



GUIDE D'ÉVALUATION DES PRODUITS

NAC Products
Insight's Technology
Assessment Services (TAS)
team has evaluated the
following products.

- Symantec™ Network Access Control
- McAfee® Policy Enforcer
- Vernier Networks

CONTRÔLE DE L'ACCÈS AU RÉSEAU

De nos jours, les frontières d'un réseau d'entreprise sécurisé sont en train de devenir de moins en moins définitives. L'ancienne stratégie pour uniquement protéger le périmètre de votre réseau ne s'applique plus à l'heure actuelle, puisque les employés utilisent de plus en plus des dispositifs sans fil. Ces terminaux peuvent bien fonctionner à l'abri du LAN protégé au sein de votre entreprise durant les heures de travail, cependant, le soir, ceux-ci s'attachent à un réseau étrange et non sécurisé aux domiciles des employés, ou dans des emplacements publics WiFi sensibles. Le portable typique n'a aucune protection pare-feu et celui-ci est vulnérable lorsqu'il s'agit des virus ou des attaques malveillantes. Lorsque les utilisateurs font la reconnexion au LAN d'entreprise, les vers et les maliciels recueillis auparavant commencent à perturber le réseau « sécurisé ». Les ordinateurs qui contiennent des correctifs logiciels Microsoft® Windows® obsolètes peuvent également contribuer à la vulnérabilité du LAN d'entreprise. Les correctifs sont généralement offerts comme téléchargements mensuels à partir du site web Microsoft. Par contre, si l'utilisateur ne fait aucun effort pour les télécharger, celui-ci pourra s'avérer vulnérable à plusieurs menaces.

Aujourd'hui, le contrôle d'accès au réseau est l'un des éléments prioritaires de toute entreprise, car les départements TI sont toujours en train d'empêcher les ordinateurs et les portables obsolètes, vulnérables et infestés de virus, à accéder au réseau corporatif. Microsoft et Cisco disposent des solutions propriétaires qui sont toujours en pleine évolutivité, mais si vous êtes à la recherche d'une solution libre et autonome pour l'encadrer au sein de votre environnement, il faudra probablement consulter les options provenant de Symantec, McAfee, Vernier Networks, Mirage Networks, Caymas Systems et d'autres.

FACTEURS CLÉ

Infrastructure

L'accès au réseau peut être contrôlé par l'entremise de l'infrastructure 802.1x (si celle-ci existe déjà); celle-ci communique au commutateur Ethernet ou au point d'accès sans fil dans le but de valider l'utilisateur à un serveur RADIUS bien avant que celui-ci puisse accéder au réseau. Lorsque le LAN 802.1x n'existe pas, il faut avoir un dispositif spécial uniquement lié à cette tâche. Ces solutions typiquement contiennent un serveur de politiques, un contrôleur d'accès et, dépendamment de la solution, un client dont le terminal a été chargé.

Politiques

Les politiques d'accès du serveur peuvent établir si l'accès aux utilisateurs est bloqué, annulé ou autorisé. Dès que ceux-ci peuvent accéder au serveur, les utilisateurs auront l'accès complet au réseau, ou seulement à certaines applications. Votre entreprise devra développer ces politiques, en se basant sur l'identité des utilisateurs et de savoir comment ceux-ci auront accès au réseau.

Atténuation de systèmes

Lorsque les systèmes des utilisateurs ont été bloqués, vous devez être en mesure de leur permettre à mettre à jour leurs systèmes ou de résoudre toute problématique liée à la politique violée – autrement, vous risquez de vous trouver avec plusieurs ordinateurs mal performants et utilisateurs frustrés qui essayent à accéder au réseau.



FONCTIONNALITÉS CLÉ

- **Dispositif de scannage non géré** – Scannage et blocage non seulement des dispositifs gérés et qui sont déjà connus par vous, mais également des dispositifs non-gérés (appartenant à des visiteurs, fournisseurs ou partenaires). Lorsqu'un dispositif non géré est détecté, la plupart des solutions NAC offrent à l'utilisateur l'option de télécharger une application Web qui scanner le système rapidement pour s'assurer que les politiques d'entreprise sont respectées en conséquence.
- **Pare-feu** – Une approche approfondie en ce qui a trait à la sécurité, à l'intention des utilisateurs. Au lieu de protéger le périmètre de votre réseau, les pare-feux des ordinateurs empêchent tout attaque de se propager à travers chaque système, en provenance du pare feu d'entreprise. Ceux-ci sont également essentiels pour les télétravailleurs qui utilisent des portables.
- **Surveillance des vulnérabilités** – Surveillance continue des points extrêmes. Les solutions choisies par le client peuvent contenir un module IDS/IPS qui détectera, comptabilisera et bloquera chaque composant de nature hostile.
- **Équilibrage de charge et basculement** – Les environnements à volume élevé peuvent nécessiter des capacités d'équilibrage de charge et de basculement afin de fournir aux utilisateurs un passage optimisé.
- **Auto conversion** – Accès limité des dispositifs bloqués vers un segment sécurisé du réseau d'où le système d'exploitation et les définitions de virus seront mis à jour, ainsi éliminant la participation du département des TI.
- **Rétention** – Lorsqu'un vers infiltre votre réseau, celui-ci sera mobilisé ou éloigné du réseau jusqu'à son élimination.

CONCLUSION

Hélas, plusieurs départements TI ont essayé de contrôler l'usage de leurs ordinateurs et la plupart ont échoué. Les employés feront toujours usage des portables de l'entreprise pour affaires personnelles et à cause de cela, les malicieux ont une bonne chance de retrouver le chemin vers votre réseau. L'inspection et la limitation des problématiques avant que les dispositifs puissent se connecter à votre réseau sont des facteurs critiques. La solution liée au contrôle de l'accès au réseau sélectionnée jouera un rôle primordial pour vous, visant à protéger la sécurité de votre réseau et renforcer les politiques en matière de sécurité informatique.

Nos directeurs de comptes spécialisés pourront s'entretenir à propos de vos besoins en matière de solutions NAC, et notre soutien à la clientèle saura fournir les ressources techniques à cette fin. Et lorsque vous faites face à un éventail de problèmes qui peuvent survenir en raison de vos efforts pour contrôler l'accès à votre réseau, Insight peut être d'une valeur inestimable.

Pour de plus amples renseignements veuillez contacter votre directeur de comptes ou l'équipe du Service d'évaluation technologique d'Insight au tas@insight.com