Fiche produit

Zscaler ITDR™

Réaliser la sécurité axée sur l'identité avec Zero Trust

Zscaler ITDR (Identity Threat Detection and Response) détecte et protège contre les attaques basées sur l'identité, telles que le vol d'informations d'identification et l'abus de privilèges, les assauts d'Active Directory et les droits d'accès risqués.

L'identité est la nouvelle surface d'attaque

Les hackers font désormais appel à des méthodes sophistiquées pour cibler les identités et les systèmes d'identité. Face à l'augmentation des attaques basées sur l'identité, les entreprises modernes doivent être en mesure de détecter si des hackers exploitent, abusent ou volent les identités de l'entreprise. Les techniques de détection des menaces et les systèmes d'identité traditionnels se révèlent souvent inefficaces, car ils n'ont pas été conçus pour gérer les menaces basées sur l'identité. Zscaler ITDR atténue le risque de cybermenaces ciblant les identités et l'infrastructure d'identité (Active Directory sur site).

Zscaler ITDR

Zscaler ITDR vous permet de surveiller votre Active Directory afin de détecter les erreurs de configuration ou les vulnérabilités qui vous exposent à des risques d'élévation des privilèges et de déplacement latéral. Il sécurise vos identités et procure une visibilité étendue sur la surface d'attaque des identités pour fournir des notifications en temps réel concernant les attaques basées sur l'identité. Vous pouvez désormais détecter et stopper les attaques basées sur l'identité telles que le vol d'identifiants, les contournements d'authentification multifacteur et les techniques d'élévation des privilèges.

Avantages

- **Détecter en temps réel les menaces liées à l'identité :** les systèmes d'identité évoluent constamment en fonction des changements de configuration et d'autorisation. Surveillance en temps réel et alerte en cas de nouvelles vulnérabilités, de nouveaux risques et de nouveaux problèmes.
- **Réduire la surface d'attaque de l'identité :** visibilité et remédiation des erreurs de configuration de l'identité et des permissions risquées sources d'exposition.
- **Atténuer le risque d'une attaque d'identité :** découverte des configurations à risque telles que l'exposition des mots de passe GPP, la délégation sans contrainte et les mots de passe périmés qui ouvrent de nouvelles voies d'attaque.
- **Accélérer l'investigation et la réponse :** les équipes de sécurité peuvent prioriser les enquêtes sur les alertes en fonction des scores de risque générés par les évaluations de l'identité.
- **Rationaliser la remédiation :** les équipes de sécurité peuvent désormais exploiter les conseils de remédiation étape par étape de Zscaler ITDR, ainsi que les tutoriels vidéo, les scripts et les commandes pour accélérer la réponse.
- **Déploiement aisé :** nul besoin de machines virtuelles supplémentaires. Le même connecteur client Zscaler permet de fournir une couche de sécurité supplémentaire pour contrecarrer les menaces basées sur l'identité.

5/10

Entreprises hackées par Active Directory

Source : EMA

80 %

Des attaques modernes sont basées sur l'identité

Source : Crowdstrike

90 %

des missions IR de Mandiant impliquent AD

Source : Dark Reading

Comment ça marche ?

Zscaler ITDR adopte une approche de la sécurité des identités à la fois simple et peu contraignante sur le plan opérationnel. Il est intégré à Zscaler Client Connector, un agent unifié qui gère en toute sécurité les connexions entre les utilisateurs et les applications/ressources.

