Libro electrónico

La guía del comprador de soluciones para la prevención de amenazas

Encuentre la solución de protección contra amenazas avanzada y basada en archivos que mejor se adapte a sus necesidades.

Contenido

Replanteo de la seguridad ante el panorama actual de amenazas

La seguridad del perímetro solamente es demasiado arriesgada para el mundo digital

El cambio hacia el trabajo híbrido y las aplicaciones alojadas en la nube han cambiado la manera de acceder a los recursos empresariales. Los usuarios 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 en la nueva red corporativa. Esto amplía su perímetro a miles, lo que hace que el modelo de seguridad castle-and-moat sea inadecuado para proteger a sus usuarios, aplicaciones y datos. Seguir confiando únicamente en controles basados en el perímetro introduce riesgos porque se dejan de lado las defensas centradas en la red en favor del acceso directo a internet y la facilidad de uso.

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:

- Los ataques de ransomware han **aumentado un 80 %** año tras año.[1]
- Las técnicas multifacéticas de extorsión están aumentando, y el ransomware de doble extorsión ha aumentado en un **117 %**.[1]
- Los ataques de phishing aumentaron un **29 %** en 2021 en comparación con 2020.[2]
- **El 85 %** de las organizaciones experimentaron un ciberataque exitoso en 2021.[3]
- **El 63 %** de las víctimas de ransomware pagaron los rescates en 2021, alentando a los ciberdelincuentes a aumentar sus ataques.[3]

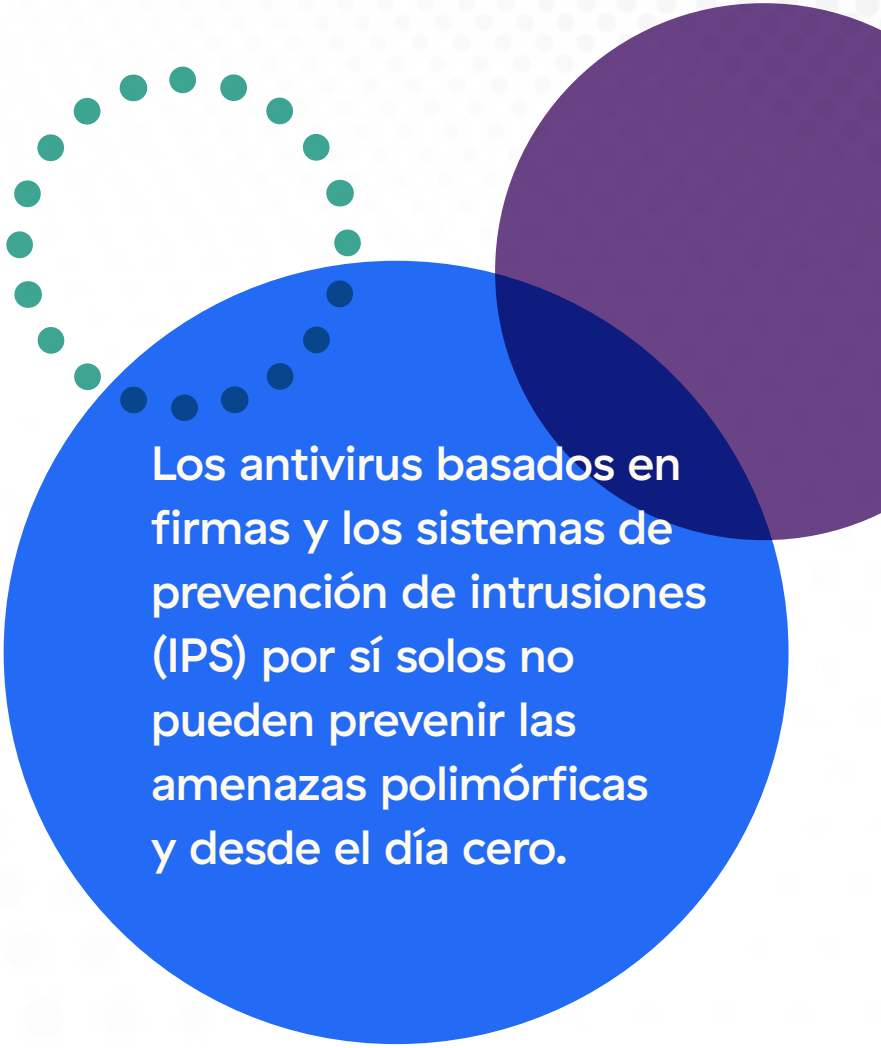
1. https://www.zscaler.com/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.com/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

Se necesita evolucionar hacia la protección contra malware desde el día cero

Los atacantes tienen dos ventajas: **velocidad** y **proliferación**. Los desarrolladores de malware están creando amenazas más rápido de lo que los encargados de la defensa pueden definirlas, extendiéndolas y transformándolas para evadir la detección.

