FORESCOUT
Active Defense for the Enterprise of Things™

Cybersécurité et gestion des risques pour les technologies d'exploitation

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

La convergence actuelle des réseaux de technologies de l'information (IT) et de technologies d'exploitation (OT) accroît la complexité et la vulnérabilité des réseaux de systèmes de contrôle industriel (ICS), qui étaient auparavant isolés. Cette évolution s'accompagne d'une croissance explosive des appareils IoT industriels (IIoT), qui a créé un important déficit de visibilité et rendu plus difficile l'application de la conformité. Les entreprises ont besoin d'un outil de sécurité capable d'assurer une visibilité approfondie des réseaux OT et ICS et de permettre une gestion efficace et en temps réel des risques opérationnels et de cybersécurité.

> **« D'ici 2021, 80 % des projets IIoT seront soumis à des exigences de sécurité propres aux environnements OT[1]. »**
>
> **GARTNER**

Principaux défis dans les environnements OT

À mesure que les entreprises modernisent leurs infrastructures, intègrent de nouvelles technologies et réunissent les réseaux OT et IT, les systèmes OT et ICS hautement vulnérables doivent être entretenus et protégés au sein d'environnements réseau modernes hétérogènes. De ce fait, des défis voient le jour pour les équipes responsables de la sécurité et des opérations, notamment :

- Identifier, classifier et contrôler tous les appareils IT connectés, les systèmes IIoT et les actifs OT, qu'ils soient gérés ou non.
- Analyser les alertes, définir la priorité des menaces et réagir aux incidents en temps utile, avec une perturbation minimale des activités.
- Garantir que tous les appareils connectés (y compris les anciens systèmes OT) sont conformes aux exigences réglementaires et aux politiques.
- Tenir un inventaire précis et à jour des actifs.

Forescout eyeInspect : cyberrésilience et gestion des risques pour l'infrastructure IIoT et OT

Forescout eyeInspect (anciennement SilentDefense™) protège les réseaux OT et ICS contre un large éventail de menaces. Il fournit des capacités de découverte passive et active qui créent un inventaire des actifs automatique, en temps réel, et permet des actions correctives ciblées en fonction de l'impact potentiel sur les activités.

- Permet une surveillance et une segmentation passives et en temps réel du réseau.
- Optimise l'analyse des menaces et les mesures correctives grâce à l'agrégation avancée des alertes.
- Fournit des intégrations approfondies avec ServiceNow® et des interfaces natives avec les solutions SIEM, les pare-feux, la gestion des actifs IT, les sandboxes et les serveurs d'authentification.
- Améliore l'efficacité du SOC et des analystes, de manière à automatiser l'analyse des risques grâce au cadre d'évaluation des risques des actifs.
- Étend les capacités exceptionnelles de visibilité, de classification et de profilage des appareils de la plateforme Forescout, du cloud à la périphérie.

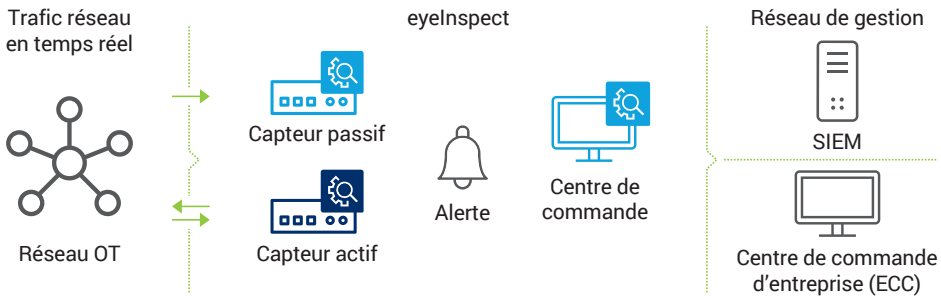

Figure 1. Modèle de déploiement de base d'eyeInspect

Cas d'utilisation d'eyeInspect

Visibilité et surveillance des actifs

eyeInspect assure une visibilité continue des actifs sur les réseaux et les sites OT. Il élabore automatiquement une carte détaillée du réseau comportant de multiples données sur les actifs et un regroupement automatique par réseau/rôle. Cette carte est disponible en différents formats vous permettant d'afficher le modèle Purdue ou la relation de communication, par exemple. eyeInspect utilise une large gamme de capacités de découverte, notamment :

VISIBILITÉ GLOBALE ET DÉTECTION DES MENACES

eyeInspect étend les capacités de pointe de la plateforme Forescout en termes de visibilité, de classification et de profilage des appareils bien plus loin dans les environnements OT et ICS. Il permet d'identifier et de corriger efficacement un large éventail de menaces, tant cybernétiques qu'opérationnelles, notamment :

