Diagnostic et atténuation en continu

Pour garantir un niveau acceptable et cohérent de confidentialité, d'intégrité et de disponibilité des informations, les services informatiques du gouvernement doivent respecter un nombre croissant de réglementations, directives et normes. L'objectif principal consiste à éliminer les intrusions (confidentialité), protéger les informations sensibles (intégrité) et atténuer l'exposition aux attaques par déni de service (disponibilité).

Le programme CDM (Continuous Diagnostics and Mitigation - Diagnostic et atténuation en continu) constitue une approche dynamique visant à renforcer la cybersécurité des réseaux et systèmes du gouvernement. CDM fournit aux services et agences fédéraux des fonctionnalités et outils qui identifient les risques liés à la cybersécurité sur une base continue, hiérarchisent ces risques en fonction de l'impact potentiel et permettent au personnel chargé de la cybersécurité de minimiser les problèmes les plus importants en premier. Le Congrès a établi le programme CDM afin de fournir une cybersécurité adéquate, rentable et basée sur les risques et d'allouer de manière plus efficace les ressources de cybersécurité.

La caractéristique « en continu » de CDM ne signifie pas nécessairement 24 heures sur 24, 7 jours sur 7 ; elle fait plutôt référence à des évaluations récurrentes intervenant à un intervalle proportionnel à la valeur des informations et au niveau de risque estimé. Les publications fédérales fournissent des directives pour déterminer la fréquence d'évaluation, en fonction de critères tels que la volatilité du contrôle de sécurité, les niveaux d'impact sur le système en termes de fonctions protégées et de faiblesses identifiées. Ces directives définissent la latence d'intervalle de détection comme métrique utilisée pour la mesure et l'audit du niveau acceptable de réponse dans un programme de sécurité CDM.

Défis liés au respect du programme CDM

Au lieu d'une approche basée sur la réaction passive et la documentation, CDM exige une action proactive, centrée sur les données, basée sur les risques. Cela nécessite généralement une modification importante de l'infrastructure de sécurité, car les intégrations de processus et de données doivent franchir les frontières qui séparent les entreprises, les données et les systèmes. Dans le cadre du programme CDM, les processus de collecte de données, de gestion des actifs et des risques se déroulent en continu, et non de manière périodique, dans l'ensemble de l'environnement. Les défis techniques les plus importants pour les services informatiques sont associés à l'intégration et la corrélation du flux continu de données.

Lorsque de nouvelles données sur l'environnement informatique sont disponibles, le système CDM doit ingérer les données et répondre en élevant les seuils et en adaptant les politiques de réseau et les actions de contrôle dans une boucle de rétroaction perpétuelle. Le programme CDM nécessite également la rationalisation des opérations de sécurité coûteuses pour permettre aux hauts fonctionnaires fédéraux de bénéficier d'une bien meilleure visibilité sur l'intégrité de la sécurité de leur organisation et sur les informations de gestion des risques. Une mise en œuvre efficace doit collecter les données des processus en cours, les corréler avec plusieurs facteurs contextuels, agir automatiquement le cas échéant et présenter les problèmes restants par ordre de priorité.

Plateforme de sécurité CounterACT

La plateforme de sécurité CounterACT de ForeScout offre des fonctions de surveillance en temps réel, de contrôle et de correction basée sur des politiques pour les appareils gérés, non gérés et non traditionnels qui forment la base d'une solution CDM. Comment ?

Voir

- Détecter des appareils dès leur connexion à votre réseau sans utiliser d'agents
- Créer des profils et classer des appareils, utilisateurs, applications et systèmes d'exploitation
- Surveiller en continu des appareils, points d'extrémité BYOD et IoT gérés

Contrôler

- Accorder, refuser ou limiter l'accès au réseau en fonction du niveau de sécurité des appareils et de vos politiques de sécurité
- Évaluer et isoler les points d'extrémité malveillants ou à haut risque
- Améliorer le respect des normes et des réglementations du secteur

Orchestrer

- Partager des informations contextuelles avec les systèmes de gestion 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

Points-clés

Visibilité en temps réel. Bénéficiez d'une visibilité en temps réel automatisée sur les points d'extrémité qui se connectent à votre réseau. Détectez même les appareils mouchards furtifs qui n'utilisent pas d'adresse IP.

Gestion active des actifs. Générez un inventaire en temps réel de votre réseau : appareils, matériel, systèmes d'exploitation, applications, niveaux de correctifs, processus, ports ouverts, appareils périphériques, utilisateurs, etc.

