Ficha de datos

Zscaler ITDR™

Llevar la seguridad con prioridad de identidad a la confianza cero

Zscaler ITDR (Identity Threat Detection and Response) detecta y le defiende contra ataques basados en la identidad, como el robo de credenciales y el abuso de privilegios, ataques de Active Directory y asignaciones arriesgadas de derechos.

La identidad es la nueva superficie de ataque

Los atacantes cibernéticos ahora están utilizando métodos sofisticados para atacar identidades y sistemas de identidad. Con los ataques basados en la identidad en aumento, las empresas de hoy en día requieren la capacidad de detectar cuándo los atacantes explotan, hacen mal uso o roban las identidades de la empresa. Las técnicas de detección de amenazas y los sistemas de identidad heredados suelen ser ineficaces, ya que no se crearon para gestionar las amenazas basadas en la identidad. Zscaler ITDR mitiga el riesgo de ciberamenazas que se dirigen a las identidades y la infraestructura de identidad (Active Directory local).

Zscaler ITDR

Supervise su Active Directory en busca de errores de configuración o vulnerabilidades que lo expongan a riesgos de escalada de privilegios y movimientos laterales con Zscaler ITDR. Protege sus identidades y ofrece una amplia visibilidad de la superficie de ataque de identidad para entregar notificaciones en tiempo real sobre ataques basados en identidad. Ahora puede detectar y detener ataques basados en la identidad, como credenciales robadas, elusiones de autenticación multifactor y técnicas de escalada de privilegios.

Ventajas

- **Detecte amenazas de identidad en tiempo real:** los sistemas de identidad están en constante desarrollo con cambios de configuración y permisos. Esté supervisando en tiempo real y reciba alertas sobre nuevas vulnerabilidades, riesgos y problemas.
- **Reduzca la superficie expuesta a ataques de identidad:** obtenga visibilidad y solucione las configuraciones incorrectas de identidad y los permisos arriesgados que generan exposición.
- **Mitigue el riesgo de un ataque de identidad:** descubra configuraciones de riesgo como contraseñas GPP expuestas, delegación sin restricciones y contraseñas obsoletas que abren nuevas rutas de ataque.
- **Acelere la investigación y la respuesta**: ayude a los equipos de seguridad a priorizar la investigación de las alertas en función de las puntuaciones de riesgo generadas por las evaluaciones de identidad.
- **Simplifique la remediación:** los equipos de seguridad ahora pueden aprovechar la guía de remediación paso a paso de Zscaler ITDR junto con tutoriales en vídeo, scripts y comandos para acelerar la respuesta.
- **Impleméntelo fácilmente:** no se requieren máquinas virtuales adicionales. Utilice el mismo conector de cliente Zscaler para proporcionar una capa adicional de seguridad que frustre las amenazas basadas en la identidad.

5/10

de las organizaciones sufren un ataque de identidad.

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 ligero y sencillo desde el punto de vista operativo para la seguridad de la identidad. Está integrado en Zscaler Client Connector, un agente unificado que negocia de forma segura las conexiones entre usuarios y aplicaciones/recursos.

