FORESCOUT
Active Defense for the Enterprise of Things™

# Segmentation Zero Trust simple et transparente pour l'OT

Sécurisez les réseaux OT étendus grâce à une gestion avancée des risques et à une segmentation dynamique

En matière de sécurisation des appareils OT (Operational Technology, technologies d'exploitation) sur les réseaux OT et ICS, l'approche traditionnelle repose de longue date sur la séparation entre, d'une part, les applications industrielles et, d'autre part, les réseaux IT et les utilisateurs disposant d'un accès à distance. Cependant, avec la modernisation des infrastructures et l'adoption de nouvelles technologies, telles que le SCADA dans le cloud ou les systèmes DCS et MES avancés, par exemple, les stratégies classiques de division en zones ne sont plus suffisantes pour protéger efficacement les environnements OT.

Parmi les défis des environnements OT, citons :

- Risque de déplacement latéral de logiciels malveillants ou de cyberattaques, menaces interzones provenant des systèmes IT, et utilisateurs distants affectant les systèmes cyber-physiques et l'infrastructure OT
- Détection et neutralisation de la propagation de logiciels malveillants et de menaces interzones affectant les systèmes cyber-physiques et l'infrastructure OT
- Complexité opérationnelle due à des fournisseurs multiples et incohérence des contrôles de la segmentation dans les environnements OT étendus

## Forescout, une solution de pointe pour l'OT

Si ces défis ne vous sont pas étrangers, le moment est venu d'évaluer la solution Forescout. Celle-ci peut vous aider à simplifier la segmentation Zero Trust et à optimiser la gestion des risques en ce qui concerne les appareils IT, OT et ICS dans votre environnement Enterprise of Things (EoT) hétérogène.

**« D'ici 2021, 80 % des projets IoT industriels (IIoT) seront soumis à des exigences de sécurité spécifiques à l'OT, contre 40 % aujourd'hui[1]. »**

**GARTNER**

**« Les technologies d'appareils IoT et réseau sont source de risques de compromissions des réseaux et des entreprises (...) Les équipes de sécurité doivent isoler, sécuriser et contrôler en permanence chaque appareil sur le réseau[2]. »**

**FORRESTER RESEARCH**



forescout.com/platform/eyeSegment info-france@forescout.com Tél. (international) +1-408-213-3191

La plateforme Forescout vous offre divers avantages :

- **Implémentation rapide de la segmentation Zero Trust** dans les divers groupes IT et OT
- **Détermination immédiate de l'état de segmentation IT/OT** en temps réel pour n'importe quel appareil, à tout emplacement de l'environnement étendu
- **Visualisation des flux de trafic** en fonction d'une taxonomie logique des utilisateurs, applications, services, fonctions, emplacements, appareils et niveaux de risque
- **Réduction de la surface d'attaque et maintien de la conformité** grâce à une segmentation dynamique des environnements IT, IoT et OT
- **Optimisation des flux de travail IT/OT** et rentabilisation des investissements existants grâce à une politique de segmentation cohérente dans toute l'entreprise
- **Réduction des coûts et des risques de conformité grâce à une gestion efficace des accès interréseau**, qui nécessite moins de personnel

**„Fast 20 % aller Unternehmen haben in den vergangenen drei Jahren mindestens einen Angriff über das Internet of Things (IoT) verzeichnet."** [3]

**GARTNER**

## Gestion des risques optimisée et segmentation Zero Trust pour les réseaux IT/OT

La solution Forescout offre une visibilité complète sur les appareils des réseaux OT et permet de gérer efficacement et en temps réel un très grand nombre de risques opérationnels et de cybersécurité. Elle permet de répondre à des défis tels que la segmentation interdomaine, la segmentation répondant à plusieurs cas d'utilisation et la réduction des risques dans les environnements OT étendus, dans le but d'accélérer la détection des menaces et l'intervention sans interruption des activités.

**Forescout eyeSegment** vous aide à concevoir et à déployer une segmentation Zero Trust en cartographiant automatiquement les flux de trafic pour établir une taxonomie logique des utilisateurs, applications, services, fonctions, emplacements, appareils et risques à l'échelle du réseau d'entreprise. Cette approche permet d'établir des valeurs de référence pour

### MAXIMISEZ LA VALEUR DE VOS INVESTISSEMENTS INFORMATIQUES ET DE SÉCURITÉ

- Gérez les risques de convergence IT/OT (mouvements latéraux) grâce à une approche unifiée des politiques de segmentation.
- Gérez les risques liés aux appareils OT grâce aux fonctions avancées de planification, surveillance et intervention relatives aux politiques de segmentation granulaires.
- Implémentez une segmentation transparente et dynamique pour les environnements OT sensibles tout en tirant parti au maximum de l'investissement existant (infrastructure).

le trafic OT en temps réel sans déployer d'agents ni modifier l'architecture de l'infrastructure. Elle permet en outre de modéliser l'impact des politiques de segmentation avant de les mettre en œuvre.

