FORESCOUT
Active Defense for the Enterprise of Things™

eyeInspect

Anciennement SilentDefense™

TECHNOLOGIE SANS AGENT

Établit un inventaire complet, unifié et en temps réel des actifs OT, et renseigne les adresses IP connectées et les appareils connectés en série.

PRÉCISION

Établit des valeurs de référence pour les actifs et protège votre réseau grâce à plusieurs milliers d'indicateurs de menaces propres aux systèmes OT et à une détection des anomalies robuste basée sur l'apprentissage automatique.

PROACTIVITÉ

Évalue les risques, identifie les menaces, mesure leur impact sur l'entreprise et priorise les tâches de correction de manière proactive.

FIABILITÉ

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

EFFICACITÉ

Automatise les tâches d'évaluation de la conformité et des risques qui prennent beaucoup de temps, tout en réduisant les erreurs humaines et en améliorant l'efficacité.

Réduisez les risques, automatisez la conformité et optimisez l'analyse des menaces pour les environnements ICS et OT

Forescout eyeInspect offre une visibilité approfondie sur les appareils des réseaux OT et permet de gérer efficacement et en temps réel toute une série de risques opérationnels et de cyberrisques.

- Établissement d'une base de référence des comportements réseau admissibles grâce à plusieurs milliers d'indicateurs de menace et de requêtes propres aux environnements ICS/OT
- Agrégation de plusieurs milliers d'alertes et de millions de journaux en fonction de leur niveau de risque et de leur cause
- Autoclassification et évaluation des appareils pour s'assurer de leur conformité aux réglementations et aux politiques

VISUALISATION

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

Surveillez en continu les appareils 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.

DÉTECTION

Identifiez divers types d'appareils IP et OT en série.

Établissez des valeurs de référence pour les appareils et les groupes d'appareils.

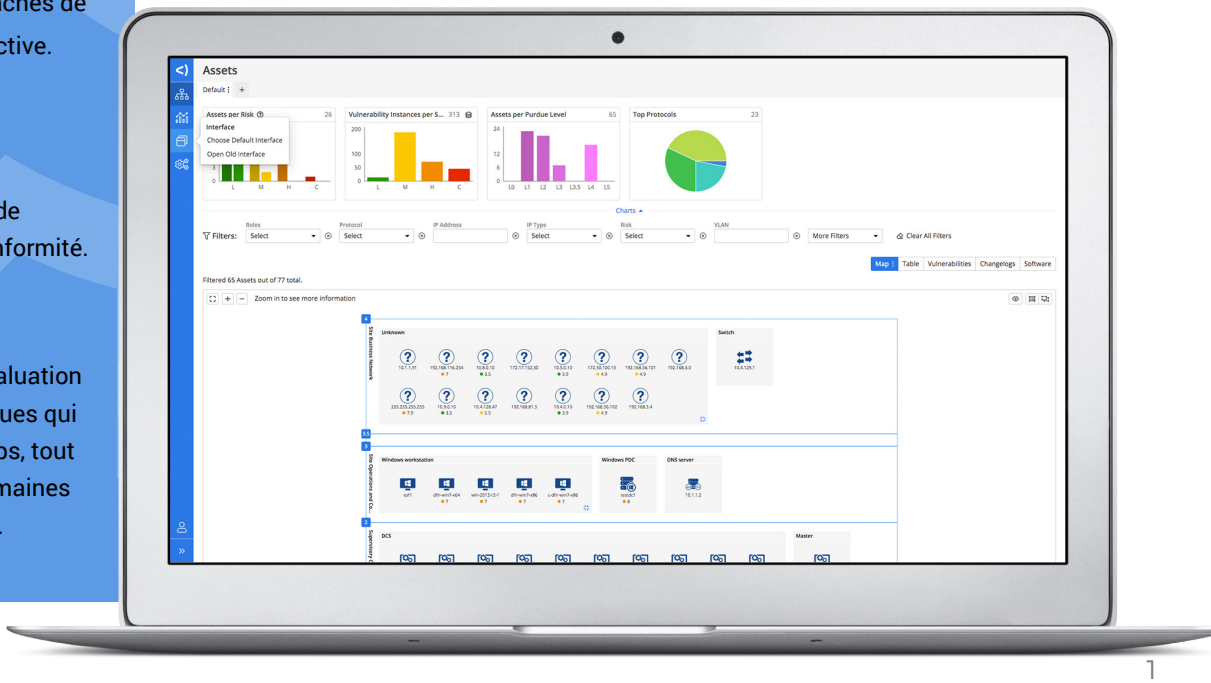
Optimisez la surveillance continue et l'efficacité de l'autoclassification.

INTERVENTION

Automatisez les évaluations de conformité.

Évaluez les risques à l'aide de scores de risques intuitifs.

Acquérez une connaissance situationnelle des cyberrisques et des risques opérationnels.



VISUALISATION

Visualisez plusieurs milliers d'appareils sur un seul écran

- Bénéficiez d'une visibilité totale. Éliminez les zones d'ombre associées aux nouveaux appareils connectés et aux appareils non approuvés.
- Obtenez un inventaire des actifs détaillé, précis et en temps réel.
- Bénéficiez d'une visibilité sur les appareils IP et série, y compris les interfaces utilisateur, les appareils SCADA, les automates programmables industriels, les contrôleurs, les capteurs, les compteurs et les E/S.

DÉTECTION

Détectez les menaces et gérez les risques intelligemment

- Détectez les cybermenaces connues et inconnues grâce à plusieurs milliers de contrôles de menaces propres aux systèmes ICS/OT et d'indicateurs de compromission.
- Détectez les cyberrisques et les risques opérationnels, et priorisez-les en fonction du degré d'urgence et de l'impact potentiel sur l'entreprise.
- Détectez les appareils non conformes et les politiques non respectées à l'échelle de votre réseau.
- Détectez les modifications du réseau, notamment les nouveaux appareils, les modifications d'infrastructure et les activités opérationnelles irrégulières.

