SOLUTION BRIEF

Description de la solution Forescout 4D Platform™

FORESCOUT

Description de la solution Forescout 4D Platform™

Autrefois, les réseaux étaient plus simples et pouvaient être efficacement sécurisés à l'aide de mesures classiques de sécurité périmétrique. Mais avec l'émergence et l'adoption croissante de nouveaux modèles économiques et des technologies de support, de plus en plus d'appareils sont connectés – le réseau s'étend ainsi davantage et devient plus difficile à contrôler.

Le nombre d'appareils IoT devrait passer de 14 milliards en 2023 à 25 milliards d'ici 2030. À mesure que la surface d'attaque augmente, les failles de sécurité, les angles morts et les conflits se multiplient – sans possibilité simple de résolution. Plus la surface d'attaque est grande, plus le risque de cyberattaque est élevé.

Que votre priori soit la cybersécurité, l'accès réseau, la protection des données, la disponibilité des systèmes, la production ou la sécurité, les questions restent les mêmes:

- Qu'est-ce qui se connecte à mon réseau ?
- Où se trouvent les vulnérabilités et les risques ?
- Quelles menaces franchissent ma défense ?
- Comment puis-je réagir de manière proactive, limiter les dommages et contenir les problèmes ?

Les environnements fortement réglementés nécessitent non seulement le respect des cadres de sécurité, des normes sectorielles et des exigences légales, mais aussi la capacité de prouver en permanence cette conformité.

Pour cela, vous avez besoin d'une plateforme centrale qui vous offre une visibilité complète sur tous les actifs de l'entreprise, un contrôle automatisé, une gouvernance et conformité IT continue, ainsi qu'une réduction efficace des risques et une réponse immédiate aux menaces.

La réponse : Forescout 4D Platform™

La plateforme Forescout 4D Platform™ est une solution de cybersécurité qui permet un contrôle intelligent et une gouvernance continue des actifs IT pour chaque appareil, quel que soit son emplacement. Elle repose sur quatre fonctions clés : Discover (Découvrir), Assess (Évaluer), Respond (Réagir) et Control (Contrôler). Ces fonctions couvrent aussi bien les environnements locaux que cloud, offrant une visibilité complète et une analyse des vulnérabilités sur les appareils managés et non managés à travers toute l'entreprise.

Découvrir

Tout commence par la découverte. La plateforme Forescout 4D utilise plus de 30 méthodes de détection, d'intégration et d'API pour assurer une visibilité complète, l'identification, la classification et la surveillance de chaque appareil connecté à votre environnement – en temps réel, pour tous les types d'appareils et à tous les niveaux du modèle Purdue.

Les informations contextuelles collectées permettent de suivre précisément le cycle de vie complet d'un actif – de son acquisition à sa maintenance, jusqu'à sa mise hors service. La plateforme identifie les appareils et conserve des enregistrements contextualisés et à jour tout au long de leur durée de vie.

Ces enregistrements complets garantissent la continuité des opérations et permettent de retracer les changements – un atout crucial pour la conformité réglementaire. La plateforme fournit également des insights détaillés pour optimiser les opérations IT, réduire les temps d'arrêt, améliorer les plans de maintenance et renforcer la performance du système.

Les fonctions de découverte peuvent également être exploitées pour unifier les domaines IT, IoT et IoMT – grâce à l'orchestration avec les CMDB, les opérations IT et les outils de gestion des services.

Évaluer

Les fonctions d'évaluation de la plateforme génèrent des insights contextuels sur les risques liés à l'état des actifs, à leur comportement et à leur conformité. La plateforme corrèle différents points de données dans des environnements hétérogènes et fournit des évaluations de risque prioritaires selon leur criticité.

Dès qu'un risque élevé ou une vulnérabilité est identifiée, la plateforme déclenche des processus automatisés de contrôle et d'orchestration pour réduire les risques et faciliter une prise de décision rapide – pour une gestion des risques en toute confiance.

Grâce à des capacités avancées de détection des vulnérabilités, la plateforme identifie les appareils non corrigés qui tentent de se connecter – en s'appuyant sur une base de données enrichie par EPSS, les KEV de la CISA et les recherches de Vedere Labs (VL-KEV). Les risques sont continuellement évalués à travers les environnements IT, OT, IoT et IoMT, avec une visibilité en temps réel sur les niveaux appareil et entreprise.

