Zscaler Zero Trust Segmentation des dispositifs pour l'Industrie 4.0



©2025 Zscaler, Inc. Tous droits réservés.

LIVRE BLANC

À l'ère de l'Industrie 4.0, où la production industrielle intelligente et les systèmes industriels interconnectés deviennent la norme, l'architecture Zero Trust s'est imposée comme un cadre de sécurité essentiel. Les approches de sécurité traditionnelles basées sur le périmètre ne suffisent plus à protéger l'écosystème complexe des appareils de technologie opérationnelle (OT) et des systèmes de contrôle industriels. Le principe fondamental du Zero Trust, « ne jamais faire confiance, toujours vérifier », élimine la confiance implicite dans le réseau en fournissant un accès sécurisé et authentifié aux systèmes critiques. Cette approche est particulièrement cruciale dans les environnements industriels où une faille de sécurité pourrait entraîner des interruptions d'activité importantes, une perte de réputation et des répercussions réglementaires.

Cybersécurité pour le secteur de la production industrielle

Les réseaux modernes de production industrielle ont évolué en écosystèmes complexes où les systèmes de technologie opérationnelle (OT) et de technologie de l'information (IT) sont profondément interconnectés. Cette convergence permet des fonctionnalités avancées telles que la maintenance prédictive, l'intégration de la chaîne d'approvisionnement et la gestion des opérations à distance. Cependant, cette interconnexion crée également de nouveaux défis en matière de sécurité, car les réseaux OT traditionnellement isolés se retrouvent exposés aux menaces liées aux technologies de l'information. Les entreprises se concentrent sur deux grands axes :

- **Accès sécurisé aux équipements OT :** les environnements de production industrielle exigent un contrôle strict des accès aux équipements technologiques opérationnels, tels que les automates programmables industriels (PLC), les interfaces homme-machine (IHM) et les systèmes de contrôle industriels. La solution Zscaler Privileged Remote Access permet un accès rapide, direct et sécurisé aux équipements technologiques opérationnels (OT) sur le terrain, en usine ou à distance, sans VPN ni agent. Pour plus d'informations sur Zscaler Privileged Remote Access, accédez à https://www.zscaler.com/fr/resources/data-sheets/privileged-remote-access-for-ot-and-iiot.pdf.

- **Segmentation :** dans les environnements de production, le risque qu'une menace se déplace latéralement dans le réseau constitue un enjeu majeur. Ce danger est particulièrement critique dans les environnements industriels où