Contrôle de l'accès basé sur les politiques. Limitez l'accès au réseau aux utilisateurs et appareils autorisés avec ou sans protocole 802.1X pour la sécurité des ports de commutateurs.

Surveillance continue. Évaluez le niveau de sécurité et de conformité des points d'extrémité en temps réel avant et après leur connexion à votre réseau. Détectez les violations de configuration de point d'extrémité et les comportements malveillants et adaptez la réponse à la gravité de la violation.

Remédiation automatisée. Automatisez la remédiation des points d'extrémité non conformes en mettant automatiquement à jour la configuration des points d'extrémité et les systèmes de protection, correctifs et mises à jour, et en installant, activant ou désactivant les applications ou périphériques.

Intégration au système de sécurité basé sur l'hôte. Améliorez votre connaissance de la situation et la réponse aux incidents en détectant automatiquement et en isolant les points d'extrémité dont les agents HBSS sont manquants ou défaillants. Autorisez, refusez ou limitez l'accès au réseau en fonction des normes de sécurité évaluées par le système HBSS.

Génération de rapports sur la conformité. Produisez des rapports en temps réel qui reflètent votre degré de conformité aux politiques. Réduisez la latence d'intervalle de détection en lançant des analyses de conformité lorsque les hôtes se connectent au réseau, au lieu d'attendre des analyses périodiques.

Exigences en matière de mise en œuvre

Pour adopter le programme CDM, les entreprises doivent investir dans des systèmes de découverte des actifs et de gestion des vulnérabilités en temps réel ; des mécanismes de réponse automatisés et basés sur les informations et une solution permettant la remontée continue de données dans le système de gestion de l'entreprise. En outre, le système doit être déployé facilement dans votre infrastructure informatique existante.

Un système de découverte des actifs et de gestion des vulnérabilités en temps réel doit utiliser une combinaison de techniques passives et actives de découverte et de surveillance pour détecter et créer un profil des appareils connectés au réseau, indépendamment de leur système d'exploitation ou de leur taille. Les techniques passives de découverte permettent de surveiller le trafic afin de découvrir les appareils actifs. Les techniques actives de découverte permettent de sonder le réseau pour traquer les appareils inactifs. Ensemble, elles garantissent une visibilité complète et constante des actifs informatiques. Dès que quelqu'un installe ou reconfigure un appareil sur le réseau, il est possible de détecter le changement et d'analyser l'appareil. Enfin, le système de gestion des actifs doit inclure une fonctionnalité d'évaluation des niveaux de sécurité et des vulnérabilités des points d'extrémité connectés au réseau.

Le mécanisme de réponse automatisé doit pouvoir recevoir les données fournies par le système de découverte des actifs et de gestion des vulnérabilités en temps réel et, sur la base de ces informations et de la connaissance du comportement du point d'extrémité, générer un ensemble de réponses intelligentes conçues pour réduire les risques courus par l'entreprise. La réponse doit être adaptée à la gravité de la violation de conformité à une politique et/ou au comportement du point d'extrémité. Par exemple, le système de réponse doit pouvoir répondre à l'aide d'actions telles que :

- Envoyer une alerte à la personne ou l'équipe de gestion informatique appropriée
- Corriger automatiquement le point d'extrémité ou déclencher un système tiers pour qu'il le corrige
- Limiter l'accès au réseau
- Bloquer l'accès au réseau

Les données sur les actifs et les actions de contrôle automatisé doivent être transmises à d'autres éléments du système CDM afin d'optimiser l'efficacité de l'ensemble du système (voir Figure 1). Par exemple, la liaison entre le système CDM et les systèmes de gestion des événements et des informations de sécurité (SIEM) de l'entreprise permet de garantir que les rapports de conformité générés par le système SIEM sont exacts.

Le système CDM doit aussi transmettre des informations aux systèmes basés sur des agents, tels que les systèmes antivirus, de gestion des correctifs et de gestion des appareils mobiles (MDM) afin de garantir que ces systèmes connaissent les points d'extrémité non gérés connectés au réseau.

Enfin, le système CDM doit pouvoir être déployé facilement et rapidement. Par exemple, le système doit :

- Se déployer dans l'infrastructure réseau existante sans qu'il soit nécessaire de recréer l'architecture du réseau
- S'intégrer avec l'infrastructure réseau existante
- Ne pas se reposer sur le déploiement en ligne ou un autre point de défaillance unique
- Ne pas nécessiter l'installation d'agents de point d'extrémité supplémentaires

Points-clés (suite)

Contrôles des appareils mobiles et sans fil. Détectez et appliquez les contrôles de sécurité sur des appareils mobiles tels que des smartphones et des tablettes. Garantissez la conformité sans fil grâce à l'intégration à l'infrastructure réseau sans fil.

