Forescout eyeSegment

Élaborez, réalisez et déployez une segmentation réseau à grande échelle en toute confiance

Forescout eyeSegment accélère la conception, la planification et le déploiement d'une segmentation dynamique des réseaux dans l'ensemble de l'entreprise étendue. Il simplifie le processus d'élaboration de politiques de segmentation sensibles au contexte et permet de visualiser et de simuler les politiques avant leur mise en œuvre en vue d'une démarche proactive d'optimisation et de validation.

eyeSegment accroît les capacités de la plateforme Forescout pour relever les défis en matière de segmentation dans des domaines et des cas d'utilisation multiples. Il permet aux entreprises d'adopter les principes Zero Trust pour tous leurs systèmes connectés par adresse IP, y compris les appareils de l'Internet des objets (IoT) et les technologies d'exploitation (OT). Il en résulte une accélération rapide des projets de segmentation à travers l'entreprise étendue, ce qui réduit la surface d'attaque, limite la propagation latérale et l'onde de choc et diminue les risques pour la réglementation, la conformité et les activités.

Difficultés

- Manque de confiance pour progresser dans des projets de segmentation
- Risque d'exposition en raison du potentiel de mouvement latéral des menaces dans les réseaux sans hiérarchie
- Contexte incomplet concernant les appareils, les applications et les utilisateurs
- Dispersion des politiques et incapacité à réaliser des contrôles cohérents sur des technologies disparates
- Complexité opérationnelle due à des fournisseurs multiples et incohérence dans les contrôles de la segmentation à travers les domaines de réseaux
- Manque de compétences, de ressources et d'outils pour élaborer, réaliser et déployer efficacement une segmentation réseau à travers l'entreprise étendue

eyeSegment

Avantages

- Accélération des projets de segmentation réseau en toute confiance
- Évaluation proactive de l'impact des politiques permettant de minimiser les perturbations des activités
- Réduction du risque de perturbation des activités
- Surveillance uniforme parmi plusieurs technologies de contrôle et domaines de réseaux grâce à un cadre de politiques unique
- Respect des exigences de la conformité et de la réglementation
- Diminution de la complexité opérationnelle des projets de segmentation
- Activation d'une approche Zero Trust pour la mise en œuvre de contrôles de sécurité granulaires

Points forts

- Création de politiques de segmentation sensibles au contexte au moyen d'une taxonomie logique par activité des utilisateurs, des applications, des services et des appareils
- Analyse rapide de l'impact avant le déploiement de politiques de segmentation
- Surveillance et validation permanentes de l'intégrité de la segmentation
- Réaction rapide aux violations de la politique de segmentation dans l'entreprise étendue

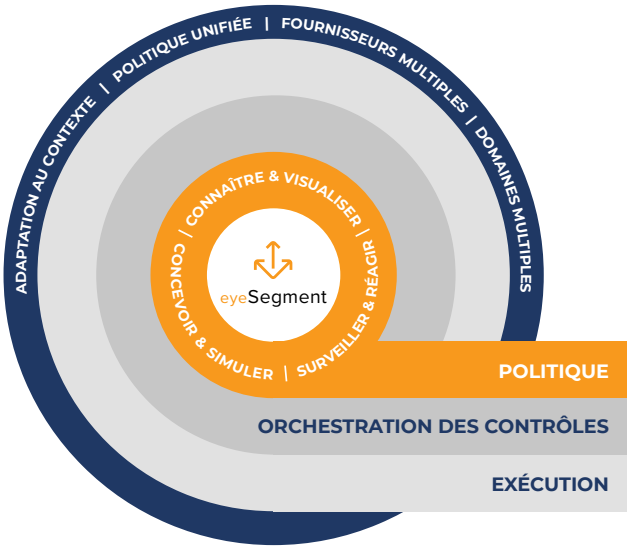

Figure 1. Forescout recommande une architecture à trois niveaux au titre des bonnes pratiques pour la segmentation des réseaux dans une entreprise complète, à commencer par un « niveau politique » reposant sur eyeSegment.

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

Forescout eyeSegment s'appuie sur la visibilité exhaustive des appareils et le contexte en temps réel approfondi que procure Forescout eyeSight. Il vous permet de visualiser les flux de trafic et les dépendances entre les utilisateurs, les applications, les services et les appareils pour ensuite concevoir, simuler et surveiller les politiques appropriées pour comprendre l'impact sur votre environnement. Mettant à profit Forescout eyeControl et eyeExtend, les politiques sont orchestrées à travers une multitude de points de segmentation mis en œuvre dans les réseaux de campus, de centres de données et de cloud. eyeSegment aide les entreprises à concevoir, réaliser et déployer une segmentation réseau à grande échelle afin qu'elles puissent segmenter les réseaux dans l'ensemble de leur organisation.

