Ficha de datos

Zscaler Sandbox

El primer motor de detección, prevención y cuarentena de malware del mundo basado en IA

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 priman los dispositivos móviles y la nube, sus usuarios acceden a los archivos sobre la marcha directamente desde Internet y las aplicaciones SaaS. Los días de lanzar clientes de correo electrónico desde la oficina corporativa rodeados de capas de seguridad quedaron atrás. A medida que las exigencias de facilidad de uso superan a las defensas centradas en la red, las organizaciones se quedan con una superficie de ataque ampliada en una era en la que los ataques son cada vez más astutos y los adversarios se aprovechan de las brechas de la pila de seguridad heredada.

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 malintencionados, el cifrado ha creado una falsa sensación de seguridad. Los sandboxes heredados con arquitectura de paso carecen de visibilidad y han permitido involuntariamente que los archivos maliciosos se cuelen por las ranuras escondiéndose en el tráfico cifrado, a salvo de la inspección profunda o la cuarentena. Se pueden adjuntar a dispositivos de descifrado SSL como ayuda, pero, como ocurre con la mayoría del hardware, no son escalables y generan más problemas administrativos y una costosa acumulación de dispositivos. Como resultado, las infecciones de paciente cero por malware desconocido siguen penetrando en las redes y obligan a los equipos de TI y de seguridad a luchar para

Beneficios de Zscaler Sandbox:

- **Motor de prevención de malware basado en IA**
  Identifique, ponga en cuarentena y prevenga de manera inteligente las amenazas desconocidas o sospechosas en línea mediante IA/ML avanzada sin volver a analizar los archivos benignos.
- **Inspección completa en línea para encontrar 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 global compartida y coherente**
  Obtenga protección automatizada frente a amenazas desconocidas hasta ahora con inteligencia sobre amenazas integrada y compartida por todos los usuarios en tiempo real.
- **Flujos de trabajo SOC aumentados con información sobre amenazas**
  Acelere la investigación y la respuesta compartiendo información sobre el comportamiento del malware, información sobre amenazas e informes avanzados mediante API robustas.
- **Se acabaron los costosos dispositivos físicos y el software**
  Realice la implementación en cuestión de segundos sin tener que comprar hardware ni gestionar software: basta con configurar e implementar una política de sandbox para obtener beneficios inmediatos.
- **Protección suministrada desde la nube con presencia en el perímetro global**
  Obtenga una seguridad y una experiencia de usuario totalmente integradas e inigualables con Zscaler Internet Access™ como parte de Zscaler Zero Trust Exchange™.

detener el movimiento lateral y la exfiltración de datos, que deberían haberse evitado en primer lugar.

