FORESCOUT

eyeSight

La source d'informations ultime pour chaque appareil connecté de votre environnement numérique

Technologie sans agent
Établit un inventaire unifié en temps réel des appareils connectés au réseau, avec leur niveau de sécurité et de risque.

Précision
Classifie chaque appareil afin d'obtenir les données contextuelles nécessaires à la mise en œuvre d'une sécurité et d'une conformité proactives.

Efficacité
Automatise les tâches répétitives comme la mesure du niveau de conformité et l'exposition aux cyberrisques et génère les rapports correspondants, tout en réduisant les erreurs humaines.

Efficience
Garantit en temps réel le bon fonctionnement des outils de sécurité et contrôles de conformité.

Forescout eyeSight s'intègre en profondeur à la structure de votre réseau pour offrir un aperçu inégalé de chaque appareil connecté.

- Découverte de votre inventaire complet d'appareils avec plus de 30 techniques actives et passives qui révèlent les lacunes de couverture de votre environnement numérique et fournissent une vue en temps réel de votre surface d'attaque
- Classification automatique des appareils et création de profils complets incluant les risques et vulnérabilités connus grâce aux renseignements sur les menaces fournis par Vedere Labs
- Préparation précoce aux menaces émergentes grâce à l'apprentissage automatique dans le cloud, qui améliore en continu le Device Cloud de Forescout, une source propriétaire de renseignements sur les appareils comptant plus de 30 milliards de points de données uniques
- Évaluation en continu du statut, du niveau de risque et de la conformité aux politiques des appareils sans avoir à installer d'agent, ce qui est essentiel à la protection des appareils IoT, IoMT et OT
- Les rapports automatisés sur le niveau de conformité et l'exposition aux cyberrisques permettent de gagner du temps, de réduire les erreurs humaines et de se concentrer sur l'essentiel

Découverte

Bénéficiez d'une visibilité sur les appareils dès qu'ils se connectent au réseau.

Surveillez en continu les appareils en transit dès qu'ils rejoignent le réseau et jusqu'à ce qu'ils le quittent.

Obtenez un inventaire des appareils en temps réel mettant en évidence les lacunes en matière de visibilité.

Classification

Identifiez divers types d'appareils IT, IoT, IoMT et OT.

Exploitez la puissance de Device Cloud pour obtenir des données contextuelles complètes sur les appareils.

Améliorez l'efficacité, la couverture et la vitesse de l'autoclassification.

Évaluation

Identifiez les vulnérabilités et les écarts de conformité.

Évaluez le respect des obligations internes et externes.

Acquérez une connaissance situationnelle des cyberrisques et des risques opérationnels.

eyeSight résout les problèmes suivants :

- **Failles de visibilité** causées par des équipes isolées et des outils de sécurité disparates
- **Risques opérationnels et commerciaux** dus aux processus manuels propices aux erreurs
- **Informations incomplètes sur les appareils** entravant l'exécution de politiques de sécurité
- **Failles de sécurité** lorsque les outils avec agent ne sont pas à jour ou sont défaillants
- **Appareils non approuvés non détectés** ou usurpation d'adresses MAC
- **Non-conformité** pouvant émerger rapidement entre les analyses ponctuelles

Découverte

Découverte approfondie en temps réel

Éliminez les angles morts et minimisez les risques grâce à une visibilité totale sur chaque aspect de votre environnement numérique :

- Infrastructures physiques et SDN, notamment les commutateurs, routeurs, points d'accès sans fil et contrôleurs
- Ordinateurs portables, tablettes, smartphones, systèmes BYOD/invités et appareils de télétravail
- Appareils IoT sur les réseaux de campus, centres de données, succursales, sites distants et réseaux périphériques
- Instances de cloud public et privé dans les environnements Amazon Web Services, Microsoft Azure et VMware
- Systèmes des technologies d'exploitation (OT) et de contrôle industriels, notamment HMI, SCADA ou PLC, et appareils immotiques (BMS et BAS)
- Appareils IoMT dans les hôpitaux et réseaux de soins de santé, tels que pompes de perfusion et équipements de diagnostic

Adaptation personnalisée des techniques de découverte et de surveillance à votre environnement

Tirez parti de la flexibilité offerte par plus de 30 techniques de surveillance active et passive sur les réseaux câblés, sans fil, VPN, virtuels et définis par logiciel. Évitez ainsi de perturber les appareils sensibles aux techniques d'analyse active.

