FORESCOUT
Active Defense for the Enterprise of Things™

# eyeSegment

Pour une conception et un déploiement accélérés des projets de segmentation Zero Trust à grande échelle

### PRATIQUES DE SEGMENTATION SAINES

Fournit des informations en temps réel sur l'état actuel de tous les actifs connectés et leurs schémas de communication.

### POLITIQUES UNIFIÉES

Crée des politiques de segmentation Zero Trust unifiées pour empêcher le déplacement latéral des menaces dans les domaines interconnectés.

### EFFICACITÉ

Réduit les cyberrisques et la probabilité de compromission grâce à des politiques de segmentation granulaires pouvant être exécutées en mode « surveillance et intervention » afin d'éviter de perturber les processus opérationnels critiques.

### COMPLEXITÉ OPÉRATIONNELLE RÉDUITE

Améliore l'adoption de la segmentation grâce à une meilleure collaboration entre les équipes informatique, de sécurité, réseau et d'ingénierie.

### APPLICATIONS AUTOMATISÉES

Automatise l'application de la segmentation en tirant parti de vos investissements antérieurs dans l'infrastructure réseau.

## Segmentation Zero Trust simple et transparente pour tous les appareils, où qu'ils soient

Forescout eyeSegment accélère la conception, la planification et le déploiement d'une segmentation dynamique dans l'ensemble de l'entreprise étendue. Il permet une accélération rapide des projets de segmentation, ce qui réduit la surface d'attaque, limite l'impact global et diminue les risques pour les activités et les obligations réglementaires. Composant essentiel de la plateforme Forescout, eyeSegment permet aux entreprises d'appliquer les principes Zero Trust à la sécurité de l'environnement Enterprise of Things (EoT). Il permet également de découvrir tous les appareils à connexion IP.

### CONNAÎTRE & VISUALISER

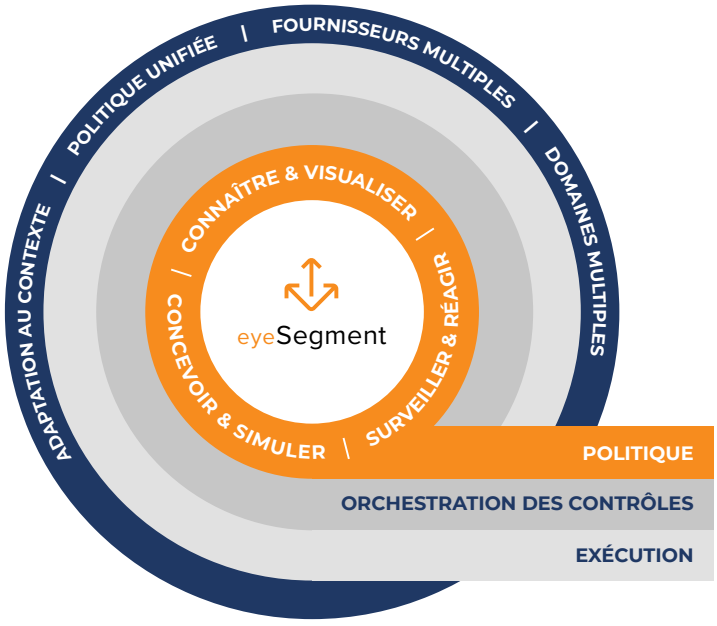
Cartographiez les flux de trafic afin d'établir une taxonomie logique des appareils, utilisateurs, applications et services.

### CONCEVOIR & SIMULER

Créez, optimisez et simulez des politiques de segmentation logiques afin d'en comprendre l'impact avant leur application.

### SURVEILLER & RÉAGIR

Surveillez en temps réel l'intégrité de la segmentation et réagissez aux violations des politiques dans l'entreprise étendue.



## Transformer la segmentation réseau à l'échelle de l'entreprise

Forescout eyeSegment tire parti des fonctionnalités complètes de visibilité et contrôle sur les appareils de la plateforme Forescout pour automatiser la segmentation fondée sur les politiques au sein d'une multitude de points de déploiement sur le campus, dans le centre de données et sur les réseaux cloud. Il vous permet de concevoir, réaliser et déployer une segmentation réseau à grande échelle en toute confiance, pour une segmentation réseau sur l'ensemble de l'entreprise étendue.

- Fournit des informations en temps réel sur l'état actuel de tous les actifs connectés et leurs schémas de communication.
- Simplifie le processus d'élaboration de politiques de segmentation sensibles au contexte au moyen d'une taxonomie logique des appareils, des utilisateurs, des applications et des services.
- Permet de visualiser et simuler les politiques avant leur mise en œuvre, dans une démarche proactive d'optimisation et de validation.
- Accroît les capacités de la plateforme Forescout pour relever les défis de segmentation dans des environnements présentant des domaines et cas d'utilisation multiples.
- Tire parti de vos investissements en infrastructure antérieurs axés sur les technologies d'application.

