Zscaler Zero Trust Device Segmentation pour OT/IoT

Prévenir le déplacement latéral, réduire la surface d'attaque & améliorer les opérations de sécurité

Présentation de la solution

La problématique

Récemment, les alertes et mises en garde se sont multipliées concernant les cyberattaques initiées par des États-nations sur des infrastructures critiques aux États-Unis. Le 7 février 2024, le Federal Bureau of Investigation (FBI), la Cybersecurity and Infrastructure Security Agency (CISA), ainsi que la National Security Agency (NSA), ont lancé un avertissement à l'intention des acteurs du service public et concernant des cybercriminels ciblant des infrastructures critiques (systèmes de transport, oléoducs et gazoducs, usines de traitement des eaux et réseaux électriques) Cette alerte vient en complément d'actions similaires prises par la Transportation Security Administration américaine (sécurisation des aéroports, des opérateurs d'avions et du chemin de fer), du récent document de référence du Département de l'Énergie des États-Unis (DoE) sur la cybersécurité et de la nouvelle version quasi définitive de la norme CIP-015-1 du NERC.

Les technologies OT/IoT ont pour priorité d'accélérer les transactions et de les rendre plus efficaces, la sécurité n'étant qu'un objectif secondaire. Il en résulte que les environnements OT/IoT sont devenus une cible privilégiée pour les cybercriminels, comme le souligne ce bond vertigineux de 400 % des attaques en un an, selon une étude de Zscaler ThreatLabz. Le ransomware est le vecteur d'attaque la plus utilisé tandis que 61 % de toutes les intrusions visaient des entreprises connectées à l'OT.

Que pouvez-vous faire ?

L'EPA (Environmental Protection Agency), la CISA et le FBI recommandent fortement aux opérateurs de systèmes d'adopter une approche Zero Trust pour renforcer leur cybersécurité.

Cette recommandation peut être mise en œuvre avec Zscaler grâce à sa solution Zero Trust Device Segmentation et à ses atouts :

- Moindre exposition à l'Internet public
- Moindre exposition aux vulnérabilités
- Segmentation du réseau
- Recueil des logs
- Neutralisation des connexions d'utilisateurs non autorisés
- Aucun service pouvant être ciblé à partir d'Internet
- Limitation des connexions OT/IoT vers Internet
- Détection pertinentes des menaces
- Inventaire des ressources OT/IT

Comment procéder ?

La segmentation a toujours été une pratique essentielle pour les réseaux, avec des outils tels que les listes de contrôle d'accès (ACL) et les pare-feu gérant le trafic entrant-sortant (client vers serveur). Cependant, la microsegmentation OT se focalise sur le trafic interne plus vulnérable, qui est acheminé latéralement entre les dispositifs et les instances. Sur les VLAN mutualisés, avec une architecture de commutation traditionnelle, les dispositifs peuvent se voir et communiquer entre eux, ce qui crée un environnement propice à la propagation des malwares. Les solutions faisant appel à des agents, conçues pour les instances cloud, ne peuvent pas segmenter les machines traditionnelles et headless, courantes dans le domaine de l'OT, tandis que les approches traditionnelles basées sur les listes ACL restent trop complexes.

