Forescout eyeSight

Découvrez , classifiez et évaluez en continu vos environnements IT et OT afin de réduire les risques

Les directeurs informatiques sont chargés de protéger un nombre croissant de systèmes connectés au réseau, dont de nombreux appareils IoT et OT. Or, une bonne protection exige une parfaite visibilité. La multiplication et la diversification des appareils rend donc d'autant plus urgente la nécessité d'une vue à 360° sur tous les appareils physiques et virtuels connectés au réseau. Cette vue doit inclure les appareils gérés, non gérés et inconnus connectés par les employés, les sous-traitants et les clients, ou même par le personnel chargé des opérations. Quel que soit l'emplacement de tous ces appareils sur le réseau (campus, centre de données, cloud privé et public, environnements OT ou systèmes de contrôle industriels), ils doivent être correctement détectés, profilés et comptabilisés.

Figure 1. Visibilité détaillée sur le campus, l'IoT, le centre de données, le cloud et les technologies d'exploitation (OT).

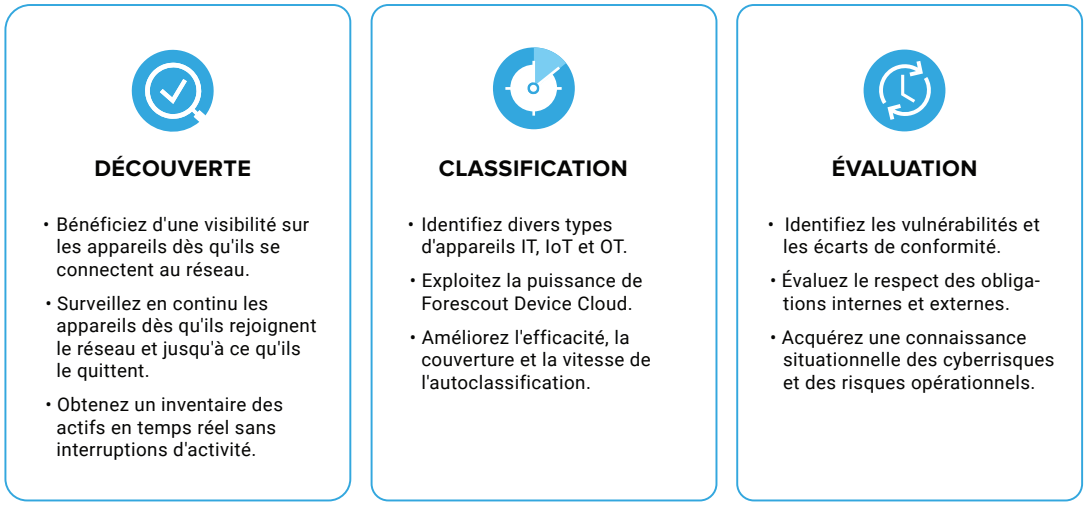
Forescout eyeSight vous fournit des informations précieuses sur l'ensemble de vos appareils sans interrompre les processus métier critiques. Dans un premier temps, il procède à la découverte de tous les appareils IP connectés aux réseaux de votre entreprise étendue. Mais ce n'est que la première étape vers une visibilité totale. Des données contextuelles exhaustives sont essentielles à la création de politiques appropriées et à la prise de décisions de contrôle éclairées. Après avoir découvert les appareils connectés, eyeSight les classifie automatiquement et évalue leur conformité aux politiques de l'entreprise. La combinaison puissante de ces trois fonctionnalités (découverte, classification et évaluation) offre la visibilité sur les appareils nécessaire pour mettre en place des politiques et des actions appropriées.

eyeSight

Avantages

- Établit un inventaire unifié en temps réel des appareils connectés au réseau, le tout sans agent
- Profile les appareils avec précision afin d'obtenir les données contextuelles nécessaires à la création de politiques de sécurité et de conformité proactives
- Identifie les appareils non approuvés, vulnérables ou non conformes et crée des politiques en vue de réduire les risques
- Garantit en temps réel le fonctionnement des outils de sécurité et des contrôles de conformité
- Mesure efficacement le niveau de conformité et l'exposition aux cyberrisques et génère les rapports correspondants
- Automatise les tâches courantes afin de réduire les erreurs humaines et d'accroître l'efficacité

Figure 2. Fonctionnalités de visibilité essentielles fournies par eyeSight.