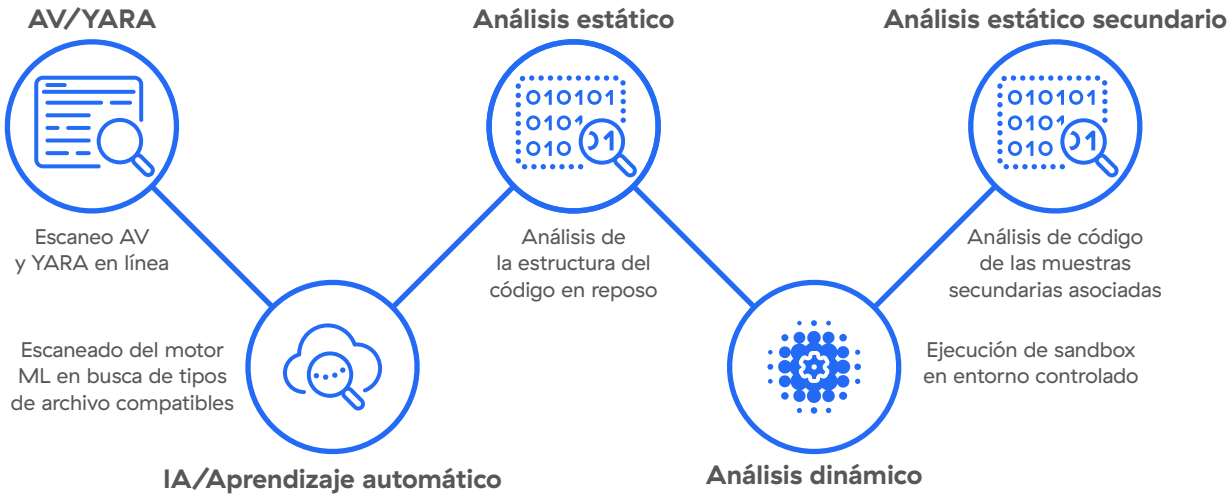
Zscaler Sandbox

Como función crítica en la pila de seguridad, el objetivo del sandbox es proporcionar medidas preventivas contra archivos maliciosos y ejecuciones de código. A diferencia de los sandboxes fuera de banda que proporcionan protección solo después del compromiso inicial, Zscaler Sandbox está diseñado específicamente para atrapar y detener amenazas modernas y escurridizas que aprovechan las técnicas de evasión y explotan las debilidades tradicionales de los sandboxes.

Construida sobre una arquitectura nativa de la nube basada en proxy, la solución Zscaler 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 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.

El archivo desconocido o sospechoso se envía primero a través de un motor de análisis de prefiltrado que comprueba el contenido del archivo con más de 40 fuentes de amenazas, firmas antivirus, reglas YARA y modelos AI/ML para emitir un veredicto rápido, bloqueando las 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 envían al instante mientras que los archivos maliciosos se bloquean para todos los usuarios globales de Zscaler como resultado de la protección compartida del efecto 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 los archivos sospechosos en línea, realizar análisis basados en IA en tiempo real y emitir veredictos instantáneos sin retrasos, los detallados informes avanzados de Zscaler Sandbox pueden llevar el sandboxing de la última línea de defensa al primer paso en la acción impulsada por la inteligencia. Al aplicar conocimientos sobre el comportamiento a partir de malware real dirigido a su organización, puede enriquecer los flujos de trabajo de SecOps para reforzar sus defensas en toda la pila de seguridad.

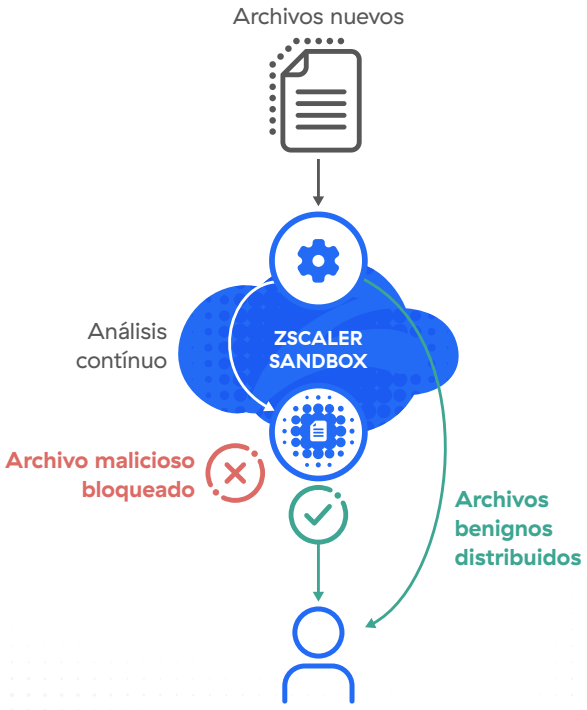
Detenga de manera inteligente las amenazas emergentes y las infecciones de paciente cero
Los adversarios están aprovechando el cifrado y las aplicaciones de confianza en la nube para lanzar ataques sigilosos. De hecho, en un informe reciente de ThreatLabZ se observó la distribución de malware desde Google Drive, AWS y OneDrive. La capacidad de escanear archivos a través de la web y FTP, en particular el tráfico cifrado, asegura la visibilidad e impide que los atacantes accedan a su red.