INTERVENTION

Réagissez grâce à la solution de sécurité OT la plus intelligente et évolutive au monde

- Répondez aux cybermenaces et menaces opérationnelles en fonction de scores clairs.
- Répondez aux alertes à l'aide de flux de travail, règles et mesures correctives automatiques prédéfinis.
- Répondez aux changements de conformité à l'aide de règles, paramètres et rapports définis sur la base des valeurs de référence des actifs.
- Bénéficiez d'une visibilité sur les systèmes de gestion des bâtiments et systèmes immotiques, notamment les systèmes CVCA et de contrôle d'accès.
- Bénéficiez d'une visibilité sur les autres infrastructures réseau physiques et SDN, notamment les commutateurs, routeurs, VPN, points d'accès sans fil et contrôleurs.
- Affichez les alertes et les journaux en fonction de divers paramètres, notamment l'heure, l'appareil, l'emplacement réseau et le type d'alerte.

Configuration requise du centre de commande d'entreprise

Configuration requise	
Matériel/hyperviseur	Serveur avec rack 19" ou Vmware ESXi 5 minimum
Processeur	Processeur 4 cœurs (Intel®) 64 bits ≥ 2,4 GHz
Mémoire	16 à 32 Go
Disque dur	> 250 Go
Interface réseau	Interface pour la communication du centre de commande et l'accès aux applications web

Configuration requise du centre de commande

	Déploiement réduit (≤ 5 capteurs)	Déploiement moyen (≤ 10 capteurs)	Déploiement à grande échelle (10 à 100 capteurs)
Hyperviseur	VMware ESXi 5 minimum		
Format	Serveur avec rack 19" ou boîtier virtuel		
Processeur	Processeur 4 cœurs 64 bits	Processeur 4 ou 6 cœurs (Intel) 64 bits	Processeur 12 cœurs (Intel) 64 bits ≥ 2,4 GHz
Mémoire	16(*) à 64 Go	32(*) à 64 Go	64 à 256 Go
Disque dur	500 Go	1 To	> 1 To
	(Sur la base d'une conservation des données de 90 jours)		
Interface réseau	Interface pour la communication des capteurs et l'accès aux applications web		

(*) Capacité de mémoire pour une licence eyeSight uniquement

Configuration requise du capteur passif

	Déploiement réduit (Jusqu'à 100 Mbit/s)	Déploiement moyen (Jusqu'à 500 Mbit/s)	Déploiement à grande échelle (Jusqu'à 1 Gbit/s)
Exemple de modèle matériel	Foxguard® IADIN-FS1	Dell® Embedded PC 5000	Dell® PowerEdge R640
Description du déploiement	Déploiements en réseaux de petite taille et en environnements hostiles	Déploiements en réseaux de taille moyenne et en environnements hostiles	Déploiements en réseaux de grande taille et installations en centres de données
Format	Ordinateur renforcé de petite taille/rail DIN	Ordinateur renforcé de taille moyenne	Serveur avec rack 1U 19"
Processeur	Processeur 2 ou 4 cœurs (Intel) 64 bits	Processeur 4 ou 6 cœurs (Intel) 64 bits avec débit 8 GT/s	Processeur 6 cœurs (Intel) 64 bits minimum 2,4 GHz
Mémoire	8 à 16 Go	16 à 32 Go	64 à 256 Go
Disque dur	64 Go à 500 Go dans des ordinateurs renforcés (SSD à plage de températures étendue)		
Interface de surveillance	Jusqu'à 4 ports de surveillance	Jusqu'à 8 ports de surveillance	Jusqu'à 8 ports de surveillance

Configuration minimale requise du capteur actif

Intégration au capteur passif
eyeInspect peut être intégré directement sur n'importe quel capteur passif pour les déploiements de petite, moyenne et grande envergure.

	Autonom	Virtuel
Processeur	Processeur 2 à 4 cœurs	4 vCPU
Mémoire	4 Go de mémoire RAM	4 Go de mémoire RAM
Interface réseau	≥ 1	≥ 1
Disque dur	50 Go	

Pour plus d'informations sur la configuration matérielle requise, consultez le lien : https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/

PROTOCOLES

Pour une liste complète de tous les protocoles des systèmes IT, OT standard et OT propriétaires, consultez ce lien : https://www.forescout.com/company/resources/eyeinspect-protocols/

ORCHESTRATION, SEGMENTATION ET CONTRÔLE

Forescout maximise la valeur d'eyeInspect et de la plateforme Forescout à l'aide d'une suite de produits permettant de concevoir et d'implémenter des politiques et des actions automatisées pour la gestion des actifs, la conformité des appareils, l'accès réseau, la segmentation réseau et l'intervention sur incident. Consultez le site www.forescout.com/platform/ pour en savoir plus sur les produits eyeSight, eyeSegment, eyeControl, eyeManage et eyeExtend de Forescout.

eyeINSPECT RÉSOUT LES PROBLÈMES SUIVANTS :

Failles de visibilité des systèmes OT causées par des réseaux d'appareils géodistribués et non homogènes.

Problèmes de protection et de vulnérabilité lorsque les correctifs ne sont pas appliqués ou que les applications sont exposées.

Risques opérationnels et cyberrisques dus à une surcharge d'alertes et une mauvaise priorisation des tâches de correction.

Cyberveille incomplète entravant l'exécution de politiques efficaces.

Tâches de conformité gourmandes en ressources et qui exposent votre entreprise à des sanctions financières lourdes.

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

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

forescout.com/platform/eyeInspect

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