FORESCOUT

Nouveautés de Forescout 8.1

Alors que la transformation numérique poursuit sa progression, les entreprises connectent un nombre croissant d'appareils intelligents à leurs réseaux en vue d'automatiser les opérations métier et d'accroître leur efficacité. Qu'ils relèvent de l'IoT, de l'IIoT ou de l'OT, leur multiplication et leur diversification sont sans précédent pour les réseaux d'entreprise.

> "D'ici 2021, 70 % de la sécurité OT sera gérée directement par le DSI, le RSSI ou le directeur de la sécurité, contre 35 % aujourd'hui."[1] – *Gartner, mai 2018*

Face à cette transformation, les entreprises doivent accroître la connectivité et le partage d'informations entre les réseaux jusque-là disparates. Elles accélèrent ainsi la convergence des technologies de l'information (IT) et des technologies d'exploitation (OT), et créent de nouveaux flux de données entre les appareils IT connectés au réseau de campus, les applications cloud et les systèmes OT. Bien que cette transformation s'accompagne de nombreux avantages, elle augmente également les risques métier. En effet, les cybercriminels peuvent se déplacer latéralement sur les réseaux désormais interconnectés afin d'accéder aux informations sensibles ou de perturber les activités de l'entreprise.

La convergence de l'IT et de l'OT impose de nouvelles exigences aux DSI et aux RSSI, qui sont désormais chargés de protéger tout l'écosystème de l'entreprise. Les responsabilités des équipes informatiques vont bien au-delà de la gestion des appareils des utilisateurs, des applications et des données. Elles doivent désormais veiller à l'exécution d'opérations métier sécurisées et rationalisées. Pour relever ce défi, elles ont besoin d'une visibilité et d'un contrôle complets sur les appareils.

Forescout 8.1: visibilité et contrôle unifiés sur les appareils pour la sécurité de l'IT et de l'OT

Forescout 8.1 est la première plateforme de visibilité et de contrôle unifiés sur les appareils permettant la convergence des réseaux IT/OT. Elle permet aux entreprises d'acquérir une connaissance situationnelle sur l'ensemble des appareils d'un environnement interconnecté, ainsi que d'orchestrer des actions en vue de réduire les cyberrisques et les risques opérationnels. Voici certaines des nouvelles fonctionnalités :

- La visibilité sur les environnements de commutation industriels Cisco ACI, Microsoft Azure et Belden étend la protection au centre de données, au cloud et aux réseaux OT, ce qui fournit aux entreprises les données contextuelles dont elles ont besoin sur les domaines IT et OT.
- Les importantes améliorations apportées à l'autoclassification pour les appareils IoT et OT, l'évaluation des vulnérabilités pour les systèmes de contrôle industriels et la détection des appareils non approuvés renforcent la cyberrésilience des réseaux IT et OT.
- L'orchestration pour la segmentation avec les pare-feu Fortinet et Cisco DNA Center, ainsi que l'intervention sur incident avec ServiceNow, permettent d'aller plus loin dans l'automatisation des contrôles et d'accroître l'efficacité des opérations de sécurité.
- Deux millions d'appareils peuvent être gérés dans un seul déploiement comprenant des environnements physiques, virtuels, cloud ou hybrides.

Évolutivité à l'échelle de l'entreprise

Gérez deux millions d'appareils dans un seul déploiement comprenant des environnements physiques, virtuels, cloud ou hybrides.

Découverte des appareils

Bénéficiez d'une visibilité inédite sur les environnements de commutation industriels Microsoft Azure, Cisco ACI et Belden, ainsi que d'une visibilité sur les couches inférieures de la pile réseau OT.

Autoclassification

La nouvelle inspection approfondie des paquets de plus de 100 protocoles IT et OT permet l'autoclassification des appareils IoT et d'automatisation médicaux, industriels et immotiques.

