FORESCOUT
Active Defense for the Enterprise of Things™

eyeSight
Visibilité totale des appareils

TECHNOLOGIE SANS AGENT
Établit un inventaire unifié en temps réel des appareils connectés au réseau.

PRÉCISION
Profile tous les appareils afin d'obtenir les données contextuelles nécessaires à la mise en œuvre d'une sécurité et d'une conformité proactives.

PROACTIVITÉ
Identifie les appareils non approuvés, vulnérables ou non conformes et crée des politiques en vue de réduire les risques.

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

EFFICACITÉ
Mesure automatiquement le niveau de conformité et l'exposition aux cyberrisques et génère les rapports correspondants, tout en réduisant les erreurs humaines et en améliorant l'efficacité.

Découvrez, classifiez et évaluez en continu tous les appareils connectés à l'échelle de l'entreprise

Forescout eyeSight vous fournit des informations précieuses sur l'ensemble de votre environnement EoT, sans interrompre les processus métier critiques.

- Découverte de tous les appareils à connexion IP
- Autoclassification des appareils et données contextuelles exhaustives
- Évaluation de la conformité aux politiques et du niveau de sécurité des appareils

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 actifs en temps réel sans interruptions d'activité.

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

Exploitez la puissance de Forescout Device Cloud.

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.

DÉCOUVERTE

Découverte continue sans agent

Éliminez les zones d'ombre et réduisez les risques opérationnels grâce à une visibilité totale sur votre environnement EoT :

- 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 AWS, Azure et VMware
- Systèmes des technologies d'exploitation (OT), notamment les appareils médicaux, industriels et immotiques
- Infrastructures réseau physiques et SDN, notamment les commutateurs, routeurs, points d'accès sans fil et contrôleurs

Tirez parti de la flexibilité offerte par plus de 20 techniques de surveillance active et passive sur les réseaux filaires, sans fil, VPN, virtuels et définis par logiciel. Évitez ainsi de perturber les appareils sensibles aux techniques d'analyse active.

DÉCOUVERTE PASSIVE D'INFRASTRUCTURES	DÉCOUVERTE PASSIVE D'APPAREILS	DÉCOUVERTE ACTIVE D'APPAREILS
Traps SNMP	Interrogation de l'infrastructure réseau	Inspection Windows sans agent • WMI • RPC • SMB
Analyse des flux de trafic SPAN • NetFlow • Flexible NetFlow • IPFIX • sFlow	Intégration SDN • Meraki • Cisco ACI	Inspection macOS et Linux sans agent • SSH
Requêtes DHCP	Intégration de cloud public/privé • VMware • AWS • Azure	NMAP
Agent utilisateur HTTP	Services d'annuaires de requêtes (LDAP)	Requêtes SNMP
Empreintes TCP	Applications web de requêtes (REST)	Requêtes HTTP
Analyse des protocoles	Bases de données de requêtes (SQL)	SecureConnector®
Requêtes RADIUS	Orchestrations eyeExtend	

CLASSIFICATION

Autoclassification intelligente

Les politiques Zero Trust peuvent uniquement être appliquées sur la base des données contextuelles complètes des appareils. L'implémentation des politiques Zero Trust sans des données contextuelles exhaustives peut mettre en péril les opérations métier. Or, il est pratiquement impossible de recueillir manuellement ces données contextuelles. L'inspection approfondie des paquets de plus de 150 protocoles IT et OT permet à eyeSight de fournir des informations de profilage détaillées sur tous les appareils IT, IoT et OT. Une 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 600 versions de système d'exploitation ;
- plus de 5 700 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).