Déploiement sans aucune interruption de l'activité. CounterACT peut être déployé de manière échelonnée, avec un minimum de perturbation et des résultats rapides.

Interopérabilité informatique. Tirez parti de l'intégration à l'infrastructure informatique existante qui comprend par exemple des services d'annuaire, des systèmes de gestion des patchs, la protection des points d'extrémité, l'évaluation de la vulnérabilité et des systèmes SIEM et MDM.

ForeScout CounterACT®, la pierre angulaire d'une solution CDM

ForeScout CounterACT® répond aux exigences CDM et peut constituer le principal composant de votre solution CDM. CounterACT fournit une visibilité en temps réel et un contrôle des points d'extrémité connectés à votre réseau, tels que les smartphones, tablettes, netbooks et autres appareils mobiles d'entreprise et personnels.

CounterACT utilise différentes méthodes de découverte pour classer avec précision les points d'extrémité à l'aide de techniques d'interrogation passives et actives. La solution sans agent de CounterACT lui permet de fonctionner avec différents types de points d'extrémité, gérés et non gérés, connus et inconnus.

CounterACT peut évaluer le niveau de sécurité des points d'extrémité de votre environnement LAN/WAN. Ce point est particulièrement important pour les points d'extrémité personnels BYOD non gérés qui ne sont généralement pas détectés par vos systèmes de gestion des points d'extrémité existants. CounterACT peut évaluer le niveau de sécurité des appareils gérés (ordinateurs connectés au domaine) sans qu'il soit nécessaire de déployer des agents supplémentaires sur ces appareils. C'est un facteur d'une importance cruciale qui contribue à accélérer le déploiement et à simplifier l'utilisation du système CounterACT. CounterACT peut évaluer le niveau de sécurité des appareils BYOD non gérés via l'installation d'un agent léger temporaire. Cet agent prend en charge Windows®, MacOS et Linux. Il peut être automatiquement déployé lorsque l'utilisateur se connecte au réseau et enregistre son identité sur le système. Qu'un agent soit utilisé ou non, CounterACT peut effectuer différentes actions de contrôle de la conformité, notamment la surveillance des logiciels requis, des versions des logiciels et des correctifs, de la configuration des appareils et des vulnérabilités des points d'extrémité. Il s'intègre aux systèmes de réseau, de sécurité basés sur les hôtes et de plateforme d'identité les plus répandus pour fournir en temps réel des informations sur les points d'extrémité et le niveau de sécurité.

ForeScout CounterACT permet d'effectuer une grande variété d'actions de correction des points d'extrémité selon le niveau de sécurité de ces derniers. CounterACT peut indiquer au serveur antivirus de mettre automatiquement à jour un hôte non conforme ou inviter le système de gestion des correctifs à mettre à jour le système d'exploitation de l'appareil, ou encore désactiver le logiciel non autorisé. En outre, CounterACT prend en charge les principaux systèmes SIEM afin de fournir des détails sur la configuration du point d'extrémité et corréler les violations d'accès et de conformité et accélérer la réponse aux incidents. CounterACT inclut des rapports intégrés destinés à vous aider à surveiller le degré de conformité aux politiques, à satisfaire aux obligations d'audit réglementaire et à produire des inventaires en temps réel.

ForeScout CounterACT est commercialisé sous forme de boîtier virtuel ou physique qui se déploie de façon transparente dans votre infrastructure existante, sans nécessiter de modification de l'infrastructure et sans ralentir le fonctionnement de votre réseau. Le boîtier CounterACT s'installe hors bande, ce qui évite la latence ou les risques de faiblesse de réseau. Il peut être administré de manière centralisée afin de gérer dynamiquement des dizaines, des centaines voire même des milliers de points d'extrémité à partir d'une console unique.

ForeScout CounterACT emploie une approche éprouvée de la gestion des risques informatiques. Les appareils qui se connectent à votre réseau sont identifiés, contrôlés, corrigés (si vous le souhaitez) et surveillés en permanence pour garantir une conformité et une protection inégalées. Le moteur de conformité de ForeScout CounterACT détecte les appareils ou utilisateurs qui ne respectent pas votre politique de sécurité et traque les utilisateurs qui ont un comportement à risque et utilisent, par exemple, des applications P2P (Peer-to-Peer), des clés USB, des smartphones ou effectuent d'autres activités non autorisées. Les ordinateurs et/ou utilisateurs non conformes seront affichés sur la console principale, en indiquant notamment le motif de la non-conformité et des détails tels que l'emplacement de l'appareil.

