Zscaler pour la production industrielle

Intégrer le Zero Trust au modèle Purdue

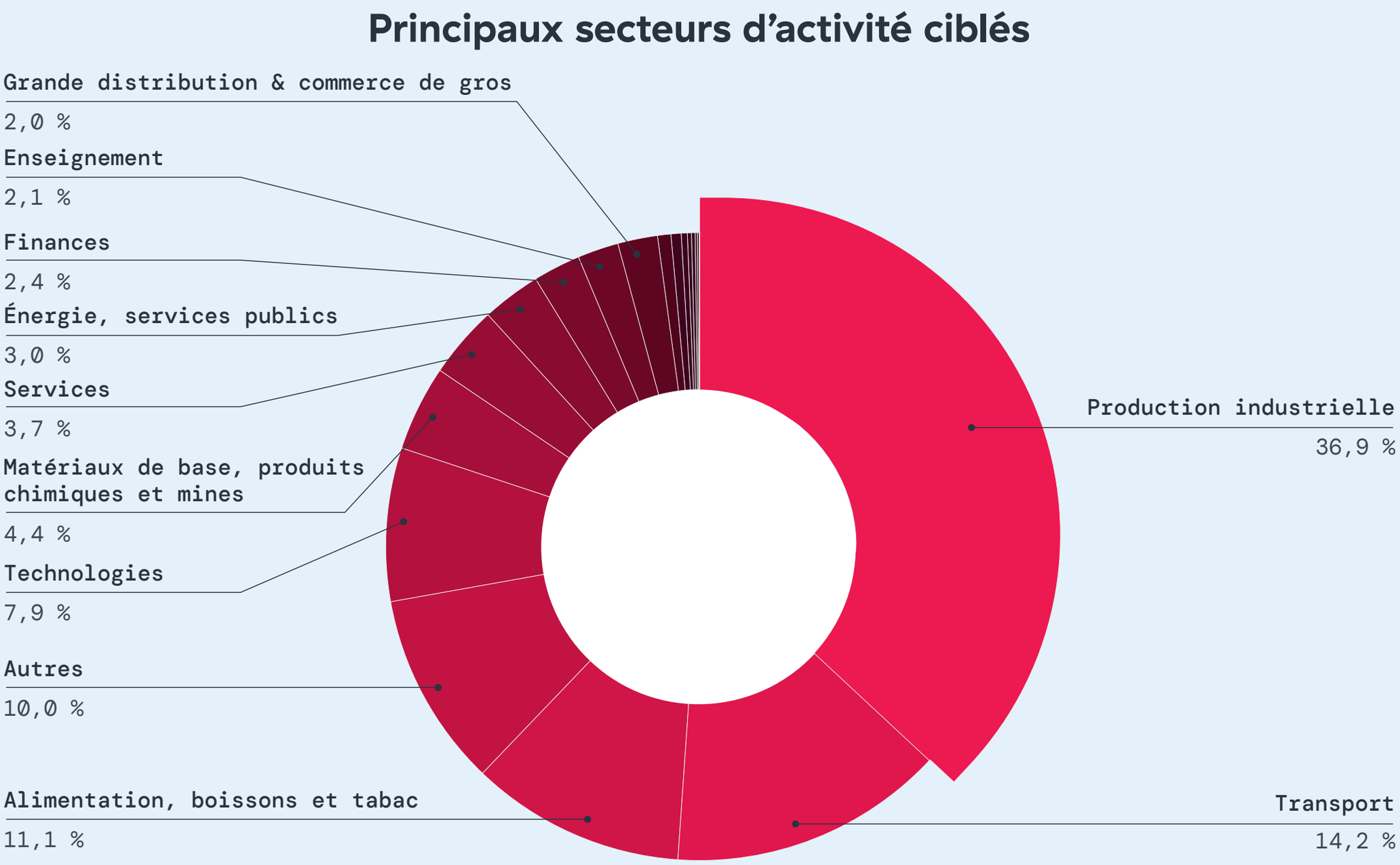
DESCRIPTIF DE LA SOLUTION

Les usines ont besoin d'une nouvelle approche pour sécuriser leurs systèmes OT

Les entreprises de production industrielle mondiales ont entrepris d'améliorer leurs lignes de production, en ajoutant des robots intelligents, des capteurs IoT sur chaque machine, des analyses basées sur le cloud et un jumeau numérique de l'ensemble de l'usine. L'objectif est simple : un rendement plus élevé, une réduction des temps d'arrêt et une maintenance prédictive qui permettent une production 24/7

Mais de nombreuses entreprises ont fait un constat troublant. Chaque nouvelle connexion élargit la surface d'attaque de l'OT. Et, une fois que les hackers se sont introduits, un système d'exploitation obsolète, des réseaux plats et une visibilité limitée sur l'OT peuvent avoir des conséquences catastrophiques. Pour poursuivre leur transformation, les usines doivent repenser leur architecture de sécurité.

