FORESCOUT

Nouveautés de Forescout 8.2

« D'ici 2023, on comptera plus de 35,2 milliards d'appareils IoT connectés dans le monde. »

– Worldwide Internet of Things Infrastructure Forecast, 2019-2023, IDC

Les attaques observées ces dix dernières années nous ont enseigné qu'un seul point faible dans un réseau suffit à exposer une entreprise à des compromissions. Avec la transformation numérique, de plus en plus d'appareils IoT et non gérés se connectent aux réseaux d'entreprise. Il est donc urgent d'élaborer des solutions innovantes qui protègent ces appareils et les réseaux.

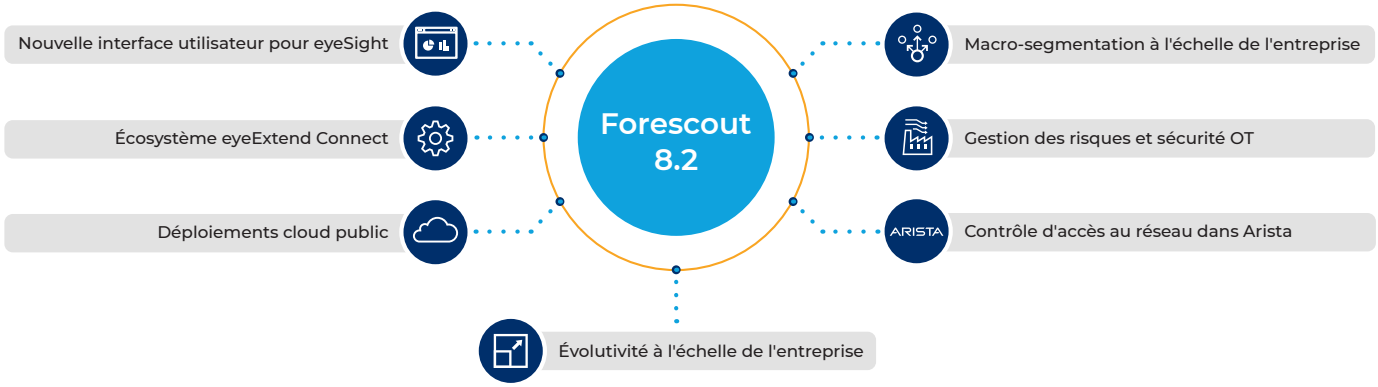
Pour pouvoir réagir rapidement et ainsi limiter les risques, une vue complète des appareils connectés aux divers domaines réseau est indispensable. Il convient donc d'identifier tous les appareils vulnérables et d'ancienne génération, les terminaux non conformes et mal configurés et les technologies IoT et d'exploitation. Les risques auxquels sont exposés les réseaux interconnectés et les emplacements doivent par ailleurs être évalués en permanence. Ce n'est qu'au prix d'une telle visibilité que vous pourrez agir, rapidement.

Forescout 8.2 : identification et intervention plus rapides

Forescout 8.2 accélère l'identification des appareils connectés, des écarts de conformité et des risques sur votre réseau. La solution vous permet d'agir rapidement et en toute confiance pour limiter les failles de sécurité et raccourcir le délai moyen d'intervention à l'échelle du réseau d'entreprise étendu.

Nouvelles fonctionnalités :

- Nouvelle interface utilisateur personnalisable de Forescout eyeSight, avec mise à disposition de données contextuelles exploitables sur les appareils afin de repérer, prioriser et limiter de manière proactive les risques
- Nouvel écosystème applicatif basé sur la communauté Forescout eyeExtend Connect afin de permettre à nos clients et partenaires de concevoir, utiliser et partager plus facilement des applications en vue de leur intégration à la plateforme Forescout
- Flexibilité et accélération des nouveaux déploiements pour les entreprises « cloud-first » qui souhaitent déployer des boîtiers Forescout dans leurs environnements de cloud public AWS et Microsoft Azure
- Segmentation à l'échelle de l'entreprise avec Forescout eyeSegment pour permettre aux entreprises de concevoir et d'implémenter en toute confiance des politiques au sein d'une multitude de domaines réseau et de points de déploiement
- Intégration à Forescout SilentDefense™, et capteurs IT/OT intégrés sur le même boîtier pour une visibilité unifiée sur les domaines IT et OT, y compris les réseaux clonés présentant des plages d'adresses IP qui se chevauchent
- Contrôle d'accès au réseau grâce à l'intégration directe à l'infrastructure Arista sans utiliser d'agents ni la norme 802.1X pour les appareils IT et IoT



Nouvelle interface utilisateur

Toutes les parties intéressées bénéficient d'un contexte centré sur la personne et d'informations exploitables grâce à la nouvelle interface utilisateur basée sur le Web. Les tableaux de bord présentent un aperçu des appareils connectés, informent les équipes de sécurité des endroits les plus exposés et mettent en lumière les progrès accomplis vers la réalisation des objectifs de conformité. L'inventaire en temps réel des appareils et les informations détaillées qu'il procure permettent aux opérateurs d'identifier rapidement les appareils afin d'anticiper les menaces à l'échelle de l'entreprise. Des options de personnalisation et de partage simples facilitent la communication des risques à l'ensemble des responsables informatiques afin de raccourcir les délais de réponse.