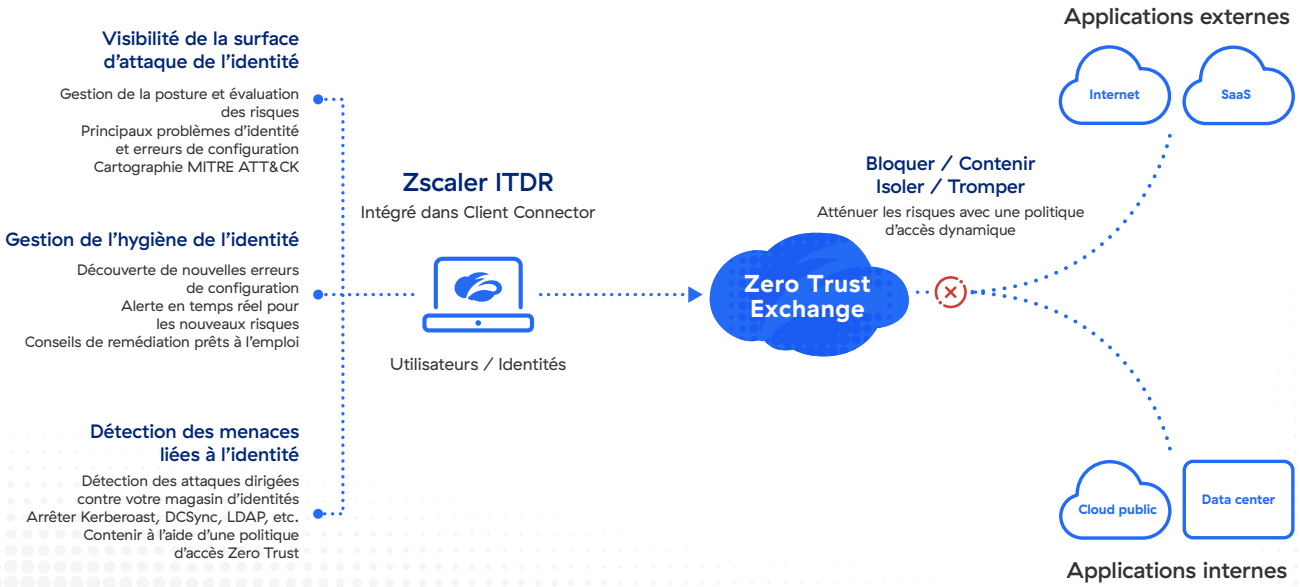
Zscaler ITDR se compose de trois fonctionnalités :

- Visibilité de la surface d'attaque de l'identité
- Détection des changements d'identité
- Détection des menaces liées à l'identité

Visibilité de la surface d'attaque

Zscaler ITDR audite l'Active Directory en exécutant des requêtes LDAP pour établir une carte des schémas, des utilisateurs, des ordinateurs, des unités organisationnelles et d'autres objets de votre magasin d'identités. Il effectue ensuite des vérifications sur ces objets pour trouver les erreurs de configuration et les vulnérabilités présentes dans votre Active Directory.

- Pour évaluer l'Active Directory, Zscaler ITDR doit s'exécuter sur un Client Connector installé sur une machine Windows reliée à un domaine.
- L'équipe de sécurité configure une analyse en spécifiant le domaine Active Directory auquel elle souhaite accéder et en sélectionnant la machine équipée du Client Connector à partir de laquelle l'analyse doit être exécutée.
- L'évaluation dure entre 15 et 30 minutes, selon la taille de l'Active Directory.
- Une fois l'évaluation terminée, les résultats sont disponibles dans le tableau de bord.
- L'évaluation comprend un score de risque du domaine, des zones de priorité pour la remédiation, une liste des utilisateurs et des ordinateurs les plus à risque, une analyse de base de la gravité et des catégorisations du risque, le mappage de la chaîne d'exécution de MITRE ATT&CK et une liste complète des erreurs de configuration découvertes.



Pour chaque erreur de configuration, la solution fournit les éléments suivants :

- Catégorisation du risque
- Gravité
- Effort de remédiation
- ID et tactique MITRE ATT&CK
- Explication de la problématique
- Impact potentiel
- Liste des utilisateurs, des ordinateurs et des objets concernés
- Directives pour la remise en état
- Tutoriels vidéo
- Scripts
- Commandes

Détection des changements d'identité

Une fois l'évaluation configurée, les équipes de sécurité ont la possibilité d'activer la détection des changements pour le domaine Active Directory. La détection des changements fait remonter à la surface les configurations qui affectent la posture de sécurité d'Active Directory en temps quasi réel, ce qui permet aux équipes de sécurité et aux administrateurs de répertoires de réagir rapidement.

- Zscaler ITDR exécute une série de contrôles de configuration prioritaires sur Active Directory.
- L'étendue de ces vérifications vise à découvrir les problèmes qui présentent le plus grand risque de violation.
- Ces vérifications sont exécutées toutes les 15 minutes à partir du endpoint muni de Client Connector pour le domaine donné.
- Les modifications sont marquées comme ayant un impact positif ou négatif.
- Un impact positif signifie qu'un problème a été résolu.
- Un impact négatif signifie qu'un problème potentiel a été introduit.

Détection en temps réel des menaces liées à l'identité

Zscaler ITDR dispose d'une capacité de détection des menaces qui alerte les équipes SOC et les chasseurs de menaces en cas d'activités potentiellement malveillantes liées à l'utilisation abusive et au vol d'identités.

Identity Threat Detection peut être activé en tant que politique de terminal sur les machines désignées équipées de Client Connector désignées.

