Ficha de datos

Zscaler Sandbox

El primer motor de cuarentena, prevención y detección de malware impulsado por IA del mundo

Zscaler Sandbox previene infecciones de paciente cero y bloquea el acceso a su red de amenazas persistentes avanzadas.

En el mundo actual, en el que los dispositivos móviles y la nube son lo primero, sus usuarios acceden a archivos sobre la marcha directamente desde Internet y aplicaciones SaaS. Atrás quedaron los días en los que se lanzaban clientes de correo electrónico desde la oficina corporativa rodeados de capas de seguridad. A medida que la demanda de facilidad de uso supera a las defensas centradas en la red, las organizaciones se quedan con una superficie de ataque ampliada justamente en una época en la que los ataques se vuelven más complicados y los adversarios se aprovechan de las brechas de seguridad heredadas.

En un esfuerzo por proteger los datos personales y comerciales confidenciales, casi todo el tráfico de Internet ahora está cifrado. Si bien esto ha disuadido a algunos ciberdelincuentes, el cifrado ha creado una falsa sensación de seguridad. Los sandboxes heredados con arquitectura de paso carecen de visibilidad y, sin querer, han permitido que archivos maliciosos se cuelen por las grietas escondiéndose en tráfico cifrado, libres de inspección profunda o cuarentena. Se pueden implementar dispositivos de descifrado SSL incorporados para ayudar; sin embargo, como ocurre con la mayoría del hardware, no logran escalar al ritmo necesario y aumentan los quebraderos de cabeza administrativos así como la costosa expansión de los dispositivos. Como resultado, las infecciones de paciente cero por malware desconocido continúan propagándose por las redes, dejando a los equipos de

Beneficios de Zscaler Sandbox:

- **Motor de prevención de malware promovido por IA** Identifique, ponga en cuarentena y evite de forma inteligente amenazas desconocidas o sospechosas en línea mediante IA/ML avanzados sin necesidad de analizar archivos benignos.
- **Inspección en línea completa para detectar ataques ocultos** Exponga y evite amenazas evasivas y malware que se ocultan en el tráfico cifrado a través de protocolos web y de transferencia de archivos sin límites de latencia y capacidad.
- **Prevención uniforme compartida globalmente** Consiga una protección automatizada frente a amenazas hasta ahora desconocidas con información sobre amenazas integrada y compartida con todos los usuarios en tiempo real.
- **Flujos de trabajo SOC aumentados con inteligencia de amenazas** Acelere la investigación y la respuesta compartiendo información sobre el comportamiento del malware, información sobre amenazas e informes avanzados mediante API potentes.
- **No más dispositivos físicos y software costosos** Implemente en segundos sin necesidad de comprar hardware ni software que administrar; simplemente configure e implemente una política de espacio aislado para ver el valor de inmediato.
- **Protección brindada en la nube con presencia global en el perímetro** Obtenga seguridad y experiencia de usuario totalmente integradas e inigualables con Zscaler Internet Access™ como parte de Zscaler Zero Trust Exchange™.

TI y de seguridad luchando por detener el movimiento lateral y la filtración de datos, que deberían haberse evitado en primer lugar.

