Scheda tecnica

Zscaler ITDR™

Sicurezza delle identità e zero trust

Zscaler ITDR (Identity Threat Detection and Response) rileva e difende dagli attacchi all'identità, come il furto delle credenziali, l'abuso dei privilegi, gli attacchi ad Active Directory e le autorizzazioni rischiose.

L'identità è la nuova superficie di attacco

Oggi, gli aggressori informatici utilizzano metodi molto sofisticati per colpire le identità e i sistemi delle identità. Dato l'incremento di questo tipo di attacchi, le aziende moderne devono essere in grado di rilevare quando un aggressore sfrutta le vulnerabilità di un sistema, usa impropriamente o ruba le identità aziendali. Le tecniche di rilevamento delle minacce e i sistemi di identità legacy si rivelano spesso inefficaci, perché non sono stati concepiti per gestire questa tipologia di minacce. Zscaler ITDR attenua il rischio di subire attacchi informatici che prendono di mira le identità e l'infrastruttura delle identità (Active Directory on-premise).

Zscaler ITDR

Monitora Active Directory per individuare gli eventuali errori di configurazione o le vulnerabilità che espongono l'azienda al rischio di escalation dei privilegi e di movimento laterale grazie a Zscaler ITDR. Questa soluzione protegge le identità aziendali e offre un'ampia visibilità sulla superficie di attacco che queste generano, per fornire notifiche in tempo reale in caso di attacchi di questo tipo. Finalmente puoi rilevare e bloccare gli attacchi rivolti alle identità, come il furto di credenziali, l'elusione dell'autenticazione a più fattori e le tecniche di escalation dei privilegi.

Vantaggi

- **Rileva in tempo reale le minacce alle identità:** i sistemi di gestione delle identità sono in costante evoluzione, e configurazioni e autorizzazioni cambiano spesso. Effettua un monitoraggio in tempo reale e ricevi notifiche sulle nuove vulnerabilità, sui rischi e sui problemi.
- **Riduci la superficie di attacco delle identità:** ottieni la massima visibilità e correggi gli errori di configurazione delle identità e le autorizzazioni a rischio che creano una superficie esposta.
- **Mitiga il rischio di subire un attacco alle identità:** rileva le configurazioni a rischio, come l'esposizione delle password GPP, la delega illimitata e le password obsolete che aprono nuovi percorsi di attacco.
- **Accelera le indagini e la risposta**: aiuta il team di sicurezza ad assegnare la giusta priorità alle indagini, sfruttando allerte basate sul punteggio di rischio generato dalle valutazioni delle identità.
- **Semplifica le azioni di correzione:** i team di sicurezza possono finalmente sfruttare le linee guida dettagliate di Zscaler ITDR per supportare le misure di correzione, oltre a video tutorial, script e comandi per accelerare la risposta.
- **Facilita la distribuzione:** non c'è necessità di ricorrere a VM aggiuntive. Utilizza lo stesso Zscaler Client Connector per fornire un ulteriore livello di sicurezza e contrastare la minacce dirette alle identità.

5 su 10

Organizzazioni che subiscono un attacco ad Active Directory

Fonte: EMA

80%

degli attacchi moderni è diretto alle identità

Fonte: Crowdstrike

90%

delle attività di IR di Mandiant coinvolge AD

Fonte: Dark Reading

Come funziona?

Zscaler ITDR adotta un approccio semplice e a bassa interazione per la protezione delle identità. Si tratta di una soluzione integrata in Zscaler Client Connector, un agente unificato e sicuro che agisce da broker delle connessioni tra utente e applicazioni/risorse.

