FORESCOUT
Active Defense for the Enterprise of Things™

# eyeControl

Application de contrôles basés sur des politiques

## CONTINUITÉ DES ACTIVITÉS

Options de déploiement et de contrôle d'accès flexibles, avec ou sans authentification 802.1X.

## TECHNOLOGIE SANS AGENT

Évaluation de l'intégrité des appareils et correction automatique pour une conformité assurée sans agents.

## EFFICACITÉ

Moteur de politiques unifié pour l'implémentation Zero Trust de l'accès sécurisé.

## SANS MISES À NIVEAU

Intégration avec l'infrastructure existante sans mise à niveau logicielle/matérielle.

## COÛT TOTAL DE POSSESSION RÉDUIT

Flexibilité, continuité des activités, technologie sans agent et prise en charge multifournisseur pour des coûts opérationnels, de déploiement et de maintenance réduits. Retour sur investissement accéléré.

# Appliquez et automatisez les actions de contrôle de l'Enterprise of Things sur des réseaux hétérogènes

ForeScout eyeControl offre la solution de contrôle d'accès au réseau la plus simple et flexible pour les réseaux d'entreprise hétérogènes. Il applique et automatise les politiques Zero Trust suivant le principe du moindre privilège pour tous les appareils gérés et non gérés dans l'Enterprise of Things (EoT) — l'Internet des objets en entreprise. Des contrôles basés sur des politiques peuvent être appliqués pour assurer la conformité des appareils, réduire de façon proactive votre surface d'attaque et intervenir rapidement en cas d'incident.

### ACCÈS AU RÉSEAU SÉCURISÉ

Contrôle de l'accès au réseau en fonction des utilisateurs, de l'identité des appareils et du niveau de sécurité

Déploiement avec ou sans authentification 802.1X dans les réseaux hétérogènes

### MISE EN CONFORMITÉ DES APPAREILS

Cumplimiento de directivas, Conformité aux politiques de sécurité, aux normes et aux réglementations

Flux de travail de correction et de réduction des risques

### AUTOMATISATION DE L'INTERVENTION SUR INCIDENT

Automatisation de l'intervention en cas d'incident de sécurité

Neutralisation des menaces pour une propagation et une interruption des activités réduites

# AUTOMATISEZ LES CONTRÔLES EN TOUTE CONFIANCE

Les politiques Zero Trust peuvent uniquement être appliquées sur la base des données contextuelles complètes des appareils. Celles-ci incluent la connaissance en temps réel de l'identité de l'utilisateur, de l'identité de l'appareil, du niveau de sécurité et du profil de risque pour tous les appareils connectés au réseau. Les contrôles implémentés sans disposer d'une visibilité totale peuvent perturber les activités et mettre en péril les opérations métier. eyeControl s'appuie sur les données contextuelles riches fournies par eyeSight pour appliquer et automatiser les contrôles Zero Trust en toute confiance.

eyeControl repose sur un moteur de politiques intuitif et flexible qui vous permet d'appliquer des actions de contrôle granulaires et ciblées. Ce moteur de politiques Zero Trust offre les avantages suivants :

- Regroupement dynamique et définition de la portée des appareils en fonction de la logique métier et du contexte de l'appareil
- Conditions et actions composées ayant recours à la logique booléenne et des politiques en cascade pour l'implémentation de flux de contrôle sophistiqués
- Graphique des politiques pour une création précise de politiques, l'analyse des flux de politiques et l'optimisation avant l'application d'actions de contrôle
- Possibilité de commencer par des actions de contrôle lancées manuellement et de renforcer progressivement l'automatisation pour accroître l'efficacité des opérations de sécurité

Les politiques sont déclenchées et évaluées automatiquement en temps réel par des événements et modifications se produisant soit sur un appareil, spécifique soit sur le réseau. La figure 1 ci-dessous montre l'éventail des actions de contrôle disponibles dans eyeControl lors du déclenchement d'une politique.

## CONTRÔLE MODÉRÉ

### Réseau

- Déplacement vers un réseau invité
- Modification du rôle de l'utilisateur de la connexion sans fil
- Affectation à un VLAN d'autocorrection
- Restriction des appareils /infrastructures non approuvés

### Système

- Lancement des applications/processus o bligatoires
- Mise à jour des agents de sécurité/antivirus
- Application de mises à jour/correctifs du système d'exploitation
- Mise en conformité des disques externes

AUTOMATISATION DE CONTRÔLES BASÉS SUR DES POLITIQUES

## CONTRÔLE RIGOUREUX

### Réseau

- Mise en quarantaine de l'appareil (VLAN, pare-feu virtuel)
- Désactivation du port du commutateur
- Blocage de l'accès sans fil ou VPN
- Utilisation de listes de contrôle d'accès (ACL)

### Système

- Fermeture des applications non autorisées
- Désactivation des cartes réseau/du dual-homing
- Désactivation des périphériques
- Déclenchement des systèmes/actions de correction

Figure 1. Application de politiques sur le réseau et les terminaux, renforçant l'automatisation au fil du temps.

