Visibilité et contrôle automatisé de tous les accès au LAN

ForeScout Technologies est l'un des principaux fournisseurs de solutions de sécurité réseau pour les entreprises qui souhaitent accélérer leur productivité tout en permettant aux utilisateurs d'accéder aux ressources réseau de l'entreprise là où ils en ont besoin et quand ils en ont besoin, sans compromettre la sécurité. La technologie ForeScout renforce les défenses et la mobilité des entreprises tout en améliorant l'efficacité informatique et la rentabilité d'autres outils de sécurité. Les solutions proposées par ForeScout sont connues pour être faciles à déployer, flexibles et extensibles.

ForeScout

Renforcez la sécurité de votre réseau de façon simple

La solution ForeScout CounterACT™ permet d'identifier, d'évaluer, de prévenir et de résoudre dynamiquement les risques de sécurité tels que les utilisateurs, appareils et applications indésirables et inconnus, les systèmes non gérés et non sécurisés, le non-respect des politiques de sécurité et les comportements malveillants.

ForeScout CounterACT™ est une plate-forme de contrôle de la sécurité automatisée permettant de visualiser, surveiller et contrôler votre réseau (dispositifs, systèmes d'exploitation, applications, utilisateurs). Elle permet aux employés et aux invités d'utiliser le réseau tout en protégeant l'accès aux ressources critiques et aux données sensibles.

- Sans agent
  Non perturbateur
- Visibilité accrue du réseau
- Gestion sécurisée des invités
- Agnostique de l'infrastructure existante
- Contrôle évolutif des terminaux mobiles

MIEL

Distribution. Formation. Assistance. Appelez le 01 60 19 34 52

Contrôle d'accès au réseau

Fondée sur la technologie de contrôle d'accès au réseau (NAC) de troisième génération, la solution ForeScout CounterACT est facile à installer car elle ne nécessite pas de déployer des agents logiciels, ni de mettre à jour ou de reconfigurer vos équipements. Les fonctionnalités de ForeScout CounterACT™ sont regroupées dans un seul boîtier.

Risques de sécurité de votre réseau

La sécurité réseau classique consiste à bloquer les attaques externes à l'aide de pare-feu et de systèmes de prévention des intrusions. Ces dispositifs ne font rien pour protéger votre réseau contre des menaces internes telles que :

Les visiteurs : Lorsque des invités et des sous-traitants viennent dans vos locaux, ils apportent leur ordinateur. Pour continuer à travailler, les invités ont besoin d'accéder à Internet et les sous-traitants peuvent avoir besoin de ressources supplémentaires. En leur accordant un accès illimité, vous risquez d'être attaqué par un logiciel malveillant ou de compromettre vos données sensibles.

Les utilisateurs sans fil et mobiles : Vos employés veulent connecter leurs Smartphones et leurs tablettes à votre réseau. Faute de contrôles appropriés, ces appareils peuvent infecter votre réseau ou provoquer des fuites de données.

Les appareils malveillants : Des employés bien intentionnés peuvent étendre votre réseau avec des hubs / switch peu onéreux et des points d'accès sans fil. Ces appareils peuvent rendre votre réseau instable. Ils peuvent également l'infecter et provoquer des fuites de données.

Les logiciels malveillants et les ordinateurs zombies : Des études ont montré que même les entreprises les mieux gérées peuvent avoir des ordinateurs infectés en raison d'attaques de type zero day et/ou d'antivirus obsolètes. Une fois compromis, ces PC peuvent être utilisés dans des attaques de type pivot au cours desquelles des personnes étrangères à l'entreprise peuvent analyser votre réseau et voler vos données.

La conformité : Les postes clients peuvent être mal configurés, des machines virtuelles peuvent apparaître sur votre réseau avec des paramétrages ou des logiciels inappropriés, et les contrôles de sécurité peuvent être désactivés. Les systèmes non conformes présentent des risques pour la sécurité.

Fonctionnement de ForeScout CounterACT

ForeScout CounterACT se déploie hors bande en se reliant au port SPAN de l'un des commutateurs existants. Depuis cet emplacement, CounterACT surveille le trafic réseau et s'intègre à l'infrastructure réseau afin de détecter la présence de nouveaux appareils au moment où ceux-ci tentent d'accéder à votre réseau.