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 Zero Trust efficaces

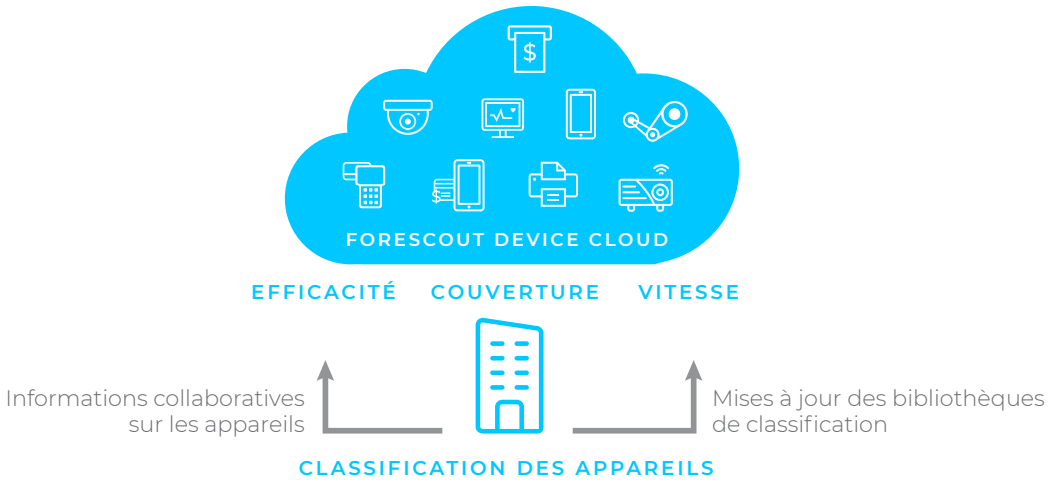
Failles de sécurité lorsque les outils avec agent ne sont pas à jour ou sont défaillants

Appareils non approuvés non détectés ou tentatives d'usurpation

Non-conformité pouvant émerger rapidement entre les analyses ponctuelles

Autoclassification optimisée par Forescout Device Cloud

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



Fonction		+ Système d'exploitation		+ Fabricant et modèle	
· Tablette	· Point de vente	· Windows 7	· iOS	· Apple iPad	· Système de traitement de l'eau GE
· Point d'accès sans fil	· Radiographie	· Windows Server 2016	· CentOS	· Apple iPhone	· Système d'alimentation Hitachi
· Imprimante	· Système CVCA	· OS X 10.7 Lion	· Android	· Apple Airport	· Équipement médical Hoana
· Serveur VoIP		· OS X 10.10 Yosemite		· Système de contrôle 3M	

ÉVALUATION

Évaluation du niveau de sécurité des appareils

Un autre élément essentiel des politiques Zero Trust réside dans l'intégration de pratiques de sécurité satisfaisantes et du profil de risque des appareils connectés. eyeSight surveille le réseau en continu pour évaluer la configuration, le niveau de sécurité et les indicateurs de risque des appareils connectés, et pour s'assurer qu'ils respectent les mandats de conformité et les normes de sécurité. Les politiques Zero Trust peuvent être basées sur des conditions de risque et de conformité 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, en particulier les systèmes IoT 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 les appareils connectés à votre réseau, lesquels sont les plus vulnérables aux dernières menaces ?

Détecter, c'est bien. Sécuriser, c'est mieux.

Contactez-nous dès aujourd'hui pour protéger efficacement votre Internet des objets en entreprise.

SURVEILLANCE

Visibilité et conformité dans les environnements EoT

Obtenez des informations exploitables à partir de tableaux de bord prêts à l'emploi et personnalisables pour identifier, prioriser et limiter les risques de manière rapide et proactive sur l'ensemble de vos objets connectés. Les vues dynamiques aident les analystes en sécurité et le SOC à réaliser de nombreux objectifs :

- Évaluer l'évolution des risques et de la conformité au fil du temps sur l'ensemble ou un sous-ensemble des politiques
- Identifier les appareils vulnérables et compromis afin d'accélérer 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 actifs EoT par attributs d'appareil ou de politique

Segmentation, orchestration et application

Maximisez la valeur d'eyeSight grâce à une suite de produits Forescout permettant de concevoir et d'implémenter des politiques Zero Trust pour le contrôle d'accès réseau, la sécurité OT et IoT, et la segmentation réseau.

Consultez le site www.forescout.com/platform/ pour en savoir plus sur les produits Forescout eyeSegment, eyeControl, eyeInspect et eyeExtend.

forescout.com/platform/eyeSight info-france@forescout.com

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