eyeControl

Application de contrôles basés sur des politiques

Appliquez et automatisez les actions de contrôle sur des réseaux hétérogènes

Forescout eyeControl offre un contrôle d'accès au réseau simple et flexible pour les réseaux d'entreprise hétérogènes. Il applique et automatise des politiques Zero Trust selon le principe du moindre privilège sur tous les appareils gérés et non gérés de votre environnement numérique. Les contrôles basés sur des politiques permettent d'assurer la conformité des appareils, de réduire proactivement votre surface d'attaque et d'intervenir rapidement en cas d'incident.

Accès sécurisé au réseau

- 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

- Automatisation de la conformité aux politiques de sécurité, aux normes et aux réglementations
- Flux de travail de correction et de réduction des risques en temps réel

Intervention automatique en cas d'incident

- Automatisation de l'intervention en cas d'incident de sécurité
- Neutralisation des menaces pour minimiser la propagation et l'interruption des activités

Continuité des activités

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

Technologie sans agent

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

Efficacité

Moteur de politiques flexible et unifié pour l'implémentation Zero Trust de l'accès réseau.

Sans mises à niveau

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

Coût total de possession réduit

Coûts de déploiement, de maintenance et opérationnels réduits pour un retour sur investissement accéléré.

Automatisez les contrôles en toute confiance

Les politiques Zero Trust ne peuvent être appliquées que sur la base d'une visibilité totale et en contexte des appareils. Cela implique de connaître en temps réel l'identité des utilisateurs, celle des appareils, ainsi que le niveau de sécurité et le profil de risque de tous les appareils connectés. 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 unifié offre les avantages suivants :

- Regroupement dynamique et définition de la portée des appareils en fonction de la logique métier et du contexte
- Définition de conditions et d'actions complexes ayant recours à la logique booléenne et à des politiques en cascade pour l'implémentation de flux de contrôle sophistiqués
- Graphiques 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 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.

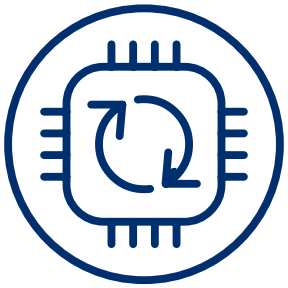
Contrôle modéré

Réseau

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

Système

- Lancement des applications/processus obligatoires
- 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 des appareils (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.

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 due à l'incapacité d'isoler rapidement les appareils compromis ou malveillants.
- **Non-conformité** due à l'incapacité de surveiller et d'appliquer les politiques en continu sur les appareils connectés.
- **Problèmes d'implémentation du contrôle d'accès au réseau** dans les environnements hétérogènes et multifournisseurs et les réseaux câblés.

Contrôle

Accès sécurisé au réseau

eyeControl est la solution d'accès au réseau la plus flexible et la moins perturbatrice pour les entreprises présentant des réseaux hétérogènes. Elle vous permet de mettre en œuvre un accès sécurisé sur les réseaux câblés et sans fil pour tous les appareils gérés et non gérés, de vous conformer aux exigences d'audit, de réduire votre surface d'attaque et d'éliminer rapidement les menaces. Vous pouvez notamment :

- Provisionner un accès Zero Trust au réseau pour les appareils des employés, des invités, des sous-traitants et BYOD
- Identifier et bloquer les appareils non approuvés, non autorisés ou utilisés à des fins d'usurpation, y compris le shadow IT
- Mettre en quarantaine ou isoler des appareils non conformes et à haut risque jusqu'à la correction
- Profiter d'un large choix de méthodes de contrôle d'accès – avec ou sans authentification 802.1X
- Évaluer le niveau de sécurité sans agent et appliquer des actions sur le réseau et les terminaux via un moteur de politiques Zero Trust unifié
- Interopérer avec l'infrastructure existante sans mise à niveau logicielle/matérielle
- Bénéficier d'une intégration directe avec plus de 30 fournisseurs d'infrastructure réseau et plusieurs centaines de modèles de produits

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, de solliciter inutilement la bande passante du réseau ou d'entraver la productivité.
- 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, IoMT et OT.
- Implémentez des politiques et automatisez les contrôles pour garantir la conformité des configurations dans les déploiements cloud, notamment Amazon Web Services, Microsoft 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 (IOC) et les risques sur les appareils en temps réel afin de réduire le délai moyen d'intervention (MTTR).
- Isolez et neutralisez automatiquement les appareils compromis ou malveillants pour éviter la propagation latérale de logiciels malveillants et limiter ainsi l'impact potentiel.
- Automatisez l'intervention sur incident et initiez des flux de travail de correction sur les appareils en temps réel.
- 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.

Déceler, évaluer, contrôler

La plateforme Forescout maximise la valeur d'eyeControl en fournissant une visibilité totale sur les appareils, une conformité sans faille, la segmentation du réseau et une base solide pour vos stratégies Zero Trust.

Pour en savoir plus, rendez-vous sur www.forescout.fr/#products.

Forescout Technologies, Inc.

Numéro gratuit (US)
1-866-377-8771
Tél. (intl) +1-408-213-3191
Support +1-708-237-6591

Plus d'infos sur Forescout.fr