir Cuarentena para acción inicial para archivos desconocidos o sospechosos, lo que garantizará que no haya infecciones del paciente cero porque el entorno limitado analizará el archivo antes de que pueda descargarse.
- **Baja tolerancia para poner en cuarentena archivos:** para las organizaciones tolerantes a riesgos que desean evitar demoras e interrupciones, puede elegir Cuarentena y aislamiento como acción inicial. Esta acción integra el entorno aislado con las capacidades de aislamiento del navegador en la nube, lo que proporciona a los usuarios acceso inmediato a un PDF de solo lectura sin contenido activo mientras el entorno aislado analiza archivos potencialmente dañinos en segundo plano.

Independientemente de cuáles sean sus necesidades, las políticas deberían ser fáciles de aplicar a todos los usuarios, grupos, departamentos, ubicaciones y grupos de ubicaciones desde una única plataforma.

Análisis inteligente e información sobre amenazas

Se sabe que los adversarios reutilizan los ataques que han tenido éxito, 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 esto al capturar 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 impulsado por IA

Los sandboxes proporcionados en la nube son capaces de soportar los modelos de IA/ML, que consumen muchos recursos informáticos, para conseguir una protección superior.

Busque un sandbox que identifique, ponga en cuarentena y prevenga de forma inteligente amenazas desconocidas o sospechosas en línea mediante IA/ML avanzados sin necesidad de analizar de nuevo los archivos benignos.

- **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 previenen las infecciones del paciente cero poniendo en cuarentena las amenazas desconocidas antes de permitir su descarga.

Flujos de trabajo SOC con inteligencia sobre amenazas

Los analistas pueden pasar muchas horas al día investigando una sola amenaza. Busque un 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 el 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 los marcos de ciberseguridad como MITRE ATT6CK®.

Lista de los elementos a comprar:

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

Asegúrese de elegir un sandbox que pueda proporcionar más de una puntuación de la amenaza. Plantéese elegir un sandbox que pueda señalar las técnicas evasivas utilizadas, como por ejemplo:

- Retraso de la ejecución de código para evitar la detección de sandbox.
- Captura y vista del tráfico según fluye por la red.
- Apertura de puertos para permitir la conexión remota.
- Intento de moverse lateralmente para encontrar activos de alto valor.
- Intento de permitir el control remoto.

Generación de informes

Las soluciones de seguridad con generación de informes son útiles en la medida en que sean prácticas. Los informes de sandbox en la nube deben:

- Incluir la totalidad del ciclo de vida del ataque malicioso.
- Ser fácil de usar y explorar.
- Ser fácil de resumir.
- Estar disponible a través de una interfaz de programación de aplicaciones (API) para poderla relacionar con los registros existentes.
- Formar parte de una plataforma más grande que también admita la generación de informes de cumplimiento.

Mejora de su SOC con el marco MITRE ATT&CK

Cuando evalúe las capacidades de generación de informes, tenga en cuenta que la inteligencia del sandbox pueda clasificarse según **el marco MITRE ATT&CK**. Con esta capacidad, los equipos de SOC pueden aplicar la información que se les ha proporcionado para crear defensas tácticas en otras partes de la pila de seguridad. De esta forma, el sandbox es una parte integral de los flujos de operaciones de seguridad.

En función de su experiencia con el marco, puede usar la generación de informes para una gran cantidad de fines:

- Reducir la carga que supone etiquetar empleando la taxonomía proporcionada.
- Ver qué técnicas sigilosas podrían estar eludiendo su solución de detección y respuesta en puntos finales (EDR).
- Comparar y contrastar otros controles.
- Centrarse en las TTP más comunes que se dirigen a su organización en lugar de prevenir todas las tácticas y técnicas sin tener un objetivo claro.
- Llevar a cabo un informe de ingeniería inversa.

Preguntas que hacer antes de comprar

Para ayudarle a tomar su decisión, aquí tiene un compendio de preguntas clave y las razones por las que preguntarlas:

¿El sandbox permite infecciones iniciales del paciente cero, aunque sea solo una?

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

¿La solución cubre 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 NGFW o implicar software EDR de terminal.

¿El sandbox examina el tráfico en protocolos HTTP, HTTPS, FTP y FTP sobre HTTP? ¿Hay limitaciones?

Es importante examinar el tráfico para desvelar el malware sigiloso. Un sandbox entregado en la nube podría ser mejor para inspeccionar todo el tráfico sin latencia.

¿Cumple con las leyes y regulaciones pertinentes, incluidos los requisitos de zero trust?

Las regulaciones de cumplimiento pueden tener requisitos estrictos sobre cómo se maneja el sandbox y sobre asuntos en materia de retención/privacidad. Es importante encontrar una solución que funcione sólo en la memoria y elimine la información identificable durante el análisis para cumplir con estos requisitos. Además, considere si las soluciones se adhieren a los principios de zero trust establecidos por los estándares globales NIST 800-207 y utilícelos como guía para reducir las superficies de ataque y proteger los datos.

¿Con qué otros módulos de seguridad trabaja el sandbox?

Ningún producto le puede proteger por completo de las amenazas avanzadas persistentes (APT). Por ello, se necesita un enfoque multicapa que abarque la prevención, la mitigación, la detección y la respuesta de amenazas. El sandbox es una capa integral y, como tal, debe funcionar bien con otros módulos y soluciones.

