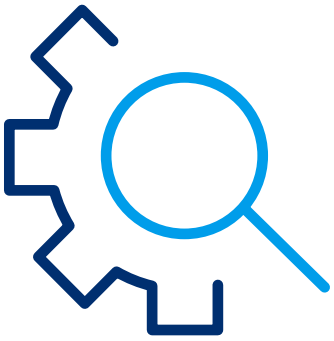

eyeInspect

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

Forescout eyeInspect offre une visibilité approfondie sur les appareils des réseaux OT/ICS et permet de gérer efficacement, en temps réel, les risques opérationnels ainsi que les cyberrisques.

- Comprenez pleinement la cyberrésilience de votre réseau OT grâce au cadre d'évaluation des risques des appareils.
- Bénéficiez d'une visibilité totale sur les appareils grâce à l'inspection approfondie des paquets de plus de 270 protocoles réseau industriels et actifs de référence.
- Protégez votre réseau grâce à plusieurs milliers d'indicateurs de menaces propres aux systèmes OT et à une détection des anomalies robuste.

Technologie sans agent

Établit un inventaire complet, unifié et en temps réel des appareils OT et ICS connectés, avec plus de 30 techniques de découverte actives et passives.

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.

Fiabilité

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

Efficacité

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

Visualisation

Bénéficiez d'une visibilité passive sur les appareils sans dépendre de SPAN pour une couverture totale.

Inspection approfondie des paquets (DPI) brevetée de plus de 270 protocoles IT et OT.

Détection

Collectez des informations exhaustives sur les appareils OT et enregistrez toutes les modifications de configuration à des fins d'analyse de la sécurité et d'enquêtes forensiques.

Automatisez la détection, la neutralisation et l'élimination des menaces grâce aux outils d'enquête sur les alertes et d'intervention.

Intervention

Simplifiez la mise en conformité avec les principales normes telles que NERC CIP, la directive européenne NIS, NIST CSF, IEC 62443 ou encore les directives TSA Pipeline Security.

Les tableaux de bord améliorent la collaboration entre utilisateurs et la richesse des détails sur les alertes renforce l'efficacité de l'intervention sur incident.

eyeInspect résout les problèmes suivants :

- **Failles de visibilité des systèmes OT** causées par des réseaux d'appareils géodistribués et hétérogènes.
- **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.

Visualisation

Visualisez plusieurs milliers d'appareils sur un seul écran

- Obtenez de manière passive un inventaire précis des actifs, en temps réel, sans interruptions d'activité.
- Bénéficiez d'une visibilité sur les appareils IP et connectés en série, notamment HMI, SCADA ou PLC, et appareils immotiques (BMS et BAS).
- Priorisez les alertes et consultez les journaux selon divers paramètres : temps, appareils, emplacement réseau, type d'alerte…

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 (IOC).
- 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 en temps réel, 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 de risque intuitifs qui facilitent la prise de décisions.
- Des flux de travail, règles et mesures correctives automatisés permettent de répondre aux menaces en temps réel, dès leur apparition.
- Répondez aux changements de conformité à l'aide de règles, paramètres et rapports définis sur la base des valeurs de référence des actifs.

Configuration requise du centre de commande d'entreprise

	DESCRIPTION DU PRODUIT
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

(*) Capacité de mémoire pour une licence eyeSight uniquement

	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 4/6 cœurs (Intel) 64 bits	Processeur 12 cœurs (Intel) 64 bits
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		

Configuration requise du capteur passif

	DÉPLOIEMENT RÉDUIT (≤ 5 capteurs)	DÉPLOIEMENT MOYEN (≤ 10 capteurs)	DÉPLOIEMENT À GRANDE ÉCHELLE (10 à 100 capteurs)
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 ≥ 2,4 GHz
Mémoire	8 à 16 Go	16 à 32 Go	64 à 256 Go
Disque dur	64 Go à 500 Go dans les ordinateurs industriels (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 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.

	AUTONOME	VIRTUEL
Processeur	Processeur 2 à 4 cœurs	4 vCPU
Mémoire	4 Go RAM	4 Go RAM
Interface réseau	≥ 1	≥ 1

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

La plateforme Forescout maximise la valeur d'eyeInspect grâce à une suite de fonctionnalités 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.

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

FORESCOUT

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