- Cyberattaques (DDoS, attaques Man-in-the-Middle et par analyse, etc.)
- Connexions réseau et communications non autorisées
- Modifications suspectes des comportements des utilisateurs/politiques
- Dysfonctionnement ou mauvaise configuration d'un appareil
- Nouveaux actifs et actifs non réactifs
- Messages corrompus
- Téléchargements de micrologiciels non autorisés Protocoles non sécurisés
- Identifiants par défaut et authentifications non sécurisées
- Modifications de logique
- Visibilité des appareils compatibles IP et série

- Inspection approfondie des paquets brevetée pour plus de 150 protocoles IT et OT
- Surveillance continue et configurable des politiques et des comportements
- Évaluation automatique des vulnérabilités des appareils, de l'exposition aux menaces et des problèmes réseau ou opérationnels
- Composant actif facultatif et non intrusif d'interrogation sélective d'hôtes spécifiques

Gestion de la configuration des actifs

eyeInspect recueille automatiquement un grand nombre d'informations sur les actifs OT, en consignant toutes les modifications de configuration à des fins d'analyse de la sécurité et d'investigation opérationnelle. Exemples d'informations recueillies :

- Adresse réseau
- Nom d'hôte
- Marque et modèle de l'actif
- Numéro de série
- Version du système d'exploitation
- Version du micrologiciel
- Version du matériel
- Informations sur les modules de l'appareil

Conformité automatisée

Le capteur eyeInspect permet aux propriétaires d'actifs d'établir facilement des valeurs de référence pour les actifs et groupes d'actifs selon des politiques de conformité spécifiques, et ainsi de détecter automatiquement les divergences par rapport à ces valeurs. Ces valeurs permettent en outre de définir des politiques de base personnalisées en fonction des besoins organisationnels ou selon des directives de conformité telles que NERC CIP, ISA99/IEC 62443, NIS et NIST CSF, ainsi que FDA et FIPS. Les propriétaires d'actifs peuvent générer des preuves/rapports admissibles de la ligne de référence pour ces cadres de conformité.

Contrôle des accès au réseau et segmentation

eyeInspect s'appuie sur les fonctionnalités d'affectation de listes de contrôle d'accès (ACL) et de VLAN de la plateforme Forescout pour assurer la segmentation fondée sur les politiques et le contrôle des accès des réseaux opérationnels. Elle permet ainsi une gestion unifiée et en temps réel des actifs dans les catégories IT, IoT et OT. Avec eyeInspect, les propriétaires d'actifs disposent d'une cartographie et d'une visualisation contextuelles (c.-à-d. connaissance des protocoles/DPI) des relations (modèles de communication) entre les actifs dans les environnements IT, OT et de soins de santé. Ils peuvent les intégrer à d'autres systèmes/produits existants de télémétrie des flux de trafic (Medigate, NetFlow, SPAN, etc.).

AVANTAGES ÉCONOMIQUES DE LA CYBERRÉSILIENCE

Forescout eyeInspect peut avoir un impact positif sur les résultats d'une entreprise. Il améliore en effet la sécurité et la résilience de ses systèmes opérationnels tout en renforçant considérablement l'efficacité administrative, la gestion des risques et la conformité.

Par exemple, Forescout a récemment étudié la contribution de la surveillance du réseau OT aux performances financières d'une importante société américaine de production alimentaire comptant 17 ETP, l'accent étant mis sur la cybersécurité ICS et la conformité[2]. Voici les conclusions de l'étude :

- Économies annuelles de 820 336 dollars en termes de réduction des coûts de main-d'œuvre, d'efficacité de gestion et d'amélioration des capacités de recherche des menaces, associées à la visibilité des actifs et du réseau.
- Économies annuelles de 346 456 dollars résultant de mises à jour exploitables de la gestion des menaces, d'interventions sur incident plus rapides et de la réduction des risques d'interruption de service, le tout associé à une amélioration des capacités de détection et de réponse aux cybermenaces.
- Économies annuelles de 158 120 dollars en coûts de conformité grâce à l'intégration de solutions de sécurité ICS et de gestion des actifs.