Antes de que un empleado descargue y abra accidentalmente un nuevo documento malicioso de Office (Maldocs) con una macro oculta, la función de cuarentena en línea impulsada por IA de Zscaler Sandbox entra en acción. Cuando el análisis profundo de archivos arroja una calificación de amenaza alta, el archivo se bloquea para el empleado y otros usuarios de Zscaler no pueden acceder a él. La capacidad de verificación instantánea de archivos sin necesidad de volver a escanearlos evita la interrupción de la productividad de los empleados, mientras que la cuarentena y el bloqueo automáticos de archivos desconocidos o maliciosos evitan lo que, de otro modo, sería un sinfín de incidencias para el servicio de asistencia técnica de TI.

Tras una rápida implementación en veinte minutos de Zscaler Sandbox, el equipo de TI y seguridad de un cliente pudo distribuir de manera segura e instantánea el 91 % de los archivos benignos a los usuarios tras 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 se bloquean para los usuarios previstos y para todos los usuarios y dispositivos globales de Zscaler, independientemente de su ubicación, para una protección compartida y uniforme.

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



Mejore los flujos de trabajo de los SOC con información sobre malware y MITRE ATT&CK
Tras el análisis profundo de archivos y la detonación segura de malware desconocido, el sandbox genera automáticamente un informe de análisis. El entorno controlado y aislado del sandbox realiza capturas de pantalla del análisis e informa a los analistas de las técnicas de evasión de polimorfismo y ofuscación, el comportamiento de devolución de llamada 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, asignándolos al marco MITRE ATT&CK.

Al hacer operativos los hallazgos del sandbox contextual con el marco ATT&CK, los equipos de seguridad y TI pueden compartir perspectivas en 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, lo que acelera la investigación y la respuesta a la vez que facilita los simulacros de caza de amenazas.

Gestión de políticas simplificada con controles granulares
Como producto suministrado desde la nube, no hay hardware que comprar y configurar ni software que gestionar, lo que reduce la complejidad y los recursos. No necesitará estar en las instalaciones para configurar y conectar cada dispositivo, y podrá poner en marcha Zscaler Sandbox con una sencilla configuración de dos pasos: **criterios** y **acción**. Además, las políticas son fáciles de gestionar, 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 se ajustan 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 la detección automatizada de huellas JA3 y configurar listas de bloqueo hash personalizadas y reglas YARA. Además, las políticas de bloqueo basadas en la puntuación pueden actuar sobre archivos de greyware y adware molestos o sospechosos que no suelen superar el umbral de puntuación de amenazas.

Desarrollado sobre una plataforma Zerto Trust nativa de la nube
Zscaler Sandbox es una capacidad totalmente integrada de Zscaler Internet Access y parte de Zscaler Zero Trust Exchange. Esta arquitectura única basada en proxy protege a los usuarios en línea en el momento dirigiendo el tráfico a la pila de seguridad en la nube más grande del sector para ofrecer una protección profunda e inteligente a cada usuario independientemente de su ubicación o red. Obtenga una protección global compartida con actualizaciones en tiempo real procedentes de 300 billones de señales de amenazas diarias combinadas con la protección de generación en la nube y los principios Zero Trust de privilegios mínimos.

Sandbox Standard vs. Advanced

	Standard Sandbox	Advanced Sandbox	
Ediciones de ZIA	Professional Edition Business Edition	Transformation Edition ELA Edition	**Advanced Sandbox puede ser un complemento de ZIA Professional y Business Edition**
Compatibilidad de archivos	.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 script en zips	
Cuarentena que utiliza la IA	–	CÍRCULO DE VERIFICACIÓN	
Políticas granulares	–	CÍRCULO DE VERIFICACIÓN	
Informes	–	CÍRCULO DE VERIFICACIÓN	
API	–	CÍRCULO DE VERIFICACIÓN	