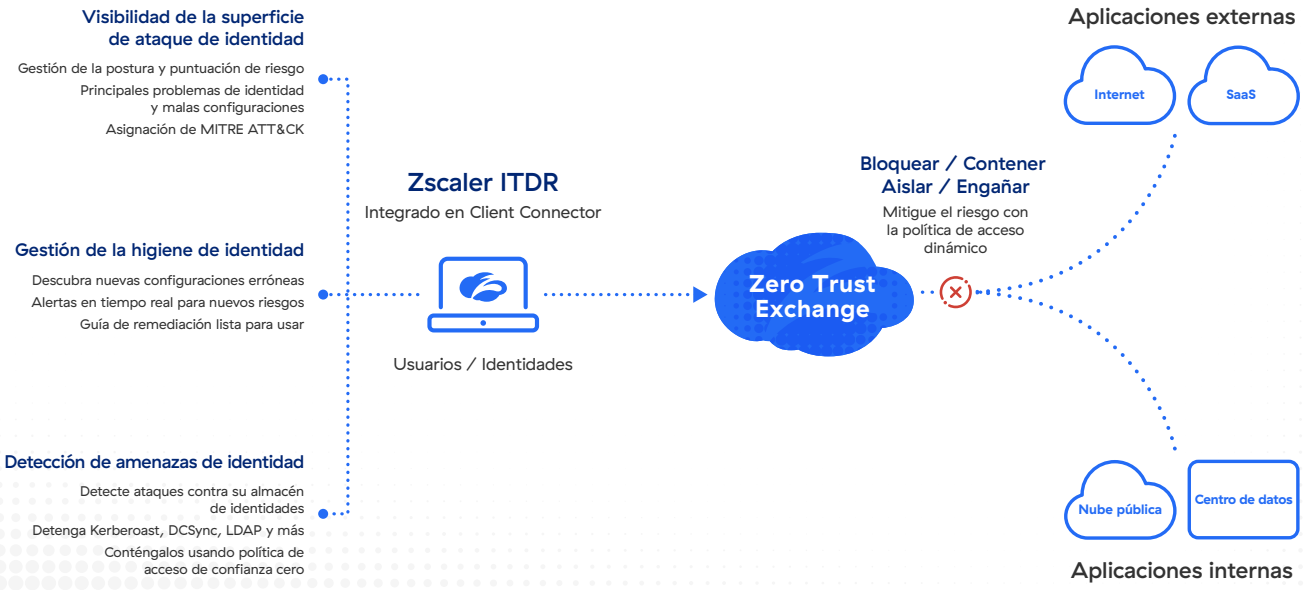
Zscaler ITDR consta de tres capacidades:

- Visibilidad de la superficie de ataque de identidad
- Detección de cambio de identidad
- Detección de amenazas de identidad

Visibilidad de superficie de ataque

Zscaler ITDR audita Active Directory mediante la ejecución de consultas LDAP para crear un mapa de esquema, usuarios, ordenadores, unidades organizativas y otros objetos en su almacén de identidad.
A continuación, ejecuta verificaciones contra estos objetos para encontrar configuraciones incorrectas y vulnerabilidades que existen en su Active Directory.

- Para evaluar Active Directory, Zscaler ITDR debe ejecutarse en un Client Connector instalado en una máquina Windows unida a un dominio.
- El equipo de seguridad configura un análisis especificando el dominio del Active Directory al que desea acceder y seleccionando la máquina instalada de Client Connector desde la cual ejecutar el análisis.
- Según el tamaño del Active Directory, se tarda entre 15 y 30 minutos en completar la evaluación.
- Una vez que se completa la evaluación, los resultados están disponibles para verlos en el tablero.
- La evaluación incluye una puntuación de riesgo de dominio, áreas de enfoque para priorizar la remediación, una lista de los usuarios y los ordenadores de más riesgo, un análisis básico de las categorías de gravedad y riesgo, la asignación de la cadena de eliminación de MITRE ATT&CK y una lista completa de configuraciones erróneas descubiertas.



Para cada configuración incorrecta, la solución proporciona lo siguiente:

- Categorización de riesgos
- Severidad
- Esfuerzo de remediación
- ID y táctica de MITRE ATT&CK
- Explicación del problema
- Impacto potencial
- Lista de usuarios, equipos y objetos afectados
- Guía de reparación
- Tutoriales en vídeo
- Scripts
- Comandos

Detección de cambios de identidad

Una vez que se ha configurado una evaluación, los equipos de seguridad pueden activar la detección de cambios para el dominio del Active Directory. Cambie las configuraciones de la superficie de detección que afectan la postura de seguridad del Active Directory casi en tiempo real, lo que permite que los equipos de seguridad y los administradores de directorios respondan rápidamente.