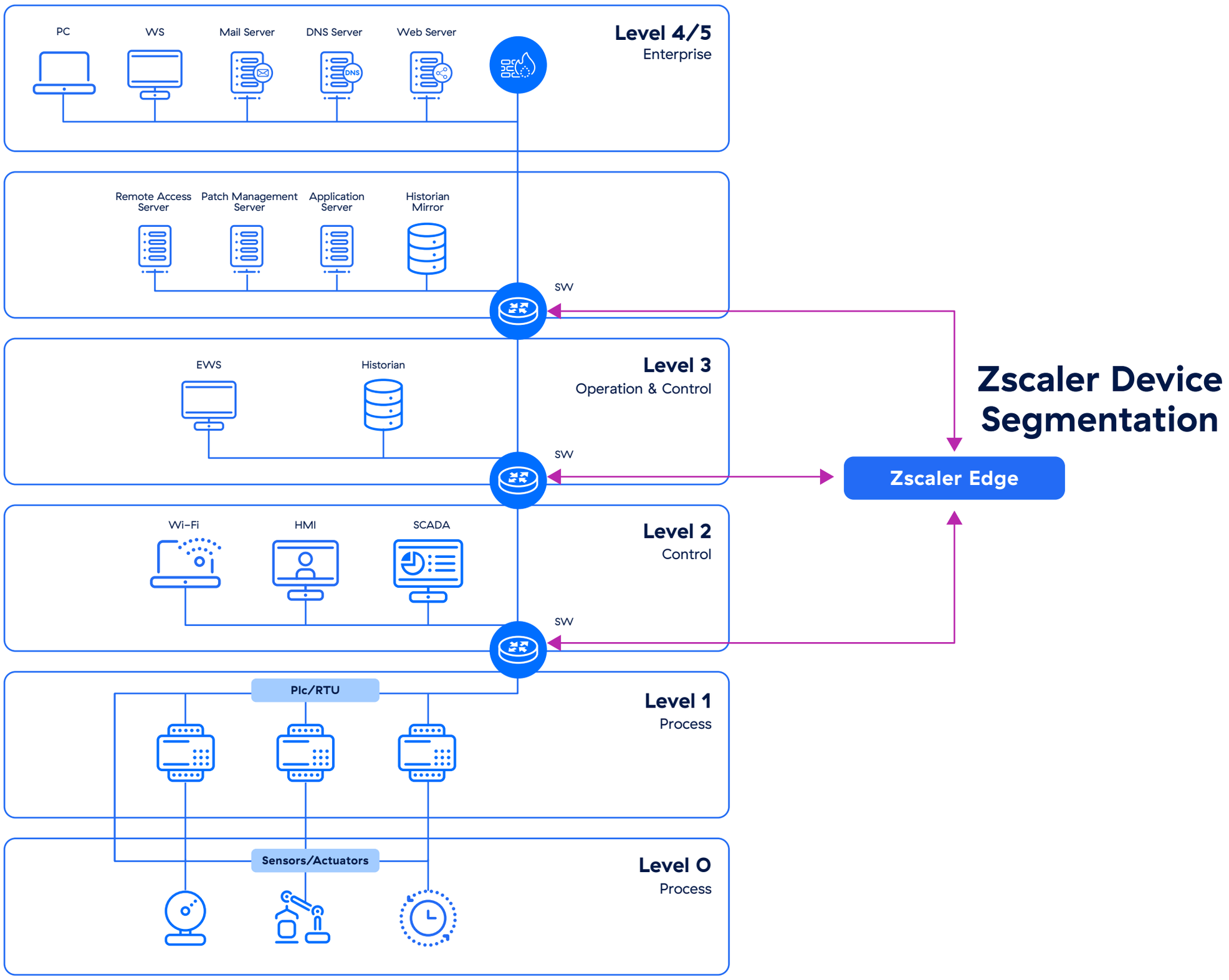
des systèmes anciens, souvent dépourvus de mécanismes de sécurité modernes, sont interconnectés avec des équipements modernes. Appliquer les principes du Zero Trust via la micro-segmentation permet de contenir ces menaces en imposant un contrôle d'accès strict fondé sur des politiques. Même en cas de violation initiale, cette approche limite fortement les déplacements latéraux d'un attaquant.

Le composant Zscaler Private Access et la segmentation Zero Trust fonctionnent de concert pour établir un cadre de sécurité robuste pour les actifs OT dans les réseaux de production industrielle. Cette stratégie de sécurité globale garantit que les opérations de production industrielle restent protégées contre les menaces externes et les vulnérabilités internes, tout en préservant la flexibilité nécessaire à un fonctionnement efficace.

© 2025 Zscaler, Inc. Tous droits réservés.

Segmentation dans le secteur de la production industrielle

Dans les réseaux de contrôle industriels ou de production industrielle typiques, plusieurs types d'appareils sont connectés au réseau. Selon le modèle Purdue, ces appareils peuvent être classés en différents niveaux.