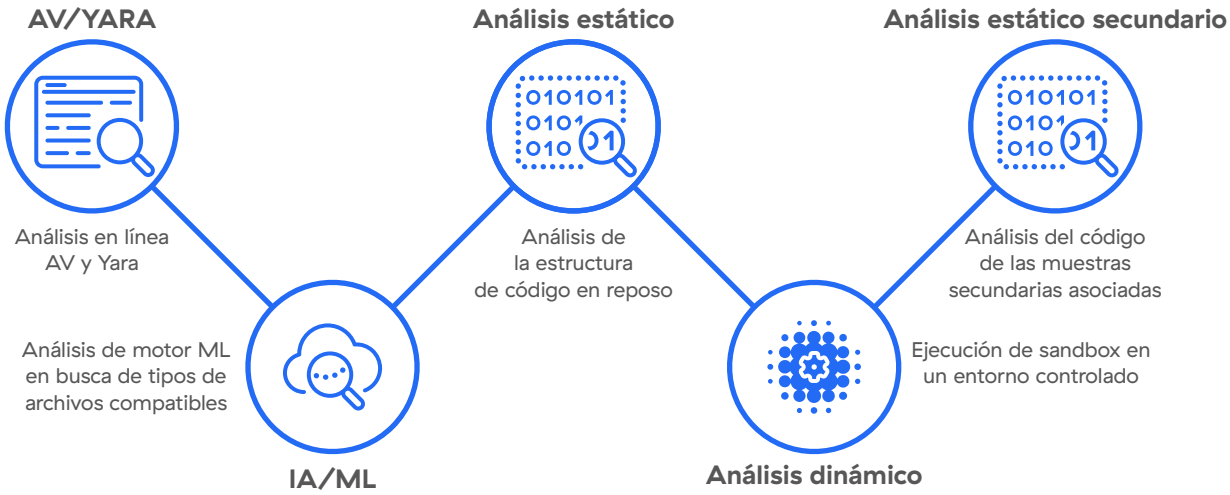
Zscaler Sandbox

Como función esencial de la pila de seguridad, los sandboxes son medidas preventivas frente a los archivos maliciosos y la ejecución de código. A diferencia de los entornos sandbox fuera de banda que brindan protección sólo después del compromiso inicial, Zscaler Sandbox está diseñado específicamente para detectar y detener amenazas modernas y esquivas que aprovechan las técnicas de evasión y explotan las debilidades tradicionales del sandbox.

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 IA del mundo que automáticamente detecta, previene y pone en cuarentena de forma inteligente amenazas desconocidas y 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 garantizar que ningún archivo desconocido llegue al usuario como descarga de un archivo malicioso.

El archivo desconocido o sospechoso pasa primero a través de un motor de análisis de filtrado previo que compara el contenido del archivo con más de 40 fuentes de amenazas, firmas antivirus, reglas YARA y modelos de IA/ML para emitir un veredicto rápido, bloqueando amenazas conocidas similares. Después de la clasificación inicial, el archivo se somete a un sólido análisis estático, dinámico y secundario que incluye la ejecución del archivo en un entorno controlado y aislado para llegar a un veredicto procesable. El último paso es el posprocesamiento, que actualiza la base de datos de amenazas de Zscaler y la aplicación de políticas del cliente.

Con los veredictos basados en IA, los archivos benignos se entregan instantáneamente mientras que los archivos maliciosos quedan bloqueados para todos los usuarios globales de Zscaler como resultado de la protección compartida del efecto de la nube. Esto detiene las infecciones de pacientes cero y las amenazas emergentes para todos los usuarios, independientemente del dispositivo o la ubicación.



Beneficios del sandbox de generación en la nube

Más allá de poner en cuarentena archivos sospechosos en línea, realizar análisis basados en IA en tiempo real y emitir veredictos instantáneos sin demoras, los informes avanzados detallados de Zscaler Sandbox pueden llevar el sandboxing desde la última línea de defensa hasta el primer paso en la acción basada en inteligencia. Al aplicar información sobre el comportamiento de malware real dirigido a su organización, puede enriquecer los flujos de trabajo de SecOps para fortalecer sus defensas en toda la pila de seguridad.

Detenga de forma inteligente las amenazas emergentes y las infecciones del paciente cero

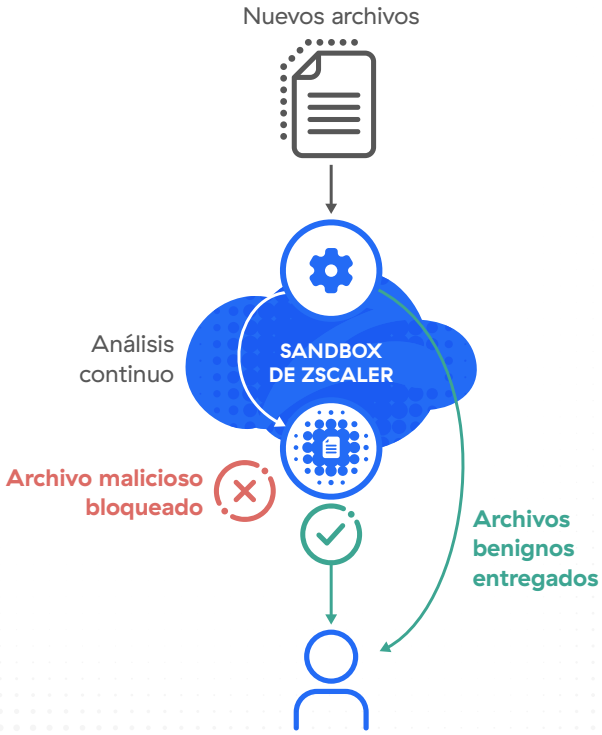
Los adversarios están aprovechando el cifrado y las aplicaciones confiables en la nube para realizar ataques sigilosos. De hecho, un informe reciente de ThreatLabZ observó que se estaba entregando malware desde Google Drive, AWS y OneDrive. La capacidad de analizar archivos a través de la web y FTP, en particular el tráfico cifrado, garantiza la visibilidad y evita que los atacantes obtengan acceso a su red.

