Ficha de datos

# Zscaler ITDR™

## Priorice la seguridad de la identidad por medio de zero trust

Zscaler ITDR (detección y respuesta a amenazas a la identidad por sus siglas en inglés) detecta y protege contra ataques basados en la identidad, como el robo de credenciales y el abuso de privilegios, asaltos a Active Directory y autorizaciones peligrosas.

### La identidad es la nueva superficie de ataque

Los ciberatacantes utilizan ahora métodos sofisticados para atentar contra las identidades y los sistemas de identidad. Con el aumento de los ataques basados en la identidad, las empresas actuales necesitan poder detectar cuándo los atacantes explotan, utilizan indebidamente o roban las identidades empresariales. Las técnicas de detección de amenazas y los sistemas de identidad heredados son a menudo ineficaces, ya que no se diseñaron para hacer frente a las amenazas relacionadas con la identidad. Zscaler ITDR mitiga el riesgo de las ciberamenazas que tienen como objetivo las identidades y la infraestructura de identidades (Active Directory on-prem).

### Zscaler ITDR

Supervisa su Active Directory en busca de cualquier error de configuración o vulnerabilidades que lo expongan a riesgos de escalada de privilegios y movimiento lateral con Zscaler ITDR. Protege sus identidades y ofrece una amplia visibilidad de la superficie de ataque de la identidad para proporcionar notificaciones en tiempo real sobre los ataques basados en la identidad. Ahora puede detectar y detener los ataques basados en la identidad, como el robo de credenciales, la omisión de la autenticación multifactor y las técnicas de escalada de privilegios.

### Beneficios

- **Detecte las amenazas a la identidad en tiempo real:** Los sistemas de identidad están en constante evolución con los cambios en los permisos y las configuraciones. Supervise en tiempo real y reciba alertas sobre nuevas vulnerabilidades, riesgos y problemas.
- **Reduzca la superficie de ataque a la identidad:** Obtenga visibilidad y corrija las configuraciones erróneas de identidad y los permisos arriesgados que generan riesgos.
- **Mitigue el riesgo de un ataque de identidad:** Descubra configuraciones de riesgo como la exposición de contraseñas GPP, la delegación sin restricciones y las contraseñas obsoletas que abren nuevas vías de ataque.
- **Acelere la investigación y la respuesta**: Ayude a los equipos de seguridad a priorizar la investigación de las alertas basándose en las puntuaciones de riesgo generadas por las evaluaciones de identidad.
- **Agilice la reparación:** Los equipos de seguridad ahora pueden aprovechar la guía de reparación paso a paso de Zscaler ITDR, videos de tutoriales, scripts y comandos para acelerar la respuesta.
- **Despliegue con facilidad:** No se necesitan equipos virtuales adicionales. Utilice el mismo cliente de Zscaler client connector para proporcionar una capa adicional de seguridad que impida las amenazas basadas en la identidad.

**5/10**

Las organizaciones sufren un ataque a Active Directory

Fuente: EMA

**80 %**

de los ataques modernos se basan en la identidad

Fuente: Crowdstrike

**90 %**

de las interacciones de Mandiant IR involucran AD

Fuente: Dark Reading

## ¿Cómo funciona?

Zscaler ITDR adopta un enfoque simple y operativamente sencillo para la seguridad de la identidad. Está integrado en Zscaler Client Connector, un agente unificado que actúa como intermediario de forma segura para las conexiones entre usuarios y aplicaciones/recursos.