RECONNAISSANCE ACTIVE D'INFRASTRUCTURE

Interrogation de l'infrastructure réseau

Intégration SDN
- Meraki
- Cisco ACI

Intégration de cloud public/privé
- VMware
- AWS
- Azure

Services d'annuaires de requêtes (LDAP)

Applications web de requêtes (REST)

Bases de données de requêtes (SQL)

Orchestrations eyeExtend

DÉCOUVERTE PASSIVE D'APPAREILS

Traps SNMP

Analyse des flux de trafic SPAN
- NetFlow
- Flexible NetFlow
- IPFIX
- sFlow

Requêtes DHCP

Agent utilisateur HTTP

Empreintes TCP

Analyse des protocoles

Requêtes RADIUS

DÉCOUVERTE ACTIVE D'APPAREILS

Inspection Windows sans agent
- WMI
- RPC
- SMB

Inspection macOS et Linux sans agent
- SSH

NMAP

Requêtes SNMP

Requêtes HTTP

Forescout SecureConnector®

Classification

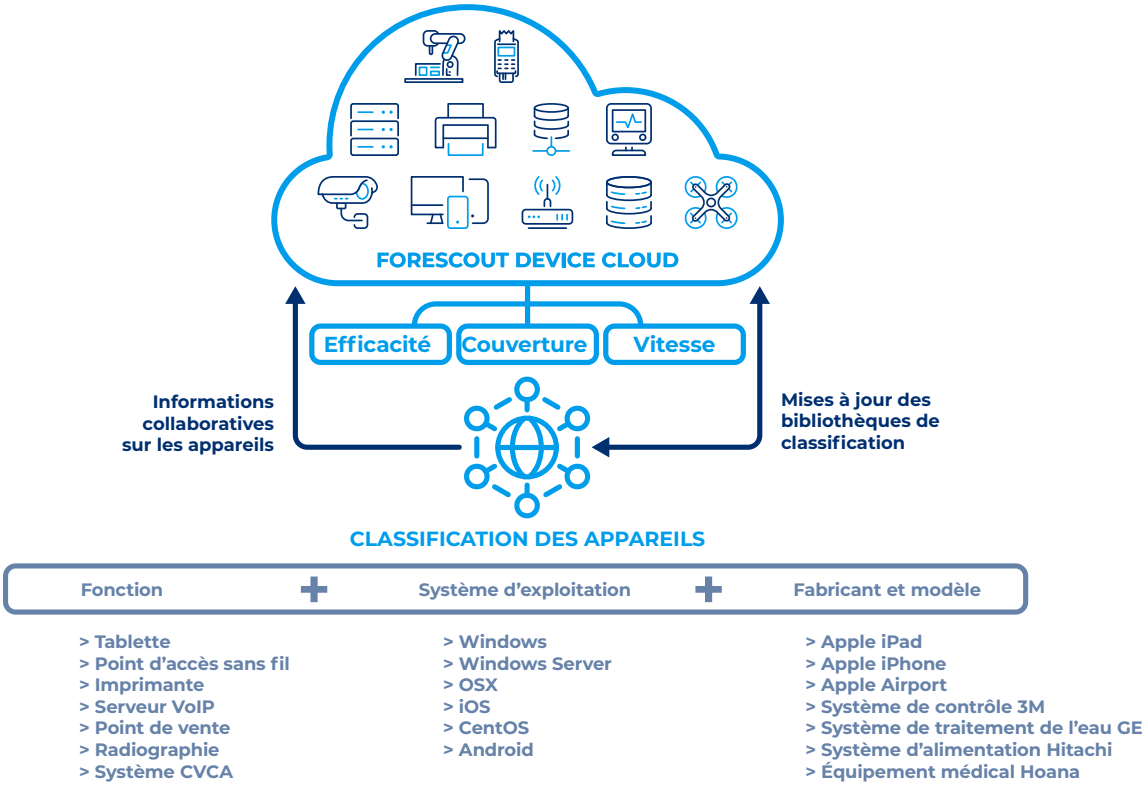
Autoclassification intelligente

L'implémentation de politiques de sécurité sans données contextuelles exhaustives peut entraîner des résultats indésirables et mettre en péril les opérations métier. Forescout Device Cloud, le plus grand référentiel de données collectées sur plus de 50 millions d'appareils, fournit automatiquement des données contextuelles complètes sur chaque appareil connecté. Notre taxonomie de classification multidimensionnelle permet d'identifier la fonction et le type d'appareil, le système d'exploitation et la version, ainsi que le fabricant et le modèle, notamment :

- plus de 1 900 versions de systèmes d'exploitation ;
- plus de 7 700 fabricants et modèles d'appareils ;
- les équipements médicaux de plus de 400 fournisseurs de technologies médicales de premier plan ;
- des milliers de systèmes de contrôle industriels et d'appareils d'automatisation utilisés dans divers secteurs (fabrication, énergie, pétrole et gaz, services publics, exploitation minière et autres infrastructures critiques).

Classification automatique optimisée par Forescout Device Cloud

Device Cloud, le plus grand référentiel au monde de données sur les appareils, offre les informations les plus complètes et précises sur les risques posés par les appareils dans le contexte de l'entreprise.



Évaluation

Évaluation sans agent de l'état des appareils