Funciones principales de la generación en la nube

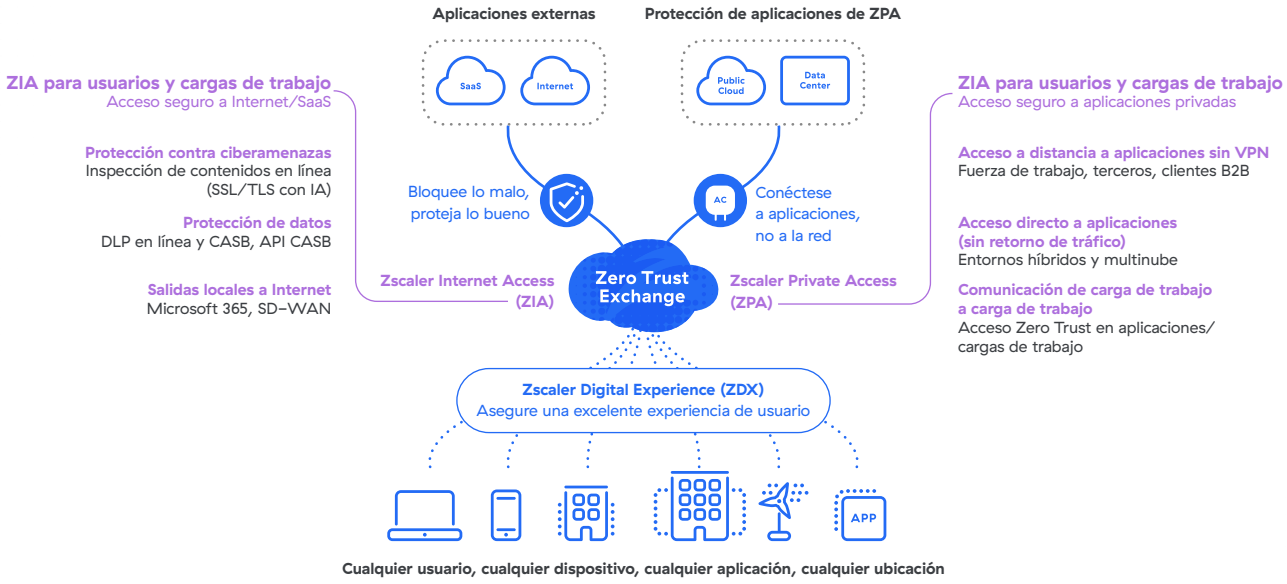
Motor de análisis de prefiltrado	AV, listas de bloqueo hash, reglas YARA, detecciones automatizadas de huellas JA3 y modelos ML/AI
Análisis estático, dinámico y secundario	Análisis estático y análisis dinámico, incluido el análisis del código y de la carga útil secundaria
Compatibilidad de archivos	.exe, .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 script en zips
Inspección de SSL	Capacidad ilimitada de 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 sistemas operativos	Windows XP, Windows 10, Android
Compatibilidad con protocolos	HTTP, HTTPS, FTP, FTP sobre 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 inteligencia sobre amenazas	Más de 40 fuentes de información sobre amenazas de socios de seguridad
Gestión y presentación de informes	Informes completos que incluyen el comportamiento y la intención del malware, indicadores de compromiso (IOC), archivos escritos en disco durante la ejecución del sandbox y PCAP.
Análisis forenses	Muestra inicial, cargas útiles secundarias, PCAP
Soporte API	Soporte API robusto, recuperación de informes a través de API en formato JSON
Políticas granulares	Facilidad de uso y configuración de políticas para usuarios, ubicación, grupos de ubicación, tipos de archivo, grupos de usuarios, departamentos, categorías de URL y protocolos.
Certificaciones de privacidad y cumplimiento	Cumple con los rigurosos requisitos globales de riesgo, privacidad y normativos, tanto comerciales como gubernamentales.
Normativa del sector y de privacidad de datos	Cumplimiento de las reglas de privacidad de datos específicas del país y del sector

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

Zscaler Zero Trust Exchange facilita las conexiones rápidas y seguras y permite a sus empleados trabajar desde cualquier lugar, utilizando Internet como red corporativa. Proporciona seguridad integral basada en el principio de Zero Trust de acceso con privilegios mínimos, mediante el cumplimiento de políticas y la comprobación de la identidad según el contexto.

Cómo ofrece Zscaler Zero Trust para los usuarios, la carga de trabajo y la IIoT/OT

Implemente en semanas para mejorar la ciberprotección y la experiencia del usuario



Gartner

Zscaler está posicionado como líder en el Gartner® Magic Quadrant™ para Security Server Edge (SSE), en la posición más alta 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, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura 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.mx** o síganos en Twitter **@zscaler**.

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