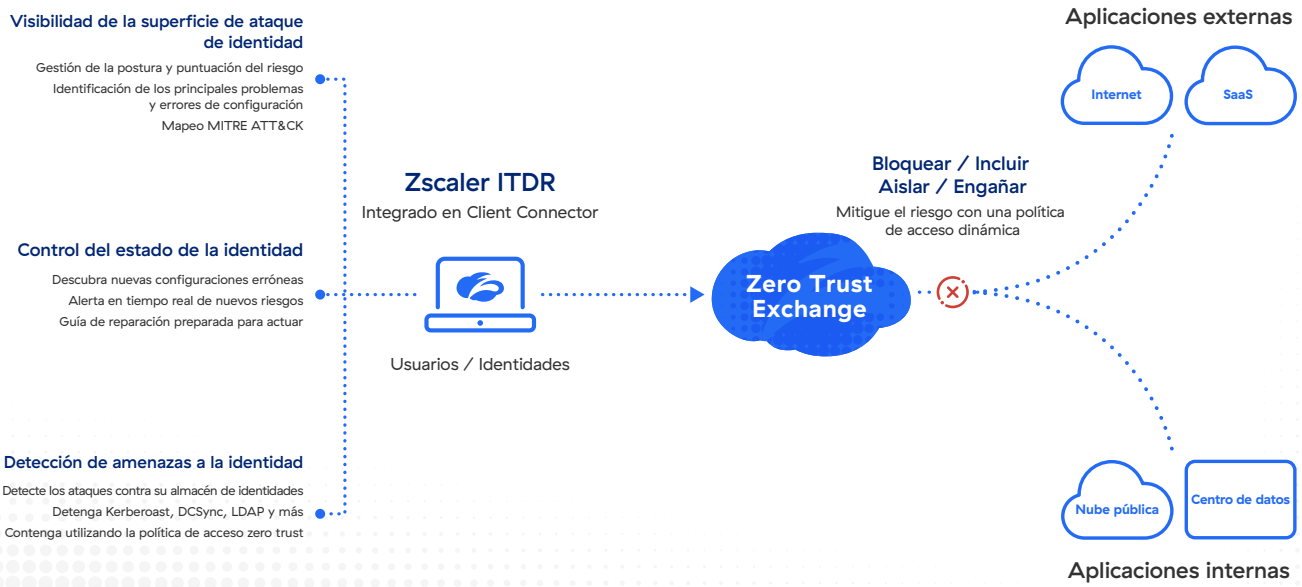
Zscaler ITDR consta de tres capacidades:

- Visibilidad de la superficie de ataque de identidad
- Detección de cambios de identidad
- Detección de amenazas a la identidad

### Visibilidad de la superficie de ataque

Zscaler ITDR audita el Active Directory ejecutando consultas LDAP para elaborar un mapa de esquemas, usuarios, equipos, unidades organizativas y otros objetos en su almacén de identidades. Luego ejecuta comprobaciones contra estos objetos para encontrar configuraciones erróneas y vulnerabilidades que existan en su Active Directory.

- Para evaluar el Active Directory, Zscaler ITDR necesita ejecutarse en un Client Connector instalado en un equipo Windows unido al dominio.
- El equipo de seguridad configura un escaneo especificando el dominio de Active Directory al que desea acceder y seleccionando el equipo instalado de Client Connector desde donde se ejecuta el escaneo.
- Dependiendo del tamaño del Active Directory, la evaluación puede tardar entre 15 y 30 minutos.
- Una vez completada la evaluación, los resultados se pueden ver en el panel de control.
- La evaluación incluye una puntuación de riesgo del dominio, áreas de enfoque para priorizar la reparación, una lista de los usuarios y equipos bajo mayor riesgo, un análisis básico de las categorizaciones de gravedad y riesgo, el mapeo de la cadena de eliminación MITRE ATT&CK y una lista completa de las configuraciones erróneas descubiertas.



Para cada configuración errónea, la solución ofrece lo siguiente:

- Categorización del riesgo
- Gravedad
- Esfuerzo de reparación
- Identificación y táctica de MITRE ATT&CK
- Explicación del problema
- Impacto potencial
- Lista de usuarios, equipos y objetos afectados
- Solución de problemas
- Tutoriales en video
- Scripts
- Comandos

### Detección de cambios de identidad

Una vez configurada una evaluación, los equipos de seguridad pueden activar la detección de cambios para el dominio de Active Directory. La detección de cambios muestra las configuraciones que afectan a la postura de seguridad de Active Directory casi en tiempo real, lo que permite a los equipos de seguridad y a los administradores de directorios responder rápidamente.

- Zscaler ITDR ejecuta una serie de comprobaciones de configuración de alta prioridad en Active Directory.
- El alcance de estas comprobaciones se centra en el descubrimiento de los puntos con mayores posibilidades de ataque por parte de los adversarios.
- Estas comprobaciones se ejecutan cada 15 minutos desde el punto final instalado de Client Connector para el dominio determinado.
- Los cambios se marcan como de impacto positivo o negativo.
- Un impacto positivo indica que se ha resuelto un problema.
- Un impacto negativo indica que se ha presentado un problema potencial.

### Detección de amenazas a la identidad en tiempo real

Zscaler ITDR tiene la capacidad de detectar amenazas para alertar a los equipos SOC y a los buscadores de amenazas de actividades maliciosas dirigidas a un uso indebido potencialmente peligroso y al robo de identidades.

La Detección de Amenazas a la Identidad puede activarse como una política de punto final en los equipos instalados de Client Connector designados.