- Les équipes de sécurité activent la politique de détection des menaces qui permet de surveiller les événements sur le système et d'analyser les modèles pour détecter les indicateurs des vecteurs de menace choisis.
- Les détecteurs disponibles sont notamment DCSync, DCShadow, kerberoasting, l'énumération des sessions, l'accès aux comptes privilégiés, l'énumération LDAP, etc.
- Les équipes de sécurité peuvent choisir d'activer tous les détecteurs ou une combinaison de détecteurs sur les endpoints désignés.
- Si un schéma est observé, Client Connector signale à Zscaler ITDR qu'une menace a été détectée.
- La plateforme enrichit le signal de menace d'informations pertinentes permettant à l'utilisateur de mener une enquête.
- L'équipe de sécurité peut configurer des capacités d'orchestration qui permettent à Zscaler ITDR d'entreprendre des actions automatisées allant de l'alerte à la remédiation en passant par la transmission.

Principaux cas d'utilisation

Visibilité de la surface d'attaque de l'identité

L'évaluation continue de votre Active Directory fournit un score de risque unifié, une liste des erreurs de configuration et des vulnérabilités, ainsi que des conseils de remédiation permettant de corriger ces problèmes.

- Score de risque unifié pour la quantification et le suivi de la posture d'identité
- Vue en temps réel des principaux problèmes d'identité et des utilisateurs/hôtes les plus risqués
- Cartographie MITRE ATT&CK pour une visibilité sur les zones d'ombre de la sécurité

Gestion de la santé des identités

Vous recevez des alertes et des notifications en temps réel lorsque de nouveaux risques sont introduits dans votre Active Directory. Visibilité en temps réel de la configuration des risques et des changements d'autorisation.

- Identifier les nouvelles vulnérabilités et les erreurs de configuration à mesure qu'elles apparaissent
- Alerte en temps réel sur les nouveaux risques introduits dans votre magasin d'identité
- Conseils, commandes et scripts de remédiation prêts à l'emploi

Identity Threat Detection and Response

Détection des menaces en temps réel pour les principales attaques liées à l'identité

- Détecter les attaques contre votre magasin d'identités
- Les détections incluent kerberoast, DCSync et l'énumération LDAP
- Confinement intégré à l'aide d'une politique d'accès Zero Trust

Principaux facteurs de différenciation

Intégré au Client Connector

Intégré au Client Connector de Zscaler, Zscaler ITDR offre de nouvelles capacités et protections prêtes à l'emploi. Le même client endpoint qui connecte en toute sécurité les utilisateurs à Internet et aux applications offre désormais des capacités de sécurité supplémentaires et atténue le risque d'attaques de l'identité.

Intégré à Zero Trust Exchange

Zscaler Identity s'intègre de manière transparente à la plateforme Zscaler Zero Trust Exchange pour une meilleure détection des menaces et une meilleure réponse aux menaces basées sur l'identité. Zero Trust Exchange peut appliquer dynamiquement des contrôles de politique d'accès afin de bloquer les utilisateurs compromis lorsqu'une attaque d'identité est détectée.

Intégrations sans faille

Renforce l'investigation et la réponse avec des intégrations étroites qui incluent des EDR tels que Crowdstrike, Microsoft Defender, VMware CarbonBlack, et tous les principaux SIEM.

Renforcer votre posture de sécurité avec Zscaler ITDR

Défense contre les menaces liées à l'identité

Une visibilité sur les identités est essentielle pour détecter les menaces basées sur l'identité. Zscaler ITDR fournit une visibilité approfondie sur les incidents et les anomalies liés aux identités dans votre environnement informatique, de sorte que vous puissiez contrecarrer les attaques basées sur l'identité avant qu'elles ne se produisent.

Détecter les attaques d'Active Directory

Les Active Directories sont des cibles très prisées pour les attaques basées sur l'identité. Zscaler ITDR surveille en permanence AD/Azure AD pour détecter les vulnérabilités et les erreurs de configuration ou les configurations risquées.

Prévenir l'utilisation abusive/le vol d'identifiants

Les hackers utilisent des identifiants volés et attaquent l'Active Directory pour élever les privilèges afin de se déplacer latéralement. Zscaler ITDR aide à détecter les exploitations d'identifiants et à prévenir leur vol ou leur utilisation abusive.

Enrayer les déplacements latéraux

Zscaler ITDR identifie les erreurs de configuration et les expositions d'identifiants qui ouvrent des voies d'attaque pour les déplacements latéraux. Il arrête les hackers qui ont franchi les défenses périmétriques et tentent de se déplacer latéralement dans votre environnement.

Zscaler ITDR débloque de puissantes nouvelles fonctionnalités qui élargissent les capacités de votre programme Zero Trust sans ajouter de surcharge opérationnelle ni de ressources supplémentaires.

zscaler™ | Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique de ses clients pour qu'ils gagnent en agilité, efficacité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications, indépendamment de l'emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SSE constitue la plus vaste plateforme intégrée de sécurité cloud. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.fr