Dans le dernier rapport de Threatlabz sur l'IoT/OT, Zscaler constate que la production industrielle a été très durement touchée avec 36 % des blocs de malwares IoT.

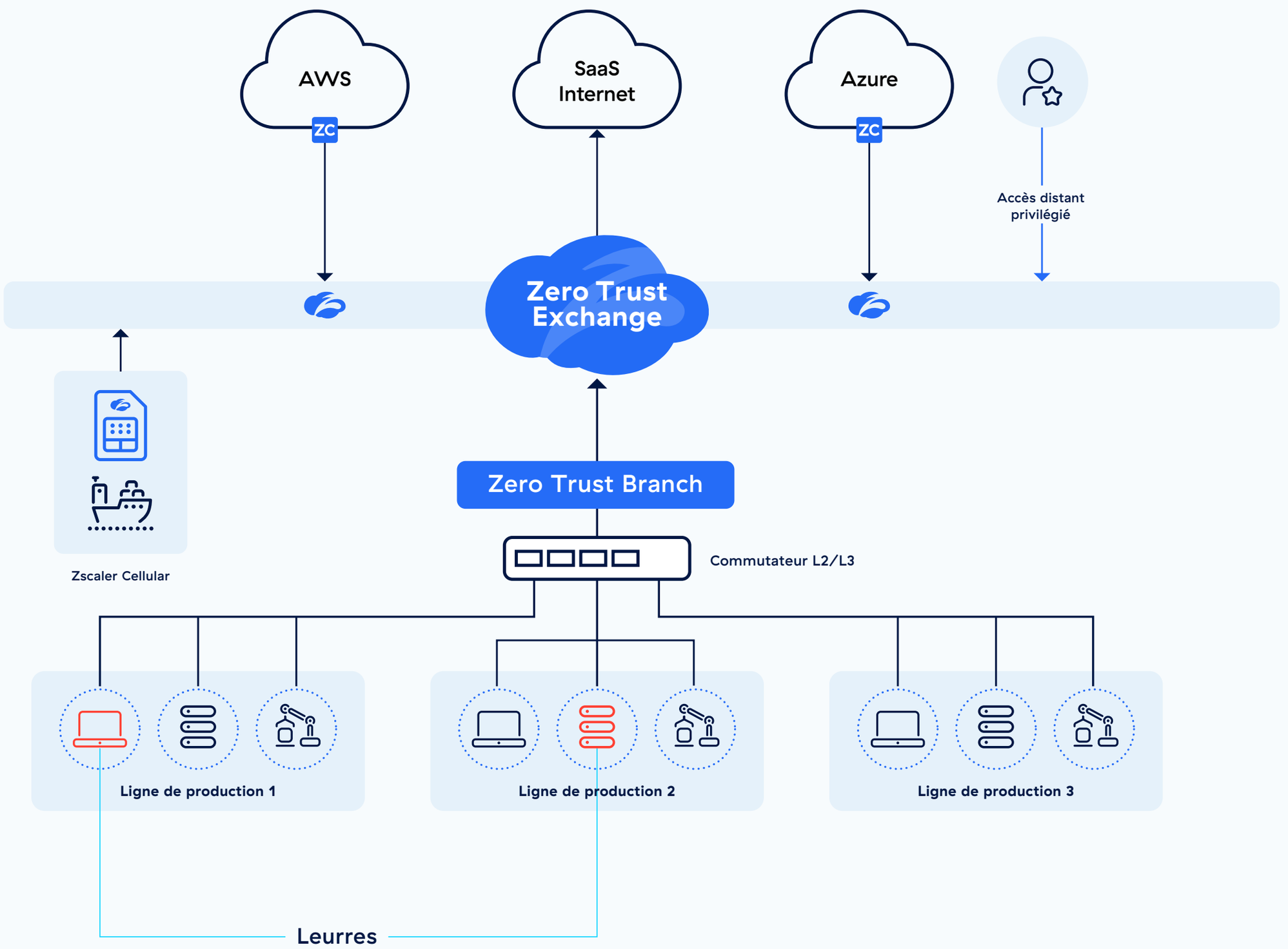


Répartition des secteurs les plus ciblés

Étendre le Zero Trust à chaque utilisateur et appareil, dans vos usines et à l'extérieur

Pour sécuriser la production et les environnements industriels, les équipes de sécurité doivent veiller à ce que chaque interaction entre l'utilisateur et l'appareil soit inspectée et exécutée conformément aux politiques du moindre privilège. Notre approche Zero Trust est spécialement conçue pour l'OT, et permet un accès, une segmentation et une connectivité sécurisés dans l'ensemble de vos opérations d'usine.