Connaître et visualiser les flux de trafic

Forescout eyeSegment cartographie automatiquement les flux de trafic pour dresser une taxonomie logique des utilisateurs, des applications, des services et des appareils à travers le réseau complet de l'entreprise, sans déployer d'agents. Vous pouvez ainsi surveiller votre trafic réseau en temps réel et définir une politique de segmentation granulaire qui prend le contexte en considération. Un cas d'utilisation typique concerne par exemple la création de contrôles destinés à garantir que seuls les collaborateurs du service financier ont accès aux applications de paiement fonctionnant dans différents domaines. Un autre consisterait à identifier les services communs nécessaires pour les appareils médicaux installés sur d'anciens systèmes d'exploitation, puis à les séparer.

La matrice de connectivité d'eyeSegment (Figure 2) vous aide à visualiser les flux de trafic. Cette fonction crée une base de référence pour le trafic, gère les données sur le trafic dans le temps et affiche les flux en temps réel entre les zones de source et de destination conformément à la définition de la politique de segmentation.

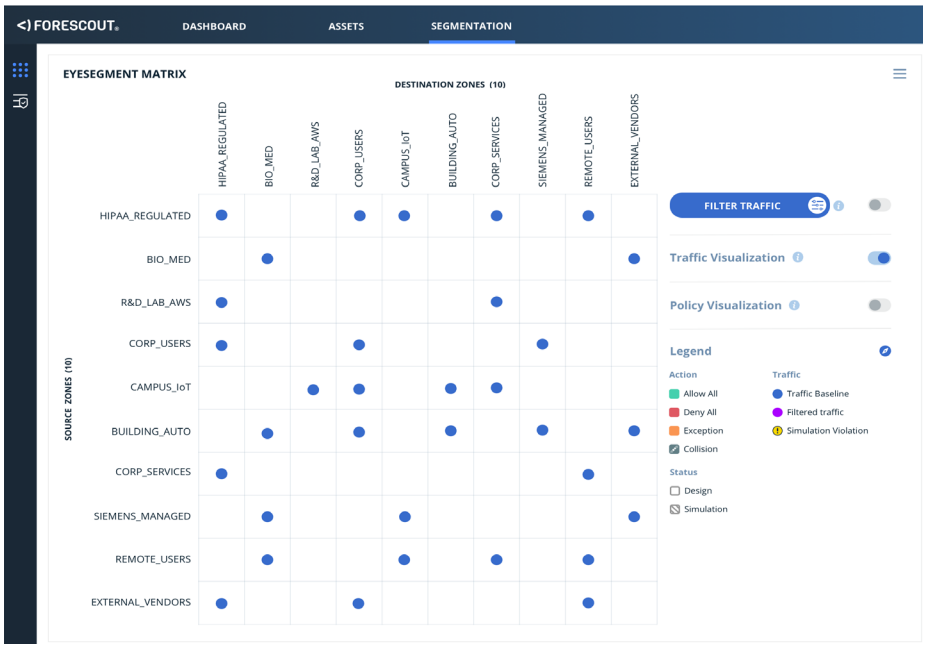

Figure 2. Matrice de connectivité d'eyeSegment illustrant les flux de trafic logiques des activités.

Concevoir et simuler des politiques de segmentation

Forescout eyeSegment vous aide à concevoir, réaliser et optimiser des politiques de segmentation efficaces fondées sur une taxonomie logique des activités, qui peuvent être mises en œuvre quelles que soient les technologies sous-jacentes existantes. Vous pouvez simuler de façon proactive l'implémentation des politiques avant leur déploiement concret dans votre environnement, ce qui minimise le risque de perturbation des activités.

Définir des politiques de segmentation unifiées et granulaires

Une politique de segmentation désigne une série de règles qui autorisent tout le trafic, refusent tout le trafic ou autorisent uniquement un trafic spécifique entre des zones de source et de destination spécifiques. Les zones sont définies sur la base de groupes standard des politiques, auxquels les membres peuvent être attribués manuellement ou par le biais d'une politique. Une zone peut également être constituée d'adresses IP individuelles ou d'objets de segments Forescout qui sont des groupes. Chaque zone de segmentation peut être une zone de source, une zone de destination ou les deux.

Vous pouvez définir des politiques de segmentation à partir d'une console unique pour refuser ou autoriser expressément un trafic spécifique à travers différentes technologies et différents domaines de réseaux. Chaque politique peut être appliquée au trafic venant d'une zone source spécifique adressé à une zone de destination spécifique. Par défaut, tout le trafic est autorisé entre toutes les zones de source et de destination. La politique, avec ses exceptions, détermine quel trafic est autorisé ou refusé. Vous pouvez ainsi définir différentes actions pour différents sous-groupes et services.

Visualiser les politiques et les dépendances du trafic

Vous pouvez visualiser les politiques et le trafic afin d'obtenir un panorama des politiques de segmentation créées et de leur statut dans la matrice de connectivité, comme le montre la figure ci-dessous. Les options de filtrage vous permettent d'explorer en détail une politique spécifique pour filtrer le trafic par service et/ou afficher l'intersection de zones de matrice avec les filtres de source et de destination.

