Forescout eyeExtend Connect

Intégration aisée à la plateforme Forescout pour obtenir des données contextuelles sur les appareils et accélérer la réponse aux menaces à l'échelle de l'entreprise

Pour rentabiliser au mieux leurs investissements dans des technologies informatiques et de sécurité, les clients Forescout s'appuient sur des intégrations clé en main avec des solutions utilisant neuf technologies de sécurité courantes. Ces intégrations se sont traduites par une amélioration considérable de l'efficacité grâce à l'orchestration des flux de travail de sécurité. Outre ces offres préconfigurées, Forescout propose désormais à ses clients un moyen plus rapide et plus simple d'intégrer à la plateforme Forescout un nombre accru de technologies existantes. eyeExtend Connect, la nouvelle solution Forescout, permet à nos clients et partenaires de concevoir, utiliser et partager rapidement des applications eyeExtend qui relient la plateforme Forescout à d'autres technologies. Nos clients et partenaires peuvent ainsi enrichir leurs solutions de sécurité existantes avec des données contextuelles détaillées sur les appareils fournis par Forescout, de même qu'automatiser les flux de travail de sécurité et la mise en œuvre des politiques au sein de solutions hétérogènes et accélérer la prise de mesures à l'échelle de l'entreprise pour limiter les risques.

La solution

Forescout eyeExtend Connect simplifie le développement d'applications faciles à utiliser et à déployer. Grâce aux applications Forescout eyeExtend, vous pouvez désormais intégrer facilement la plateforme Forescout à vos technologies informatiques et de sécurité et orchestrer les flux de travail de sécurité au sein de technologies de cybersécurité hétérogènes.

Avec eyeExtend Connect, vos technologies de sécurité existantes peuvent tirer parti des données contextuelles détaillées de Forescout eyeSight (propriétés des appareils, niveau de sécurité, conformité des appareils avec les politiques internes, emplacement sur le réseau, contexte utilisateur, etc.). Ces données peuvent être automatiquement extraites par d'autres logiciels informatiques et de sécurité, lesquels peuvent aussi transmettre leurs propres données à la plateforme Forescout. eyeExtend Connect accélère également la réponse aux menaces grâce à l'automatisation d'actions basées sur des politiques à l'échelle du système pour limiter les risques, les incidents et les écarts de conformité.

eyeExtend Connect met à disposition les outils suivants pour l'orchestration des flux de travail et le partage de données contextuelles.

eyeExtend connect

Problèmes

- L'utilisation des fonctionnalités d'intégration préconfigurées de Forescout ou de ses partenaires technologiques empêche l'orchestration des flux de travail avec d'autres technologies de sécurité en interne.
- La longueur des cycles de développement des intégrations personnalisées allonge le délai de rentabilité des investissements en sécurité existants.
- Les outils de sécurité indépendants qui ne partagent pas leurs données contextuelles sur les appareils et les utilisateurs nécessitent de nombreuses tâches manuelles pour répondre à des incidents de sécurité, ce qui augmente le cyberrisque et la perte de productivité.

Avantages

- La capacité d'intégration à tous les types d'outils tiers permet de maximiser la rentabilité des investissements technologiques existants.
- L'intégration simple et rapide à la plateforme Forescout via les applications eyeExtend permet d'accélérer le retour sur investissement.
- Le renforcement de votre sécurité passe par une meilleure collaboration entre vos différents outils informatiques et de sécurité, la récupération plus rapide de données exploitables sur vos appareils et l'automatisation de la prévention des risques et des menaces.

Caractéristiques

- Création et déploiement aisés d'applications eyeExtend à des fins d'intégration à la plateforme ouverte Forescout
- Partage de vos applications avec la communauté afin d'apporter votre contribution et de recueillir des commentaires
- Développement d'applications portables à l'aide de scripts Python et du format JSON
- Intégration à un large éventail de services Web tiers
- Extension des fonctionnalités de visibilité et de contrôle de Forescout grâce à des données contextuelles et contrôles sur les appareils tiers
- Possibilités d'intégrations bidirectionnelles à des API REST ouvertes basées sur des normes
- Transmission/extraction d'informations en langage SQL (Structured Query Language)
- Génération de requêtes personnalisées pour extraire/transmettre des informations depuis et vers un serveur LDAP standard
- Envoi et réception d'informations via Syslog vers et depuis un serveur désigné