Niveau Purdue	Dispositifs	Description	Risque
Niveau 3	Systèmes des historiques de données, serveurs de saut, serveurs de correctifs	Fonctionne avec des systèmes d'exploitation bien connus, par exemple, Windows. Malgré l'existence d'options EDR, les menaces latérales présentent toujours des risques de sécurité.	Moyen à élevé
Niveau 2	IHM, SCADA	Fonctionne avec des systèmes d'exploitation intégrés (par exemple, Windows CE, Windows XP). Ces systèmes anciens présentent de graves vulnérabilités et des risques de sécurité importants.	Gravité élevée
Niveau 1	PLC, RTU	Appareils headless bas de gamme nécessitant des outils spéciaux pour programmer et modifier les paramètres.	Faible à moyen
Niveau 0	Capteurs, actionneurs	Systèmes principalement non basés sur le protocole IP qui effectuent des fonctions très spécifiques.	Bas

© 2025 Zscaler, Inc. Tous droits réservés.

Ces différents types d'appareils OT établissent des schémas de communication et des interdépendances complexes qui permettent des processus de production industrielle sans faille, maintiennent la continuité opérationnelle et garantissent une production fiable sur l'ensemble de la chaîne de production. La solution Zscaler Zero Trust Device Segmentation (Zscaler ZTDS) fournit des mesures de sécurité complètes pour protéger les opérations de production industrielle en mettant en œuvre des contrôles d'accès robustes et en établissant des limites de communication claires entre différents types d'appareils industriels. Cette stratégie de segmentation avancée contribue à maintenir l'intégrité et la fiabilité des processus de production industrielle tout en protégeant les entreprises contre les menaces de sécurité potentielles et les tentatives d'accès non autorisé.

Cas d'utilisation 1

Communications Internet

Dans les environnements modernes de production industrielle, les systèmes OT nécessitent de plus en plus une connectivité Internet pour divers besoins opérationnels, notamment les mises à jour logicielles, l'assistance aux fournisseurs et l'analyse de données dans le cloud. Cependant, cette exposition à Internet augmente considérablement la surface d'attaque des réseaux industriels. Les systèmes OT auparavant isolés deviennent vulnérables aux cybermenaces courantes telles que les malwares, les ransomwares et les menaces persistantes avancées (APT). Les risques sont particulièrement aigus, car de nombreux appareils OT ont été conçus sans fonctionnalités de sécurité intégrées et fonctionnent souvent avec des systèmes d'exploitation obsolètes qui ne peuvent pas être facilement corrigés ou mis à jour.

Toutes les communications Internet sont protégées par Zscaler ZIA, les connexions sortantes des ressources OT étant acheminées via ce service.

VALEUR CLÉ DE ZSCALER ZIA :

- **Protection avancée contre les menaces :** ZIA assure une protection complète contre les malwares, les ransomwares et les menaces de type « zero day » grâce à une inspection multicouche de l'ensemble du trafic Internet provenant des ressources OT.

- **Filtrage du trafic sortant :** la solution applique des contrôles d'accès stricts en limitant les communications des appareils OT aux seules destinations autorisées et en bloquant les sites Web/contenus potentiellement malveillants.

- **Renseignements sur les menaces en temps réel :** la solution exploite les renseignements du cloud au niveau mondial pour identifier et bloquer les menaces émergentes avant qu'elles n'affectent les actifs OT.

© 2025 Zscaler, Inc. Tous droits réservés.

Cas d’utilisation 2

Communications entre les systèmes OT et IT

Les communications entre les systèmes OT et IT dans les environnements de production industrielle représentent un point de convergence critique où les systèmes OT doivent interagir avec l’infrastructure informatique. Cette intégration permet des fonctions essentielles telles que l’analyse de données, la surveillance à distance et la planification des ressources de l’entreprise. Cependant, ces communications créent également d’importantes failles de sécurité. Les réseaux informatiques, généralement connectés à Internet et régulièrement mis à jour, doivent communiquer avec des systèmes OT qui utilisent souvent des logiciels et des protocoles obsolètes, non conçus pour répondre aux exigences de sécurité modernes.

Cette disparité en matière de capacités de sécurité crée des points d’entrée potentiels pour les cyberattaques.

