SONICWALL®

CE QUE LES ADMINISTRATEURS DOIVENT RECHERCHER QUAND ILS ACHÈTENT UNE SOLUTION DE SÉCURITÉ DES TERMINAUX

Nouvelle perspective sur les défis de la protection des terminaux

Résumé

Les administrateurs se heurtent aux défis posés par les produits de sécurité des terminaux. Cet article se penche sur plusieurs de ces défis persistants, dont :

- l'exécution et le maintien de la sécurité
- les menaces chiffrées et évoluées
- les alertes et les mesures correctives

Introduction

La gestion et la sécurité des terminaux sont essentielles dans un environnement de cybercriminalité aussi changeant que le nôtre. Les utilisateurs finaux se connectent et sortent continuellement du réseau avec leurs terminaux. Dans le même temps, ces terminaux sont le champ de bataille des menaces d'aujourd'hui. De plus en plus, les menaces chiffrées atteignent les terminaux sans être contrôlées, les ransomwares prolifèrent et le vol d'identité persiste sournoisement. Cependant, la menace toujours plus grande que représentent les ransomwares et autres attaques par logiciels malveillants a prouvé que les solutions de protection des clients ne peuvent se mesurer uniquement en termes de conformité des terminaux.

La protection des terminaux et ses défis

Des produits de sécurité des terminaux sont commercialisés depuis de nombreuses années, mais les administrateurs sont confrontés aux difficultés suivantes :

- maintenir les produits de sécurité à jour
- appliquer les règles et garantir la conformité
- obtenir des rapports
- faire face aux menaces pénétrant à travers les canaux chiffrés
- comprendre les alertes et les mesures correctives
- gérer les licences
- stopper les menaces évoluées tels que les ransomwares

Maintenir les produits de sécurité à jour

Les administrateurs doivent s'assurer que les terminaux gérés exécutent la version appropriée des logiciels de sécurité installés, conformément aux règles de conformité.

Pour contrer les attaques émergentes, les administrateurs de la sécurité réseau ont besoin de terminaux gérés à même d'évaluer le niveau de sécurité et de rendre compte de leur état en continu.

Certains administrateurs ont besoin de stopper le trafic est-ouest entre leurs centres de données, qui représente bien souvent la majorité du trafic entre leurs commutateurs. Ils doivent pouvoir mettre un dispositif en quarantaine localement s'il n'est plus conforme ou est infecté. Dans ces cas, le pare-feu doit bloquer son accès à Internet et au réseau local, limitant ainsi les chemins réseau aux emplacements de quarantaine appliqués par le pare-feu.

De plus, les administrateurs de la sécurité doivent faire en sorte que toutes les données entre le client unifié et la console de gestion centralisée ne puissent être falsifiées pendant le transit, afin d'assurer l'intégrité des données.

Appliquer les règles et garantir la conformité

Si le terminal n'est pas conforme aux règles, les administrateurs doivent pouvoir l'empêcher d'utiliser les services UTM pour laisser passer le trafic à travers le pare-feu. Les utilisateurs finaux ont également un rôle important à jouer dans la sécurité des terminaux. Ils utilisent les ordinateurs portables et autres terminaux de l'entreprise pour faire leur travail. Ils doivent donc savoir immédiatement si un logiciel ou un comportement malveillant est détecté, afin de pouvoir prendre les mesures nécessaires ou ouvrir un ticket.

Obtenir des rapports

Dans certains cas, les administrateurs peuvent gérer plusieurs pare-feux, mais leurs utilisateurs sont configurés dans un seul pool. Ils doivent pouvoir obtenir une authentification unique (SSO) provenant de toute console d'administration de pare-feu ou de gestion de la sécurité pour gérer les règles clients. Dans le même temps, les réglementations de conformité exigent bien souvent que tous les rôles administratifs respectent le principe du moindre privilège, de sorte que la gestion des clients unifiés dispose d'un contrôle d'accès à base de rôles suffisant pour l'accès privilégié. Par exemple, cela peut se limiter à deux rôles, l'un ayant un accès en lecture/écriture et l'autre un accès en lecture seule.