- Procurer aux techniciens et aux tiers un accès aux systèmes OT critiques sans VPN
- Appliquer une segmentation granulaire est-ouest pour empêcher le déplacement latéral des menaces
- Connecter en toute sécurité les systèmes OT au cloud et au data center pour l'analyse
- Étendre le Zero Trust aux systèmes OT cellulaires tels que les camions, les kiosques et les scanners de points de vente.
- Détecter les hackers à un stade précoce et les empêcher d'élever leurs privilèges



Architecture d'usine Zero Trust

Composants de la solution Zscaler

Accès distant privilégié

Permettre aux tiers et aux techniciens distants de se connecter en toute sécurité à des cibles RDP/SSH/VNC via n'importe quel navigateur.

CAPACITÉS PRINCIPALES

Contrôles du presse-papiers Limitez les capacités de copier/coller en fonction de stratégies Zero Trust afin de protéger les données sensibles.	**Contrôles d'audit et de gouvernance** Réduisez les risques liés aux tiers grâce à l'enregistrement des sessions, au partage des sessions et à l'accès contrôlé.
Coffre-fort et mappage des informations d'identification Stockez les informations d'identification des systèmes cibles dans un coffre-fort cloud et partagez l'accès via des stratégies de mappage.	**Accès limité dans le temps et juste à temps** Attribuez des fenêtres de maintenance et fournissez un accès JIT (« Just in Time » ou limité dans le temps) pour la maintenance d'urgence.

Segmentation Zero Trust

Procéder à une microsegmentation des systèmes OT et appliquer des politiques qui garantissent uniquement les communications autorisées entre vos systèmes OT et OT-IT.

Microsegmentation granulaire Isoler les systèmes OT pris en charge dans un segment d'un seul (en utilisant /32).	**Découverte et classification des appareils** Découvrez et classez automatiquement les dispositifs OT.
Ransomware Kill Switch Automatisez la réponse aux incidents à l'aide de politiques prédéfinies pour verrouiller progressivement les systèmes OT.	**Application des politiques** Regroupez automatiquement

Sécuriser l’accès aux salles d’opération

Permettre aux caméras, capteurs, moniteurs, kiosques et autres systèmes OT de se connecter en toute sécurité aux applications cloud et à Internet. Empêcher les communications avec des applications et des URL risquées ou malveillantes.

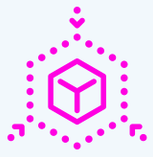
Provisionnement sans contact Tirez parti d’un déploiement entièrement automatisé sans intervention avec des modèles prédéfinis.	**Politiques Zero Trust unifiées** Inspectez et appliquez les politiques pour IoT/OT aux applications privées et à Internet.
Application granulaire des politiques Appliquez des politiques basées sur la géolocalisation de l’utilisateur/appareil, l’emplacement, les URL accédées, les données sensibles, et plus encore.	**Zero Trust Cellular** Connectez sans peine des appareils cellulaires tels que des camions, des kiosques, des plateformes, etc. grâce au Zero Trust.

Zscaler Deception

Utiliser des leurres pour détecter les menaces ciblant l’OT qui ont contourné les défenses en place. Identifier les utilisateurs compromis, arrêter les déplacements latéraux et se protéger des ransomwares et des menaces internes malveillantes.

Détection du déplacement latéral Déployez des PLC leurres et des systèmes SCADA pour détecter les hackers qui tentent de se déplacer latéralement.	**Détection avant une brèche** Vous recevrez des alertes pertinentes lorsque des acteurs malveillants étudient votre environnement avant une attaque.
Déploiement cloud natif Zscaler Deception s’intègre à Zscaler Private Access (ZPA) pour créer, héberger et diffuser des leurres.	**Zéro connexion au réseau** Dites adieu au trunking VLAN, aux ports SPAN et aux tunnels GRE pour acheminer le trafic vers les leurres.

Particularités de Zscaler



ÉLIMINER LES FAILLES DE SÉCURITÉ

Appliquez des politiques Zero Trust cohérentes dans tous les environnements tant au sein de vos usines qu'en dehors.

RÉDUIRE LES TEMPS D'ARRÊT

Appliquez la segmentation Zero Trust en perturbant le moins possible votre environnement OT, ce qui réduira le risque de temps d'arrêt que pourrait occasionner un déplacement latéral.

RÉDUIRE LES COÛTS ET LA COMPLEXITÉ

Diminuez le nombre de pare-feu, de NAC, de VPN, de VDI et d'outils de microseg-mentation, ou regrou-pez-les, grâce à une architecture de sécurité plus simple, conforme au modèle Purdue, au sein de vos usines.

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

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

zscaler™

Zero Trust Everywhere