Présentation de l'entreprise

L'entreprise en bref

Secteur

Sécurité de l'entreprise

Clients

Plus de 2 000 entreprises et agences gouvernementales dans plus de 60 pays*

Marchés

Services financiers, défense et gouvernement, santé, fabrication, éducation, commerce de détail et infrastructure critique

Année de création

2000

Employés

500+*

PDG

Michael DeCesare

Principaux investisseurs

Accel Partners, Amadeus Capital Partners, Meritech Capital Partners et Pitango Venture Capital

ForeScout offre à 2 000 entreprises et administrations dans le monde entier la possibilité unique de visualiser leurs équipements, y compris les équipements non traditionnels, à l'instant même où ils se connectent au réseau. Tout aussi important, ForeScout vous permet de contrôler ces appareils et d'orchestrer l'exploitation et le partage des informations sur des outils de sécurité hétérogènes afin d'accélérer la réponse aux incidents. Contrairement aux solutions de sécurité traditionnelles, ForeScout ne nécessite aucun agent logiciel ou aucune connaissance préalable des équipements. Nos solutions s'intègrent avec les principaux logiciels de gestion des réseaux, de la sécurité, de la mobilité et des SI, pour éliminer les silos de sécurité, automatiser les flux de travail et générer des économies significatives.

Les solutions proposées par ForeScout sont faciles à déployer, flexibles et évolutives. Ainsi, plus de 2 000 clients* répartis dans plus de 60 pays renforcent la sécurité de leur réseau et leur conformité grâce à ForeScout.

Transformer la sécurité grâce à la visibilité

Les fonctionnalités uniques de ForeScout peuvent se résumer en trois mots :

Voir La plateforme ForeScout CounterACT® fournit une visibilité en temps réel sur les appareils connectés à l'aide d'une adresse IP, qu'ils soient gérés ou non gérés, d'entreprise ou personnels, filaires ou sans fil. Étant donné que CounterACT ne nécessite aucun agent de point d'extrémité, il détecte aussi les appareils IoT (internet des objets) non traditionnels et les points d'extrémité détenus à titre personnel (BYOD). CounterACT identifie et évalue les points d'extrémité et applications du réseau et détermine l'utilisateur, le propriétaire, le système d'exploitation, la configuration de l'appareil, les logiciels, les services, l'état des patchs et la présence d'agents de sécurité.

Contrôler CounterACT analyse le réseau et surveille en permanence l'activité de chaque appareil. Contrairement aux systèmes qui se contentent de signaler les violations et d'envoyer des alertes au personnel chargé de la gestion des SI et de la sécurité, CounterACT vous permet d'automatiser et d'appliquer une gamme complète de contrôles basés sur des politiques d'accès aux réseaux, de conformité des points d'extrémité et de sécurité des appareils mobiles.

Orchestrer CounterACT s'intègre avec plus de 70 produits de gestion du réseau, de la sécurité, de la mobilité et des SI * via l'architecture ForeScout ControlFabric®. Cette capacité à orchestrer le partage des informations et les différentes opérations entre les outils de gestion de la sécurité que vous possédez et utilisez déjà vous permet de :

- partager les informations de contexte et de contrôle entre les systèmes afin d'appliquer une politiques unifiée de sécurité réseau ;
- réduire les fenêtres de vulnérabilité en automatisant la réponse aux menaces à l'échelle du système ;
- augmenter la rentabilité de vos outils de sécurité existants tout en gagnant du temps grâce à l'automatisation des flux de travail.

Défis liés à la sécurité informatique des entreprises

Les solutions ForeScout vous aident à relever ces défis formidables en matière de sécurité :

- **Manque de visibilité et de contrôle.** La gestion traditionnelle des points d'extrémité nécessite l'utilisation d'agents sur les appareils afin de détecter qui les contrôle. En outre, certains appareils se connectent et se déconnectent du réseau, ce qui nécessite une surveillance en temps réel et des diagnostics continus.
- **Cybermenaces sophistiquées.** De nos jours, les pirates sont des cybercriminels et des États-nations qui bénéficient de financements importants. Il s'agit d'ingénieurs informatiques qualifiés qui connaissent bien la conception des réseaux et des applications, les failles de la sécurité et le comportement des utilisateurs finaux. Leur méthode d'attaque de prédilection consiste de plus en plus à tirer parti des points d'extrémité vulnérables, d'obtenir un accès au réseau et de voler des données personnelles ou la propriété intellectuelle.
- **Augmentation rapide de la vulnérabilité.** Le nombre d'appareils non gérés et sans agent augmente de manière exponentielle car les employés et sous-traitants utilisent désormais leurs appareils personnels (BYOD) au travail et, avec le phénomène de l'Internet des objets (IoT), de nombreux appareils non traditionnels se connectent chaque jour au réseau.
- **Une sécurité fragmentée ouvre la porte aux attaquants et retarde les mesures correctives.** Une grande entreprise classique possède au moins une douzaine de systèmes de gestion de la sécurité. Pourtant, en moyenne moins de trois de ces systèmes partagent des informations sur la sécurité. Cette approche de la sécurité en silos empêche une réponse de sécurité coordonnée, à l'échelle de l'entreprise, ce qui laisse plus de temps aux attaquants pour profiter des vulnérabilités du système.