Résultat: une gestion proactive des risques et une résilience opérationnelle renforcée.

Réagir

Forescout transforme immédiatement les évaluations en actions – grâce à des vérifications de conformité automatisées et des remédiations. Cela inclut l'isolement des appareils, le blocage du trafic, ainsi que des réponses coordonnées entre les équipes IT et de sécurité.

La plateforme utilise des techniques modernes de détection des menaces telles que l'inspection approfondie des paquets, l'analyse des événements et les renseignements sur les menaces issus de Vedere Labs, couvrant les environnements IT, OT, IoT et IoMT. Les actions automatisées, basées sur les politiques et l'orchestration se déclenchent dès qu'une menace, une mauvaise configuration ou une violation des règles est détectée.

Des alertes SOAR personnalisées peuvent être configurées pour enrichir les webhooks et les workflows automatisés avec du contexte supplémentaire.

Que ce soit pour les opérations réseau ou dans un SOC : des tableaux de bord basés sur les rôles affichent les alertes et incidents pertinents selon les responsabilités définies.

Contrôler

L'application centralisée des politiques de sécurité et des règles d'accès garantit une gouvernance cohérente et à grande échelle. Forescout 4D Platform™ propose une gestion unifiée des politiques aux points de décision critiques – pour une conformité, une cohérence et un contrôle automatisé à l'échelle de l'entreprise.

Les administrateurs peuvent définir des politiques granulaires à l'aide de modèles ou de profils personnalisés pour simplifier la conformité et les rapports. La plateforme prend également en charge le contrôle d'accès basé sur les rôles et la segmentation Zero Trust – afin de réduire la surface d'attaque sans perturber les opérations en cours.

Composants de la Forescout 4D Platform™

Forescout eyeSight: Visibilité des actifs en temps réel

- Surveillance passive du réseau avec détection des appareils en temps réel
- Sans agent – aucune installation logicielle requise
- Intelligence complète sur les actifs (type d'appareil, système d'exploitation, logiciels)

Forescout eyeScope

- Vue console de tous les actifs
- Supervision de l'état et de la performance de l'environnement de déploiement
- Tableaux de bord et rapports basés sur l'IA ; extensibles avec Xplorer
- Gestion des utilisateurs et contrôle d'accès basé sur les rôles

Forescout eyeControl: Contrôle basé sur les politiques

- Accès réseau automatisé selon le niveau de sécurité
- Blocage, isolement ou restriction des appareils
- Remédiation orchestrée (patchs, mises à jour)
- Réaction rapide et automatique sans interruption

Forescout eyeInspect: Protection OT/ICS

- Visibilité complète sur IT, OT, IoT et IoMT
- Surveillance passive des réseaux industriels
- Gestion automatisée des vulnérabilités
- Détection des menaces basée sur les protocoles et détection d'anomalies

Forescout eyeExtend: Intégration écosystémique

- Connexion avec ITSM, NGFW, SIEM, EDR, etc.
- Orchestration des workflows entre outils
- Extension vers les environnements cloud, OT et tiers

Forescout eyeFocus: Évaluation & remédiation des risques

- Scoring automatisé des risques liés aux vulnérabilités et mauvaises configurations
- Priorisation basée sur la criticité
- Recommandations d'action et remédiation automatisée