## CONTRÔLE

### Sécurisation de l'accès au réseau

eyeControl est la solution de contrôle d'accès au réseau la plus flexible, la plus hétérogène et la moins perturbatrice pour les entreprises. Avec eyeControl, vous pouvez mettre en œuvre un accès sécurisé sur les réseaux câblés et sans fil pour tous les systèmes EoT gérés et non gérés, vous conformer aux exigences d'audit, réduire votre surface d'attaque et éliminer rapidement les menaces. À titre d'exemple :

- Provisionnez un accès Zero Trust au réseau pour les appareils des employés, des invités, des sous-traitants et BYOD.
- Identifiez et bloquez les appareils non approuvés, non autorisés, shadow IT et utilisés à des fins d'usurpation.
- Mettez en quarantaine ou isolez des appareils non conformes et à haut risque jusqu'à la correction.
- Profitez d'un large choix de méthodes de contrôle d'accès — avec ou sans authentification 802.1X.
- Évaluez le niveau de sécurité sans agent et appliquez des actions sur le réseau et les terminaux via un moteur de politiques Zero Trust unifié.
- Établissez une interopérabilité avec l'infrastructure existante sans mise à niveau logicielle/matérielle.
- Bénéficiez d'une intégration directe avec plus de 30 fournisseurs d'infrastructure réseau et plusieurs centaines de modèles de produit.

## CONFORMITÉ

### Mise en conformité des appareils

Automatisez l'évaluation du niveau de sécurité et appliquez des contrôles de correction pour garantir une adéquation constante avec les politiques de sécurité internes, les normes externes et les réglementations sectorielles.

- Vérifiez la configuration des terminaux et appliquez des mesures correctives pour les violations de configuration critiques.
- Identifiez et corrigez les appareils gérés dont les agents sont défectueux ou manquants.
- Détectez et désactivez les applications non autorisées susceptibles d'engendrer des risques ou de solliciter inutilement la bande passante du réseau ou d'entraver la productivité.

### EyeControl RÉSOUT LES PROBLÈMES SUIVANTS :

**Appareils non approuvés, non autorisés ou utilisés à des fins d'usurpation** qui sont connectés au réseau et présentent des risques et des problèmes de conformité.

**Failles de sécurité** lorsque les outils avec agent ne sont pas à jour ou sont défaillants.

**Réseaux sans hiérarchie ni segmentation** qui rendent les entreprises vulnérables aux menaces et augmentent l'impact global.

**Risques de perturbation des activités** dus aux appareils vulnérables, à l'absence de correctifs critiques et aux applications non autorisées.

**Propagation latérale** des menaces dues à l'incapacité d'isoler rapidement les appareils compromis ou malveillants.

**Non-conformité** due à l'incapacité de surveiller et corriger en continu le niveau de sécurité des appareils connectés.

**Problèmes d'implémentation du contrôle d'accès au réseau** dans les environnements hétérogènes et multifournisseurs et les réseaux câblés.

- Identifiez les appareils présentant des vulnérabilités à haut risque et des correctifs critiques manquants et appliquez les mesures correctives qui s'imposent.
- Exécutez des actions de correction ou de réduction des risques sans agent sur l'ensemble des appareils Windows, Mac, Linux, IoT et OT.
- Implémentez des politiques et automatisez les contrôles pour garantir la conformité des configurations dans les déploiements cloud, notamment AWS, Azure et VMware.

## AUTOMATISATION

### Accélérez l'intervention sur incident

- Neutralisez les menaces et intervenez en cas d'incident de sécurité de façon rapide et efficace, afin de minimiser les interruptions d'activité et l'impact pour l'entreprise. Automatisez les tâches d'intervention sur incident de base répétitives afin de permettre au personnel qualifié de se consacrer aux problèmes prioritaires ou ayant un impact plus important.
- Identifiez les indicateurs de compromission et les risques sur les appareils dès qu'ils se connectent au réseau afin de réduire le délai moyen d'intervention.
- Isolez rapidement les appareils compromis ou malveillants pour éviter la propagation latérale de logiciels malveillants.
- Automatisez l'intervention sur incident et initiez des flux de travail de correction sur les appareils.
- Réduisez le délai moyen d'intervention en fournissant des données contextuelles précieuses sur les appareils (connexion, emplacement, classification et niveau de sécurité) aux équipes interfonctionnelles d'intervention sur incident et aux technologies isolées.

## 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/eyeControl 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