eyeSight découvre les appareils en continu et en évalue immédiatement la configuration, le niveau de sécurité et les indicateurs de risque pour savoir s'ils respectent les règles de conformité et les politiques de sécurité. Les politiques peuvent aider à mieux quantifier les risques en évaluant les conditions de conformité, notamment :

- Un logiciel de sécurité est-il installé, opérationnel et à jour avec les derniers correctifs ?
- L'appareil joue-t-il un rôle vital dans l'activité de l'entreprise ?
- Certains appareils exécutent-ils des applications non autorisées ou enfreignent-ils les normes de configuration ?
- Certains appareils, en particulier les systèmes IoT, IoMT et OT, utilisent-ils des mots de passe faibles ou par défaut ?
- Des appareils non approuvés ont-ils été détectés, notamment des équipements qui tentent d'usurper l'identité d'appareils légitimes ?
- Parmi vos appareils connectés, lesquels sont les plus vulnérables aux dernières menaces ?

Surveillance

Visualisation des données de conformité

Obtenez des informations exploitables à partir de tableaux de bord prêts à l'emploi capables d'identifier, de prioriser et de limiter les risques de manière rapide et proactive dans votre environnement numérique. Les vues personnalisables sur les tableaux de bord aident les analystes en sécurité et le SOC à réaliser de nombreux objectifs :

- Évaluer l'évolution des risques et de la conformité sur l'ensemble ou un sous-ensemble des politiques
- Identifier les appareils vulnérables et compromis afin d'accélérer et de cibler l'intervention sur incident
- Suivre l'évolution des tendances de conformité au fil du temps
- Personnaliser et partager des affichages des risques et de la conformité créés à l'intention des cadres dirigeants et des auditeurs
- Rechercher et filtrer rapidement les appareils par politique ou attribut d'appareil

Segmentation, orchestration et application

La plateforme Forescout maximise la valeur d'eyeSight grâce à une suite de fonctionnalités de cybersécurité automatisées permettant de concevoir et d'implémenter des politiques de sécurité pour le contrôle d'accès réseau et la segmentation dynamique du réseau, et elle pose les bases d'une sécurité Zero Trust.

Pour en savoir plus sur la plateforme Forescout, rendez-vous sur www.forescout.fr/#platform.

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