CounterACT accorde automatiquement les autorisations d'accès en fonction de l'identité de l'utilisateur ainsi que du type et du niveau de sécurité de l'appareil. Une fois que l'appareil est autorisé sur votre réseau, CounterACT peut vous faire part d'un problème de sécurité, le résoudre pour vous ou mettre l'appareil en quarantaine jusqu'à la résolution du problème. CounterACT protège en permanence le réseau grâce à la surveillance des appareils et au blocage des attaques.

La différence ForeScout

ForeScout CounterACT est beaucoup plus facile et rapide à déployer que les produits de contrôle d'accès au réseau classiques. Voilà pourquoi :

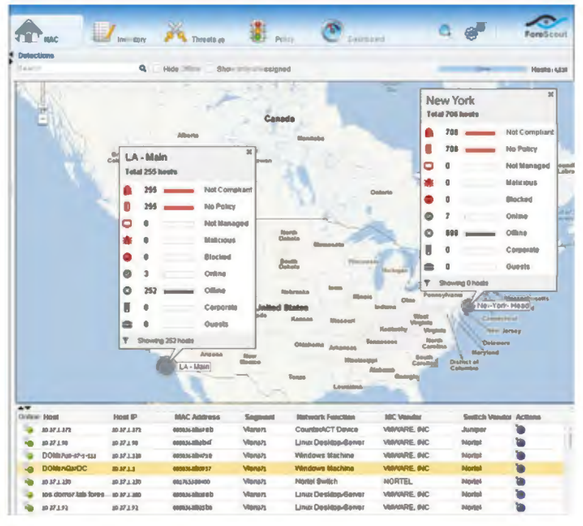
Un boîtier installé dans la journée. Les fonctionnalités sont regroupées dans un seul boîtier, aisément paramétrable grâce aux assistants de configuration intégrés.

Fonctionne avec l'infrastructure existante. ForeScout fonctionne avec vos équipements existants (commutateurs, routeurs, pare-feu, systèmes de gestion des correctifs, antivirus, répertoires, systèmes d'émission de tickets). Il n'est pas nécessaire de modifier vos infrastructures ni de mettre à niveau vos équipements.

Aucun logiciel n'est requis. ForeScout CounterACT est sans agent, ce qui lui permet de fonctionner avec tous les équipements (gérés et non gérés, connus et inconnus, autorisés et malveillants). Aucune installation n'est nécessaire sur le poste client.

N'entraîne aucune interruption. Contrairement aux produits de contrôle d'accès réseau de première génération qui perturbent systématiquement les activités des utilisateurs avec des contrôles d'accès fastidieux, ForeScout CounterACT peut être déployé de manière échelonnée, avec un minimum d'impact et des résultats rapides.

Résultats rapides. ForeScout CounterACT fournit des résultats utiles dès le premier jour de sa mise en oeuvre en identifiant les problèmes que comporte votre réseau.
La base de connaissances intégrée vous permet de configurer les politiques de sécurité avec rapidité et précision.



Caractéristiques générales

Technologies Control Fabric	ForeScout CounterACT est le principal composant de l'architecture ControlFabric, qui permet à ForeScout CounterACT et à d'autres solutions d'échanger des informations et de résoudre une grande variété de problèmes liés au réseau et à son exploitation ainsi qu'à la sécurité.
Visibilité	Le module Asset Inventory (inventaire des actifs) de ForeScout CounterACT offre en temps réel des fonctionnalités multidimensionnelles de visibilité et de contrôle réseau qui permettent de suivre et de contrôler les activités des utilisateurs, des applications, des processus, des ports, des appareils externes, etc. (voir figure 1).
Intégration à l'infrastructure informatique existante	Contrairement aux produits de contrôle d'accès au réseau propriétaires, CounterACT s'installe rapidement et facilement car il prend en charge un large éventail d'équipements et logiciels de réseau et de sécurité tiers (commutateurs réseau, points d'accès sans fil, VPN, antivirus, gestion des correctifs, émission de tickets, systèmes SIEM, évaluation de la vulnérabilité, gestion des appareils mobiles, etc.).
Déploiement hors-bande	ForeScout CounterACT se déploie hors bande, ce qui supprime les problèmes liés à la latence et aux points de faiblesse de votre réseau.
Gestion des politiques	ForeScout CounterACT permet de définir des politiques de sécurité adaptées à votre entreprise. La configuration et l'administration s'effectuent rapidement et aisément, grâce à l'assistant intégré de politiques de CounterACT et à sa base de connaissances de règles, rapports et classifications des appareils.
Évolutivité	ForeScout CounterACT a fait ses preuves sur des réseaux comportant plus de 250 000 endpoints. Les boîtiers CounterACT sont proposés dans une large variété de tailles pour s'adapter à toutes tailles de réseaux.
Génération de rapports	ForeScout CounterACT dispose d'un moteur de génération de rapports entièrement intégré permettant de surveiller le degré de conformité aux politiques, de satisfaire aux obligations d'audit réglementaire et de produire des inventaires en temps réel.

