Libro electrónico

La guía de prevención de amenazas del CISO

Encuentre la mejor solución de protección contra las amenazas avanzadas y basadas en archivos.

Índice

Reconsiderar la seguridad para el panorama de amenazas actual

La seguridad que solo 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. Al hacerlo, amplían su perímetro a otras miles de personas, por lo que la seguridad de castillo y foso es inadecuada para proteger a sus usuarios, sus aplicaciones y sus datos. Seguir confiando únicamente en los controles que se basan en el perímetro introduce riesgos, ya que las defensas centradas en la red se evitan para acceder directamente a Internet y obtener una facilidad de uso.

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:

- Los ataques de ransomware **han aumentado un 80 %** de un año a otro.[1]
- Las técnicas de extorsión polifacéticas siguen creciendo y el ransomware de doble extorsión ha aumentado un **117 %**.[1]
- Los ataques de phishing **aumentaron un 29 %** en 2021 en comparación con 2020.[2]
- **El 85 %** de las organizaciones sufrió un ataque que tuvo éxito en 2021.[3]
- **El 63 %** de las víctimas de ransomware pagaron rescates en 2021, lo que animó a los cibercriminales a llevar a cabo más ataques.[3]

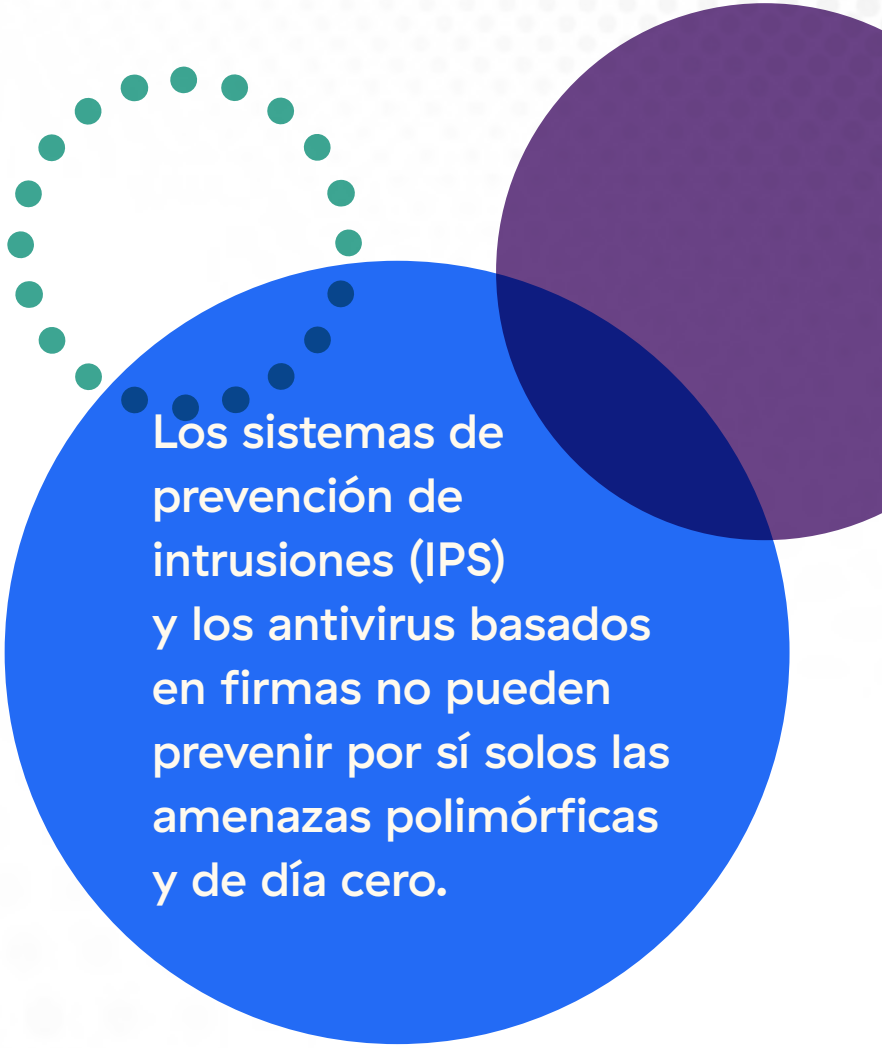
1. https://www.zscaler.es/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.es/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

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

Los adversarios cuentan con dos ventajas: **la velocidad** y **la proliferación**. Los desarrolladores de malware están creando amenazas más rápido de lo que los defensores pueden definirlas, y se expanden y cambian de forma para evadir la detección.

El phishing con archivos adjuntos o enlaces maliciosos sigue siendo el método de entrega más común en la actualidad. Ya que las amenazas se ocultan en el tráfico cifrado, si no inspecciona todo el tráfico (ya sea web o no web), incluidos los protocolos de transferencia de archivos y SSL/TLS, puede que, sin saberlo, esté dejando entrar al malware en su red y permitiendo que los adversarios exfiltren datos confidenciales o exijan un rescate.