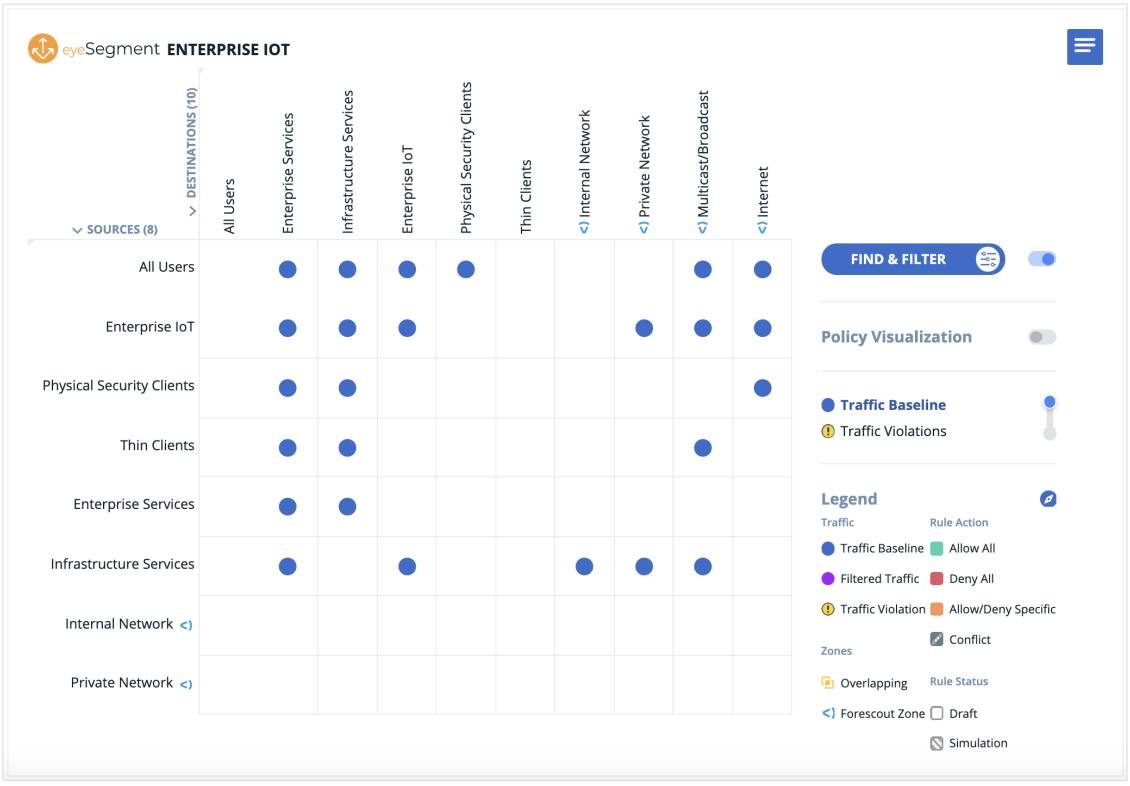
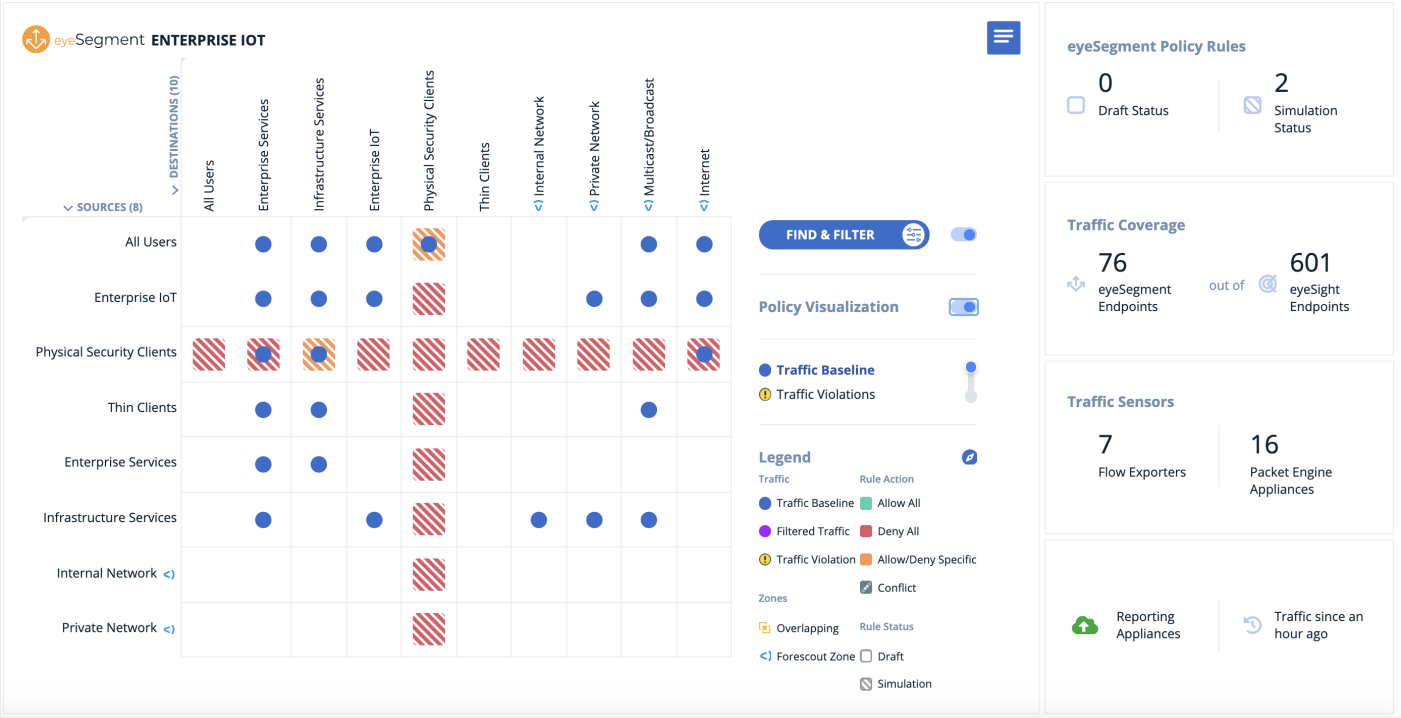