Sécurisation des terminaux qui se connectent

Conformité du device	ForeScout CounterACT peut garantir la conformité des devices sur votre réseau à votre politique antivirus, l'application de patchs appropriés et l'absence de logiciels non autorisés tels que P2P.
Détection des menaces	La technologie brevetée de détection des menaces ActiveResponse™ proposée par ForeScout surveille le comportement des appareils après leur connexion. ActiveResponse bloque les menaces auto-propagées de type « jour zéro » ainsi que les autres types de comportement malveillant. À la différence des autres approches, ActiveResponse ne s'appuie pas sur les mises à jour de signature pour conserver son efficacité : les coûts de gestion sont ainsi minimisés.
Détection des appareils malveillants	ForeScout CounterACT peut détecter des infrastructures malveillantes telles que des commutateurs et des points d'accès sans fil non autorisés, en déterminant si ces équipements sont des appareils NAT ou s'ils figurent sur la liste des appareils autorisés, ou en identifiant les configurations où plusieurs hôtes sont connectés au port d'un commutateur. CounterACT peut même détecter les appareils sans adresse IP tels que les systèmes de capture de paquets destinés à voler des données sensibles.
Contrôle en temps réel	ForeScout CounterACT détecte et contrôle les appareils mobiles portatifs connectés à votre réseau Wi-Fi. Les appareils des appareils mobiles suivants sont pris en charge : iPhone/iPad, Blackberry, Android, Windows Mobile, Nokia Symbian.

Sécurisation des accès

Enregistrements des invités	Le processus automatisé de ForeScout CounterACT permet aux utilisateurs d'accéder au réseau sans compromettre la sécurité de votre réseau interne. CounterACT offre plusieurs options d'enregistrement des invités, permettant ainsi de personnaliser leur processus d'admission par rapport aux besoins de votre entreprise.
Options de contrôle flexibles	Contrairement aux produits NAC de première génération qui effectuaient des contrôles d'accès fastidieux et perturbaient les activités des utilisateurs, ForeScout CounterACT offre toute une panoplie d'options de mise en oeuvre qui vous permettent d'élaborer une réponse personnalisée adaptée à la situation. Il est possible de traiter les intrusions à faible risque en envoyant à l'utilisateur final une notification et/ou en corrigeant automatiquement son problème de sécurité. L'utilisateur peut ainsi continuer à travailler pendant la mise en oeuvre de cette remédiation.
802.1X ou non	ForeScout CounterACT offre le choix entre le protocole 802.1X et d'autres technologies telles que LDAP, Active Directory, Oracle et Sun. Le mode hybride permet d'utiliser plusieurs technologies en parallèle, ce qui accélère le déploiement NAC dans des environnements variés et de grandes dimensions.
Accès basé sur les rôles	ForeScout CounterACT vérifie que seules les personnes habilitées utilisent les ressources réseau auxquelles elles ont le droit d'accéder. ForeScout se base pour cela sur les répertoires dans lesquels les rôles sont attribués aux utilisateurs.
Authentification	CounterACT prend en charge les normes existantes en matière d'authentification et de répertoires (802.1X, LDAP, RADIUS, Active Directory, Oracle, Sun, etc.).
Serveur RADIUS intégré	ForeScout CounterACT intègre un serveur RADIUS pour faciliter le déploiement du protocole 802.1X. Vous pouvez également utiliser les serveurs RADIUS existants en configurant CounterACT de manière à le faire fonctionner comme un proxy RADIUS.

Téléchargez ce document en PDF en vous rendant sur notre site web

http://www.miel.fr/forescout