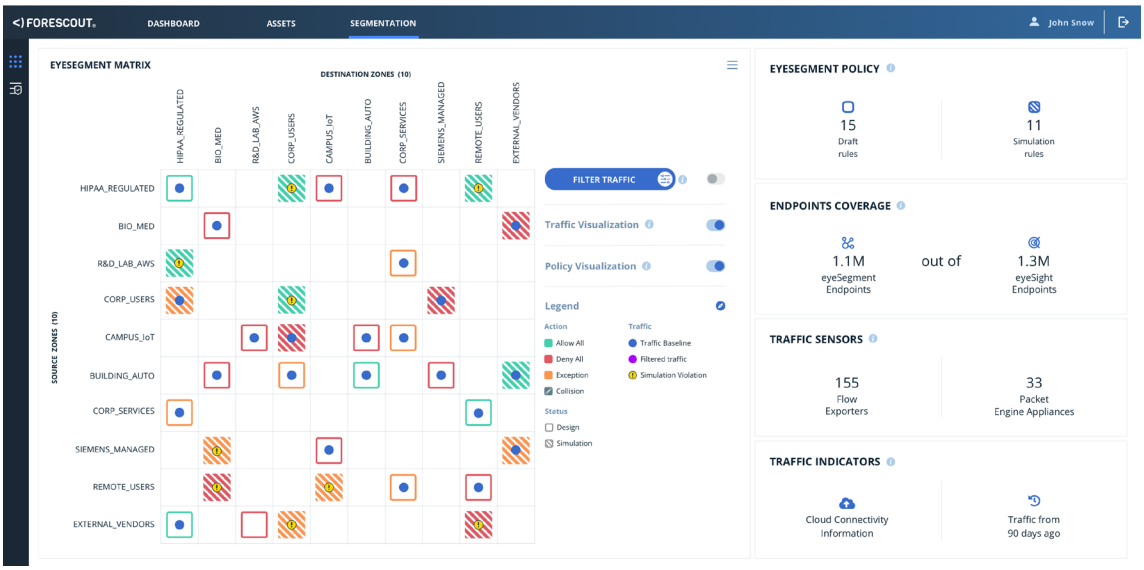

Figure 3. Visualisation d'une politique et affichage d'une simulation.

Surveiller et réagir

Avec le système unifié de gestion des politiques et de tableau de bord d'eyeSegment, vous pouvez surveiller de façon centralisée les flux de trafic entre différentes zones de source et de destination. La possibilité de surveiller en permanence les politiques de segmentation et d'y réagir indépendamment des contrôles sous-jacents peut offrir un outil précieux pour instaurer un contrôle progressif ou lorsqu'une infrastructure de contrôle n'est pas disponible. eyeSegment contribue également à surveiller en permanence les contrôles de l'infrastructure de l'entreprise et à s'assurer que les contrôles de segmentation sont bien implémentés et fonctionnent efficacement après le déploiement de contrôles dans toute l'entreprise étendue.

Cas d'utilisation

La plateforme Forescout répond à une large gamme de cas d'utilisation d'une segmentation réseau. 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 :

Protection des applications stratégiques d'une entreprise	• Protéger les applications stratégiques, garantir que les contrôles soient effectivement exécutés et exercer une surveillance permanente afin d'assurer une protection ininterrompue. Opérer les contrôles appropriés à l'intérieur et à l'extérieur de l'entreprise à travers un ensemble de services, d'applications et de domaines. • Contrôler l'accès des utilisateurs aux services critiques de l'entreprise à travers différents domaines. Protéger les applications stratégiques contre une utilisation inappropriée par les utilisateurs, garantir que les contrôles soient effectivement exécutés et exercer une surveillance constante de la protection permanente.
Définition de privilèges pour l'accès à l'infrastructure IT stratégique	• Limiter l'accès des administrateurs IT aux appareils sensibles du réseau (commutateurs, pare-feux de nouvelle génération, etc.) et aux centres de données/charges de travail cloud (Active Directory/LDAP, Domain Name System, Oracle Cluster, etc.) sur la base de la désignation d'administrateurs (par fonction), de l'état du terminal des administrateurs IT (chiffrement, domaines joints, etc.) et de la sécurisation des communications (port/service spécifique).
Protection des appareils IoT/OT d'une entreprise (imprimantes, caméras, téléphones VoIP, lecteurs de cartes, systèmes de chauffage, ventilation et conditionnement d'air, etc.)	• Protéger le réseau informatique des appareils IoT/OT. • Protéger les appareils IoT/OT des attaques.
Assurance d'une segmentation à l'échelle d'une entreprise	• Assurer que tous les points de déploiement à travers différents domaines (campus, centres de données et IoT) gérés par d'autres équipes satisfont aux exigences de la politique de segmentation et sont configurés correctement.
Confinement des appareils vulnérables	• Limiter les accès entre les appareils vulnérables (WannaCry, non corrigés, en fin de vie, etc.) et le reste du réseau.
Protection des applications/appareils d'ancienne génération	• Réduire la surface d'attaque en séparant les appareils fonctionnant sur un ancien système d'exploitation et les applications qui y sont installées. • Limiter le risque de menaces pour les appareils fonctionnant sur un système d'exploitation en fin de vie.

FORESCOUT

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

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

Pour en savoir plus, consultez le site Forescout.fr