El phishing con archivos adjuntos o enlaces maliciosos sigue siendo el mecanismo de distribución más común en la actualidad. Dado que las amenazas se esconden en el tráfico cifrado, si no está inspeccionando todo el tráfico web y no web, incluidos los protocolos de transferencia de archivos y SSL/TLS, es posible que deje involuntariamente, que el malware se infiltre en su red y permita que los atacantes exfiltren datos confidenciales o exijan un rescate.

Como función crítica en la pila de seguridad, los sandboxes son una medida de prevención contra archivos maliciosos y ejecuciones de código. Están destinados a ser la última línea de defensa y el primer punto de detección en las investigaciones contra amenazas desconocidas. Lamentablemente, los dispositivos de sandbox heredados están fuera de banda y requieren dispositivos adicionales para el descifrado y la inspección SSL. Dado que la protección se aplica una vez que el malware ya ha pasado por el usuario o el dispositivo, no se puede lograr zero trust.



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

La siguiente sección tiene como objetivo ayudarle a comprender los requisitos específicos que debe considerar al seleccionar un 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.

Ddescifrar e inspeccionar el tráfico es un proceso de computación intensiva y es la práctica más reciente. Los sandboxes heredados con arquitectura de paso permiten involuntariamente la infiltración del malware entre el tráfico no inspeccionado. Los dispositivos de inspección de SSL dedicados y agregados pueden ayudar, pero como todos los dispositivos, carecen de la capacidad de escalar, lo que causa una expansión costosa de dispositivos mientras que se siguen filtrando las infecciones de paciente cero por las redes.

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 han aumentado más del 314 % año tras año, superando el aumento del 250 % por segundo año consecutivo.[4]

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	XLX(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	

4. *https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks*

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
- ☐ Administración de políticas centralizadas
- ☐ Controles granulares para archivos de greyware y adware

Reglas y administración de políticas centralizadas

Evite la administración incorrecta de reglas y la configuración manual de sandboxes en cada puerta de enlace con reglas y administración de políticas centralizadas y distribuidas en la nube. Considere soluciones con políticas adaptativas y dinámicas que sigan los postulados de tero 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 que se distribuyen en la nube tienen beneficios adicionales que pueden permitirle bloquear amenazas en todos los usuarios de la organización una vez identificada una amenaza. Hacerlo significa que las retrospectivas de archivos (ejemplos: inspecciones fuera de banda y protecciones después del hecho) ya no son necesarias para ofrecer una seguridad más sincronizada.

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 hacer cumplir las políticas que se adaptan a las necesidades únicas de su organización. Comience por determinar si tiene:

- **Baja tolerancia a archivos maliciosos:** para las organizaciones que evitan riesgos, puede elegir la acción de poner en cuarentena por primera vez los archivos desconocidos o sospechosos.
- **Baja tolerancia para poner archivos en cuarentena:** para las organizaciones tolerantes al riesgo que desean evitar retrasos e interrupciones, puede elegir la acción de permitir y analizar por primera vez. Para una protección adicional, considere la posibilidad de integrar las capacidades de aislamiento del navegador en la nube para reproducir el archivo como una imagen y evitar la fuga de datos y la distribución de amenazas activas.

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 inteligencia de amenazas

Se sabe que los atacantes reutilizan ataques exitosos, por lo que es esencial compartir protecciones con la comunidad de seguridad para detener rápida e inmediatamente las amenazas. Los sandboxes en la nube desempeñan un papel importante a la hora de capturar datos de telemetría y compartir información de amenazas recientemente identificadas con fuentes de amenazas y con la comunidad de seguridad.

Motor de prevención de malware con IA

Los sandboxes distribuidos en la nube pueden administrar modelos de IA y ML con una capacidad de computación intensiva para obtener 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 analizar archivos benignos.
Esto asegura:

- **Decisiones más rápidas con respecto a los archivos:** Al enrutar inmediatamente los archivos benignos y analizar los archivos sospechosos o desconocidos, puede beneficiarse de un menor trabajo manual.
- **Prevención desde el día cero:** Al poner en cuarentena las amenazas desconocidas sin trabajo adicional, puede evitar que los días cero se conviertan en una amenaza mayor para su entorno.

Flujos de trabajo SOC con inteligencia de 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 de comportamiento e inteligencia de amenazas sobre cargas útiles maliciosas. Asegúrese de que las fuentes de amenazas estén integradas en sus herramientas de seguridad existentes. Deben incluir: contexto actualizado sobre las URL reportadas, indicadores de compromiso extraídos (IOC) y tácticas, técnicas y procedimientos (TTP) que cumplan con los marcos de ciberseguridad como MITRE ATT&CK®.