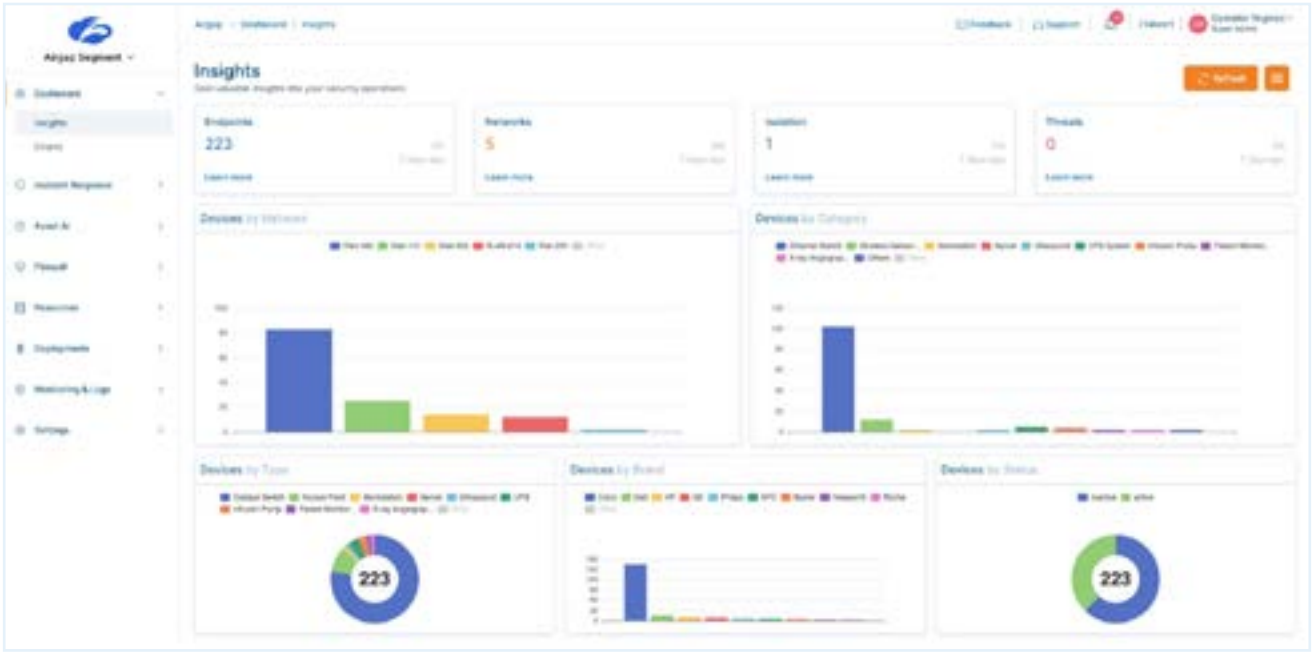


Tableau de bord de Zero Trust Device Segmentation

Zscaler simplifie la segmentation intra-VLAN grâce à une solution sans agent qui empêche toute menace de se propager latéralement : chaque terminal IP, y compris les systèmes traditionnels et headless, est cloisonné dans un « segment de réseau unique ». Cette approche se substitue à la gestion complexe des listes ACL. Elle n'implique aucune modification de l'infrastructure existante, tout en offrant une segmentation granulaire et efficace.

Cas d'utilisation

Voici les cas d'utilisation les plus courants de cette segmentation des dispositifs, sans agent :

Microsegmentation du LAN

Déployez le Zero Trust sur le réseau local grâce à une segmentation du trafic interne. Cette approche réduit votre surface d'attaque interne et élimine le risque de déplacement latéral au sein des réseaux OT/IoT critiques, sans recourir à une segmentation basée sur un contrôle NAC ou un pare-feu.

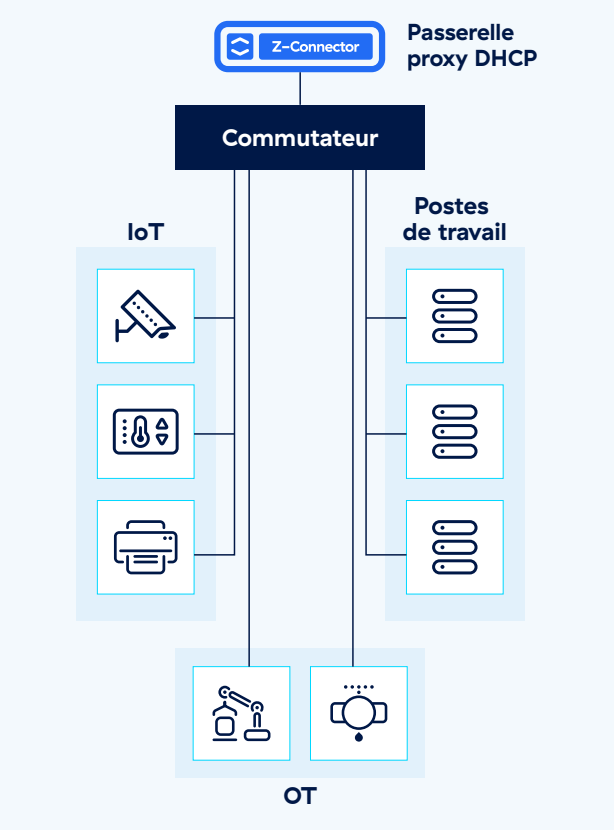
Pour appliquer une segmentation Zero Trust sur votre réseau :

