Pourquoi les clients choisissent CounterACT

Prise en charge hétérogène. Fonctionne avec les infrastructures réseau, les systèmes d'exploitation, les logiciels de points d'extrémité et les solutions de sécurité tierces les plus répandus.

Approche sans agent. Aucun agent n'est nécessaire aux points d'extrémité pour l'authentification et le contrôle d'accès au réseau.

Visibilité exceptionnelle. Détectez des appareils que les autres solutions ne voient pas :

- Ordinateurs de bureau, portables, serveurs, routeurs, smartphones et tablettes
- Réseaux locaux câblés/sans fil et imprimantes
- Appareils IoT (projecteurs, contrôles industriels, santé, fabrication, appareils POS, etc.)

Contrôle automatisé. Automatisez une large gamme d'actions :

- Autorisation, refus ou limitation de l'accès au réseau en fonction du niveau de sécurité des appareils et de vos politiques de sécurité
- Mise en quarantaine et isolation des points d'extrémité malveillants ou à haut risque

Retour sur investissement rapide. Déploiement rapide pour bénéficier d'une visibilité sur le réseau en quelques heures.

Mise en œuvre de politiques. Mise en œuvre du contrôle d'accès au réseau, de la conformité des points d'extrémité et de la sécurité des appareils mobiles.

Productivité. Attribution d'un accès réseau approprié aux personnes et appareils, sans intervention du personnel.

Fiabilité. Amélioration de la stabilité du réseau avec l'identification et la suppression des infrastructures malveillantes.

Réduction des coûts. Suppression des tâches manuelles associées à l'ouverture ou à la fermeture des ports réseau pour l'accès des invités.

Conformité. Automatisation des processus d'identification des violations de politiques, de correction des défaillances des points d'extrémité et d'évaluation du respect des normes de conformité.

ForeScout CounterACT®

Bénéficiez d'une surveillance en temps réel, d'un contrôle accru et d'une correction basée sur des politiques de vos appareils gérés, non gérés et non traditionnels.

ForeScout CounterACT® est un boîtier de sécurité sans agent qui identifie et évalue de manière dynamique les points d'extrémité et les applications dès leur connexion à votre réseau. CounterACT identifie rapidement 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. Il effectue ensuite des actions de correction, de contrôle et de surveillance continue sur ces équipements.

CounterACT réalise ces actions sur des points d'extrémité d'entreprise ou détenus à titre personnel (BYOD) ainsi que sur des appareils non traditionnels, sans nécessiter d'agent ou d'une connaissance préalable des équipements. Il se déploie rapidement dans votre environnement existant et nécessite rarement des modifications d'infrastructure, des mises à niveau ou une reconfiguration des points d'extrémité.

Risques de sécurité et angles morts du réseau

La sécurité réseau classique consiste à bloquer les attaques externes à l'aide de pare-feu et de systèmes de prévention des intrusions. Toutefois, ces outils de gestion de la sécurité ne font rien pour protéger votre réseau contre le déluge des menaces internes qui génèrent un nombre croissant d'incidents et de violations de sécurité. Ces menaces incluent :

- **Les visiteurs :** les invités et sous-traitants apportent leur ordinateur dans votre entreprise. Ils ont besoin d'accéder à Internet, et les sous-traitants peuvent demander des ressources supplémentaires. Si vous donnez un accès illimité à ces visiteurs, vous exposez votre réseau à une attaque.