Faire face aux menaces pénétrant à travers les canaux chiffrés

De plus en plus, les applications Web sont sécurisées via des canaux chiffrés comme HTTPS et les logiciels malveillants recourent au chiffrement pour contourner l'inspection reposant sur le réseau. Il est donc impératif de permettre le filtrage applicatif du trafic SSL/TLS (DPI-SSL). Toutefois, cela n'est pas facile à mettre en œuvre sans le déploiement massif de certificats SSL/TLS fiables sur tous les terminaux pour éviter les problèmes d'expérience utilisateur et de sécurité. Cela nécessite un mécanisme sous-jacent pour distribuer et gérer les certificats et la manière dont les navigateurs leur font confiance.

Comprendre les alertes et les mesures correctives

Les utilisateurs finaux sont généralement moins conscients des risques de sécurité que les professionnels de la sécurité. À ce titre, ils auraient besoin que leur plate-forme de protection des terminaux les alerte du profil de risque changeant lorsqu'ils se déplacent avec leur ordinateur et les conseille sur la façon de se protéger.

Par exemple, une alerte peut être générée à partir d'un client unifié ou d'un logiciel tiers, ou fournir une redirection vers une source externe, telle qu'une page Web.

Pour remédier rapidement à toute infraction aux règles de l'entreprise, l'accès à des informations d'auto-assistance peut être utile pour les utilisateurs finaux et le service informatique. Si le dispositif d'un utilisateur n'est plus conforme aux règles et que cet utilisateur est mis en quarantaine, ce dernier a également besoin de conseils sur les actions requises pour rétablir la conformité.

Gérer les licences

Les administrateurs doivent s'assurer que tout logiciel de sécurité des terminaux acheté est automatiquement mis à jour dans leur interface de gestion, afin d'être sûrs que les terminaux disposent des bonnes licences. Par exemple, toutes les informations de licence relatives à un client doivent faire l'objet d'un contrôle et d'un stockage centralisés. En cas d'achat d'une nouvelle licence, un signal doit être envoyé à la gestion centralisée du client unifié pour l'alerter et démarrer les droits de licence logicielle.

Certains administrateurs doivent, à intervalles réguliers, générer des rapports de conformité pour toutes les licences tierces déployées afin de payer leurs partenaires.

Stopper les menaces évoluées tels que les ransomwares

Les approches traditionnelles engendrent parfois le non-respect des exigences administratives. L'approche basée sur les signatures des technologies antivirus traditionnelles, longtemps combattue, a échoué face au rythme de développement des nouveaux logiciels malveillants et à leurs techniques d'évasion, ce qui a fait ressortir la nécessité d'adopter une approche différente de la protection des clients. Une telle protection doit non seulement fournir des moteurs de détection des menaces évoluées, mais aussi prendre en charge une stratégie de défense multicouche au niveau des terminaux.

L'une des principales limites des solutions d'aujourd'hui (connues sous le nom de Enforced AV Client) réside dans le fait que le développement est spécifique à un tiers et qu'il a été intégré dans les offres de ce tiers. Les administrateurs ont besoin d'un modèle plus ouvert leur permettant d'ajouter assez rapidement des modules de sécurité supplémentaires si l'entreprise ou l'industrie l'exige.

Conclusion

En raison de l'utilisation accrue des terminaux comme vecteurs de cyberattaques, les professionnels de la sécurité doivent prendre des mesures en vue de protéger les terminaux. En outre, avec la prolifération du télétravail, de la mobilité et du BYOD, il est absolument nécessaire d'offrir une protection cohérente à tous les clients, où qu'ils se trouvent.

Les administrateurs de la sécurité doivent évaluer les solutions de terminaux en tenant compte des exigences du monde réel.

Pour en savoir plus, lisez notre dossier « La sécurité des terminaux adaptée à votre entreprise » ou rendez-vous sur www.sonicwall.com/capture-client.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com