Enfin, CounterACT aide les responsables informatiques à obtenir des métriques de latence d'intervalle de détection acceptables en s'intégrant avec des analyseurs de conformité afin d'ajouter une fonctionnalité d'analyse basée sur les événements. Cette intégration permet à CounterACT de déclencher l'analyseur de conformité lorsqu'un hôte se connecte au réseau. L'ajout de l'analyse basée sur les événements permettra d'améliorer considérablement votre métrique de latence d'intervalle de détection. ForeScout CounterACT s'intègre à la plupart des analyseurs d'évaluation de la vulnérabilité les plus courants tels que Tennable® Nessus, BeyondTrust® Retina et Qualys®, et d'autres intégrations sont en cours de développement.

Réduire la complexité et augmenter l'efficacité

Auparavant, les responsables de la sécurité informatique avaient tendance à contrecarrer chaque risque à l'aide d'une solution technique spécifique. La conformité aux normes réglementaires était obtenue grâce à des contrôles spécialisés. Cela garantissait un niveau acceptable de sécurité et de conformité à court terme. Aujourd'hui, nous savons que les solutions de sécurité autonomes augmentent la complexité, et que la complexité augmente les risques ainsi que les coûts d'administration. Le manque d'interconnectivité entre les contrôles informatiques constitue un défi majeur qui empêche les équipes informatiques de gérer efficacement les risques. Il en résulte également une mauvaise connaissance de la situation et des informations exploitables limitées qui entravent la détection rapide des menaces et l'atténuation des risques.

ForeScout CounterACT vous aide à résoudre ce problème. CounterACT s'intègre aux systèmes existants afin de créer un système de surveillance continue réactif et précis réduisant la complexité pour vous garantir une plus grande efficacité. Ainsi, le système garantit une visibilité en temps réel, une inspection approfondie des points d'extrémité, une surveillance continue, des mesures correctives automatisées, une intégration à d'autres systèmes de gestion de la sécurité, un déploiement rapide et un faible coût total de possession.

Figure 1 : État souhaité : CounterACT de ForeScout garantit une visibilité en temps réel sur votre réseau et le partage bidirectionnel des informations avec l'infrastructure opérationnelle et de sécurité existante.

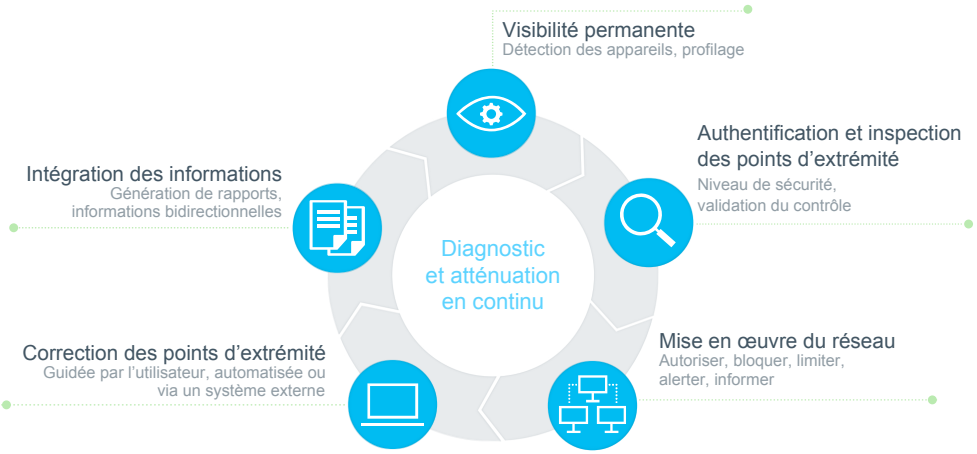

Figure 2 : La plateforme d'automatisation de la sécurité intelligente de ForeScout fournit une visibilité en temps réel et un contrôle automatisé.