Détection des menaces et intervention sur incident

Automatisez la détection, l'isolement et la neutralisation des menaces grâce aux outils d'enquête sur les alertes et d'intervention d'eyeInspect. Les tableaux de bord et les widgets améliorent la collaboration entre utilisateurs. La richesse des détails des alertes permet d'analyser les causes premières et d'intervenir de manière rapide et efficace. Le Centre de commande d'entreprise (ECC) permet aux utilisateurs de zoomer sur toutes les alertes émanant de leurs réseaux multisites ou géodistribués. Ils peuvent ainsi analyser un incident en détail, y compris les appareils impliqués et le contexte de l'alerte.

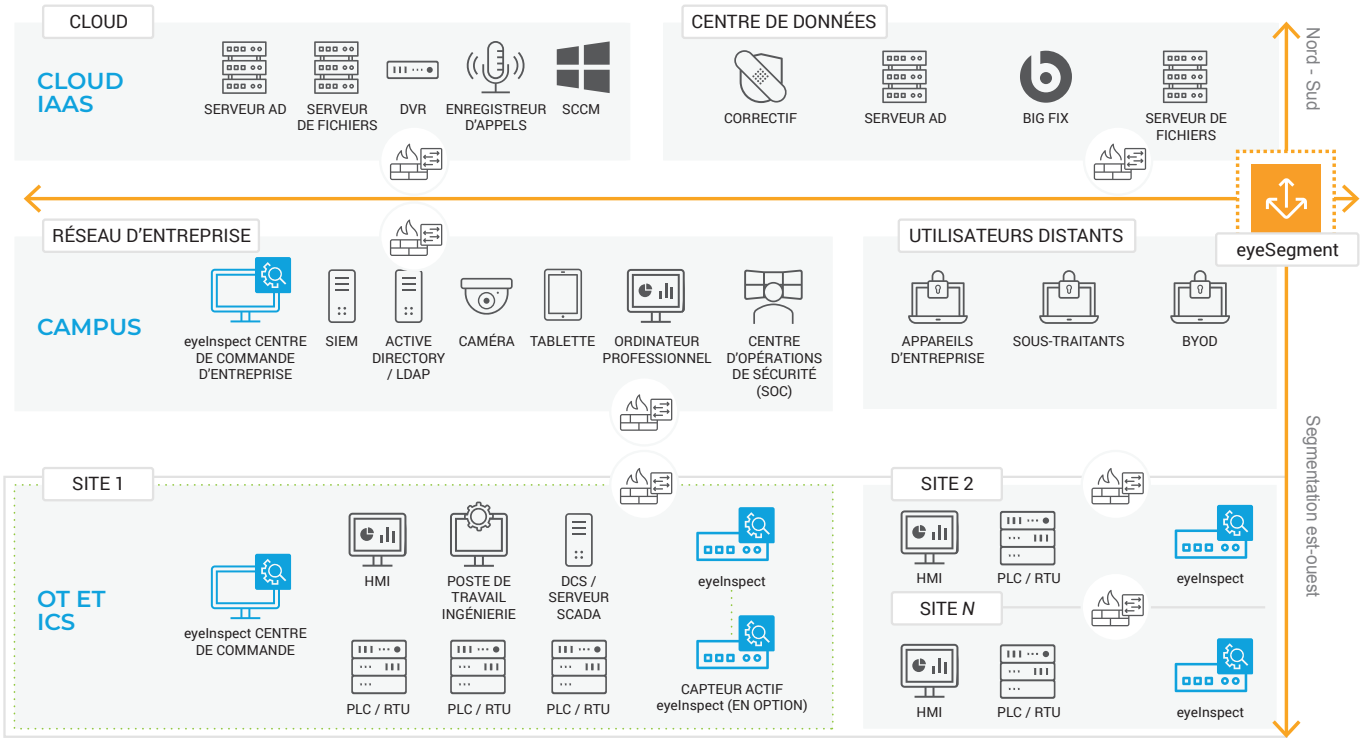

Figure 2. eyeInspect fait partie de la plateforme de sécurité IT-OT unifiée de Forescout. Celle-ci fournit une connaissance situationnelle et un contrôle automatisé des risques opérationnels et de cybersécurité dans l'entreprise étendue.

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

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

1. 7 Questions SRM Leaders Aren't Asking OT Security Providers During Technology Selection (Sept questions que les responsables GRS ne posent pas aux fournisseurs de solutions de sécurité OT lors du processus de sélection d'une technologie), Saniye Alaybe yi, Gartner, 2018, https://www.forescout.com/gartner-report-7-questions-for-OT- security-providers

2. Projections basées sur des données clients normalisées. Les économies réelles peuvent varier en fonction de divers facteurs.

forescout.com/platform/eyeInspect info-france@forescout.com Tél. (international) +1-408-213-3191

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