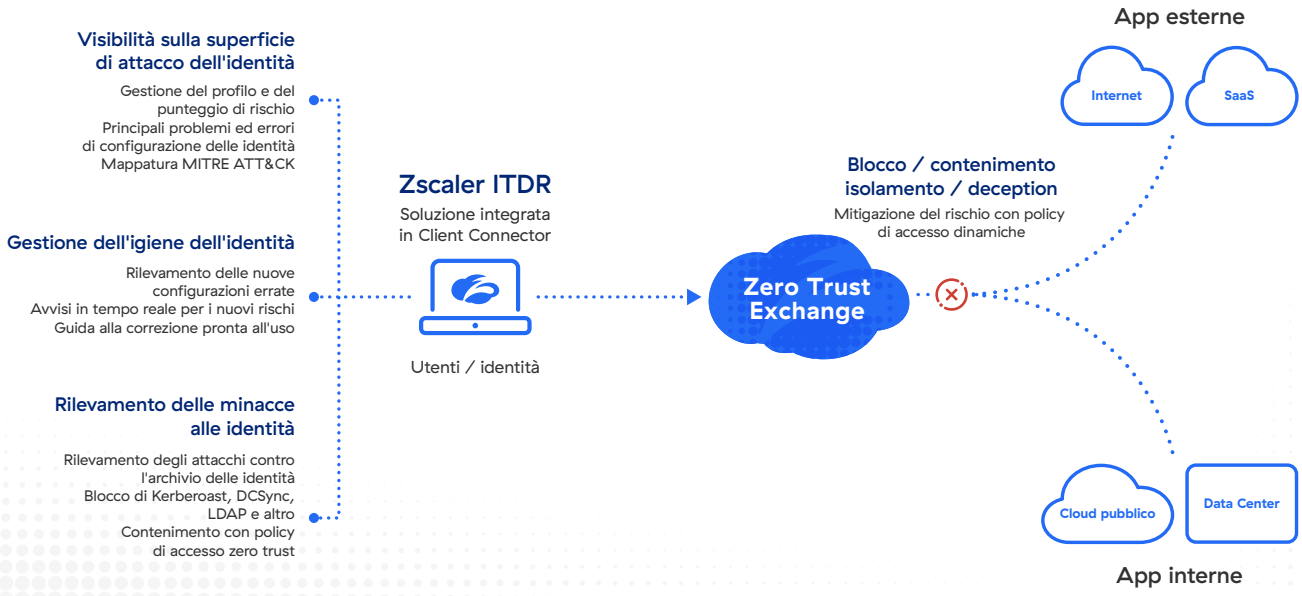
Zscaler ITDR presenta tre funzionalità:

- Visibilità sulla superficie di attacco dell'identità
- Rilevamento della modifica delle identità
- Rilevamento delle minacce alle identità

Visibilità sulla superficie di attacco

Zscaler ITDR esegue una verifica dell'Active Directory attraverso query LDAP, in modo da creare una mappa di schemi, utenti, computer, UO e altri oggetti dell'archivio delle identità. Esegue quindi controlli su questi oggetti per individuare gli errori di configurazione e le vulnerabilità presenti in Active Directory.

- Per eseguire la valutazione di Active Directory, Zscaler ITDR deve essere eseguito su un Client Connector installato su un computer Windows collegato al dominio.
- Il team responsabile della sicurezza configurerà una scansione specificando il dominio di Active Directory a cui desidera accedere e selezionando il computer su cui è installato Client Connector da cui eseguire la scansione.
- A seconda delle dimensioni dell'Active Directory, il completamento della valutazione può richiedere dai 15 ai 30 minuti.
- Una volta completata la valutazione, i risultati saranno disponibili nel pannello di controllo.
- La valutazione include un punteggio di rischio del dominio, gli ambiti prioritari per le azioni correttive, un elenco degli utenti e dei computer più a rischio, un'analisi della gravità e delle categorie di rischio, la mappatura della kill chain rispetto a MITRE ATT&CK e un elenco completo degli errori di configurazione rilevati.



Per ogni errore di configurazione, la soluzione fornisce quanto segue:

- Categorizzazione del rischio
- Gravità
- Azione di bonifica
- ID e tattica MITRE ATT&CK
- Spiegazione del problema
- Impatto potenziale
- Elenco di utenti, computer e oggetti interessati
- Guida alla correzione
- Video tutorial
- Script
- Comandi

Rilevamento delle modifiche alle identità

Una volta configurata una valutazione, il team responsabile della sicurezza ha la possibilità di attivare il rilevamento delle modifiche per il dominio di Active Directory. Il rilevamento delle modifiche fa emergere le configurazioni che influiscono sul profilo di sicurezza di Active Directory praticamente in tempo reale, consentendo ai team della sicurezza e agli amministratori delle directory di reagire rapidamente.

- Zscaler ITDR esegue una serie di controlli prioritari sulle configurazioni in Active Directory.
- Lo scopo di questi controlli è quello di rilevare le problematiche che hanno più probabilità di essere sfruttate dagli aggressori.
- Questi controlli vengono eseguiti ogni 15 minuti dal Client Connector installato sull'endpoint del dominio interessato.
- Le modifiche sono contrassegnate come aventi un impatto positivo o negativo.
- Un impatto positivo indica che un problema è stato risolto.
- Un impatto negativo indica che è stato introdotto un potenziale problema.

Rilevamento in tempo reale delle minacce alle identità

Zscaler ITDR dispone di una funzionalità di rilevamento delle minacce che avvisa i team del SOC e i cacciatori di minacce della presenza di attività dannose che possono comportare un uso potenzialmente malevolo delle risorse e il furto di identità.

Identity Threat Detection può essere attivato sotto forma di una policy dell'endpoint sui computer designati su cui è installato Client Connector.

