Forescout eyeControl

Appliquez et automatisez des contrôles basés sur des politiques pour réduire de façon proactive votre surface d'attaque et intervenir rapidement en cas d'incident

Les équipes de sécurité informatique sont submergées par un nombre croissant de problèmes de sécurité et de conformité, signalés par divers outils de sécurité générant constamment des alertes, mais sans possibilité d'intervenir directement. Malheureusement, ces outils ne disposent pas de données contextuelles suffisantes sur les appareils pour que des fonctions de priorisation ou d'automatisation puissent appliquer des contrôles en vue de réduire les risques. Par conséquent, ces experts en sécurité perdent un temps précieux à résoudre manuellement des problèmes mineurs, au lieu de se consacrer à la réduction proactive des risques ou à la neutralisation rapide des menaces.

Application de contrôles basés sur des politiques

Forescout eyeControl s'appuie sur les données contextuelles riches sur les appareils qui sont fournies par Forescout eyeSight afin de permettre aux équipes de sécurité de prioriser, appliquer et automatiser des contrôles basés sur des politiques. Les entreprises peuvent ainsi améliorer leurs pratiques de sécurité, réduire leur surface d'attaque et accélérer l'intervention sur incident et l'exécution de mesures de correction afin d'éliminer rapidement les menaces, les incidents de sécurité et les failles de conformité.

En fonction de vos stratégies de sécurité, vous pouvez mettre en œuvre des actions sur le réseau et les points d'extrémité à l'aide d'eyeControl. Pour orchestrer des actions sur le réseau, eyeControl s'intègre directement aux infrastructures hétérogènes de réseaux physiques et virtuels : commutateurs, sans fil, VPN, cloud et définis par logiciel. Des actions peuvent être exécutées sans agent sur les points d'extrémité Windows, Mac et Linux, ou via l'utilisation de SecureConnector™.

eyeControl

Avantages

- Protège les données sensibles contre les menaces externes
- Empêche les appareils infectés, vulnérables ou non conformes de propager des logiciels malveillants
- Empêche les vols de données et indisponibilités réseau dus aux attaques ciblées
- Garantit l'accès au réseau et sa disponibilité pour les employés, clients et sous-traitants
- Assure la conformité aux politiques internes et aux réglementations externes
- Automatise des actions de contrôle afin de prendre des mesures adaptées à chaque situation

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

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

Hôte

- 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 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)

Hôte

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

Automatisez les contrôles en toute confiance

eyeControl tire parti d'un moteur de politiques intuitif et flexible qui permet aux entreprises d'appliquer des contrôles granulaires et ciblés. Il est possible d'implémenter des flux de travail sophistiqués et des actions composées grâce à une définition dynamique de la portée facile à configurer, à une logique booléenne et à des politiques en cascade. Le Graphique des politiques facilite la création précise de politiques, l'analyse des flux de politiques et l'optimisation des politiques avant l'application d'actions de contrôle.

Des actions de contrôle peuvent être déclenchées manuellement par les équipes de sécurité. Sinon, les opérations de sécurité peuvent être progressivement automatisées pour renforcer leur efficacité. En commençant par des tâches répétitives de base, puis en intégrant des contrôles plus complexes au fil du temps, l'automatisation permet au personnel informatique qualifié de se consacrer aux problèmes ayant un impact plus important. Cette approche garantit une interruption d'activité minimale tout en améliorant considérablement l'accès au réseau, la conformité des appareils, la segmentation du réseau et les stratégies d'intervention sur incident.

"La plupart du temps, nous pouvons automatiser une action sur un point d'extrémité, mais quand une intervention manuelle est nécessaire, un simple clic droit suffit." – *Joseph Cardamone, Analyste en sécurité informatique et responsable de la protection de la vie privée pour l'Amérique du Nord, Haworth*

Difficultés

- Les appareils non conformes ou non autorisés qui sont connectés au réseau présentent un risque important.
- Les réseaux sans hiérarchie ni segmentation rendent les entreprises vulnérables aux menaces latérales.
- Il est impossible de réagir rapidement et efficacement aux menaces et aux incidents de sécurité.
- Les outils de sécurité ne permettent pas d'évaluer le niveau de protection des appareils en permanence.
- Le risque d'interruptions d'activité limite l'automatisation des contrôles de sécurité.

Contrôlez l'accès au réseau

Contrôlez l'accès aux ressources de l'entreprise en fonction du profil de l'utilisateur (invité, employé, sous-traitant), de la classification de l'appareil et de son niveau de sécurité.

