Gestion de l'exposition des actifs : obtenez des informations CAASM précises et exploitables

Suivez tous vos actifs. Corrigez vos lacunes. Réduisez les risques.

Défi commercial

Les équipes de sécurité passent d'innombrables heures à concilier les informations provenant de plusieurs systèmes disparates dans le but de créer un inventaire précis des actifs. Malgré tous ces efforts, les listes d'actifs restent incomplètes et inexactes, ce qui compromet gravement l'évaluation des risques. De plus, lorsque les équipes relèvent des informations manquantes ou incorrectes, les outils actuels compliquent considérablement la mise à jour des données. La plupart des équipes ont du mal à répondre à des questions de sécurité critiques telles que :

- De combien d'actifs disposons-nous actuellement ?
- Quelle est la précision de notre CMDB ?
- À qui attribuer une demande d'assistance pour corriger un actif spécifique ?
- Quel est le niveau de protection de chacun de nos actifs les plus précieux ?
- Quel est l'utilisateur, la zone géographique, le service, etc. de chaque actif ?
- Quels actifs ne disposent pas de logiciels de protection comme l'EDR ?

Obtenir un « enregistrement de référence » haute fidélité de tous vos actifs grâce à notre approche fondamentalement différente de la CAASM

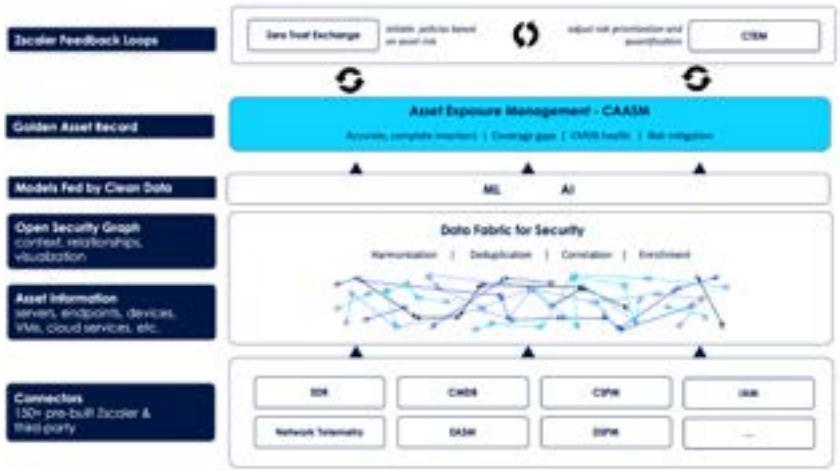
La solution de gestion de l'exposition des actifs de Zscaler, Asset Exposure Management, fournit l'inventaire d'actifs le plus complet, le plus précis et le plus riche en contexte du secteur. En exploitant la corrélation des données rendue possible par la Data Fabric for Security brevetée, l'approche unique de la CAASM de Zscaler vous permet d'identifier les lacunes en termes de couverture, d'automatiser l'hygiène de la CMDB, de générer des flux de travail pour l'atténuation et de réduire le risque lié aux actifs. Elle sert de source unique et fiable des actifs sur laquelle l'équipe chargée de la sécurité et de l'informatique, ainsi que d'autres groupes de l'entreprise, peuvent s'appuyer pour améliorer la sécurité et la conformité, ainsi que de base pour les solutions de gestion continue de l'exposition aux menaces (CTEM).

- **Créer un inventaire fiable des actifs :**
  Facilitez la résolution des actifs à travers des dizaines de systèmes sources pour créer un inventaire global et précis.
- **Découvrir et combler les lacunes en ternes de couverture des actifs :**
  Corrélez tous les détails des actifs pour identifier les erreurs de configuration et les contrôles manquants.
- **Minimiser les risques qui pèsent sur votre entreprise :**
  Activez des politiques d'atténuation des risques, assignez et suivez les flux de travail, et mettez automatiquement à jour votre CMDB.
- **Mener un programme de CTEM efficace :**
  Veillez à ce que votre programme de gestion de l'exposition de bout en bout est alimenté par des informations détaillées et complètes sur les actifs.

Comment ça marche ?

Une gestion efficace de l'exposition des actifs nécessite la découverte et la corrélation d'une myriade de sources de données qui étaient auparavant cloisonnées. Zscaler a été le premier fournisseur à utiliser une « data fabric » ou structure de données qui transforme fondamentalement l'évolutivité et l'efficacité de la gestion de la surface d'attaque des actifs numériques (CAASM).

Le composant Zscaler Data Fabric for Security agrège et corrèle de manière transparente les informations sur les actifs de plus de 150 outils de sécurité et systèmes d'entreprise, ce qui permet aux entreprises de mieux comprendre et gérer leur surface d'attaque. En harmonisant, dédupliquant, corrélant et enrichissant des millions de points de données, la Data Fabric permet de mieux comprendre les actifs, les contrôles, les lacunes et les erreurs de configuration. Les boucles de rétroaction au sein de l'écosystème Zscaler élargi renforcent davantage la capacité à atténuer automatiquement ces expositions des actifs.



Pour en savoir plus, rendez-vous sur : zscaler.com/fr/caasm

Réduisez la surface d'attaque de vos actifs grâce aux mesures suivantes :

- **Créer un inventaire d'actifs unifié et dédupliqué :**
  Bénéficiez d'une visibilité complète sur tous vos actifs, y compris les terminaux, les ressources cloud, les périphériques réseau, etc. Obtenez une représentation complète de la surface d'attaque de vos actifs en effectuant en continu la déduplication, la corrélation et la résolution des détails des actifs entre les sources.
- **Identifier et suivre les problèmes de conformité et les erreurs de configuration :**
  Identifiez facilement les problèmes de conformité et erreurs de configuration potentiels, tels que les actifs dépourvus d'EDR ou les versions d'agent obsolètes, et transformez-les en tâches exploitables pour améliorer votre posture de sécurité.
- **Augmenter le niveau de confiance en votre CMDB :**
  Améliorez la précision et l'exhaustivité de la CMDB. Identifiez les actifs non enregistrés dans votre CMDB ou les informations manquantes sur le propriétaire, l'emplacement ou d'autres détails. Créez des flux de travail pour vos équipes de gestion d'actifs afin de garantir l'exhaustivité et la précision des détails des actifs.
- **Mener des actions d'atténuation des risques efficaces :**
  Initiez des ajustements de politiques et d'autres contrôles pour réduire les risques, activez des flux de travail pour attribuer les violations de politiques à leurs propriétaires et suivez les progrès de l'atténuation, et mettez automatiquement à jour votre CMDB pour davantage de précision et d'exhaustivité.
- **Améliorer la collaboration entre les équipes grâce à des rapports et des tableaux de bord robustes :**
  Générez des tableaux de bord et des rapports relatifs à l'état de santé de la CMDB et aux contrôles de conformité en vous appuyant sur une bibliothèque de métriques prédéfinies et personnalisées.

zscaler™ | **Experience your world, secured.™**

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288

Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134

zscaler.com/fr