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 la última línea de defensa y el primer punto de detección para las investigaciones de amenazas desconocidas. Desgraciadamente, los dispositivos de sandbox heredados son fuera de banda y requieren servicios adicionales para que descrifren e inspeccionen el SSL. Como la protección se aplica una vez que el malware ya ha pasado a través de un usuario o dispositivo, no sirve para tener una confianza 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.

Al ser una práctica novedosa, descifrar e inspeccionar el tráfico es un proceso que requiere un gran esfuerzo informático. Los sandboxes heredados con arquitecturas de paso permiten involuntariamente que el malware se cuele en el tráfico sin inspeccionar. Los dispositivos de inspección de SSL adicionales y dedicados pueden ser de ayuda, pero al igual que todos los dispositivos, carecen de la habilidad para ajustarse, por lo que causan una proliferación de dispositivos costosa mientras las infecciones de paciente cero continúan introduciéndose en las redes.

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 han aumentado más de un 314 % con respecto al año anterior, y han superado un crecimiento del 250 % por segundo año consecutivo.[4]

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	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 de script en archivos ZIP
SWF	BZ2	

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

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
- ☐ Controles granulares para los archivos de tipo greyware y adware.

Gestión y reglas de política centralizadas

Evite administrar incorrectamente las reglas y configurar manualmente los sandboxes en cada puerta de enlace con la gestión y las reglas de políticas centralizadas y proporcionadas en la nube. Tenga en cuenta soluciones con políticas adaptables y dinámicas que sigan los principios de confianza cero que enumera la norma **NIST 800-207**. Al establecer el acceso y las políticas de seguridad basándose en el contexto (que incluye el rol del usuario y la ubicación, la postura del dispositivo y los datos solicitados), la confianza cero minimiza las superficies de ataque. Las soluciones que se proporcionan en la nube garantizan ventajas adicionales que le podrían permitir bloquear las amenazas para todos los usuarios de la organización cuando se identifica una amenaza. Hacerlo significa que no habría que analizar archivos de forma retroactiva (por ejemplo, no habría que hacer inspecciones fuera de banda ni aplicar protecciones tras el evento), dado que la seguridad disfruta de mayores niveles de sincronía.

Los controles granularen 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 los archivos maliciosos:** para las organizaciones que evitan a toda costa el riesgo, puede seleccionar que su primera acción sea poner en cuarentena a los archivos desconocidos o sospechosos.
- **Baja tolerancia a la cuarentena de archivos:** para las organizaciones tolerantes al riesgo que quieren evitar los retrasos e interrupciones, puede seleccionar que su primera acción sea permitir y escanear. Si quiere obtener una protección adicional, considere la posibilidad de integrar capacidades de aislamiento del navegador en la nube para que el archivo se represente en forma de imagen y evitar así la filtración de datos y la entrega de amenazas activas.

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 inteligencia sobre amenazas

Se sabe que los adversarios reutilizan ataques exitosos, por lo que es esencial compartir las protecciones con la comunidad de seguridad para detener de inmediato las amenazas. Los sandboxes en la nube juegan un importante papel en este aspecto porque capturan los datos de telemetría y comparten información de las amenazas nuevas identificadas con las fuentes 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. De esa forma, obtendrá:

- **Veredictos más rápidos sobre los archivos:** al enrutar los archivos benignos inmediatamente y analizar los desconocidos o sospechosos, tendrá menos trabajo que hacer.
- **Prevención de ataques de día cero:** al poner en cuarentena las amenazas desconocidas sin tener que hacer nada más, puede evitar que las amenazas de día cero se conviertan en una amenaza mayor para su entorno.

Flujos de trabajo SOC con inteligencia sobre amenazas

Los analistas pueden pasarse muchas horas al día investigando una sola amenaza. Busque un sandbox en la nube que reduzca ese tiempo y acelere la investigación y la respuesta compartiendo información sobre el comportamiento y la inteligencia sobre amenazas relacionada con las cargas útiles maliciosas. Asegúrese de que las fuentes de amenazas se integren con sus herramientas de seguridad existentes. Estas deberían incluir: contexto actualizado sobre las URL reportadas, indicadores de compromiso (IOC) extraídos y tácticas, técnicas y procedimientos (TTP) que estén en consonancia con marcos de ciberseguridad como el MITRE ATT&CK®.