Critères d'une solution de diagnostic et d'atténuation en continu[1]		ForeScout CounterACT
Découverte et classification des actifs	Découvrez les équipements non autorisés ou non gérés connectés à un réseau, détectez les configurations logicielles non autorisées ou non gérées au sein des actifs informatiques d'un réseau.	CounterACT détecte en temps réel les appareils présents sur le réseau et gère une base de données complète des actifs matériels et logiciels. Il est possible de faire des recherches dans l'inventaire et de l'organiser en fonction de différents attributs matériels et logiciels. Des inventaires peuvent être générés.
Évaluation	Il est essentiel d'évaluer le niveau de sécurité des points d'extrémité pour obtenir un inventaire précis et actualisé des logiciels et pouvoir suivre et contrôler efficacement les vulnérabilités des logiciels et les paramètres de configuration de la sécurité.	CounterACT peut évaluer le niveau de sécurité des points d'extrémité de votre environnement LAN/WAN. Ce point est particulièrement important pour les points d'extrémité personnels BYOD non gérés qui ne sont généralement pas détectés par vos systèmes de gestion des points d'extrémité existants. CounterACT peut effectuer différentes actions de contrôle de la conformité, notamment la surveillance des logiciels requis, des versions des logiciels et des correctifs, de la configuration des appareils et des vulnérabilités des points d'extrémité. Il s'intègre à d'autres agents/outils et analyseurs de vulnérabilité basés sur les hôtes afin d'obtenir des informations de conformité supplémentaires.
Authentification et contrôle d'accès	Interdisez, supprimez et limitez les connexions/accès au réseau non autorisés pour empêcher les attaquants d'exploiter les limites internes et externes du réseau et de lancer une attaque de type pivot pour obtenir un accès plus complet au réseau et/ou capturer des données véhiculées ou stockées sur le réseau. Gérez l'accès aux comptes, les comportements liés à la sécurité, les informations de connexion et l'authentification.	CounterACT peut bloquer ou restreindre l'accès aux appareils non autorisés ainsi qu'à ceux qui deviennent non conformes alors qu'ils sont connectés au réseau. CounterACT est piloté par les événements et réévalue un point d'extrémité dès que son système d'exploitation est modifié.
Atténuation et mise en œuvre de mesures correctives automatisées	Evitez que votre système ne soit piraté en le concevant de façon à minimiser ses faiblesses afin de réduire la surface d'attaque et d'augmenter l'effort que doivent fournir les pirates pour atteindre les parties du système qui restent vulnérables.	Lorsque des violations de conformité sont détectées, CounterACT peut répondre en fonction de la gravité de la violation en envoyant simplement une alerte ou une notification au personnel informatique ou au moyen d'une remédiation automatique, par exemple en mettant en quarantaine ou en bloquant les points d'extrémité non conformes. Il peut aussi interagir avec un système tiers, par exemple un système de gestion des patchs.
Connaissance de la situation	Il est essentiel de connaître l'état précis et actualisé des points d'extrémité pour permettre l'identification et le contrôle efficace d'éventuels problèmes de sécurité ainsi que la génération de rapports.	CounterACT permet d'avoir une connaissance approfondie de la situation grâce à l'identification des points d'extrémité connectés au réseau et à l'intégration à d'autre systèmes de gestion de la sécurité, tels que des produits de gestion du cycle de vie des points d'extrémité, des systèmes de gestion des actifs, des bases de données, des solutions de gestion des événements et des informations de sécurité (SIEM), des systèmes d'évaluation de la vulnérabilité et des antivirus, afin de disposer d'informations en temps réel sur les points d'extrémité et de connaître l'état de sécurité du réseau. En outre, il prend en charge les systèmes de gestion des événements et des informations de sécurité (SIEM) pour fournir des détails sur la configuration des points d'extrémité et corréler les violations d'accès et de conformité.

[1]Référence « Critères d'une solution de diagnostic et d'atténuation en continu »
https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f154da08471898c2e7a9ab05595c3df6

Architecture ControlFabric® de ForeScout

L'intégration entre ForeScout CounterACT et votre solution CDM n'est qu'une des nombreuses intégrations de systèmes d'information qui tirent parti de l'architecture ControlFabric de ForeScout. ControlFabric est une technologie ouverte qui permet à ForeScout CounterACT et aux autres solutions d'échanger des informations et de minimiser plus efficacement une grande variété de problèmes de sécurité. Pour en savoir plus, visitez le site www.forescout.com/controlfabric.

Relevez le défi ForeScout

Indiquez-nous la solution ForeScout qui vous convient, et nous organiserons une évaluation sur site gratuite.

À propos de ForeScout

ForeScout Technologies, Inc. donne une nouvelle dimension à la sécurité grâce à la visibilité. 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. Plus de 2 000 clients répartis dans plus de 60 pays renforcent la sécurité de leur réseau et leur conformité grâce aux solutions ForeScout*.

Pour en savoir plus, visitez le site www.forescout.com.

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