  Les utilisateurs sans fil et mobiles (BYOD) : les employés veulent utiliser leurs smartphones, tablettes et ordinateurs personnels sur votre réseau. Faute de contrôles appropriés, ces appareils peuvent infecter votre réseau ou provoquer des pertes de données.
- **Appareils IoT (Internet des objets) :** les appareils non traditionnels continuent d'augmenter votre vulnérabilité en ajoutant des appareils non gérés connectés via IP, tels que des projecteurs, thermostats, contrôles de l'éclairage, caméras de sécurité, etc.
- **Appareils malveillants :** des employés bien intentionnés peuvent étendre votre réseau avec des hubs de câblage, serveurs de départements et routeurs peu onéreux et des points d'accès sans fil susceptibles de rendre le réseau instable et vulnérable.
- **Les logiciels malveillants et les réseaux d'ordinateurs zombies :** une fois votre réseau compromis, les appareils qui y sont connectés peuvent être utilisés dans des attaques de type pivot au cours desquelles des personnes étrangères à l'entreprise analysent votre réseau et volent vos données.
- **Conformité :** les points d'extrémité et machines virtuelles mal configurés peuvent comporter des paramètres ou des logiciels inappropriés. De plus, ils peuvent être désactivés de manière intentionnelle par l'utilisateur ou le logiciel malveillant afin de désactiver les contrôles de sécurité.

On ne peut pas protéger ce que l'on ne voit pas.

Une visibilité limitée entraîne l'apparition d'angles morts en matière de sécurité. La plupart des systèmes de sécurité des points d'extrémité nécessitent la présence d'agents récents sur tous les appareils afin que ces derniers puissent être détectés et gérés. En général, les responsables de la sécurité informatique n'ont aucune visibilité sur les points d'extrémité BYOD non gérés et le nombre croissant d'appareils IoT qui se connectent chaque jour au réseau.

Les analystes, clients et partenaires choisissent CounterACT

- Position de leader dans le carré magique Gartner pour le contrôle d'accès au réseau** pour sa capacité d'exécution et l'exhaustivité de sa vision (quatre rapports consécutifs)
- Élu meilleur produit NAC par SC Magazine, juin 2015
- Élu meilleur produit par SC Magazine, octobre 2014

« Nous avions besoin d'une solution NAC pouvant être déployée rapidement et sans risque d'interruption de l'activité. En outre, elle devait prendre en charge notre infrastructure informatique mixte Aruba® et Cisco®. ForeScout CounterACT nous a offert tout cela et bien plus encore, y compris des fonctionnalités impressionnantes d'intégration avec nos outils de sécurité existants FireEye® et ArcSight®. C'est pourquoi nous appelons CounterACT le « couteau suisse » de notre équipe de sécurité informatique, car il facilite et optimise les nombreux contrôles de sécurité et de conformité automatisés ».

- Ali Kutluhan Aktaş, Responsable de la sécurité du système d'information/ gestion des risques chez KKB

Fonctionnement de ForeScout CounterACT®

ForeScout CounterACT offre la possibilité unique de détecter les appareils connectés au réseau via IP, de les contrôler et d'orchestrer l'exploitation et le partage des informations sur des outils de sécurité hétérogènes. Comment ?

Voir. Le boîtier CounterACT se déploie hors bande sur votre réseau. Ensuite, il surveille en permanence le trafic réseau et s'intègre à votre infrastructure réseau afin d'identifier les appareils dès qu'ils se connectent au réseau. CounterACT a la possibilité unique de détecter un vaste ensemble de points d'extrémité, utilisateurs et applications connectés par IP. En fait, les technologies sophistiquées de CounterACT permettent de détecter des appareils invisibles aux produits concurrents.

CounterACT ne s'arrête pas là. Il classe de manière précise les points d'extrémité de votre réseau à l'aide de techniques d'interrogation passives et actives. CounterACT peut identifier le type d'appareil, son emplacement, l'utilisateur, si le périphérique appartient à votre domaine, ainsi que d'autres informations de base. Il obtient aussi des informations détaillées sur le niveau de sécurité de l'appareil en utilisant des identifiants d'administrateur pour interroger les appareils détenus par l'entreprise.