Découverte continue sans agent

Les appareils IoT et OT posent des problèmes particuliers en matière de visibilité. Un tel volume d'appareils complique l'évolutivité, car la découverte manuelle n'est plus une option. En outre, un grand nombre de ces appareils ne prennent pas en charge les agents et sont sensibles aux techniques de sondage et d'analyse actives susceptibles de perturber les systèmes et les activités de l'entreprise. À l'aide de plus de 20 techniques de surveillance active et passive (voir la figure 3), eyeSight évite toute faille de visibilité potentielle grâce à la découverte automatique des éléments suivants :

- Laptops, tablets, smartphones, BYOD/guest systems and IoT devices on campus networks
- Virtual machines, hypervisors and physical servers in data centers
- AWS, Azure and VMware instances across public and private clouds
- Medical, industrial and building automation devices on operational technology networks
- Physical and software-defined network infrastructure including switches, routers, VPNs, wireless access points and controllers

Ensemble, ces fonctionnalités de découverte réduisent les risques opérationnels et éliminent les zones d'ombre afin de dresser un inventaire complet et continu des appareils à l'échelle de l'entreprise étendue.

Figure 3. Techniques de découverte active et passive.

DÉCOUVERTE PASSIVE D'INFRASTRUCTURES
Traps SNMP
Trafic SPAN
Analyse des flux • NetFlow • Flexible NetFlow • IPFIX • sFlow
Requêtes DHCP
Agent utilisateur HTTP
Empreintes TCP
Analyse des protocoles
Requêtes RADIUS

DÉCOUVERTE PASSIVE D'APPAREILS
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 ACTIVE D'APPAREILS
Inspection Windows sans agent • WMI • RPC • SMB
Inspection macOS et Linux sans agent • SSH
NMAP
Requêtes SNMP
Requêtes HTTP
SecureConnector®

Difficultés

- Les équipes, outils de sécurité et processus isolés présentent des failles sur le plan de la visibilité.
- Les processus manuels propices aux erreurs engendrent des risques opérationnels et métier.
- Des informations incomplètes sur les appareils ne fournissent pas assez de contexte aux équipes informatiques, qui en ont besoin pour créer des politiques efficaces.
- Il n'est pas possible de vérifier que les outils de sécurité sont installés et configurés correctement, et qu'ils sont pleinement opérationnels.
- Les appareils non approuvés qui n'ont pas été détectés engendrent des risques inutiles pour la sécurité et la conformité.
- Les analyses ponctuelles obsolètes conduisent à un manque de confiance dans le niveau de conformité.