VALEUR CLÉ DE ZSCALER DEVICE SEGMENTATION :

- Traditionnellement, les réseaux IT et OT étaient construits séparément, avec des espaces physiques entre eux. Cependant, avec la modernisation, ces frontières s’estompent. La solution Zscaler Device Segmentation contribue à maintenir la séparation entre les réseaux IT et OT sans compromettre la productivité et la valeur que la modernisation apporte aux réseaux industriels.

- Malgré l’existence de VLAN distincts, les systèmes IT et OT finissent souvent par partager le même réseau en raison d’une mauvaise configuration ou de changements rapides au niveau de l’entreprise. La technologie brevetée de Zscaler ZTDS identifie tous les systèmes IT et OT du réseau partagé (par exemple, les VLAN) et les sépare logiquement sans nécessiter de reconfiguration des VLAN, de modifications d’adresse IP ou de refonte du réseau.

- Pour protéger les équipements existants et empêcher l’accès non autorisé aux réseaux OT, Zscaler ZTDS contribue à éliminer la confiance implicite et restreint l’accès au réseau à partir d’un système spécifique tel que JumpHosts, Zscaler ZPA et Zscaler PRA.

- Un système de gestion centralisé et hautement évolutif basé sur le cloud, doté d’un contrôle d’accès robuste s’appuyant sur les rôles et de capacités multi-entité, simplifie les opérations réseau IT et OT tout en maintenant des tâches et des contrôles administratifs distincts.

© 2025 Zscaler, Inc. Tous droits réservés.

Cas d’utilisation 3

Communications au niveau des opérations

Au niveau 3, les communications opérationnelles englobent les interactions entre divers systèmes d’exécution de la production (MES), systèmes des historiques de données et autres applications de gestion opérationnelle. Ces systèmes fonctionnent généralement selon les réseaux TCP/IP et utilisent souvent des protocoles comme OPC UA, MQTT ou les API REST pour l’échange de données. La segmentation du réseau est particulièrement importante ici, car ces systèmes font souvent le lien entre les réseaux IT et OT, ce qui en fait des cibles potentielles pour les cyberattaques.

VALEUR CLÉ DE ZSCALER DEVICE SEGMENTATION :

- Contrairement aux pare-feu traditionnels, Zscaler ZTDS fonctionne indépendamment du réseau et permet un contrôle dynamique des politiques, quelle que soit la manière dont les systèmes opérationnels se connectent au réseau. Un moteur de politique adaptatif centralisé réduit considérablement la complexité opérationnelle associée aux pare-feu traditionnels.

- Une réponse efficace aux incidents est cruciale pour réduire l’impact des cyberincidents dans les environnements critiques. Outil puissant de réponse aux incidents, le composant Zscaler Ransomware Kill-Switch prépare les entreprises aux interventions d’urgence et empêche la propagation des menaces au niveau du réseau avec une extrême précision.

- L’architecture unique de Zscaler ZTDS centralise tous les renseignements au niveau du réseau et élimine les dépendances vis-à-vis des produits ponctuels et des technologies complexes telles que les VLAN, les ACL, la norme 802.1X, les pare-feu et le routage L3.

Cas d’utilisation 4

Communications au niveau des systèmes de supervision

Au niveau 2, les communications via les systèmes de supervision impliquent des interactions critiques entre les IHM, les systèmes SCADA et d’autres systèmes de contrôle de supervision établis via les réseaux TCP/IP. Ces systèmes communiquent généralement à l’aide de protocoles industriels tels que Modbus TCP, EtherNet/IP et OPC UA, fonctionnant sur des ports réseau standard (502 pour Modbus, 44818 pour EtherNet/IP, 4840 pour OPC UA). Ils sont chargés de surveiller et de contrôler les processus industriels, de collecter des données en temps réel et de fournir des interfaces opérateur. En raison de la nature ancienne de nombreux systèmes de supervision, de leur utilisation de protocoles potentiellement vulnérables et de leur rôle critique dans les opérations, la sécurisation de ces communications est particulièrement importante grâce à une segmentation appropriée du réseau et à des contrôles de sécurité spécifiques aux protocoles. Ces communications peuvent être divisées selon les catégories suivantes :

© 2025 Zscaler, Inc. Tous droits réservés.