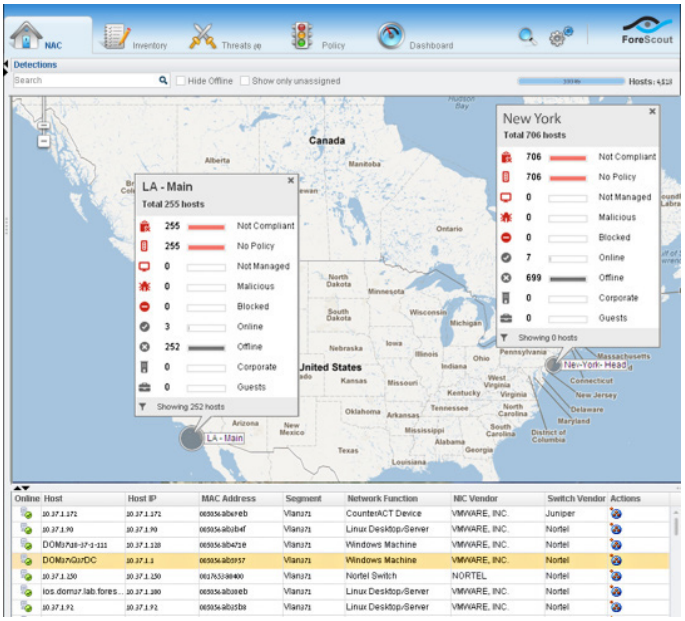

Figure 1 : ForeScout CounterACT fournit des informations générales et détaillées sur tous les appareils de votre réseau.

Contrôler. Lorsque CounterACT détecte un problème de sécurité sur un point d'extrémité, son gestionnaire de politiques sophistiqué exécute automatiquement différentes réponses selon la gravité du problème. Des violations mineures peuvent entraîner l'envoi d'un message d'avertissement à l'utilisateur final. Les employés et sous-traitants qui utilisent leurs propres appareils peuvent être redirigés vers un portail d'accueil automatisé. De graves violations peuvent entraîner des actions telles que le blocage ou la mise en quarantaine de l'appareil, la réinstallation d'un agent de sécurité, le redémarrage d'un agent ou d'un processus, l'obligation pour un point d'extrémité d'installer un correctif de système d'exploitation, ou d'autres actions de remédiation.

L'efficacité de l'architecture ControlFabric

L'architecture ControlFabric sert de ciment entre les fonctionnalités de ForeScout CounterACT et celles des produits tiers de gestion des réseaux, de la sécurité, de la mobilité et des SI. Elle permet d'éliminer les silos de gestion de sécurité pour :

- Unifier la gestion de la sécurité à l'échelle du système
- Améliorer l'efficacité opérationnelle
- Accélérer la réponse aux menaces
- Augmenter la rentabilité de votre système de sécurité
- Améliorer considérablement le niveau de sécurité et de conformité de votre réseau

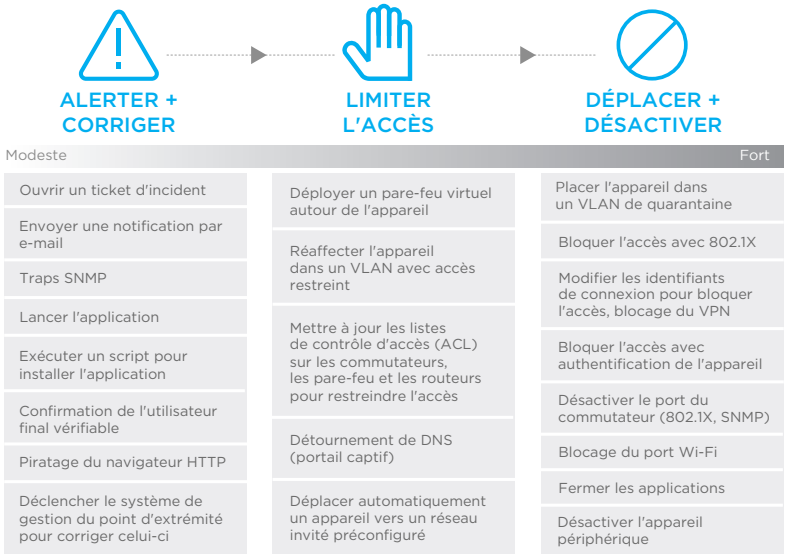

Figure 2 : ForeScout CounterACT gère la totalité des actions de contrôle.

