

Surveillance active et sélective pour une visibilité globale des technologies d'exploitation

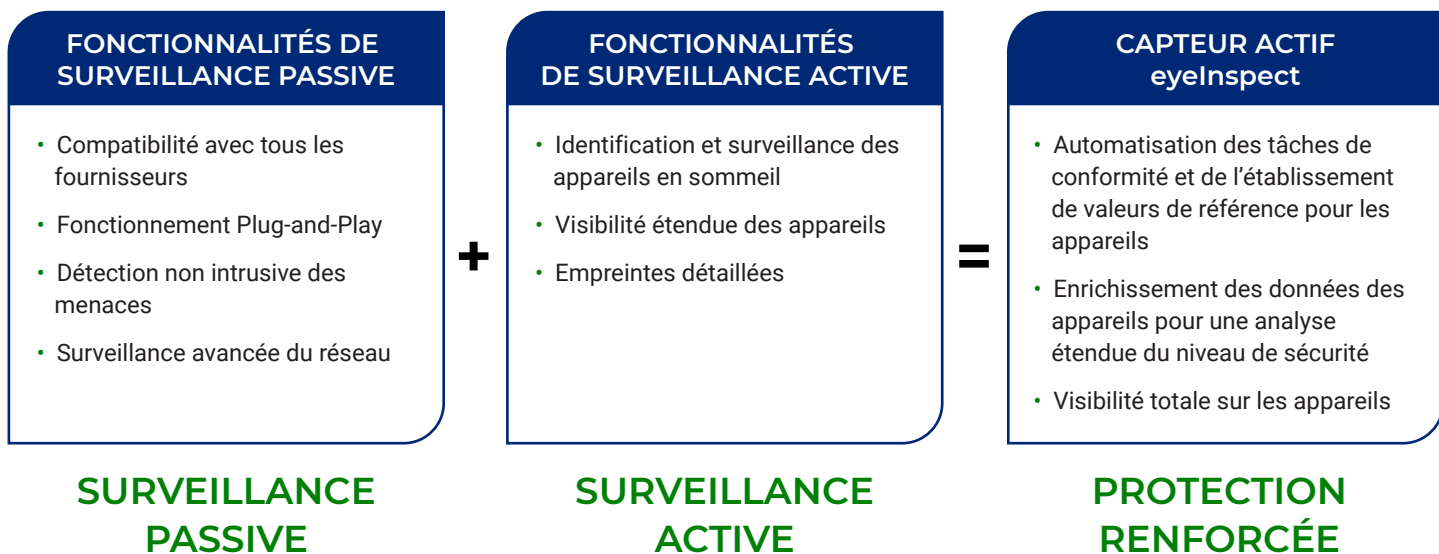
Réduisez les problèmes de conformité et les coûts grâce à l'automatisation des tâches de conformité à grande échelle

Les réseaux des acteurs de la cybersécurité des technologies d'exploitation (OT) et des propriétaires d'actifs ICS peuvent présenter des zones d'ombre qu'une solution de cybersécurité ICS entièrement passive n'est pas à même de protéger. Des informations lacunaires sur les actifs et une visibilité partielle des appareils peuvent exposer les réseaux à des risques opérationnels et de cybersécurité élevés.

Le capteur actif eyeInspect fournit aux propriétaires d'actifs OT les données contextuelles nécessaires pour simplifier l'analyse des menaces, tout en réduisant le nombre de tableaux de bord et en augmentant le nombre d'alertes exploitables pour une analyse des menaces et une conformité à grande échelle optimisées.

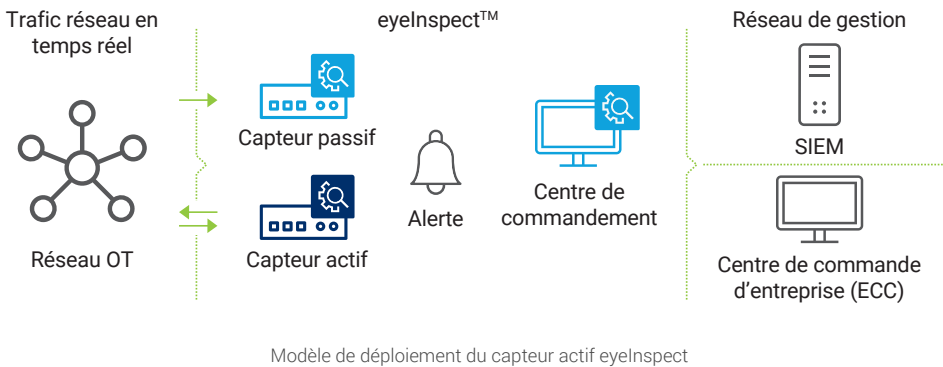
79 % des entreprises gérant un réseau SCADA/ICS ont signalé une compromission au cours des 24 derniers mois¹