Applications eyeExtend

Concevez des applications s'appuyant sur les principales fonctionnalités de la plateforme Forescout pour obtenir et partager des données contextuelles sur les terminaux, exécuter des actions de contrôle du réseau et appliquer des politiques à l'échelle du système. eyeExtend Connect met à disposition un schéma JSON convivial pour la définition des paramètres, des marqueurs et des configurations contrôlées par l'utilisateur afin de rendre vos applications eyeExtend portables (migration de l'environnement de test à celui de production, de la région A vers la B, d'environnements IT à OT, etc.). De plus, les interactions avec les API tierces sont définies au moyen de scripts Python courants, qui offrent une grande souplesse grâce aux nombreux types d'intégrations qu'ils permettent de créer. Des cas d'utilisation et mesures essentiels, comme la prévention des menaces, l'intervention sur incident et la gestion de la conformité, peuvent être automatisés à l'aide de modèles de politiques intégrables aux applications.

Principales fonctionnalités des applications eyeExtend :

- Prêtes à l'emploi
- Découverte de nouveaux appareils et propriétés
- Actions de contrôle d'appareils tiers externes
- Modèles de politiques personnalisés
- Interactions avec des API utilisables dans des scripts
- Icônes tierces personnalisables

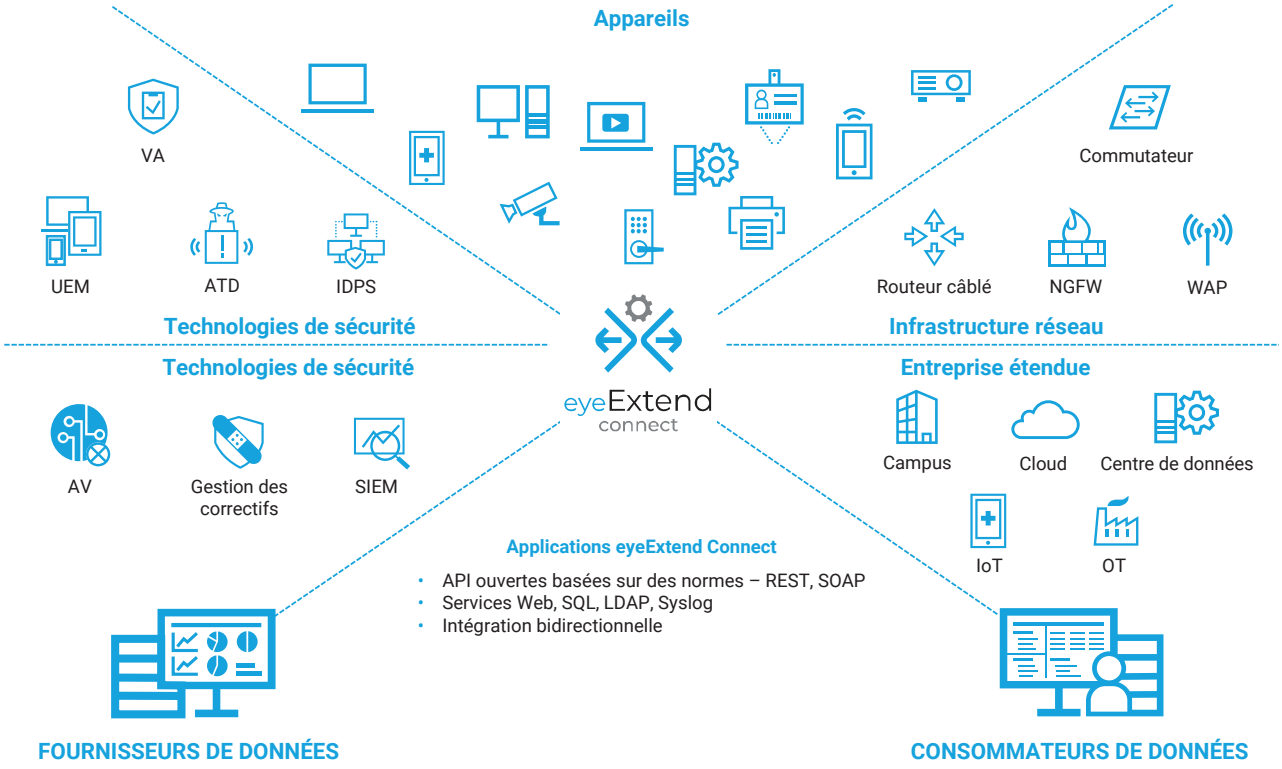
API Web et Data Exchange (DEX)
La plateforme Forescout met à disposition un ensemble d'API RESTful qui permettent à des applications externes de collecter les propriétés des appareils Forescout et des informations sur les politiques. Le plug-in DEX (Data Exchange) permet le partage en temps réel des données contextuelles sur les appareils grâce à une communication bidirectionnelle entre la plateforme Forescout et des API RESTful tierces.

