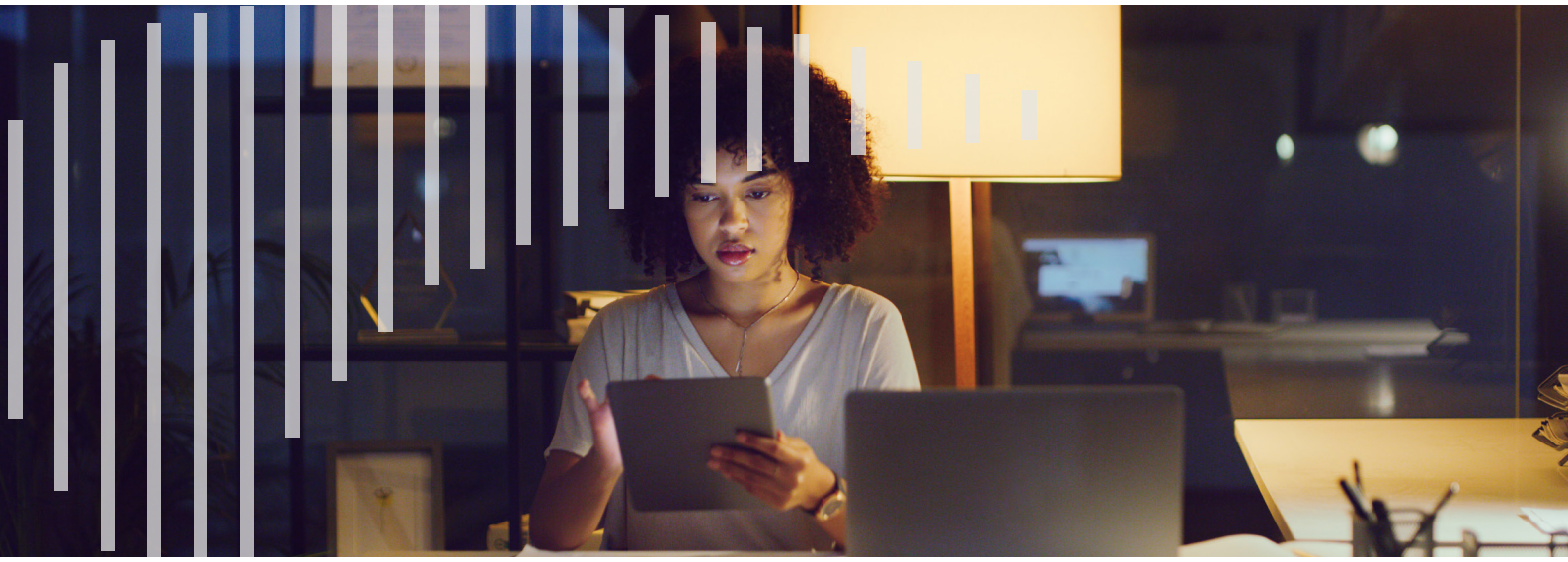

PRÉSENTATION

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 :

- Mise en œuvre et maintien de la sécurité
- Menaces chiffrées et évoluées
- Gestion des alertes et mesures de correction
- Création et gestion de règles
- Visibilité de la santé des locataires
- Vulnérabilités sans correctif

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. La menace en constante expansion que représentent les ransomwares et autres attaques par logiciels malveillants montre que l'efficacité des solutions de protection client ne se mesure pas à la simple conformité des terminaux.

La difficulté augmente encore lors d'une gestion mutualisée, que ce soit au sein d'une seule organisation ou pour plusieurs clients. Celle-ci requiert souvent différentes règles et configurations en fonction du groupe d'utilisateurs, de l'appareil et du lieu.

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 les mesures de conformité Web
- Obtenir des rapports et gérer les accès
- Détecter les menaces empruntant des canaux chiffrés
- Comprendre les alertes et les mesures correctives
- Gérer les licences
- Bloquer les menaces évoluées telles que les ransomwares
- Ne pas savoir où se situent les vulnérabilités critiques
- Connaître la santé des locataires et gérer des règles globales

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 afin d'évaluer en continu le niveau de sécurité et de rendre compte de leur état de manière régulière.

Certains administrateurs doivent 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, afin d'assurer l'intégrité des données, 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.

Appliquer les règles et les mesures de conformité Web

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.

Lorsque les employés travaillent en dehors du bureau, il est possible d'exécuter les règles d'utilisation d'Internet de l'entreprise en intégrant un filtrage de contenu ou Web à la solution de sécurité. Celui-ci est vital pour bloquer l'accès aux sites malveillants connus, mais il est également important lorsqu'il s'agit de bloquer les adresses nuisant à la productivité ou encore les sites réservés aux adultes. Si les utilisateurs chargent des données vidéo sur des serveurs locaux par VPN, une restriction de la bande passante peut être envisagée pour les sites à grands volumes de données.

Obtenir des rapports et gérer les accès

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. La gestion des clients unifiés devrait donc disposer 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.

Menaces empruntant des 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 l'inspection approfondie des paquets du trafic SSL/TLS (DPI-SSL). Toutefois, pour y parvenir sans entraver l'expérience utilisateur et la sécurité, le déploiement massif de certificats SSL/TLS fiables sur tous les terminaux s'avère indispensable. 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.

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.

Bloquer les menaces évoluées telles que les ransomwares

Les approches traditionnelles engendrent parfois le non-respect des exigences administratives. L'ancienne approche basée sur les signatures des technologies antivirus traditionnelles est obsolète face au rythme de développement des nouveaux logiciels malveillants et des techniques d'évasion, et ne fait que souligner la nécessité d'adopter une approche différente de la protection des terminaux. 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, incluant l'intégration à un environnement de sandboxing.

L'une des principales limites des solutions existantes (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 de déployer assez rapidement des modules de sécurité supplémentaires si l'entreprise ou l'industrie l'exige.

Ne pas savoir où se situent les vulnérabilités critiques

Le développement massif des applications métier a entraîné une croissance exponentielle des menaces liées aux vulnérabilités de ces dernières. Rien qu'en 2019, un grand nombre de vulnérabilités d'une criticité supérieure à 9,0 selon le système CVSS ont donné du fil à retordre aux équipes informatiques et créé de nombreuses failles. Les entreprises doivent avoir un moyen d'identifier le nombre et la classification des vulnérabilités afin de pouvoir envisager soit une correction, soit la désinstallation des applications dangereuses.

Connaître la santé des locataires et gérer des règles globales

Dans les grandes entreprises, il n'est pas rare d'avoir à gérer un nombre important de terminaux, ou une solution de sécurité des terminaux couvrant plusieurs régions, groupes d'utilisateurs ou types d'appareils. souvent même, c'est les deux. La réussite de la démarche dépend de la rapidité avec laquelle les entreprises peuvent créer un nouveau locataire et de la disponibilité d'un tableau de bord global offrant une bonne visibilité de la santé des locataires. Les administrateurs se trouvant dans ce genre de situations doivent pouvoir modifier rapidement une règle globale associée à des locataires ou des groupes. Les fournisseurs de services (de sécurité) gérés (MSP et MSSP) doivent également pouvoir créer librement des règles personnalisées pour les locataires qui ne sont pas concernés par les modifications de la règle globale. La fonction de gestion devrait leur fournir des statistiques de haut niveau sur les infections et les vulnérabilités sans qu'ils aient à zoomer sur chaque locataire.

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, 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 « Fitting endpoint security to your organization » (Adapter la sécurité des terminaux à votre organisation) ou rendez-vous sur www.sonicwall.com/capture-client.

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

ExecBrief-WhatAdminNeed-A4-VG-3575