Produits

- ForeScout CounterACT
- Modules avancés ForeScout
- CounterACT Enterprise Manager

Offre

Boîtiers physiques ou virtuels ; modules logiciels

Solutions intégrées

Modules disponibles pour les principales solutions de réseau, de sécurité, de gestion informatique et d'infrastructure mobile (70 modules disponibles actuellement)*

Avantages de ForeScout

- **Meilleure visibilité des points d'extrémité.** Identifiez instantanément les appareils dotés d'une adresse IP, y compris les systèmes BYOD (PC, tablettes et smartphones), les appareils IoT (appareils portables, capteurs et machines) et les points d'extrémité malveillants, sans recourir à des agents ou sans avoir une connaissance préalable des équipements.
- **Productivité accrue.** Automatisez l'accès sécurisé des invités, sous-traitants et appareils BYOD afin de permettre aux employés, au personnel informatique et aux équipes d'assistance de se concentrer sur les tâches à forte valeur ajoutée plutôt que sur les problèmes quotidiens d'accès au réseau.
- **Conformité préservée.** Renforcez vos efforts de conformité en vous assurant que les points d'extrémité identifiés sont bien configurés, les logiciels antivirus s'exécutent normalement et sont à jour, les vulnérabilités sont corrigées et les dernières versions des logiciels sont installées.
- **Retour sur investissement rapide.** CounterACT s'intègre facilement à votre infrastructure informatique existante, ce qui vous permet de bénéficier d'une visibilité et d'un contrôle sur le réseau en quelques heures ou quelques jours tout au plus. CounterACT s'installe rapidement hors bande pour éviter les risques liés à un point de défaillance unique et à la réorganisation de l'architecture réseau.
- **Retour sur investissement optimisé.** Les modules facultatifs d'intégration de ControlFabric augmentent la valeur de vos outils de sécurité existants en permettant le partage des informations, l'automatisation des flux de travail et la rationalisation des processus de gestion de la sécurité.
- **Gestion automatisée de la sécurité.** Les fonctionnalités d'identification, d'autorisation et de contrôle basé sur les règles permettent de minimiser les tâches d'administration fastidieuses.
- **Sécurité améliorée à l'échelle du système.** L'intégration avec plus de 70 produits de gestion de réseau, de sécurité et de gestion des SI* accélère la détection, les mesures correctives et la réponse aux menace à l'échelle du système.
- **Coûts d'administration réduits.** Économisez du temps et de l'argent en automatisant les principaux flux de travail associés à la détection des appareils dotés d'une adresse IP et en partageant ces informations avec les systèmes de gestion et de sécurité informatique déjà en place.
- **Croissance adaptée à vos besoins.** Une gamme d'options de boîtier physique ou virtuel s'adapte aux besoins croissants de votre entreprise. ForeScout a fait ses preuves sur des réseaux comportant plus de 1 000 000 de points d'extrémité.

Distinctions récentes

- Position de leader dans le carré magique Gartner pour le contrôle d'accès au réseau en 2011, 2012 et 2014
- Prix de la meilleure solution de contrôle d'accès au réseau 2015 décerné par SC Magazine
- Prix des lecteurs 2015 de la revue Secure Computing Magazine et élu en 2013, 2014 et 2015 par ce même magazine « meilleur produit » sur l'ensemble des solutions testées
- Prix Frost & Sullivan Global Technology Innovation Award en 2014
- Élu meilleur produit pour l'enseignement supérieur 2014 par HigherEd TechDecisions
- Figure dans le classement des 20 entreprises de sécurité à la croissance la plus rapide de la Silicon Valley Business Review publié en octobre 2015

Pour en savoir plus, visitez le site **www.ForeScout.com**

ForeScout®

Bureaux dans le monde

Siège :
9900 East Hamilton Ave., Suite 300
Campbell, CA 95008, États-Unis
+1-408-213-3191

EMA : Londres +44-1256-843633
Israël : Tel Aviv +972-3-6449987
Asie-Pacifique : Hong-Kong +852-2411-4388

* En janvier 2016