Obtenez des renseignements plus rapidement. Les tableaux de bord préconfigurés sur la visibilité et la conformité des appareils vous offrent diverses possibilités :

- Identifier la fonction, le système d'exploitation, le fournisseur et le modèle de tous vos appareils connectés
- Définir un seuil de conformité et surveiller le respect de toutes les politiques en vigueur
- Repérer les appareils à haut risque, par exemple :
  - appareils IoT utilisant des identifiants faibles ou des ports ouverts, ou présentant d'autres problèmes de configuration
  - appareils Windows sur lesquels les mises à jour de sécurité n'ont pas été installées ou présentant des vulnérabilités
  - appareils utilisant des agents de sécurité défectueux ou des applications non autorisées
  - appareils OT présentant des vulnérabilités et failles de sécurité courantes critiques
- Identifier les violations de politiques, notamment les défaillances les plus fréquentes, ainsi que les appareils en infraction avec plusieurs politiques (exécutant des applications P2P sans pare-feu ni antivirus, par exemple)

Corrigez les écarts de manière proactive. Utilisez la nouvelle vue des ressources dans la console Web pour effectuer rapidement les tâches suivantes :

- Lancer une recherche dans l'inventaire des appareils à l'échelle du campus, centre de données, cloud et l'environnement OT
- Filtrer par politique, segment de réseau et propriété de l'appareil
- Repérer avec précision l'emplacement des appareils afin de raccourcir le délai moyen d'intervention

Écosystème d'applications eyeExtend Connect

Les clients peuvent intégrer leurs autres technologies informatiques et de cybersécurité à la plateforme Forescout afin de partager des données contextuelles sur les appareils, orchestrer les flux de travail et automatiser les interventions. La gamme actuelle de modules eyeExtend de Forescout propose des intégrations prêtes à l'emploi avec plus de 25 solutions phares et vous permet de rentabiliser davantage vos investissements existants. Outre ces offres conçues et soutenues par Forescout, Forescout 8.2 offre un nouvel écosystème d'applications basé sur la communauté pour assurer l'intégration à d'autres technologies.

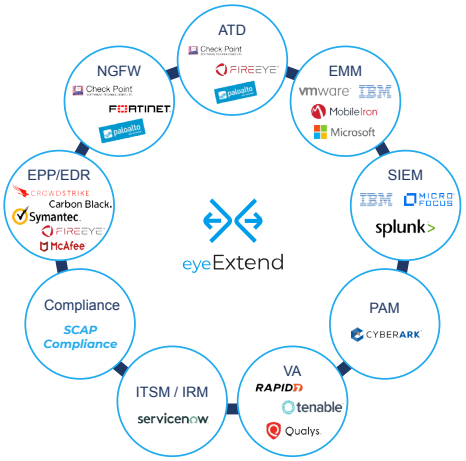
eyeExtend Connect tire parti de la puissance de la collaboration pour permettre aux clients et partenaires de concevoir, utiliser et partager rapidement des applications en vue de leur connexion à la plateforme Forescout. Vous pouvez ainsi partager facilement des données contextuelles sur les appareils avec d'autres outils, automatiser les flux de travail et prendre des mesures pour accélérer la réponse à l'échelle des systèmes et ainsi raccourcir le délai moyen d'intervention.

Facile à concevoir. Créez vos propres applications en toute simplicité grâce à la flexibilité des scripts universels Python et à la norme d'échange de données JSON, et gagnez en rentabilité.

Facile à utiliser. Faites votre choix parmi les diverses applications créées par la communauté, faciles à déployer et à personnaliser, et utilisables dans vos environnements réseau.

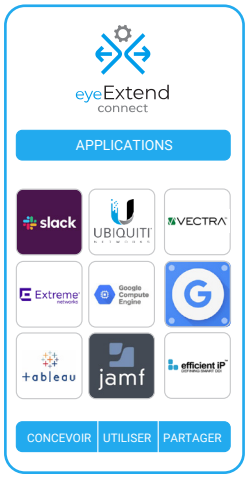
Facile à partager. Apportez votre contribution et inspirez-vous des bonnes pratiques de la communauté, partagez des applications avec vos pairs et tirez parti de la collaboration pour maximiser la valeur de vos investissements informatiques.