**Forescout eyeInspect** (anciennement SilentDefense) protège les infrastructures critiques grâce à une inspection approfondie et brevetée des paquets et à une vaste bibliothèque d'indicateurs de menaces propres aux ICS. La solution surveille les communications réseau en temps réel et procure des informations contextualisées sur les ressources réseau, les protocoles et le contenu des communications. Grâce à des fonctions puissantes telles que l'agrégation avancée des alertes et l'établissement de valeurs de référence pour les actifs, vous pouvez automatiser les tâches de détection des menaces et de maintien en conformité afin de réduire les risques et de prendre en charge l'application de contrôles de segmentation OT.

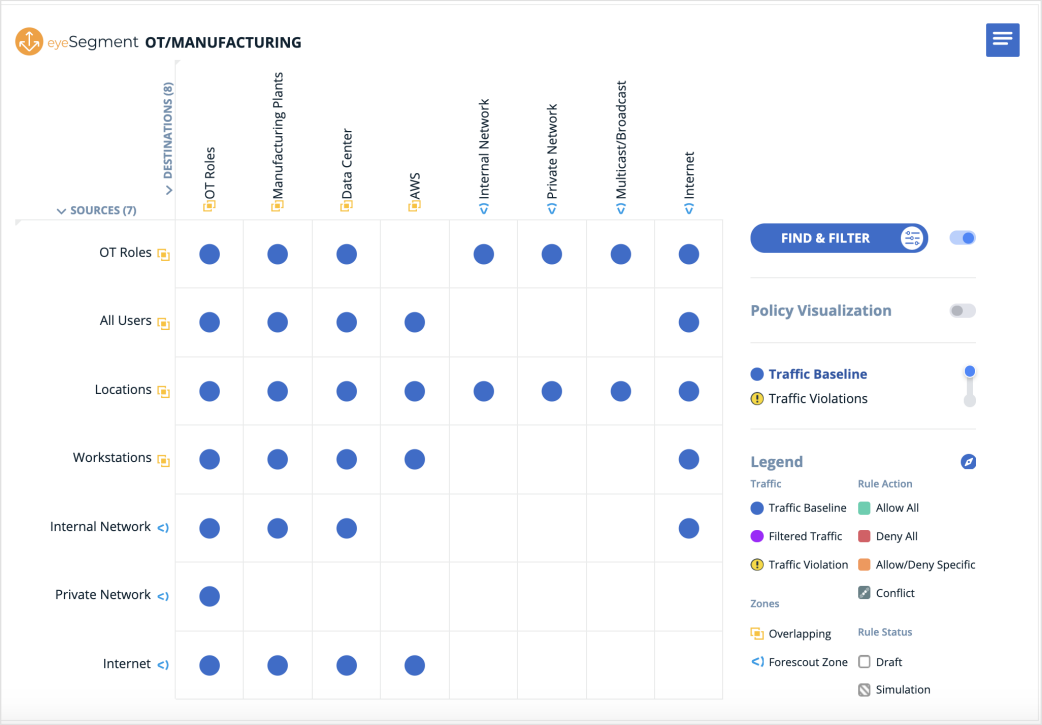


Figure 1. La matrice d'eyeSegment vous permet de vous concentrer sur les événements importants, pour que vous puissiez examiner et analyser un modèle de trafic précis dans votre environnement. Où que vous soyez dans la hiérarchie de la matrice, vous pouvez instantanément élaborer les politiques eyeSegment pertinentes pour segmenter un modèle de trafic spécifique et protéger l'entreprise tout en assurant la continuité de la production et des activités au sens large.