SQL
Le plug-in DEX offre la possibilité de transmettre et extraire des informations vers et depuis une base de données SQL standard. Ce type d'intégration permet le partage d'informations entre des applications développées en interne et des solutions tierces capables de se connecter via une base de données externe ou interne. Vous pouvez rechercher des informations dans des bases de données externes et créer des propriétés système pour stocker les données recueillies par la plateforme Forescout. Ces propriétés peuvent être utilisées dans les politiques Forescout et visualisées dans un système d'exploitation en réseau (contrôle d'accès au réseau ou NAC) et des vues d'inventaire. Vous pouvez également mettre à jour des bases de données externes sur la base des informations collectées par la plateforme Forescout, de façon à ce qu'elles puissent être exploitées par des solutions tierces.

LDAP
Générez des requêtes personnalisées via le plug-in DEX afin de transmettre et d'extraire des informations vers et depuis un serveur LDAP standard. Vous pouvez, par exemple, rechercher des informations sur le serveur LDAP et créer des propriétés système Forescout pour stocker les données récupérées. Ces propriétés peuvent être utilisées dans les politiques de la plateforme Forescout et visualisées dans un système NAC et des vues d'inventaire.

Syslog
Le plug-in DEX peut être configuré pour envoyer et recevoir des informations vers et depuis un serveur désigné via Syslog. Ce type d'interface est utilisé pour diverses intégrations à des solutions qui agrègent les journaux et permettent leur analyse (produits de gestion des événements et des informations de sécurité (SIEM), par exemple), de même qu'à d'autres solutions capables d'envoyer et recevoir des alertes de cette manière. Le format des messages peut être personnalisé.

Figure 1. Orchestration des flux de travail entre différents appareils, environnements et technologies de sécurité



VA : évaluation des vulnérabilités ; **ATD** : détection des menaces avancées ; **IDPS** : prévention des intrusions réseau ; **UEM** : gestion unifiée des terminaux ; **AV** : antivirus ; **SIEM** : gestion des événements et informations de sécurité ; **WAP** : point d'accès sans fil ; **NGFW** : pare-feu de nouvelle génération

Cas d'utilisation généraux

Forescout propose 25 solutions prêtes à l'emploi pour résoudre des cas d'utilisation spécifiques, tandis que les applications eyeExtend peuvent être utilisées pour résoudre des cas d'utilisation propres au client. En voici quelques exemples :

Découverte, classification et évaluation de tout appareil connecté au réseau dès la connexion établie
La solution Forescout eyeExtend Connect, optimisée par Forescout eyeSight, permet à un logiciel informatique ou de sécurité intégré de fournir des données contextuelles afin de faciliter l'identification des appareils à l'échelle de l'entreprise (campus, centre de données, environnements cloud et OT, notamment). Par exemple, l'application eyeExtend pour Ubiquiti permet aux clients de bénéficier d'une meilleure visibilité sur leurs appareils connectés en Wi-Fi et d'utiliser les attributs des appareils identifiés pour prendre des décisions mieux informées en matière de politiques au sein de la plateforme Forescout. L'application eyeExtend pour Ubiquiti peut ainsi transmettre les informations sur les appareils Ubiquiti connectés en Wi-Fi à une autre solution de gestion des services informatiques (ITSM) ou des ressources afin de mettre à jour leur base de données de gestion de la configuration (CMDB). L'application eyeExtend pour Google Cloud aide quant à elle les clients à bénéficier d'une visibilité en temps réel sur leurs instances cloud en constante évolution grâce à l'intégration à Google Cloud et à la récupération de données contextuelles d'inventaire Google Cloud.