Modules eyeExtend



Conçu par la communauté Forescout

Applications eyeExtend



NOUVEAUTÉ

Conçu par la communauté Forescout

Macro-segmentation à l'échelle de l'entreprise

Forescout 8.2 complète eyeSegment en le dotant des dernières innovations d'eyeSight et eyeControl afin d'assurer la segmentation à l'échelle de l'entreprise au sein d'une multitude de domaines réseau et points de déploiement. Grâce à cette expérience homogène, vous pourrez concevoir et implémenter en toute confiance la segmentation réseau et la sécurité Zero Trust à grande échelle.

- Cartographiez et visualisez les flux de trafic afin d'établir une taxonomie logique des utilisateurs, appareils, applications et services.
- Concevez, simulez et optimisez des politiques de segmentation logiques afin d'en comprendre l'impact avant leur application.
- Surveillez en temps réel l'intégrité de la segmentation et réagissez aux violations des politiques.
- Appliquez des contrôles de segmentation en toute confiance sur les domaines réseau et les divers points de déploiement.

Gestion des risques et de la sécurité dans les environnements OT

Tirez parti de l'intégration entre SilentDefense et Forescout 8.2 pour prendre en charge divers scénarios de gestion des risques et de la sécurité dans des environnements OT et convergents.

- Partagez la classification et les vulnérabilités des appareils OT entre SilentDefense et eyeSight et utilisez la nouvelle interface utilisateur d'eyeSight pour bénéficier d'une visibilité unifiée sur l'ensemble des réseaux IT et OT.
- Déployez des capteurs IT et OT intégrés sur le même boîtier afin d'identifier et classifier les appareils au sein des environnements convergents.

- Identifiez de façon unique les appareils et appliquez des politiques dans des environnements réseau clonés qui réutilisent des plages d'adresses IP dupliquées sur plusieurs sites, lignes de production ou usines.
- Utilisez les dernières fonctionnalités de SilentDefense pour les environnements OT, notamment la génération de rapports de conformité améliorés NERC CIP, l'inspection active sélective et non intrusive pour une meilleure visibilité et un cadre d'évaluation des risques des ressources qui agrège plusieurs facteurs de risque pour obtenir des scores basés sur l'impact.

Contrôle d'accès au réseau dans les environnements Arista

Forescout 8.2 propose une intégration directe à l'infrastructure Arista afin de garantir la mise en œuvre de contrôles d'accès au réseau dans Arista, ainsi que dans des environnements hétérogènes. Vous pouvez ainsi identifier et réglementer les appareils IT et IoT sans devoir recourir à des agents ou à la norme 802.1X.

- Identifiez et évaluez en temps réel tous les appareils IT et IoT lorsqu'ils se connectent au réseau.
- Provisionnez un accès réseau approprié basé sur des données eyeSight et contextuelles tierces, notamment le type d'appareil, le propriétaire, le rôle de l'utilisateur et le niveau de conformité et de sécurité de l'appareil.
- Limitez les risques en automatisant diverses interventions réseau en fonction de la situation (restriction, segmentation, mise en quarantaine ou blocage d'appareils, par exemple).

Déploiements cloud public

Les entreprises qui ont adopté une approche « cloud-first » de la technologie sont limitées à des déploiements physiques ou virtuels sur site en ce qui concerne la visibilité et le contrôle sur les appareils. Avec Forescout 8.2, vous pouvez déployer des boîtiers de capteurs Forescout et un système de gestion d'entreprise dans vos environnements cloud Amazon Web Services ou Microsoft Azure sans encombrement sur site. Vous pouvez en outre combiner des déploiements cloud public avec des boîtiers physiques et des boîtiers virtuels dans une infrastructure cloud privé VMware, Hyper-V ou KVM.

Physique | Virtuel | Cloud public | Hybride
Combinez tout ou partie des options ci-dessus

Évolutivité à l'échelle de l'entreprise

Forescout 8.2 offre une évolutivité inégalée afin de répondre aux exigences strictes des grandes entreprises et faire face à l'explosion des appareils connectés au sein du campus, centre de données, cloud et des environnements IoT et OT.

- Classifiez les appareils à l'aide de la plus grande base de connaissances cloud regroupant plus de 11 millions d'appareils d'entreprise pour une identification plus précise et rapide des ressources IoT, OT et IT connectées.
- Gérez deux millions d'appareils avec un seul déploiement, quel que soit le type d'implémentation (physique, virtuelle, cloud ou hybride).

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 (États-Unis)

Email info-france@forescout.com
Tél. (International) +1-408-213-3191
Support +1-708-237-6591

Pour en savoir plus, consultez le site Forescout.fr