Figure 2. La matrice d'eyeSegment vous permet de vous concentrer sur les événements importants. Par exemple, vous pouvez examiner et analyser un modèle de trafic particulier dans votre environnement, comme illustré ci-dessus. Où que vous soyez dans la hiérarchie de la matrice, vous pouvez instantanément élaborer et surveiller des politiques eyeSegment efficaces pour segmenter un modèle de trafic spécifique et protéger l'environnement EoT tout en assurant la continuité des activités.

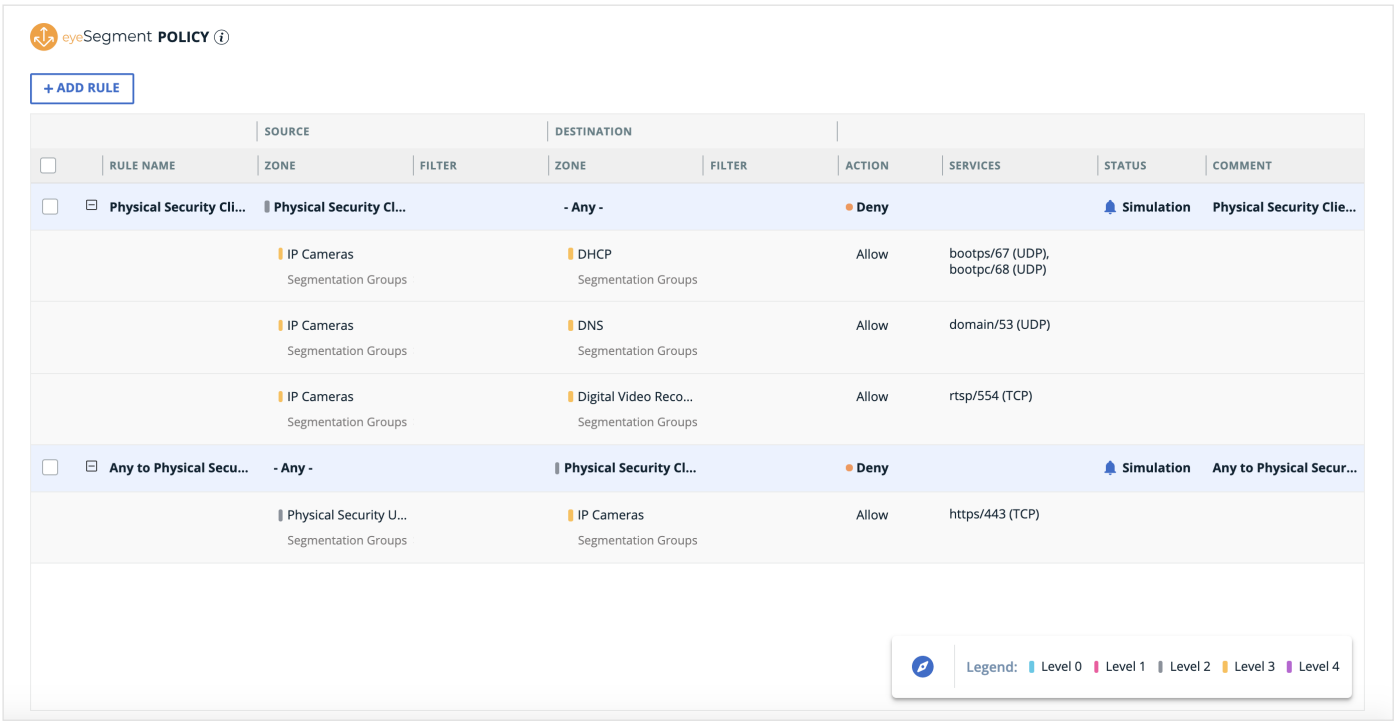
## Connaître et visualiser les flux de trafic