FORRESTER



Capteur actif eyeInspect : visibilité totale

Le capteur actif eyeInspect (anciennement SilentDefense™) allie la détection passive des anomalies à des fonctionnalités de cybersécurité actives pour étendre la visibilité des réseaux ICS et les renseignements d'exploitation de façon non intrusive. Proposé sous forme de composant distinct en option, le capteur actif eyeInspect permet d'interroger des hôtes spécifiques de manière sélective en fonction d'une ou plusieurs des caractéristiques de l'inventaire des actifs. Cette couche de visibilité supplémentaire améliore en outre considérablement les tâches de reporting et de surveillance de la conformité grâce à la fonction d'établissement de valeurs de référence pour les actifs.



Capteur actif eyeInspect

- Établissement de valeurs de référence pour les actifs et les groupes d'actifs par rapport aux politiques de conformité pour les contrôles de conformité automatisés et à la demande
- Automatisation du reporting et des contrôles de conformité pour la classification NERC CIP et d'autres cadres de conformité
- Informations détaillées sur l'inventaire des actifs et la capture d'empreintes des appareils, notamment les correctifs installés, les applications installées ou les ports et services ouverts
- Connaissance situationnelle des OT et réseaux ICS améliorée
- Protection des équipements sensibles grâce à l'utilisation de politiques d'analyse propres aux OT par le capteur actif

Cas d'utilisation du capteur actif

Découverte complète du réseau et des appareils

Le capteur actif eyeInspect interroge des hôtes spécifiques sur le réseau ICS de façon sélective et sécurisée, afin d'améliorer la visibilité des actifs et de fournir des inventaires plus complets comprenant notamment l'état de l'hôte, la version du système d'exploitation, le fabricant, les logiciels et les applications, les numéros de série, le comportement des utilisateurs du réseau et les correctifs installés.

Évaluation complète des risques et des vulnérabilités

Un processus automatisé non intrusif de collecte d'informations sur les actifs permet aux parties prenantes de la cybersécurité d'évaluer les risques et les vulnérabilités potentielles de manière encore plus

détaillée. Le capteur actif eyeInspect enrichit les détails des alertes avec des données contextuelles pertinentes qui n'auraient peut-être pas été visibles avec une solution passive seule.

Automatisation des tâches de conformité et de l'établissement de valeurs de référence pour les actifs

Le capteur actif eyeInspect permet d'établir des valeurs de référence pour les actifs, permettant ainsi aux utilisateurs de comparer des actifs individuels et des groupes d'actifs à des politiques réglementaires et mesures de conformité spécifiques, telles que les normes 007 et 010 de la classification NERC CIP. Grâce au capteur actif eyeInspect, les utilisateurs peuvent exporter toutes les informations de manière sélective pour constituer facilement une documentation périodique de l'état du réseau, ce qui contribue à réduire les coûts d'exploitation et les risques de sanctions financières pour non-conformité aux normes telles que la classification NERC CIP et la directive NIS.

1. Forrester Research, Protecting Industrial Control Systems And Critical Infrastructure From Attack (Protéger les systèmes de contrôle industriels et les infrastructures critiques des cyberattaques), 2018

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 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

© 2020 ForeScout Technologies, Inc. Tous droits réservés. Forescout Technologies, Inc. est une société ayant son siège aux États-Unis dans l'État du Delaware. Les logos et marques commerciales de Forescout sont disponibles à l'adresse suivante : www.forescout.com/company/legal/intellectual-property-patents-trademarks. Les autres marques, produits ou noms de services mentionnés dans ce document peuvent être des marques commerciales de leurs propriétaires respectifs. Version 08_20