Forescout eyeAlert: Détection précoce des menaces

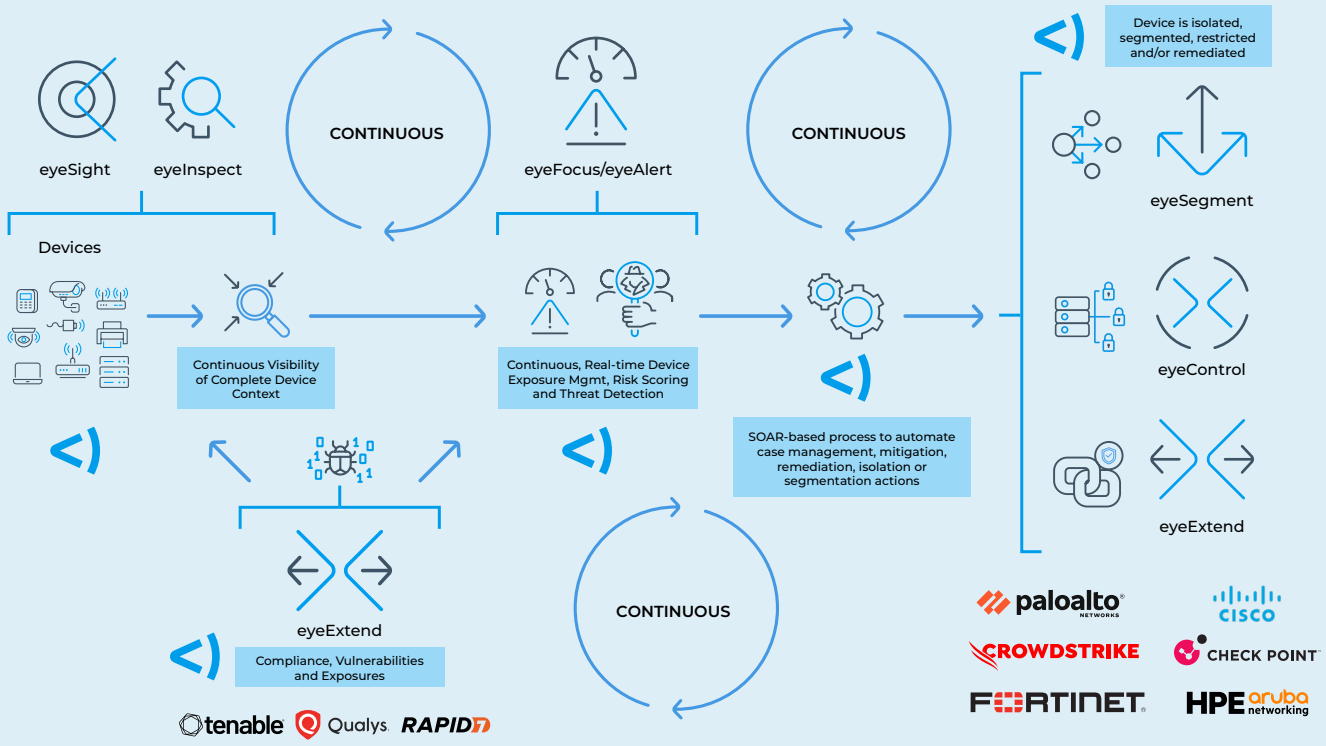
- Analyse comportementale avec apprentissage automatique
- Intégration de flux de menaces mondiaux
- Réponse automatisée aux incidents avec eyeControl

Chaque actif. Chaque risque. Sous contrôle.

La Forescout 4D Platform™ propose des solutions de cybersécurité évolutives, avec les insights et la flexibilité nécessaires pour gérer les actifs numériques en continu, presque en temps réel – quels que soient les modèles de déploiement.

Forescout voit tout. Avec Forescout, votre réseau est sous contrôle.

Une journée dans la vie d'un appareil



1. L'appareil apparaît sur le réseau et s'authentifie éventuellement
2. Il est classifié, évalué, éventuellement corrigé ou segmenté
3. Les appareils OT peuvent également être identifiés et analysés
4. Les flux de communication sont visualisés de manière contextuelle
5. Les vulnérabilités et les risques sont consolidés en un score dynamique
6. Les journaux et données de télémétrie permettent une détection précoce
7. Des actions SOAR, des politiques ou des outils tiers peuvent être déclenchés
8. L'appareil est isolé, corrigé ou son trafic est segmenté
9. Le risque est ainsi contenu

À propos de Forescout

Forescout Technologies, Inc., leader mondial en cybersécurité, identifie en continu, protège et contribue à assurer la conformité de tous les actifs cybernétiques – gérés ou non – qu'ils soient IT, IoT, IoMT ou OT. Depuis plus de 20 ans, les entreprises du Fortune 100 et les agences gouvernementales font confiance à Forescout pour fournir une cybersécurité automatisée, indépendante des fournisseurs, à grande échelle.

La plateforme Forescout 4D™ offre des capacités complètes en matière de sécurité réseau, de gestion des risques et des expositions, ainsi que de détection et de réponse aux menaces. Grâce à un partage de contexte fluide et une orchestration des flux de travail via ses partenaires de l'écosystème, elle permet aux clients de gérer plus efficacement les risques cybernétiques et de mieux atténuer les menaces.

Leader en sécurité IoT, Forescout est engagé à protéger la qualité des soins de santé à l'échelle mondiale.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com