Orchestrer. CounterACT tire parti de l'architecture ControlFabric® de ForeScout pour orchestrer le partage des informations et des opérations entre les outils de gestion et de sécurité que vous possédez déjà. L'architecture ControlFabric permet une telle orchestration grâce à des intégrations personnalisées ou des modules logiciels prêts à l'emploi. Développés en collaboration avec les partenaires technologiques de ForeScout, les modules de base et avancés de ForeScout fournissent la puissance de CounterACT à plus de 70 produits phares de gestion de réseau, de sécurité, de mobilité et de SI* pour :

- Partager des informations contextuelles avec les systèmes de gestion informatique et de sécurité
- Automatiser les principaux flux de travail, tâches informatiques et processus de sécurité dans l'ensemble des systèmes
- Accélérer la réponse à l'échelle du système pour atténuer rapidement les risques et les pertes de données

Caractéristiques

Caractéristiques générales

Déploiement hors bande : déploiement hors bande sur votre réseau sans ajouter de latence ou de point de faiblesse potentiel.

Visibilité : la fonctionnalité d'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).

Interopérabilité ouverte : CounterACT fonctionne avec les équipements réseau les plus courants (commutateurs, routeurs, VPN, pare-feu, systèmes de gestion des patchs, antivirus, répertoires et systèmes d'émission de tickets) et sur les principaux systèmes d'exploitation de points d'extrémité (Windows®, Linux, iOS, OS X, Android), sans nécessiter de modification ou de mise à niveau des équipements.

Génération de rapports : un moteur de génération de rapports entièrement intégré permet de surveiller le degré de conformité aux politiques, de satisfaire aux obligations d'audit réglementaire et de produire des inventaires en temps réel.

Évolutivité : a fait ses preuves sur des réseaux comportant plus de 1 000 000 de points d'extrémité. Les boîtiers CounterACT sont proposés dans une large variété de tailles.

Certifications : CounterACT satisfait aux spécifications militaires et a obtenu les certifications américaines suivantes :

- USMC ATO
- US Army CoN
- UC APL
- Common Criteria EAL 4+

N'entraîne aucune interruption : déploiement sans impact sur les utilisateurs ou les appareils. Vous pouvez mettre progressivement en œuvre un contrôle automatisé en commençant par les emplacements les plus problématiques et en sélectionnant un plan d'action approprié.

Gestion des politiques : permet de définir des politiques de sécurité adaptées à votre entreprise. La configuration et l'administration s'effectuent rapidement et aisément, grâce à des modèles de politiques, règles et rapports intégrés.

Architecture ControlFabric : l'architecture ControlFabric® offre une interopérabilité complète avec les logiciels de fournisseurs tiers et une architecture d'intégration ouverte.

Point d'extrémité

Approche sans agent : identifiez, classez, authentifiez et contrôlez l'accès au réseau sans agent. Vous pouvez effectuer une inspection approfondie d'un point d'extrémité sans utiliser d'agent si CounterACT dispose d'un identifiant d'administrateur pour le point d'extrémité. Si CounterACT ne dispose pas d'identifiant d'administrateur, par exemple pour un appareil BYOD, une inspection approfondie est possible grâce à notre agent facultatif SecureConnector, qui est fourni sans frais supplémentaires avec CounterACT.

Conformité du point d'extrémité : garantie de la conformité de chaque point d'extrémité de votre réseau à votre politique antivirus, de l'application de patchs appropriés et de l'absence de logiciels non autorisés. CounterACT identifie les violations de politiques, corrige les défaillances des points d'extrémité et évalue le respect des normes règlementaires, tout cela de manière automatique.