Évaluation des risques

La cyberrésilience est renforcée par la nouvelle évaluation des vulnérabilités OT et des systèmes de contrôle industriels, ainsi que par la détection des appareils non approuvés permettant d'identifier et de bloquer les usurpateurs.

Automatisation des contrôles

Vous bénéficiez d'une nouvelle fonctionnalité d'orchestration pour la segmentation réseau avec les pare-feu Fortinet et Cisco DNA Center, ainsi que de l'intervention sur incident avec ServiceNow ITSM et Security Operations.

Découverte étendue des appareils

La sécurité commence par une bonne visibilité sur les appareils connectés au réseau. Il est donc essentiel d'identifier tous les appareils dès qu'ils se connectent au réseau. En 2019, 900 millions d'appareils physiques et virtuels supplémentaires devraient se connecter aux réseaux d'entreprise. La majeure partie de cette croissance est attribuable aux appareils IoT et OT, ainsi qu'aux instances de cloud public et privé.

> "D'ici 2023, les DSI devront gérer plus de trois fois plus de points d'extrémité qu'en 2018."[2]
> *– Gartner, septembre 2018*

- Forescout 8.1 continue d'étendre la visibilité dans ces domaines afin d'offrir une vue unifiée sur l'ensemble de vos appareils au sein du campus, du centre de données, dans le cloud et sur les réseaux OT.
- La visibilité multicloud inclut désormais Microsoft Azure, en plus des fonctionnalités existantes pour AWS et VMware.
- L'intégration avec Cisco ACI offre une visibilité sur les environnements SDN pour les centres de données.
- L'intégration avec les produits de commutation industriels Belden offre une visibilité étendue sur les réseaux OT.
- La surveillance passive des couches inférieures de la pile réseau OT offre une visibilité sur les appareils de surveillance, de contrôle des processus et d'instrumentation.

Autoclassification de pointe

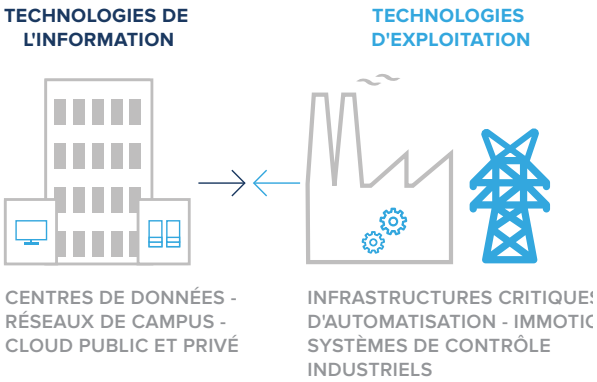
La diversité des appareils IoT et OT complique leur identification et leur catalogage précis par les entreprises. Sans classification granulaire, il est difficile de créer et d'appliquer des politiques ciblées pour protéger ces appareils. Forescout 8.1 inclut d'importantes améliorations vous permettant de classifier automatiquement davantage d'appareils et d'exploiter ces données contextuelles pour appliquer des politiques grâce aux avantages suivants :

- Couverture étendue permettant d'identifier plus de 500 versions de système d'exploitation et plus de 5 000 fabricants et modèles d'appareils.
- Classification des équipements médicaux de plus de 350 fournisseurs de technologies médicales, dont les vingt premiers du classement mondial.
- Nouvelle inspection approfondie des paquets de plus de 100 protocoles IT et OT permettant de classifier automatiquement des milliers d'appareils d'automatisation industriels utilisés dans divers secteurs (fabrication, énergie, pétrole et gaz, services publics, exploitation minière et infrastructures critiques).
- Efficacité, vitesse et couverture accrues de la classification grâce à *Forescout Device Cloud*, qui réunit plus de 8 millions d'appareils en environnements IT, IoT et OT.