- Différenciez l'accès pour les appareils invités et BYOD.
- Appliquez des politiques d'accès au réseau avec ou sans
  authentification basée sur la norme 802.1X.
- Prenez des mesures contre les appareils suspects, non approuvés ou relevant de l'informatique de l'ombre qui sont connectés au réseau.
- Limitez ou bloquez l'accès au réseau pour les appareils compromis ou malveillants.
- Mettez en quarantaine ou isolez les appareils non conformes jusqu'à ce que les écarts de conformité aient été résolus

"L'une des raisons pour lesquelles nous avons choisi la plateforme Forescout est que cette technologie ne repose pas sur le protocole 802.1X, ce qui simplifie grandement le déploiement. En outre, le fait de ne pas avoir à installer d'agents permet de bénéficier de hautes performances en toute simplicité."
—*Juan Ignacio Gordon, Directeur de la sécurité informatique, ACCIONA*

Améliorez la conformité des appareils

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

- Assurez-vous que les points d'extrémité sont correctement configurés et prenez des mesures correctives pour les violations de configuration critiques, notamment les mots de passe faibles ou par défaut.
- Assurez-vous que les applications et les agents de sécurité requis sont installés, en cours d'exécution et à jour.
- Désactivez ou bloquez les applications non autorisées qui pourraient engendrer des risques ou solliciter inutilement la bande passante du réseau et la productivité des ressources.
- Identifiez les vulnérabilités à haut risque et les correctifs critiques manquants, puis prenez des mesures correctives qui s'imposent.
- Ciblez de manière proactive des actions de correction telles que l'installation des logiciels de sécurité requis, la mise à jour des agents ou l'application de correctifs de sécurité.
- Implémentez des politiques et automatisez des contrôles pour garantir la conformité des configurations dans les déploiements cloud, notamment AWS, Azure et VMware®.

"Avec la solution Forescout, nous espérons économiser des millions de dollars grâce à des audits nettement plus rapides, qui produisent moins de résultats à analyser et nécessitent moins d'efforts de correction."
— *Phil Bates, Chief Information Security Officer, State of Utah*

Implémentez une segmentation dynamique du réseau

Appliquez des politiques de segmentation réseau dynamique aux technologies de contrôle disparates dans votre entreprise étendue, grâce à un cadre de politiques commun.

- Attribuez dynamiquement des appareils à des groupes de segmentation en vous basant sur les propriétés, la classification et le niveau de sécurité des appareils.
- Appliquez des contrôles de segmentation via des VLAN, des listes de contrôle d'accès (ACL), des WLAN et un marquage sur les réseaux de campus et d'exploitation.
- Appliquez des contrôles de segmentation via des groupes/marqueurs de sécurité dans des environnements cloud publics et privés tels qu'AWS et VMware NSX.
- Segmentez les appareils non conformes et vulnérables en zones distinctes afin d'assurer la continuité des activités tout en réduisant votre surface d'attaque. Concentrez-vous en particulier sur les appareils auxquels il n'est possible d'appliquer des correctifs ou des mesures de correction qu'au cours des périodes de maintenance planifiées.
- Appliquez des politiques de segmentation pour isoler les appareils et les flux de données critiques du reste du réseau, conformément aux réglementations telles que la loi HIPAA, la norme PCI et le programme CSP de SWIFT.

"Non seulement Forescout peut isoler les appareils et procéder à la segmentation du réseau, mais il peut également découvrir des réseaux sur lesquels nous n'avions aucune visibilité auparavant."
–RSSI adjoint, Grand établissement de soins de santé

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 le préjudice pour l'entreprise.

- Identifiez les appareils à haut risque qui n'ont pas été isolés ou corrigés.
- Identifiez les indicateurs de compromission 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 compromis.
- 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

"Avec Forescout, c'est comme si nous disposions dans l'équipe d'un spécialiste de la traque des menaces, qui analyse inlassablement et de façon ininterrompue notre réseau mondial. Nous sommes désormais en mesure de traiter des problèmes auxquels nous ne pouvions pas consacrer de temps auparavant. Des tâches qui nous auraient pris des heures ne prennent plus que quelques minutes."
— Nick Duda, Principal Security Engineer, HubSpot

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Numéro gratuit (États-Unis)
1-866-377-8771
Tél. (International) +1-408-213-3191
Support +1-708-237-6591

Pour en savoir plus, consultez le site Forescout.fr