Lista de control de compras:

- ☐ Capacidades de ML/AI que se integran estrechamente con el proceso de análisis
- ☐ Capacidades de cuarentena que utilice IA y que puedan aprovechar ML/AI para retener archivos potencialmente maliciosos, analizarlos y emitir veredictos rápidos a la velocidad de la máquina
- ☐ Contribución autónoma a las protecciones diarias contra amenazas compartidas entre usuarios y redes independientemente de la ubicación
- ☐ Capacidad para compartir datos forenses y presentar veredictos mediante una plataforma
- ☐ Integración de la fuente de amenazas con las herramientas de seguridad existentes

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

Generación de informes

Las soluciones de seguridad con generación de informes son útiles cuando permiten tomar decisiones. Los informes de sandboxing en la nube deben:

- Incluir todo el ciclo de vida de los ataques maliciosos
- Ser fáciles de usar y de navegar
- Ser fáciles de incorporar
- Estar disponibles a través de una interfaz de programación de aplicaciones (API) para que se pueden correlacionar 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

Al evaluar las capacidades de generación de informes, considere inteligencia del sandbox que pueda mapear al **marco MITRE ATT&CK**. Con esta capacidad, los equipos del SOC pueden aplicar los conocimientos proporcionados para construir defensas tácticas en otras partes de la pila de seguridad. De esta manera, 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 con 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 que debe hacer 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 solución protege a todos los usuarios y sus dispositivos, independientemente de su ubicación?
Sus usuarios pueden estar accediendo a recursos corporativos sobre la marcha, en sus propios dispositivos o a través de redes no seguras. Es fundamental proteger todos los dispositivos que sean esenciales para sus tareas.[5]

¿La solución funciona en línea o en modo de punto de acceso de prueba (TAP)?
Las soluciones que funcionan en línea pueden identificar amenazas y bloquearlas directamente sin necesidad de crear nuevas reglas a través de dispositivos de terceros como firewalls.

¿Examina el sandbox 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. Un sandbox distribuido en la nube puede ser mejor para inspeccionar todo el tráfico sin latencia.

¿Cumple con las leyes y regulaciones pertinentes, incluyendo los requisitos de zero trust?
Las regulaciones de cumplimiento pueden tener requisitos estrictos sobre cómo se maneja sandboxing y en materia de retención de archivos/privacidad. Encontrar una solución que opere solo en la memoria y elimine la información identificable durante el análisis le ayuda a cumplir con estos requisitos. Además, considere si las soluciones cumplen con 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 funciona el sandbox?
Ningún producto puede proteger completamente contra las amenazas persistentes avanzadas (APT). En cambio, se requiere un método multicapa de prevención de amenazas, mitigación, detección y respuesta. El uso de sandbox es una capa integral y, como tal, debe funcionar bien con otras soluciones y módulos.

¿La solución complementa los sandboxes proporcionadas por el proveedor o sandboxing de EDR?
Una verdadera estrategia de defensa en profundidad puede requerir soluciones complementarias y protección por capas para interrumpir adecuadamente la cadena de muerte del malware que podría ser devastadora para su organización. Si falla un nivel en su ecosistema, puede contar con otro. El punto final, la red, y el control de políticas deben funcionar armoniosamente juntos para detener a los atacantes.

5. https://image-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 un verdadero sandbox en línea nativo y en la nube

Mientras que las organizaciones se ocupan de las superficies de ataque más grandes y los atacantes aprovechan los puntos débiles de la pila de seguridad heredada, nunca ha habido un mejor momento para elegir un verdader sandbox nativo en la nube en línea. Zscaler Cloud Sandbox está diseñado 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.

La solución Zscaler Cloud Sandbox está construida sobre una arquitectura nativa de la nube basada en proxy y es el primer motor de prevención de malware que utiliza la IA del mundo y 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 el 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 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
- Ponga en práctica inmediatamente los cambios de política
- 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
- Las fuentes del marco de inteligencia colectiva (CIF, por su sigla en inglés) permiten a Zscaler integrarse con más de 60 fuentes de amenazas, además de la fuente de amenazas propia de Zscaler, impulsada por miles de millones de transacciones 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 halló que Zscaler Zero Trust Exchange creaba una reducción del 90 % en los dispositivos de seguridad.[6]

- 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 una rica investigación forense, incluidos el usuario, el origen de la ubicación, las tácticas evasivas y más

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

Para obtener más información, visite **zscaler.com/custom-product-demo.**

6. https://info.zscaler.com/resources-industry-report-esg-economic-validation

Experience your world, secured.™

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 al conectar de forma segura a los usuarios, dispositivos y aplicaciones 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. Obtenga más información en **zscaler.com** o síganos en Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com