---

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

Zscaler Cloud Sandbox y protección contra amenazas avanzadas

Es hora de tener un verdadero sandbox nativo de la nube y en línea

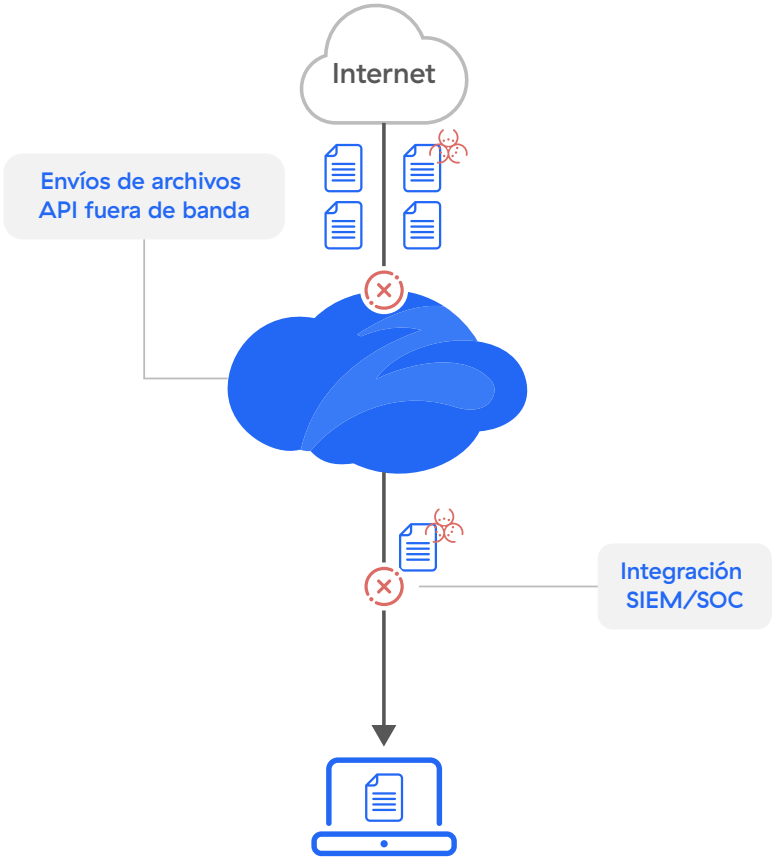
Nunca ha habido mejor momento que este para optar por un sandbox nativo de la nube y en línea, ahora que las organizaciones se enfrentan a superficies de ataque ampliadas y que los adversarios se están aprovechando de las brechas en las pilas de seguridad heredadas. Zscaler Cloud Sandbox se ha construido específicamente para atrapar y detener las amenazas modernas a la vez que asegura que todos los usuarios tengan una protección contra el malware de día cero en todas las ubicaciones.

Al estar construido sobre una arquitectura basada en proxy y nativa de la nube, Zscaler Cloud Sandbox es el primer motor de prevención del malware impulsado por la IA del mundo que automáticamente detecta, previene y pone en cuarentena de forma inteligente las amenazas desconocidas y los archivos sospechosos en línea. Gracias a su capacidad ilimitada y que no genera latencia para inspeccionar la web y los protocolos de transferencia de archivos (FTP), incluidos SSL y TLS, el sandbox en la nube puede llevar a cabo análisis dinámicos profundos y en tiempo real para asegurar que ningún archivo desconocido llegue al usuario como descarga de un archivo malicioso.

Ventaja de Zscaler Sandbox AI: con información procedente de más de 500 millones de muestras, con actualizaciones de seguridad en tiempo real provenientes de 300 billones de señales diarias.

La cuarentena impulsada por IA detiene el malware nunca visto

IProtección en línea con entrega instantánea de archivos benignos, defensa del paciente cero y controles de políticas granulares



Reducción de la complejidad y los costes

- Fácil de implementar, no hay que administrar hardware ni software.
- Elimine los productos puntuales redundantes y desconectados.
- Acabe con el retorno del tráfico de Internet a través de MPLS o VPN.

Protección inmediata y adaptable para todos los usuarios y ubicaciones

- Defina políticas globales en una única consola centralizada.
- Aplique inmediatamente cambios en la política.
- Identifique las amenazas una sola vez y bloquéelas inmediatamente para todos los clientes.

Descubra amenazas ocultas

- Detenga las infecciones de paciente cero y las amenazas emergentes con la cuarentena basada en IA.
- Cargar archivos para análisis (portal de comprobación de archivos)

Plataforma integrada entregada como servicio

- Filtrado previo de todas las amenazas conocidas utilizando antivirus, listas de bloqueo de hash, reglas YARA de clasificación del malware, detecciones automatizadas mediante toma de huellas JA3 y modelos de IA/ML.
- Las fuentes del Collective Intelligence Framework (CIF) permiten a Zscaler integrar más de 60 fuentes de amenazas, además de la propia fuente de amenazas de Zscaler, obtenidas mediante las miles de millones de transacciones de su base de clientes
- Combine un sandbox en la nube con una solución EDR para aumentar la eficacia de la seguridad y mitigar el acceso inicial, la ejecución y las tácticas persistentes.

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

- Análisis estático, dinámico y secundario, incluido el análisis de código y análisis de carga útil secundario.
- Inspección de SSL ilimitada y sin latencia.
- Protección del tráfico entrante y saliente
- Mejore la investigación y la respuesta de seguridad con análisis forense en profundidad de archivos API que incluye usuarios, origen de la ubicación, tácticas de evasión, etc.

Zscaler Cloud Sandbox™es una funcionalidad totalmente integrada de Zscaler Internet Access y forma parte de Zscaler Zero Trust Exchange™.

Para obtener más información, visite
zscaler.com/es/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. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de los usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en línea en la nube del mundo. Si desea más información, visite **www.zscaler.com/es**.

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