Antes de que un empleado descargue y abra accidentalmente un nuevo documento malicioso de Office (Maldocs) con una macro oculta, se activa la función de cuarentena en línea impulsada por IA de Zscaler Sandbox. Cuando el análisis profundo del archivo arroja una calificación de amenaza alta, el archivo se bloquea para el empleado y ningún otro usuario de Zscaler puede acceder a él. Los veredictos instantáneos de archivos sin volver a analizar los archivos evitan la interrupción de la productividad de los empleados, mientras que la cuarentena y el bloqueo automáticos de archivos desconocidos o maliciosos

Después de una rápida implementación de veinte minutos de Zscaler Sandbox, el equipo de seguridad y TI de un cliente pudo entregar de forma segura e instantánea el 91 % de los archivos benignos a los usuarios después de recibir un veredicto basado en IA. Los archivos desconocidos restantes se enviaron para un análisis dinámico y en profundidad que reveló que 5 % de los archivos contenían malware o intenciones maliciosas. Los archivos quedan bloqueados para los usuarios previstos y para todos los usuarios y dispositivos globales de Zscaler, independientemente de su ubicación, para una protección compartida y consistente.

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



impiden lo que de otro modo sería una avalancha de tickets de asistencia técnica de TI.

Mejore los flujos de trabajo de SOC con información sobre malware y MITRE ATT&CK Después de un análisis profundo de archivos y de la detonación segura de malware desconocido, el sandbox genera automáticamente un informe de análisis. El entorno aislado y controlado de la zona de pruebas hace capturas de pantalla de análisis e informa a los analistas sobre el polimorfismo y las técnicas de evasión de ofuscación, el comportamiento de devolución de llamadas y otras acciones. Este informe detalla el ciclo de vida del ataque y la cadena de eliminación de eventos, el comportamiento del malware y la intención de la carga útil, y los asigna al marco MITRE ATT&CK.

Al poner en práctica los hallazgos del sandbox contextual con el marco ATT&CK, los equipos de seguridad y TI pueden compartir información sobre toda la pila de seguridad. Esto permite que el sandbox de generación en la nube no solo sea la última línea de defensa contra el malware, sino también el primer paso en la detección, acelerando la investigación y la respuesta al tiempo que fomenta el ejercicio de búsqueda de amenazas.

Gestión de políticas simplificada con controles granulares Como producto entregado en la nube, no hay hardware que comprar ni configurar ni software que administrar, lo que reduce la complejidad y los recursos. Sin necesidad de estar en las instalaciones de la empresa para configurar y conectar cada dispositivo, puede estar en funcionamiento con Zscaler Sandbox con una sencilla configuración de dos pasos: **criterios** y **acción**. Como beneficio adicional, las políticas son fáciles de administrar, configurar e implementar. Con unos pocos clics, los administradores pueden implementar políticas, incluido el orden de las reglas para una ejecución precisa y otras políticas que siguen a los usuarios o grupos de usuarios independientemente de su ubicación.

Para controles más granulares, el sandbox de generación en la nube puede mejorar el análisis de archivos estáticos y dinámicos con detección automatizada de huellas dactilares JA3 y configurar listas de bloqueo de hash personalizadas y reglas YARA. Además, las políticas de bloqueo basadas en puntuaciones pueden tomar medidas contra archivos de greyware y adware molestos o sospechosos que normalmente no superan el umbral de puntuación de amenaza.

Construido sobre una plataforma de confianza cero nativa de la nube, Zscaler Sandbox es una capacidad totalmente integrada de Zscaler Internet Access y parte de Zscaler Zero Trust Exchange. La arquitectura única basada en proxy protege a los usuarios en línea, no a posteriori, al dirigir el tráfico a la mayor pila de seguridad en la nube del sector para brindar protecciones inteligentes y profundas a cada usuario, independientemente de su ubicación o red. Obtenga protección global compartida con actualizaciones en tiempo real provenientes de 300 billones de señales de amenazas diarias combinadas con protección de generación de nube y principios de privilegios mínimos y confianza cero.

Standard Sandbox frente a Advanced Sandbox

	Standard Sandio	Advanced Sandbox	
Ediciones ZIA	Professional Edition Business Edition	Transformation Edition Edición ELA	**Advanced Sandbox puede ser un complemento de ZIA Professional y Business Edition**
Archivos compatibles	.exe, .dll,	.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, archivos de escritura en zips	
Cuarentena impulsada por IA	—	✓	
Políticas granulares	—	✓	
Informes	—	✓	
API	—	✓	