Autoclassification intelligente

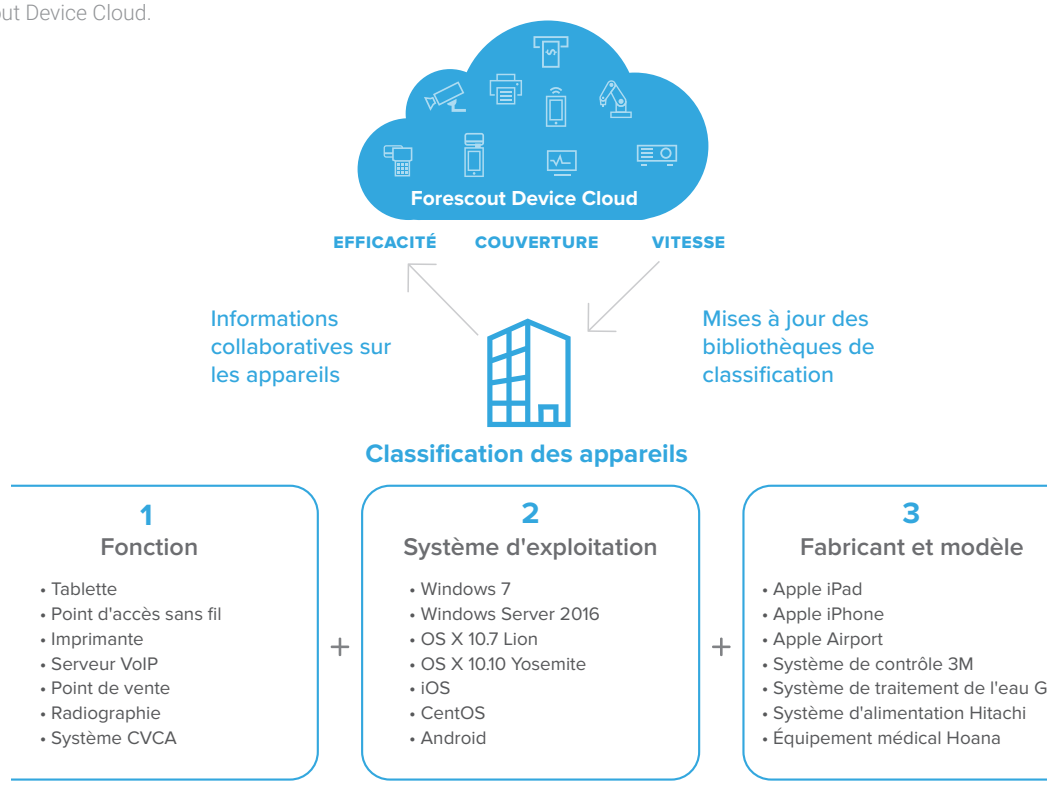
Des données contextuelles exhaustives sur chaque appareil sont essentielles à la création de politiques granulaires. Vous devez connaître le contexte ou l'objectif opérationnel de chaque appareil pour déterminer comment le protéger et le gérer de manière optimale. La multiplication et diversification des appareils rendent presque impossible la collecte manuelle de ces données contextuelles, et la création de politiques sans contexte met en péril les opérations. eyeSight classifie automatiquement les appareils traditionnels, IoT et OT à l'aide d'une taxonomie de classification multidimensionnelle permettant d'identifier la fonction et le type d'appareil, le système d'exploitation et la version, ainsi que le fabricant et le modèle. L'inspection approfondie des paquets de plus de 100 protocoles IT et OT permet à eyeSight d'obtenir des informations détaillées sur l'identité des appareils de ce type.

eyeSight classifie automatiquement :

- plus de 500 versions de système d'exploitation ;
- plus de 5 000 fabricants et modèles d'appareils ;
- les équipements médicaux de plus de 350 fournisseurs de technologies médicales de premier plan ;
- des milliers d'appareils de contrôle et d'automatisation industriels utilisés dans divers secteurs (fabrication, énergie, pétrole et gaz, services publics, exploitation minière et autres infrastructures critiques).

L'autoclassification est une fonctionnalité d'eyeSight optimisée par **Forescout Device Cloud**, qui garantit que cette précieuse source de données contextuelles s'adapte à l'augmentation du nombre et de la diversité des appareils. Forescout Research exploite les données de quelque 8 millions d'appareils réels dans notre cloud* et publie fréquemment ces nouveaux profils afin d'améliorer l'efficacité, la couverture et la vitesse de la classification pour l'ensemble de vos appareils.

Figure 4: Forescout Device Cloud.