- Zscaler ITDR ejecuta una serie de comprobaciones de configuración de alta prioridad en el Active Directory.
- El alcance de estas comprobaciones se centra en el descubrimiento de problemas que tienen la mayor posibilidad de abuso por parte de los adversarios.
- Estas comprobaciones se ejecutan cada 15 minutos desde el extremo instalado de Client Connector para el dominio determinado.
- Los cambios se marcan según tengan un impacto bueno o malo.
- Un buen impacto indica que se ha resuelto un problema.
- Un impacto negativo indica que se ha introducido un problema potencial.

Detección de amenazas de identidad en tiempo real

Zscaler ITDR tiene una capacidad de detección de amenazas que alerta a los equipos SOC y a los cazadores de amenazas de actividades maliciosas dirigidas al uso indebido y robo de identidades potencialmente maliciosos.

La detección de amenazas de identidad se puede activar como una política de punto final en las máquinas instaladas de Client Connector designadas.

- Los equipos de seguridad habilitan la política de detección de amenazas que permite supervisar eventos en el sistema y analizar patrones para identificar indicadores de los vectores de amenazas elegidos.
- Los detectores disponibles incluyen DCSync, DCShadow, kerberoasting, enumeración de sesiones, acceso a cuentas privilegiadas, enumeración LDAP y otros.
- Los equipos de seguridad pueden optar por activar todos los detectores o una combinación de ellos en los puntos finales designados.
- Si se detecta un patrón, Client Connector indica a Zscaler ITDR que se ha detectado una amenaza.
- La plataforma enriquece la señal de amenaza con información relevante para que el usuario realice una investigación
- El equipo de seguridad puede configurar capacidades de orquestación en Zscaler ITDR para tomar acciones automatizadas desde alertas hasta reenvío y remediación.

Casos de uso clave

Visibilidad de la superficie de ataque de identidad

La evaluación continua de su Active Directory proporciona una puntuación de riesgo unificada, una lista de configuraciones incorrectas y vulnerabilidades, y orientación para solucionar esos problemas.

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

Gestión de la higiene de la identidad

Reciba alertas y notificaciones en tiempo real a medida que se introduzcan 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 surjan
- Alertas en tiempo real de los nuevos riesgos introducidos en su almacén de identidades
- Orientación, comandos y scripts para la remediación listos para usarse

Detección y respuesta de amenazas de identidad

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

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

Diferenciadores clave

Integrado en Client Connector

Como parte de Zscaler Client Connector, Zscaler ITDR 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 la aplicación ahora proporciona capacidades de seguridad adicionales y mitiga el riesgo de ataques de identidad.

Integrado con Zero Trust Exchange

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

Integraciones perfectas

Fortalezca la investigación y la respuesta con integraciones estrechas que incluyen EDR como Crowdstrike, Microsoft Defender, VMware CarbonBlack y todos los principales SIEM.

Refuerce su postura de seguridad con Zscaler ITDR

Defiéndase de las amenazas de identidad

Obtener visibilidad de las identidades es esencial para detectar amenazas basadas en la identidad. Zscaler ITDR brinda una visibilidad profunda de los incidentes y anomalías basados en la identidad en todo su entorno de TI, para que pueda frustrar los ataques basados en la identidad antes de que se produzcan.

Detectar ataques de Active Directory

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

Evite el uso indebido/robo de credenciales

Los atacantes usan credenciales robadas y atacan a Active Directory para aumentar los privilegios y moverse lateralmente. Zscaler ITDR ayuda a detectar vulnerabilidades de credenciales y evitar el robo o uso indebido de credenciales.

Detener el movimiento lateral

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

Zscaler ITDR desbloquea nuevas y potentes capacidades que amplían lo que su programa de confianza cero es capaz de hacer sin agregar gastos adicionales operativos o de recursos.

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. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE 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