Évaluation des risques interdomaines

Évaluation des vulnérabilités OT

Compte tenu de la connectivité croissante entre les réseaux IT et OT, il est important de comprendre le profil de risque des deux catégories d'appareils. D'un côté comme de l'autre, les appareils vulnérables peuvent être compromis, ce qui permet aux menaces d'infiltrer des domaines et d'engendrer des interruptions d'activité et des pertes financières.



- Forescout 8.1 intègre l'évaluation des vulnérabilités OT et des systèmes de contrôle industriels aux fonctionnalités d'évaluation des vulnérabilités existantes de Windows, ce qui vous procure des informations sur les appareils à haut risque qui se trouvent sur votre réseau.
- Les mises à jour fréquentes proposées par Forescout fournissent des informations récentes sur les dernières vulnérabilités et failles de sécurité courantes des systèmes de contrôle industriels, afin que vous puissiez identifier les appareils vulnérables et orchestrer des actions de correction.
- Pour les appareils industriels et opérationnels vulnérables auxquels il n'est possible d'appliquer des correctifs ou des mesures de correction qu'au cours des périodes de maintenance planifiées, Forescout peut appliquer des contrôles de réduction des risques, par exemple en segmentant ces appareils en zones réseau « sécurisées » jusqu'à ce qu'ils puissent être corrigés.

Détection des appareils non approuvés

L'usurpation des appareils et des adresses MAC constitue un autre défi qui s'explique par l'explosion de l'IoT et de l'OT. Les cybercriminels qui cherchent à accéder aux réseaux peuvent cibler un plus grand nombre d'adresses MAC, car les appareils IoT et OT font souvent partie de longues listes blanches régissant l'accès aux réseaux. La plupart du temps, ces appareils possèdent des écrans d'affichage non sécurisés qui sont susceptibles de révéler leur adresse MAC à n'importe qui. Les usurpateurs peuvent facilement se faire passer pour des appareils légitimes afin d'accéder au réseau pour perturber les activités de l'entreprise ou dérober des informations sensibles.

Forescout 8.1 intègre une nouvelle fonctionnalité de détection des appareils non approuvés (en attente de brevet) permettant d'identifier et de bloquer les cybercriminels qui utilisent des techniques d'usurpation des adresses MAC.

- La surveillance continue du réseau permet de détecter plusieurs scénarios d'usurpation sur les réseaux filaires et sans fil, notamment les tentatives de connexions simultanées, de remplacement au même emplacement et de remplacement à un autre emplacement.
- Forescout identifie les appareils des victimes et ceux des usurpateurs. Il s'appuie ensuite sur des politiques pour bloquer les tentatives d'usurpation afin d'empêcher tout accès malveillant.
- Forescout vous permet de démontrer aux auditeurs la résilience de votre entreprise à l'usurpation des adresses MAC, ainsi que d'améliorer votre conformité lors des audits.

Orchestration et automatisation des contrôles

Les équipes de sécurité informatique sont submergées par un nombre croissant de problèmes de sécurité et de conformité, signalés par divers outils de sécurité qui ne disposent pas de données contextuelles suffisantes sur les appareils pour que des fonctions de priorisation ou d'automatisation puissent appliquer des contrôles. Par conséquent, ces experts en sécurité perdent un temps précieux à résoudre manuellement des problèmes mineurs, au lieu de se consacrer à la réduction proactive des risques ou à la neutralisation rapide des menaces. Forescout 8.1 vous offre des données contextuelles sur les appareils et vous permet d'orchestrer des actions ainsi que d'automatiser des contrôles.