*En date du 31 décembre 2018

Évaluation du niveau de sécurité des appareils

La classification des appareils fournit un contexte opérationnel concernant l'objectif de chacun d'entre eux. Toutefois, pour obtenir des données contextuelles exhaustives, il est nécessaire d'adopter une autre approche afin d'évaluer le niveau de sécurité et d'intégrité de chaque appareil.

eyeSight surveille le réseau en continu et évalue la configuration, l'état et le niveau de sécurité des appareils connectés afin de déterminer leur profil de risque et leur respect des politiques de sécurité et de conformité réglementaire. Il répond à des questions critiques telles que :

- Un logiciel de sécurité est-il installé, opérationnel et à jour avec les derniers correctifs ?
- Certains appareils exécutent-ils des applications non autorisées ou enfreignent-ils les normes de configuration ?
- Certains appareils utilisent-ils des mots de passe faibles ou par défaut (ce qui est particulièrement dangereux pour les appareils IoT) ?
- Des appareils non approuvés ont-ils été détectés, notamment des équipements qui se font passer pour des appareils légitimes à l'aide de techniques d'usurpation ? Si oui, ces appareils sont-ils connectés au réseau ?
- Parmi les appareils connectés à votre réseau, lesquels sont les plus vulnérables aux dernières menaces ?

La puissance des informations sur les appareils

Les fonctionnalités de découverte, de profilage, d'autoclassification et d'évaluation d'eyeSight offrent une visibilité sur les appareils évidente à l'utilisation de la console Forescout. Celle-ci vous permet d'obtenir des informations générales par le biais de tableaux de bord personnalisables, ainsi que de partager cet aperçu de la réalisation de vos objectifs en matière de risques et de conformité. Ces vues dynamiques peuvent aider les équipes à réaliser de nombreux objectifs :

- Évaluer la réussite de l'implémentation d'une politique particulière
- Identifier les appareils vulnérables en cas de compromission afin d'accélérer l'intervention sur incident
- Évaluer le respect d'exigences de conformité spécifiques au fil du temps
- Créer des affichages des risques, de la conformité et des vulnérabilités potentielles à l'attention des cadres dirigeants et des auditeurs
- Accéder à des informations détaillées pour résoudre les problèmes liés à des politiques spécifiques, aux types d'appareils, aux emplacements, etc.

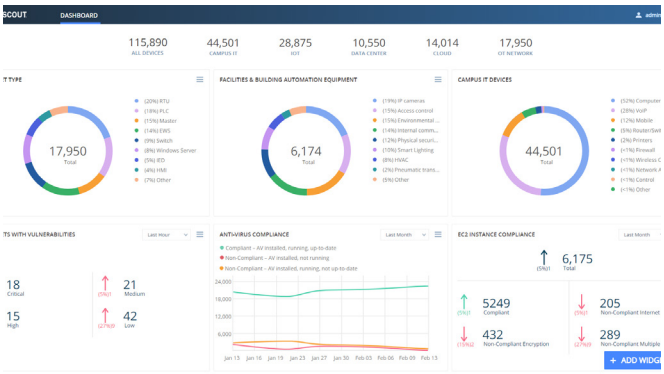


Figure 5. Personnalisez le tableau de bord pour fournir aux parties prenantes les données contextuelles dont elles ont besoin.

La visibilité sur les appareils fournie par eyeSight peut également être partagée avec des acteurs informatiques interfonctionnels via des actions de notification et des API. La gamme de produits eyeExtend partage ces données contextuelles sur les appareils avec d'autres produits informatiques et de sécurité de premier ordre en vue d'automatiser les flux de travail et d'orchestrer la prise de mesures à l'échelle du système.

Sans les données contextuelles critiques fournies par eyeSight, les entreprises pourraient manquer de la confiance nécessaire pour implémenter des politiques de contrôle, car toute action basée sur des informations insuffisantes peut mettre en péril les opérations métier. eyeSight vous offre les informations détaillées dont vous avez besoin pour créer et implémenter des politiques granulaires et automatiser des actions pour la gestion des ressources, la conformité des appareils, l'accès au réseau, la segmentation du réseau et les stratégies d'intervention sur incident. Vous pouvez ainsi mettre en place des contrôles efficaces basés sur des politiques et orchestrer des actions en toute confiance à l'aide des produits Forescout eyeControl et Forescout eyeExtend.

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