Transposez les adresses IP dans une taxonomie logique des appareils, applications, utilisateurs et services.



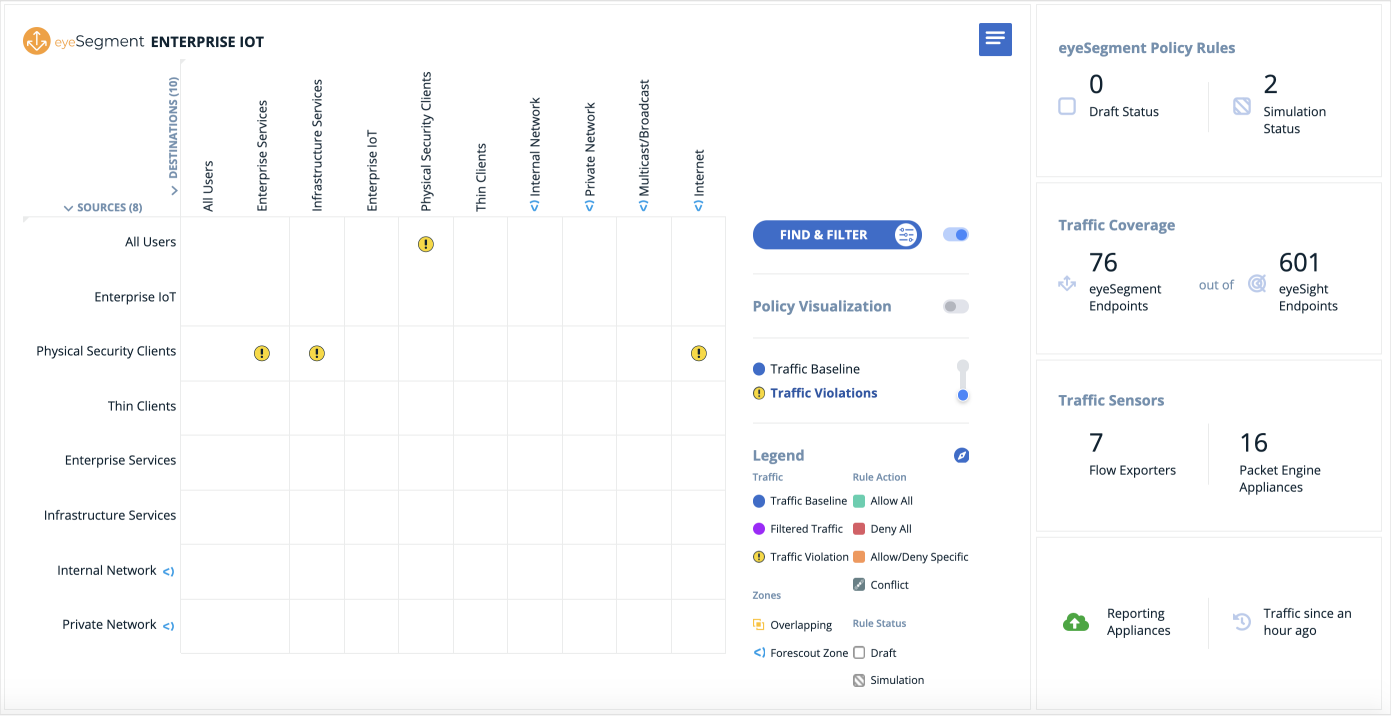

## Concevoir et simuler des politiques

Concevez, réalisez et optimisez des politiques de segmentation efficaces fondées sur une taxonomie logique des activités.



## Surveiller, automatiser et réagir

Implémentez et surveillez des politiques unifiées pour identifier les violations de politique en temps réel sur les environnements multifournisseurs et sur différents domaines réseau tout en préservant la continuité des activités.




# 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

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