- I team responsabili della sicurezza abilitano le policy per il rilevamento delle minacce, che consentono di monitorare gli eventi sul sistema e di analizzare i modelli per identificare gli indicatori di specifici vettori delle minacce.
- I rilevatori disponibili includono DCSync, DCShadow, kerberoasting, enumerazione delle sessioni, accesso agli account con privilegi, enumerazione LDAP e altro ancora.
- I team di sicurezza possono scegliere di attivare tutti o una combinazione di questi rilevatori sugli endpoint designati.
- Se viene rilevato uno schema di attacco, Client Connector segnala a Zscaler ITDR che è stata individuata una minaccia.
- La piattaforma arricchisce il segnale della minaccia con informazioni rilevanti per l'utente allo scopo di eseguire un'indagine.
- Il team della sicurezza può configurare le funzionalità di orchestrazione in Zscaler ITDR per intraprendere azioni automatizzate, dalla segnalazione all'inoltro e alla correzione.

Casi d'uso principali

Visibilità sulla superficie di attacco delle identità

La valutazione continua di Active Directory fornisce un punteggio di rischio unificato, un elenco di errori di configurazione e vulnerabilità e una guida per la risoluzione dei problemi.

- Punteggio di rischio unificato per valutare e monitorare il profilo di sicurezza delle identità
- Visione in tempo reale dei principali problemi relativi alle identità e degli utenti/host più a rischio
- Mappatura MITRE ATT&CK per la visibilità sui punti ciechi nella sicurezza

Gestione dell'igiene digitale delle identità

Ricevi allerte e notifiche in tempo reale quando vengono introdotti nuovi rischi in Active Directory e ottieni la massima visibilità sulle modifiche di configurazioni e autorizzazioni a rischio.

- Identifica le nuove vulnerabilità e gli errori di configurazione non appena emergono
- Segnalazione in tempo reale dei nuovi rischi introdotti nell'archivio di identità
- Procedure guidate, comandi e script pronti all'uso per l'attività di correzione

Identity Threat Detection and Response

Rilevamento delle minacce in tempo reale per i principali attacchi rivolti alle identità

- Rileva gli attacchi diretti all'archivio delle identità
- Il rilevamento include kerberoast, DCSync e l'enumerazione LDAP
- Contenimento integrato con policy di accesso zero trust

Differenze principali

Integrazione in Client Connector

Zscaler ITDR, una soluzione integrata in Zscaler Client Connector, consente da subito di usufruire di nuove funzionalità e protezioni. Lo stesso client di endpoint che connette in modo sicuro e senza rischi l'utente a Internet e alle applicazioni ora fornisce ulteriori funzionalità di sicurezza e attenua il rischio di subire attacchi diretti alle identità.

Integrazione in Zero Trust Exchange

Zscaler Identity si integra perfettamente nella piattaforma Zscaler Zero Trust Exchange per migliorare il rilevamento e la risposta alle minacce dirette alle identità. Zero Trust Exchange è in grado di applicare dinamicamente controlli delle policy di accesso per bloccare gli utenti compromessi in caso di attacco alle identità.

Integrazioni perfette

Rafforza le indagini e le azioni di risposta sfruttando integrazioni con strumenti EDR come Crowdstrike, Microsoft Defender, VMware CarbonBlack e tutti i principali SIEM.

Rafforza il tuo profilo di sicurezza con Zscaler ITDR

Difenditi dalle minacce alle identità

Disporre di una visibilità massima sulle identità è essenziale per rilevare le minacce che possono colpirle. Zscaler ITDR fornisce una visibilità approfondita su anomalie e incidenti relativi alle identità in tutto l'ambiente IT, in modo da poter contrastare gli attacchi prima che si verifichino.

Rileva gli attacchi ad Active Directory

Le Active Directory sono bersagli molto popolari per gli attacchi alle identità. Zscaler ITDR monitora costantemente AD/Azure AD alla ricerca di vulnerabilità e configurazioni errate o a rischio.

Previeni l'uso improprio/furto di credenziali

Gli aggressori utilizzano le credenziali rubate e attaccano Active Directory per elevare i privilegi e muoversi lateralmente. Zscaler ITDR aiuta a rilevare gli exploit e a prevenire il furto o l'abuso delle credenziali.

Blocca il movimento laterale

Zscaler ITDR identifica gli errori di configurazione e l'esposizione delle credenziali che rendono possibile il movimento laterale; In questo modo, ti consente di bloccare gli aggressori che hanno superato le difese basate sul perimetro e che cercano di mettere in atto queste tecniche nell'ambiente aziendale.

Zscaler ITDR sblocca nuove potenti funzionalità che estendono le capacità del tuo programma zero trust senza aggiungere ulteriori costi operativi o risorse.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata su SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter su **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it