La solution Forescout de segmentation réseau s'adapte à de très nombreux cas d'utilisation dans les environnements OT. Sa flexibilité contribue dans tous les cas à réduire le risque de perturbation des activités et à minimiser les frais d'exploitation liés aux projets de segmentation. Voici quelques cas d'utilisation courants :

- Réduction des risques, maintien de la conformité et diminution des coûts opérationnels sur les réseaux OT
- Visibilité immédiate sur les environnements OT en temps réel pour permettre l'élaboration de politiques de segmentation assurant la continuité des activités
- Accélération de la segmentation Zero Trust IT/OT

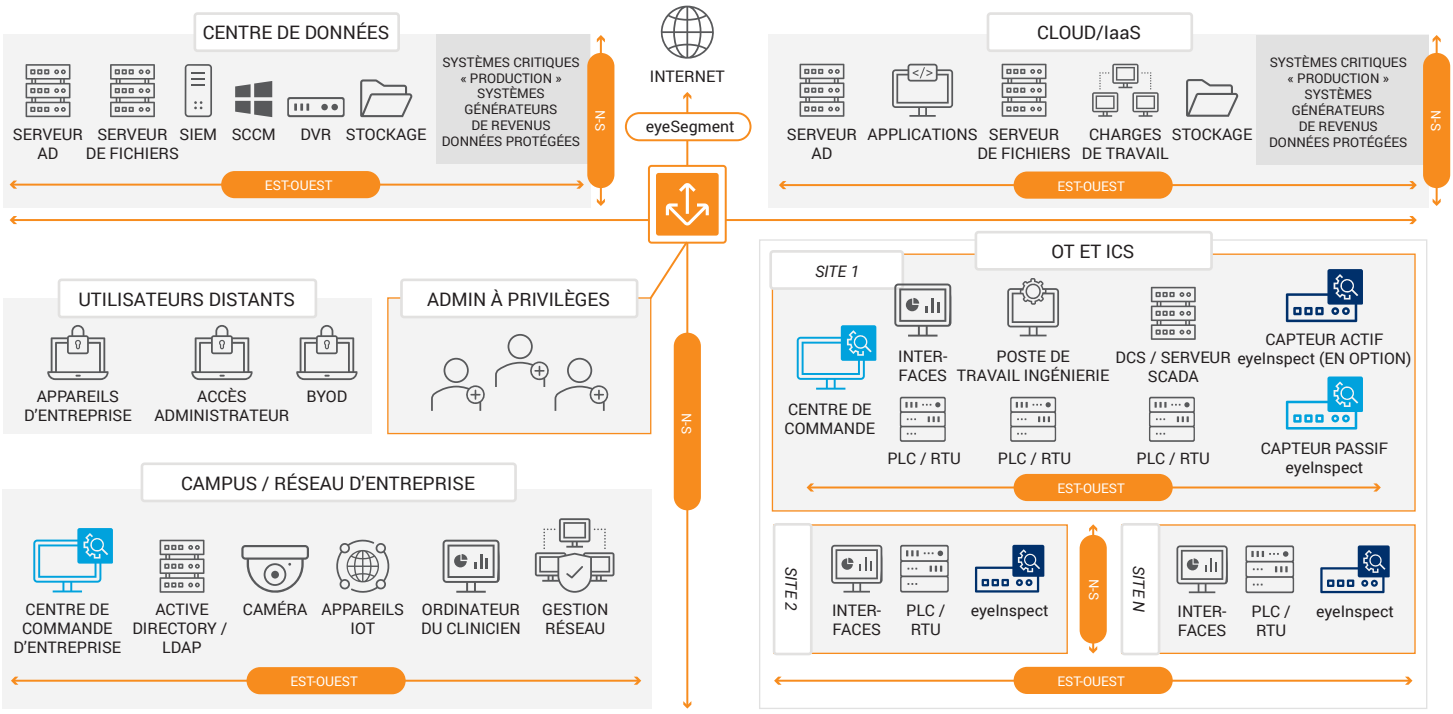


Figure 2. La solution Forescout peut vous aider à neutraliser les menaces et à déterminer votre état de segmentation en temps réel. Dans l'exemple ci-dessus, eyeSegment empêche les appareils connectés d'accéder aux domaines IT/OT et dédiés aux soins de santé.

1. *Invest Implications : Cool Vendors in Industrial IoT and OT Security* (Fournisseurs émérites en matière de sécurité IIoT et OT), Gartner Research, avril 2018
2. *Mitigating Ransomware With Zero Trust* (Réduction des risques liés aux ransomwares grâce au modèle Zero Trust), Forrester Research, Inc., 8 juin 2020
3. *IoT Security Primer: Challenges and Emerging Practices* (Introduction à la sécurité IoT : défis et pratiques émergentes), Gartner, janvier 2020

# Détecter, c'est bien. Sécuriser, c'est mieux.

Contactez-nous dès aujourd'hui pour protéger efficacement votre Internet des objets en entreprise.

forescout.com/platform/eyeSegment  info-france@forescout.com  Tél. (international) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 (États-Unis)

Email info-france@forescout.com
Tél (Intl) +1-408-213-3191
Support 1-708-237-6591

Pour en savoir plus, consultez le site Forescout.fr