- Cloisonnez automatiquement chaque dispositif au sein d'un segment unique.
- Regroupez automatiquement les dispositifs, les utilisateurs et les applications en analysant leurs schémas de trafic, empêchant ainsi les dispositifs indésirables d'usurper une adresse MAC pour accéder au réseau.
- Appliquez de manière dynamique des politiques pour le trafic interne en fonction de l'identité et du contexte des utilisateurs et dispositifs.

Segmentation IT/OT

La technologie Zero Trust Device Segmentation de Zscaler agit comme un coupe-circuit anti-ransomware. Elle désactive les communications non essentielles des dispositifs pour prévenir le déplacement latéral des menaces, sans perturber les opérations métiers. Cette solution neutralise les menaces avancées telles que les ransomwares sur les dispositifs IoT, les systèmes OT et les dispositifs qui ne peuvent acceuillir un agent logiciel.

- Regroupez et appliquez de manière autonome la politique pour les adresses MAC connues sur n'importe quel dispositif (par exemple, l'accès RDP aux caméras refusé sauf pour les administrateurs).
- Isolez automatiquement les adresses MAC inconnues pour limiter le rayon d'impact d'une intrusion sur un dispositif.
- Procédez à une intégration avec les systèmes de gestion de ressources/d'actifs dans le cadre de politiques de contrôle d'accès sécurisé.



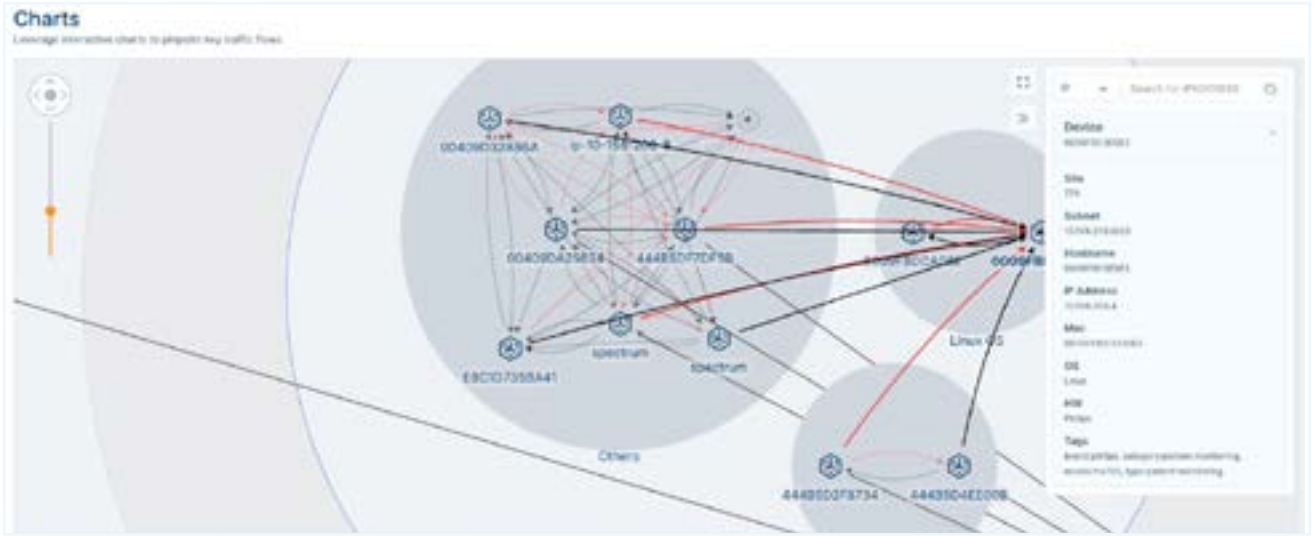
Segmentation OT/IoT automatisée – Segment « unique » pour chaque appareil