Amélioration de la visibilité et du contrôle des appareils connectés par VPN accédant au réseau
eyeExtend Connect identifie tous les appareils qui se connectent au réseau d'entreprise par VPN. Grâce à l'intégration à la plateforme Forescout, les responsables de la sécurité peuvent déterminer si la ressource qui se connecte par VPN appartient à l'entreprise, de même que contrôler l'accès des appareils qui se connectent depuis des emplacements non autorisés.

Orchestration du flux de travail des informations sur les violations des politiques informatiques ou de sécurité
Envoyez en temps réel des alertes sur les violations des politiques grâce aux différentes plateformes de collaboration et de messagerie. Lors de l'élaboration de politiques pour automatiser les actions de contrôle du réseau, vous pouvez configurer une politique afin que la plateforme Forescout envoie des données sur les incidents liés aux appareils par e-mail ou via une plateforme de messagerie ou de collaboration. Par exemple, l'application eyeExtend pour Slack s'intègre à la plateforme de collaboration pour envoyer des alertes en temps réel concernant des violations de politiques à un canal utilisé par l'équipe informatique ou de sécurité sur Slack.

Automatisation de l'enregistrement des appareils mobiles, amélioration de la gestion de la sécurité et mise en œuvre d'une conformité continue
eyeExtend Connect orchestre les actions de partage et de contrôle des informations relatives aux appareils avec des systèmes UEM, garantissant ainsi une gestion unifiée des politiques de sécurité des appareils connectés à votre réseau, quel que soit leur type (PC, Mac, Linux®, tablette, smartphone), la connexion (filaire, sans fil, VPN) ou le propriétaire de l'appareil (entreprise ou particulier). Cette gestion complète des appareils permet d'automatiser l'enregistrement des appareils, assurer la conformité des appareils au moyen d'actions basées sur des politiques, appliquer des contrôles personnalisés d'accès au réseau et accélérer les mesures d'intervention et de correction. Par exemple, l'application eyeExtend pour le service Gestion des appareils mobiles Google offre désormais aux clients une visibilité sur les données contextuelles des appareils Chromebook. Ces données permettent d'optimiser les politiques de l'entreprise en matière de sécurité et d'accès des appareils BYOD.

Automatisation des actions et des flux de travail au sein de l'écosystème de solutions informatiques et de sécurité afin d'améliorer les opérations et renforcer la sécurité à l'échelle de l'entreprise
eyeExtend Connect permet d'envoyer ou recevoir des déclencheurs indiquant à la plateforme Forescout ou à une autre solution intégrée d'exécuter une action spécifique. Ces déclencheurs reposent sur une automatisation fondée sur des politiques et non sur une prise de décision selon un modèle nécessitant une intervention humaine. Les délais de réponse sont ainsi plus courts et les réseaux plus sûrs à tous les niveaux.

Utilisation de données contextuelles détaillées sur les appareils pour l'analyse de corrélation afin d'accélérer l'intervention sur incident
eyeExtend Connect permet à la plateforme Forescout d'alimenter un système SIEM en données détaillées sur les appareils à des fins d'analyse de corrélation. Cette approche permet d'obtenir une vue complète de la surface d'attaque de votre entreprise et réduire le délai d'obtention des informations, en plus de faciliter les investigations. La plateforme Forescout permet également de rationaliser les opérations de sécurité grâce à l'automatisation des actions basées sur les politiques ; vous pouvez ainsi limiter l'accès de l'appareil au réseau en fonction de la gravité de l'incident communiquée en temps réel par le système SIEM.

En résumé, eyeExtend Connect améliore rapidement le retour sur investissement dans le domaine de la sécurité en éliminant le cloisonnement des outils de sécurité et en les intégrant à la plateforme intelligente Forescout afin d'optimiser l'automatisation des mesures de prévention des menaces et de conformité aux politiques.

Remarque : certaines fonctionnalités d'eyeExtend Connect faisaient autrefois partie de la solution OIM. Toutes les fonctionnalités d'OIM sont désormais intégrées à eyeExtend Connect.

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
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