1. **Communications au sein du niveau 2 (par exemple, interactions IHM à IHM)**
2. **Communications entre niveau 2 et niveau 3 (par exemple, transfert de données de l'IHM vers le système des historiques de données)**

VALEUR CLÉ DE ZSCALER DEVICE SEGMENTATION :

- La technologie brevetée ZTDS de Zscaler isole de manière unique les systèmes de supervision (par exemple, IHM) connectés au niveau 2 selon le modèle Purdue, créant des limites d'isolation sécurisées qui réduisent considérablement la surface d'attaque de ces systèmes anciens et vulnérables.

- Zscaler ZTDS détecte et visualise toutes les communications entre appareils au niveau des systèmes de supervision, ainsi que les interactions avec le niveau 3 (niveau opérationnel), quelle que soit la configuration VLAN. La solution crée des cartes de trafic de ces communications et conserve les journaux de transactions dans le SIEM Elastic intégré.

- Conçu selon les principes du Zero Trust, Zscaler ZTDS s'intègre à divers outils d'entreprise, notamment CMDB et EDR, pour ajuster automatiquement les politiques de contrôle d'accès en fonction des changements de comportement. Un cadre de politiques hiérarchique permet la mise en œuvre de politiques sur un seul site, plusieurs groupes de sites ou tous les sites.

- Le cadre de politique simplifié utilise les attributs et les balises des appareils (par le biais de l'étiquetage automatique, de la saisie manuelle ou de l'importation tierce) plutôt que les adresses IP et MAC complexes.

- L'un des principaux avantages de la solution Zscaler ZTDS est qu'elle est sans agent, interopérable avec les équipements réseau existants (quel que soit le fournisseur, le modèle ou la version) et ne nécessite que des modifications minimales de la configuration réseau.

Cas d'utilisation 5

Communication au niveau du contrôle

Au niveau 1, les automates programmables industriels (PLC) et les unités terminales distantes (RTU) échangent entre eux pour coordonner les opérations des machines et le contrôle des processus. Ces appareils communiquent également avec les systèmes de niveau 2, tels que les IHM et les systèmes SCADA, afin de permettre la surveillance et le contrôle en temps réel des processus industriels. Cette couche de communication est essentielle au

maintien de l'efficacité opérationnelle et nécessite des mesures de sécurité robustes pour protéger les entreprises contre les cybermenaces potentielles tout en garantissant une latence minimale et une fiabilité élevée. Ces communications se répartissent en plusieurs catégories :

1. **Communications au sein du niveau 1 (par exemple, communications PLC à PLC)**
2. **Communications entre niveau 1 et niveau 2 (par exemple, communications PLC à IHM)**

© 2025 Zscaler, Inc. Tous droits réservés.

VALEUR CLÉ DE ZSCALER DEVICE SEGMENTATION :

- Grâce à son architecture unique, la solution Zscaler ZTDS visualise et analyse diverses communications, et offre la possibilité d'identifier et de profiler les systèmes OT connectés. Elle analyse les différents protocoles (HTTP, ENIP, Modbus, SSL, etc.) et extrait les métadonnées afin d'identifier et d'étiqueter avec précision les actifs OT.

- La solution visualise toutes les communications entre les appareils de niveau 1/L1 (PLC, RTU) et les systèmes de niveaup 2/L2 (IHM, SCADA). Elle met en œuvre des contrôles d'accès restreints pour protéger les appareils L1 sensibles (par exemple, PLC) contre des appareils L2 potentiellement vulnérables et à haut risque (par exemple, IHM).

- Lorsqu'elle est déployée en mode d'apprentissage, la solution Zscaler ZTDS identifie avec précision les modèles de communication des appareils L1 (PLC, RTU) vers les appareils L2 (IHM, etc.). Cela permet de modéliser les politiques de segmentation.