Funciones principales de generación de nube

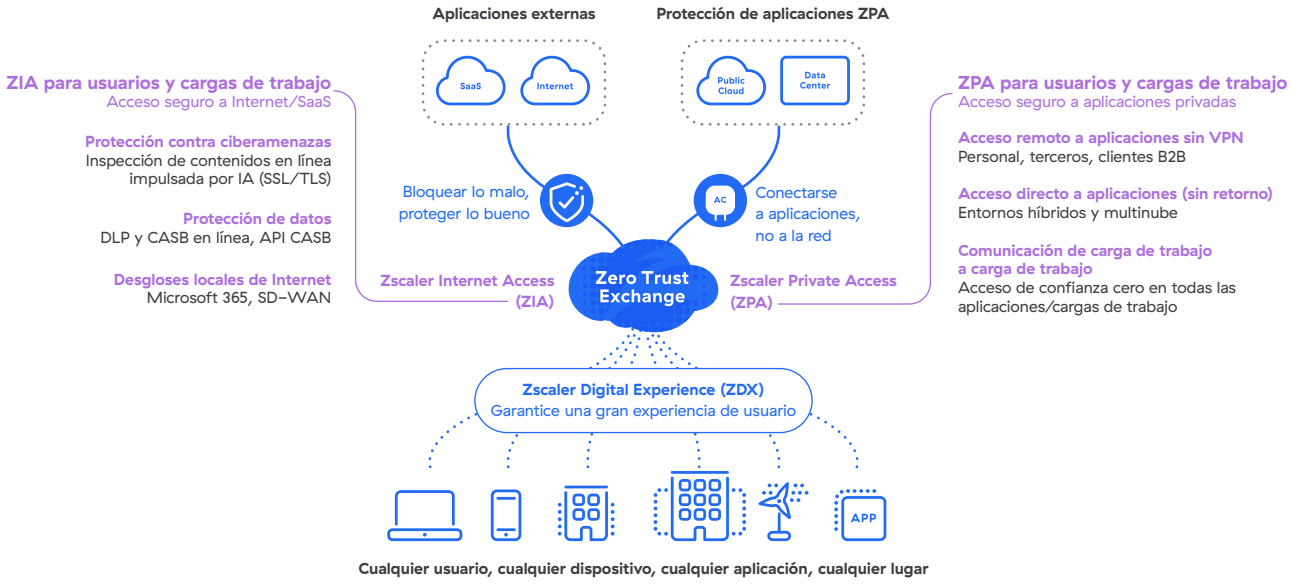
Motor de análisis de filtrado previo	AV, listas de bloqueo de hash, reglas YARA, detecciones automatizadas de huellas dactilares JA3 y modelos ML/IA
Análisis estático, dinámico y secundario	Análisis estático y análisis dinámico, incluido análisis de código y análisis de carga útil secundaria
Archivos compatibles	.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, archivos de escritura en zips
Inspección SSL	Capacidad ilimitada para inspección SSL/TLS
Retención de archivos	Zscaler Cloud Sandbox funciona únicamente en la memoria. Los archivos se despojan de información identificable durante el análisis. Una vez completado el análisis, los archivos benignos se eliminan de la memoria, mientras que los archivos maliciosos se cifran y almacenan indefinidamente, compartiendo información entre todos los usuarios de Zscaler para una protección continua.
Compatibilidad con OS	Windows XP, Windows 10, Android
Protocolos compatibles	HTTP, HTTPS, FTP, FTP por HTTP
Archivos por día	Ilimitado
Tamaño máximo de archivo	20 MB para Windows y 50 MB para Android
Método de implementación	Nativo de la nube
Integración de información sobre amenazas	Más de 40 actualizaciones de información sobre amenazas de socios de seguridad
Gestión y elaboración de informes	Informes completos que incluyen el comportamiento y la intención del malware, indicadores de compromiso (IOC), archivos descartados y PCAP
Información forense	Muestra inicial, cargas útiles secundarias, PCAP
Soporte de API	Potente soporte de API, recuperación de informes a través de API en formato JSON
Políticas granulares	Políticas fáciles de usar y configurar para usuarios, ubicación, grupos de ubicación, tipos de archivos, grupos de usuarios, departamentos, categorías de URL y protocolos.
Certificaciones de privacidad y cumplimiento de la normativa	Cumple con los rigurosos requisitos de riesgo, privacidad y cumplimiento de la normativa comercial y gubernamental a nivel mundial.
Normativas industriales y de privacidad de datos	Cumplimiento de las normativas de privacidad de datos específicas del sector y el país.

Zscaler Sandbox está completamente integrado con Zscaler Internet Access™ y forma parte del Zero Trust Exchange global

Zscaler Zero Trust Exchange habilita conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier lugar utilizando Internet como la red corporativa. Basado en el principio de confianza cero de acceso con menos privilegios, proporciona una seguridad integral utilizando la identidad basada en el contexto y la aplicación de políticas.

Cómo Zscaler ofrece confianza cero para usuarios, cargas de trabajo y IIoT/OT

Implementación en semanas para mejorar la protección cibernética y la experiencia del usuario



Gartner

Zscaler es nombrado uno de los líderes en el Cuadrante Mágico para SSE de Gartner, posicionado en lo más alto en capacidad de ejecución.

Más información →

zscaler™ | 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. 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 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