Lista de los elementos a comprar:

- ☐ Capacidades de ML/IA que se integren estrechamente con el proceso de análisis.
- ☐ Capacidades de cuarentena basada en IA que puedan aprovechar el ML/la IA para retener y analizar los archivos potencialmente maliciosos y que emitan veredictos rápidos, a la velocidad de la máquina.
- ☐ Contribución autónoma a las protecciones diarias contra amenazas compartidas con todos los usuarios y las redes, independientemente de la ubicación.
- ☐ Capacidad de compartir datos forenses y veredictos de archivos a través de una plataforma.
- ☐ Integración de las fuentes de amenazas con las herramientas de seguridad existentes.

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 tan útiles como accionables. La generación de informes de un sandbox en la nube debe contar con las siguientes características:

- Incluye el ciclo de vida entero 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 que proporciona.
- 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:

¿La solución protege a todos los usuarios y sus dispositivos, independientemente de dónde se encuentren?

Sus usuarios podrían estar accediendo a recursos corporativos cuando están viajando, a través de sus propios dispositivos o de redes no protegidas. Es de suma importancia proteger todos los dispositivos esenciales para realizar sus actividades.[5]

¿La solución opera en línea o en modo Test Access Point (TAP)?

Las soluciones que operan en línea pueden identificar las amenazas y bloquearlas directamente sin tener que crear nuevas reglas a través de dispositivos de terceros, como cortafuegos.

¿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 normativas relevantes, incluidos los requisitos de confianza cero?

Puede que las normativas de cumplimiento tengan requisitos estrictos sobre cómo emplear el sandbox y sobre las cuestiones de almacenamiento/privacidad. Una solución que opere solo en la memoria y extraiga la información identificable durante el análisis le ayudaría a cumplir con esas normativas. Además, considere si la solución cumple con los principios de confianza cero de la norma global NIST 800-207, y utilícelos como guía para reducir la superficie 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.

¿La solución complementa sandboxes de proveedores o sandboxes de EDR?

Una verdadera estrategia de defensa en profundidad podría necesitar soluciones complementarias y protección por capas para acabar adecuadamente con la cadena de cierre del malware que podría devastar su organización. Así, si un nivel de su ecosistema falla, puede contar con otro. Los controles de puntos finales, redes y políticas deben funcionar en armonía para detener a los adversarios.

5. https://image-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

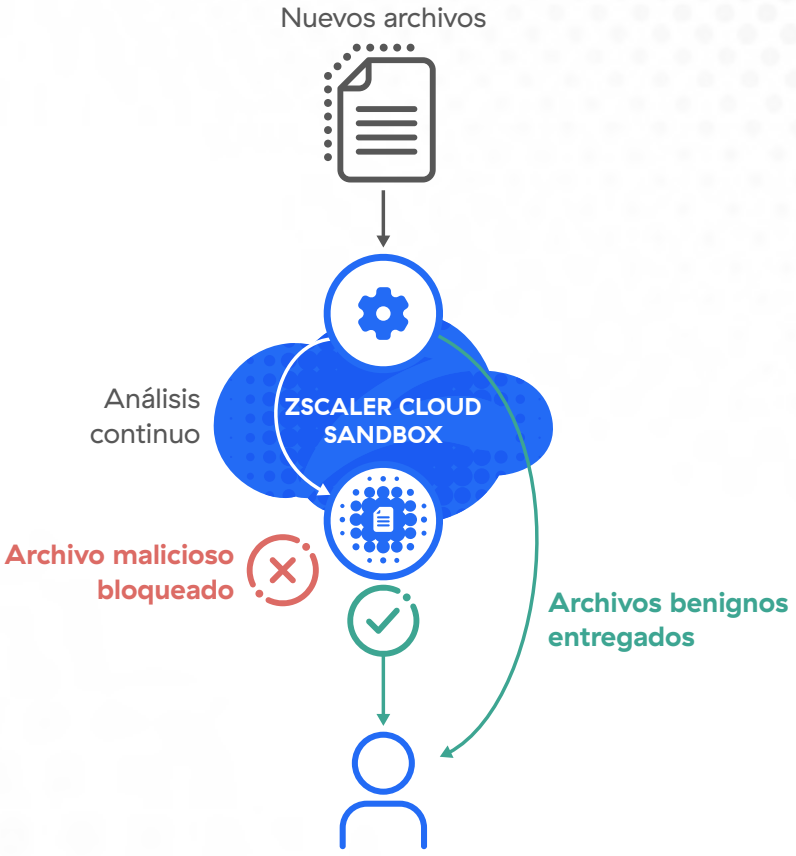
Es hora de tener un verdadero sandbox nativo de la nube y en línea

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.

La cuarentena impulsada por IA detiene el malware nunca visto

Protección 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, producida 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 de ESG descubrió que Zscaler Zero Trust Exchange consiguió reducir en un 90 % los dispositivos de seguridad.[6]

- 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
- Mejora de la investigación y la respuesta de seguridad con análisis forense en profundidad que incluye usuarios, orígenes y las de evasión, etc.

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

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

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

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 mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

+1 408.533.0288

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

zscaler.es