- Los equipos de seguridad activan la política de detección de amenazas que permite supervisar los eventos del sistema y analizarlos en busca de patrones que sirvan para identificar los vectores de amenaza elegidos.
- Los detectores disponibles incluyen DCSync, DCShadow, kerberoasting, enumeración de sesiones, acceso a cuentas privilegiadas, enumeración LDAP y más.
- Los equipos de seguridad pueden optar por encender todos los detectores o una combinación de los mismos en los puntos finales designados.
- Si se observa un patrón, Client Connector señala a Zscaler ITDR que se ha detectado una amenaza.
- La plataforma refuerza la señal de amenaza con información relevante para que el usuario pueda realizar una investigación
- El equipo de seguridad puede configurar las capacidades de orquestación en Zscaler ITDR para tomar acciones automatizadas que van desde la alerta hasta el reenvío y la reparación.

## Casos importantes de uso

### Visibilidad de la superficie de ataque a la identidad

La evaluación continua de su Active Directory le brinda una puntuación de riesgo unificada, una lista de configuraciones erróneas y vulnerabilidades, y una guía de reparación para solucionar esos problemas.

- Puntuación de riesgo unificada para la cuantificación y el rastreo de la postura de identidad
- Vista en tiempo real de los problemas principales de identidad y de los usuarios/hosts con mayor riesgo
- Asignación de MITRE ATT&CK para obtener visibilidad de los puntos ciegos de seguridad

### Control de la integridad de la identidad

Reciba alertas y notificaciones en tiempo real a medida que se introducen nuevos riesgos en su Active Directory. Obtenga visibilidad en tiempo real de la configuración de riesgos y los cambios de permisos.

- Identifique nuevas vulnerabilidades y configuraciones erróneas a medida que aparecen
- Alertas en tiempo real de los nuevos riesgos introducidos en su almacén de identidades
- Orientación, comandos y scripts preparados para usarse en la reparación

### Detección y respuesta de amenazas a la identidad

Detección de amenazas en tiempo real para los principales ataques a la identidad

- Detecte los ataques contra su almacén de identidades
- Las detecciones incluyen kerberoast, DCSync y enumeración LDAP
- Contención integrada que emplea la política de acceso zero trust

## Diferenciadores clave

### Integrado en Client Connector

Zscaler ITDR está integrado en el Zscaler Client Connector y desbloquea nuevas capacidades y protecciones listas para usar. El mismo cliente de punto final que conecta de forma segura a los usuarios a Internet y a las aplicaciones, ahora ofrece capacidades de seguridad adicionales y mitiga el riesgo de ataques a la identidad.

### Integrado con Zero Trust Exchange

Zscaler Identity se integra perfectamente con la plataforma Zscaler Zero Trust Exchange para brindar una mejor detección de amenazas y respuesta a las amenazas basadas en la identidad. Zero Trust Exchange puede aplicar dinámicamente controles de políticas de acceso para bloquear a los usuarios comprometidos cuando se detecta un ataque a la identidad.

### Integraciones sin problemas

Refuerce la investigación y la respuesta con integraciones sólidas que incluyen EDR (detección y respuesta de puntos finales) como Crowdstrike, Microsoft Defender, VMware CarbonBlack y todos los SIEM (información de seguridad y control de eventos) más importantes.

## Refuerce su postura de seguridad con Zscaler ITDR

### Defiéndase contra las amenazas a la identidad

Obtener visibilidad sobre las identidades es esencial para detectar las amenazas basadas en la identidad. Zscaler ITDR proporciona una visibilidad exhaustiva de los incidentes y anomalías basados en la identidad en todo su entorno de TI, para poder neutralizar los ataques basados en la identidad antes de que se produzcan.

### Detecte los ataques a Active Directory

Los directorios activos son objetivos atractivos para los ataques de identidad. Zscaler ITDR supervisa continuamente AD/Azure AD en busca de vulnerabilidades y configuraciones erróneas o arriesgadas.

### Prevenga el uso indebido/robo de credenciales

Los atacantes utilizan credenciales robadas y atacan Active Directory para escalar privilegios y moverse lateralmente. Zscaler ITDR ayuda a detectar los ataques a las credenciales y a evitar el robo o el uso indebido de las mismas.

### Detenga el movimiento lateral

Zscaler ITDR identifica las configuraciones erróneas y las exposiciones de credenciales que crean rutas de ataque para el movimiento lateral. Detenga a los atacantes que han burlado las defensas basadas en el perímetro y están intentando moverse lateralmente a través de su entorno.

**Zscaler ITDR incorpora nuevas y potentes capacidades que mejoran su programa zero trust sin que ello suponga una sobrecarga operativa o recursos adicionales.**

zscaler™ | Experience your world, secured.™



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