- Les appareils de niveau 1 selon le modèle Purdue sont conçus pour des fonctions spécifiques et n'appliquent pas tous les principes de réseau standard. La mise en œuvre de Zscaler ZTDS Ringfence est donc plus complexe pour ces appareils. Toutefois, l'absence de segmentation ou de cloisonnement par appareil ne compromet pas les contrôles de sécurité globaux.

- Étant donné que les menaces proviennent généralement d'appareils de niveau 2 vulnérables et à haut risque, ZTDS limite l'accès des appareils de niveau 1 aux seuls appareils de niveau 2 nécessaires aux opérations commerciales.

- Plutôt que la segmentation par appareil, ZTDS met en œuvre une segmentation au niveau macro (utilisant la définition du réseau existant) ou une segmentation au niveau groupe (les appareils L1 peuvent être regroupés en petits segments à l'aide d'Airgap–Plus).

- Étant donné que la communication entre les appareils L1 à L1 nécessite une programmation spéciale, ZTDS réduit les modifications de programmation non autorisées ou incorrectes en limitant l'accès entrant aux appareils L1.

- Toutes les autres fonctionnalités, y compris la découverte et le profilage des actifs, la visualisation du trafic, le contrôle adaptatif des politiques et le composant Ransomware Kill Switch, restent pleinement applicables aux appareils L1.

Les appareils de niveau O ou de niveau de processus selon le modèle Purdue (par exemple, capteurs et actionneurs) ne prennent pas en charge TCP/IP et communiquent généralement directement à chaque appareil de niveau 1 en utilisant les protocoles personnalisés, le bus série, etc. Ces appareils ne font pas partie du champ d'application de Zscaler Device Segmentation.

© 2025 Zscaler, Inc. Tous droits réservés.

Synthèse

Zscaler Zero Trust Device Segmentation, en tant que composante clé de la sécurité Zero Trust, joue un rôle essentiel dans l'élimination de la confiance implicite en créant des frontières logiques entre différents types d'appareils et de systèmes industriels. En mettant en œuvre des politiques de segmentation granulaires, les entreprises peuvent isoler les systèmes de production critiques des appareils potentiellement vulnérables, contenir les failles de sécurité potentielles et maintenir des contrôles d'accès stricts entre les différentes couches.

	Cas d'utilisation 1 (Internet)	Cas d'utilisation 2 (IT et OT)	Cas d'utilisation 3 (L3 — Opérations)	Cas d'utilisation 4 (L2 — Supervision)	Cas d'utilisation 5 (L1 — Contrôle)
Sans agent	✓	✓	✓	✓	✓
Indépendant du réseau	✓	✓	✓	✓	✓
Identification et profilage des ressources	✓	✓	✓	✓	✓
Visibilité du trafic	✓	✓	✓	✓	Inter-segment
Intégrations tierces	N/A	✓	✓	✓	✓
Contrôle adaptatif des politiques	✓	✓	✓	✓	Inter-segment
Ransomware Kill Switch	N/A	✓	✓	✓	✓
Gestion centralisée	✓	✓	✓	✓	✓

Les projets de segmentation échouent souvent car les solutions actuelles nécessitent des modifications importantes du réseau (comme des mises à niveau ou des actualisations d'équipements), manquent de contrôle précis ou ne couvrent pas toutes les couches des réseaux de production. Zscaler ZTDS offre une solution unique, assurant une couverture complète grâce à une plateforme sans agent, indépendante du réseau et conviviale. Zscaler ZTDS se déploie rapidement et ne nécessite aucune interruption de service. Les entreprises manufacturières peuvent désormais rejoindre les entreprises du classement Fortune 500 en utilisant Zscaler Zero Trust Device Segmentation (ZTDS) pour mettre en œuvre rapidement une segmentation Zero Trust, protégeant ainsi leurs technologies opérationnelles critiques (OT) et leurs réseaux de contrôle industriel.

À propos de Zscaler

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 de 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 **www.zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

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

zscaler™

Zero Trust Everywhere