Identification et classification automatiques des dispositifs

Étant donné qu'une part importante du trafic OT/IoT reste sur le périmètre interne du réseau local, vous devez impérativement disposer d'une visibilité continue sur le trafic interne. Grâce à l'identification et à la classification automatiques des dispositifs, les administrateurs réseau peuvent mieux gérer les performances, le temps de fonctionnement et la sécurité des systèmes IoT/OT, sans subir une gestion complexe de l'inventaire.

Pour la visibilité sur le réseau et les dispositifs :

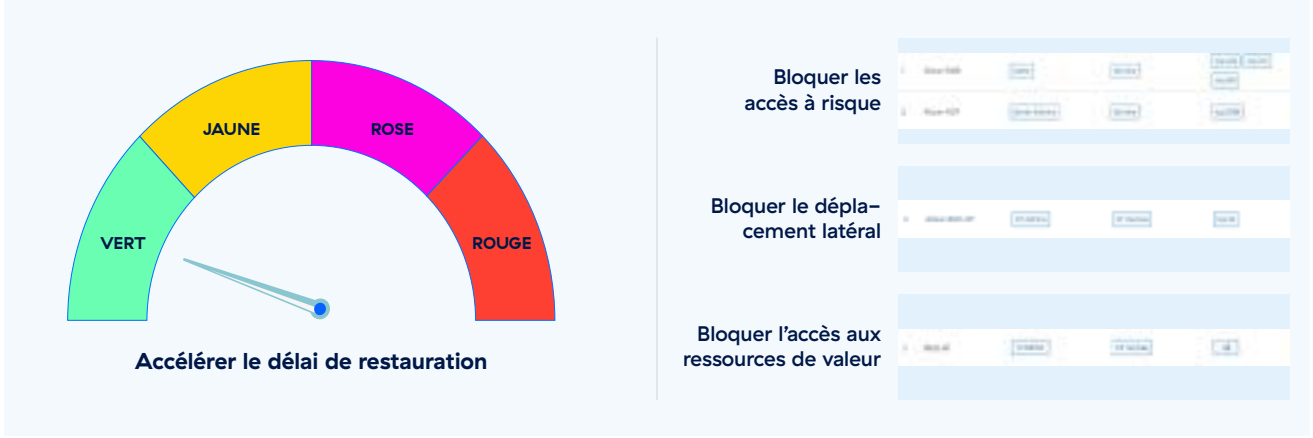
- Identifiez, classifiez et inventoriez les dispositifs OT/IoT sans faire appel à un agent logiciel.
- Établissez une base de référence de vos schémas de trafic et de comportements de vos dispositifs pour identifier les accès autorisés et non autorisés.
- Obtenez des informations précises sur le réseau pour gérer les performances et cartographier les menaces.



Cartographie des dispositifs identifiés

Réponse automatisée aux incidents

Zscaler Ransomware Kill Switch permet à l'utilisateur de réduire sa surface d'attaque. Choisissez simplement un niveau de gravité prédéfini pour verrouiller progressivement les protocoles et ports vulnérables connus, et même désactiver instantanément l'accès à des réseaux entiers, comme ceux d'une chaîne de production ou d'un hôpital. La prise en charge des intrusions est précise : identifiez et jugulez chaque menace sans freiner vos activités métiers.



Échangez avec un expert technique

Vous souhaitez en savoir plus sur l'accompagnement de Zscaler pour vous aider à protéger vos activités critiques ? Prenez rendez-vous avec un de nos experts techniques.

zscaler™ | Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, 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 dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. 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