> "D'ici 2021, 70 % des entreprises seront dotées de fonctionnalités d'automatisation, d'orchestration et d'intervention sur incident, par le biais de leur solution SIEM ou d'une plateforme dédiée, contre moins de 5 % en 2018."[3]
> *– Gartner, December 2018*

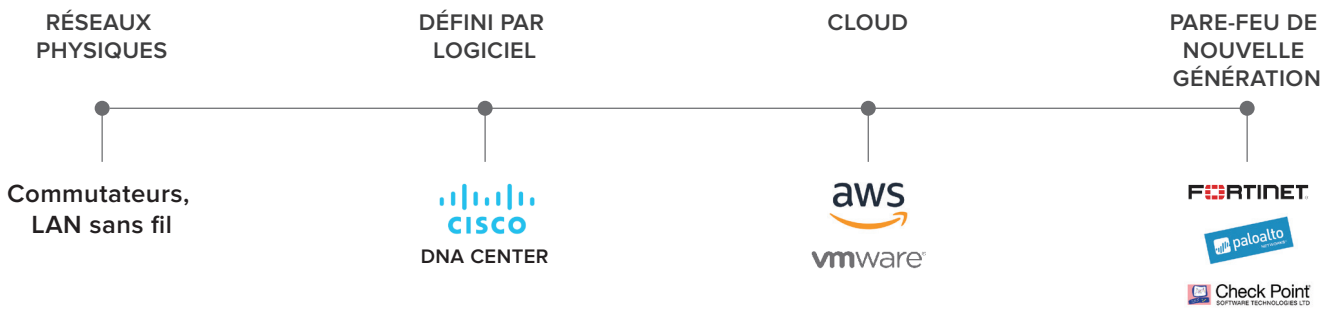
Segmentation réseau

La segmentation joue un rôle majeur dans la définition des architectures de sécurité de nouvelle génération pour l'IoT et l'OT. Contrairement aux appareils traditionnels, il n'est pas possible d'appliquer régulièrement des correctifs aux appareils IoT et OT, ni de les protéger par le biais d'agents. La segmentation de ces appareils en zones de sécurité logiques est donc une stratégie essentielle de réduction des risques.

Forescout 8.1 vous permet d'orchestrer la segmentation pour plusieurs technologies de contrôle, notamment plusieurs nouvelles intégrations :

- Automatisation de contrôles de segmentation avec les pare-feu Fortinet, ce qui complète l'orchestration existante avec Palo Alto Networks et Check Point, pour une prise en charge hétérogène des pare-feu de nouvelle génération.
- Orchestration de contrôles de segmentation avec Cisco DNA Center, ce qui complète les intégrations existantes avec des technologies cloud et définies par logiciel telles que VMware NSX et AWS.