Détection des menaces : la surveillance continue fournit des informations plus précises et actualisées que des analyses ponctuelles de la vulnérabilité, puisque des appareils peuvent se connecter et se déconnecter du réseau entre deux analyses.

Détection des appareils malveillants : détectez des infrastructures malveillantes telles que des commutateurs et des points d'accès sans fil non autorisés. CounterACT peut même détecter les appareils sans adresse IP tels que les systèmes de capture de paquets destinés à voler des informations sensibles.

Accès

Enregistrement des invités : permet aux utilisateurs d'accéder au réseau sans compromettre la sécurité de votre réseau interne. Plusieurs options d'enregistrement des invités permettent ainsi de personnaliser leur processus d'admission par rapport aux besoins de votre entreprise.

Accès basé sur les rôles : CounterACT vérifie que les personnes habilitées utilisent les ressources réseau auxquelles elles ont le droit d'accéder. Il se base pour cela sur les répertoires où les rôles sont attribués aux utilisateurs.

Options de contrôle flexibles : contrairement à des produits traditionnels qui emploient des contrôles oppressifs qui perturbent les activités des utilisateurs, CounterACT offre toute une panoplie d'options de mise en œuvre qui vous permettent d'élaborer une réponse personnalisée adaptée à la situation. Traitez les intrusions à faible risque en envoyant à l'utilisateur final une notification ou en corrigeant automatiquement le problème de sécurité. L'utilisateur peut ainsi continuer à travailler pendant la mise en œuvre de cette remédiation (voir Figure 2).

Authentification basée ou non sur la norme 802.1X : Optez pour la norme 802.1X ou d'autres technologies d'authentification telles que LDAP, Active Directory®, RADIUS®, 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.

Serveur RADIUS intégré : un serveur RADIUS intégré facilite 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.

Modèles extensibles

CounterACT a fait ses preuves sur des réseaux comportant plus de 1 000 000 points d'extrémité. Il est disponible dans une vaste gamme de boîtiers physiques ou virtuels afin de s'adapter aux besoins croissants de votre entreprise. Les grands réseaux qui nécessitent davantage de boîtiers peuvent être gérés de manière centralisée par CounterACT Enterprise Manager. Chaque boîtier CounterACT comporte une licence permanente pour un nombre spécifique d'équipements réseau. Pour plus de détails sur la politique de concession de licences, consultez le site www.forescout.com/licensing.

Gestion et contrôle centralisés

CounterACT Enterprise Manager peut être déployé en tant que boîtier physique ou virtuel afin de permettre une gestion et un contrôle centralisés des déploiements de CounterACT. Entreprise Manager supervise les actions et les politiques de CounterACT, et recueille les informations concernant les activités malveillantes détectées au niveau d'un boîtier ainsi que les actions d'identification, de restriction et de correction effectuées par CounterACT. Ces informations peuvent être affichées ou publiées dans des rapports au niveau de la console CounterACT.

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

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 (États-Unis)

Numéro gratuit (depuis les États-Unis) 1-866-377-8771
Tél. (depuis les autres pays) +1-408-213-3191
Assistance technique 1-708-237-6591
Fax 1-408-371-2284

*En janvier 2016.
**Gartner, Inc., « Carré magique Gartner pour le contrôle d'accès au réseau », Lawrence Orans et Claudio Neiva, 10 décembre 2014. Gartner n'avalise aucun fournisseur, produit ou service décrit dans ses publications de recherche, et ne conseille aucunement les utilisateurs de technologies de ne sélectionner que les fournisseurs ayant obtenu les classements les plus élevés ou toute autre désignation. Les publications de recherche de Gartner ne reflètent que les opinions de l'organisme de recherche Gartner et ne sauraient être interprétées comme des déclarations factuelles. Gartner exclut toute garantie, expresse ou implicite, concernant cette recherche, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.