Segmentation réseau interdomaines



Automatisation de l'intervention sur incident

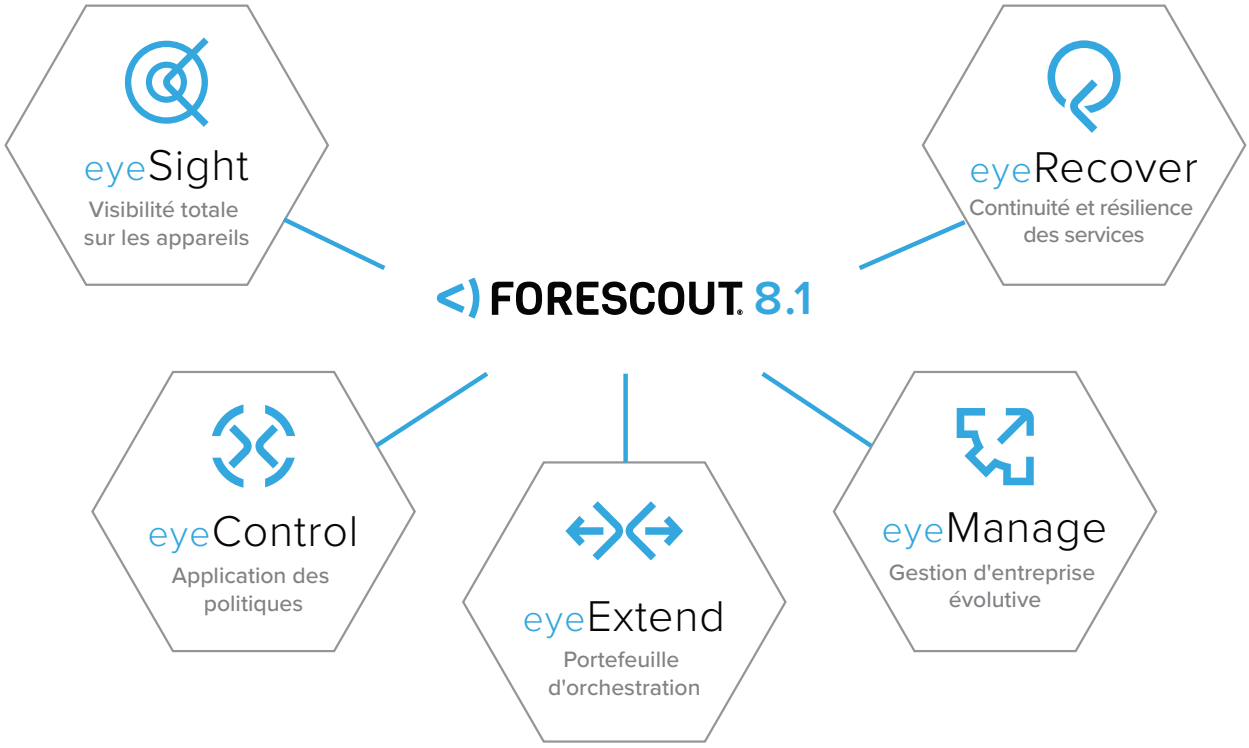
Les équipes informatiques et de sécurité se tournent de plus en plus vers l'automatisation de l'intervention sur incident pour résoudre les problèmes mineurs, afin que leurs ressources qualifiées puissent se consacrer à l'atténuation des risques et à d'autres enjeux métier à fort impact. Forescout 8.1 s'intègre désormais avec les produits ServiceNow ITSM et Security Operations afin d'automatiser et d'accélérer l'intervention sur incident.

- La nouvelle fonctionnalité d'orchestration avec ServiceNow ITSM automatise la création d'incidents de service et les actions basées sur des politiques pour garantir la conformité des configurations.
- La nouvelle fonctionnalité d'orchestration avec ServiceNow Security Operations automatise la création d'incidents de sécurité et la neutralisation des menaces pour les appareils compromis ou à haut risque.
- L'orchestration améliorée avec ServiceNow CMDB exécute la mise à jour des éléments de configuration une fois la correction des incidents terminée, afin de faciliter les flux de travail de service en boucle fermée et de gestion de la sécurité.

Une plateforme évolutive et flexible

Forescout 8.1 offre une évolutivité et une flexibilité de déploiement optimales afin de satisfaire les exigences rigoureuses des environnements d'entreprise complexes :

- Avec une seule installation, vous pouvez gérer jusqu'à deux millions d'appareils physiques ou virtuels au sein du campus, du centre de données, dans le cloud et sur les réseaux OT.
- Cette suite de produits modulaire vous offre la flexibilité nécessaire pour répondre à vos exigences d'entreprise en évolution constante. En commençant par Forescout eyeSight pour la visibilité sur les appareils, chaque produit supplémentaire apporte des fonctionnalités puissantes pour l'automatisation des contrôles, l'orchestration de la sécurité, la résilience opérationnelle et la sécurité OT.
- Profitez de plusieurs options d'achat : tous les produits logiciels Forescout sont désormais disponibles via une licence perpétuelle ou un abonnement trimestriel.



1 Gartner, *2018 Strategic Roadmap for Integrated IT Security*, mai 2018
2 Gartner, *Top Strategic IoT Trends and Technologies Through 2023*, septembre 2018
3 Gartner, *Emerging Technology Analysis: SOAR Solutions*, 7 décembre 2018, Eric Ahlm

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Numéro gratuit (États-Unis)
1-866-377-8771
Tél. (International) +1-408-213-3191
Support +1-708-237-6591

Pour en savoir plus, consultez le site Forescout.fr