7 problèmes de sécurité modernes

que vous pouvez solutionner grâce à la gestion du trafic chiffré

L'utilisation des communications chiffrées SSL/TLS est en pleine croissance, il en va de même des risques dus aux menaces cachées. En réponse, les entreprises déploient des pare-feu de nouvelle génération (NGFW), des systèmes de prévention des intrusions (IPS), des technologies contre les logiciels malveillants et d'autres solutions. Mais ces mesures ne peuvent pas découvrir les logiciels malveillants à l'intérieur du trafic chiffré, sans ralentir le réseau, résultant à davantage de complexité et à des coûts plus élevés.

Seules les solutions de gestion du trafic chiffré (ETM) de Blue Coat accélèrent efficacement les capacités de votre infrastructure de sécurité réseau tout en gérant le trafic SSL/TLS

Découvrez comment les solutions ETM de Blue Coat peuvent vous aider à relever les défis dans votre infrastructure de sécurité réseau :

1. Une visibilité réduite sur le trafic chiffré, favorisant la fuite et l'exfiltration de données
2. Sandboxing incomplet incapable d'analyser toutes les menaces
3. Protection inadéquate contre les intrusions qui ne bloque pas les attaques
4. Faibles capacités de recherche de la preuve incapables de surveiller et de bloquer les attaques sophistiquées
5. Déchiffrement SSL décentralisé ajoutant de la complexité et des coûts
6. Inspection et déchiffrement du trafic SSL qui vous ralentissent considérablement
7. Se conformer aux demandes croissantes concernant la conformité et la confidentialité des données

1. Visibilité réduite sur le trafic chiffré, favorisant la perte et l'exfiltration de données

Problèmes

- Le trafic SSL/TLS va au-delà du trafic HTTPS/Web/Port 443, en effet, les applications cloud et mobiles innovantes, ainsi que les logiciels malveillants sophistiqués, utilisent de plus en plus des ports différents et non standard.
- Les outils de sécurité de protection contre la fuite et le vol de données (DLP), n'ont aucune visibilité sur le trafic SSL/TLS, ce qui entraîne un risque important, et des problèmes de non-conformité aux politiques et réglementations.

Solution

- Les solutions ETM Blue Coat suppriment les angles morts en visualisant automatiquement l'ensemble du trafic SSL/TLS, indépendamment du port, de l'application ou du service, sans configuration ni règles complexes.
- Les solutions ETM Blue Coat alimentent intelligemment des solutions comme les technologies DLP avec des flux chiffrés et non chiffrés leur permettant de faire leur travail de manière plus efficace pour surveiller les mouvements de données critiques.

2. Sandboxing incomplet incapable d'analyser toutes les menaces

Problèmes

- Les solutions de sandboxing et de protection contre les logiciels malveillants n'ont aucune visibilité sur le trafic chiffré et ne peuvent pas inspecter, isoler et supprimer les logiciels malveillants cachés dans le SSL/TLS.
- Votre retour sur investissement des solutions de sandboxing est entravé par le trafic SSL/TLS. En effet, ces outils sont moins efficaces pour arrêter les menaces persistantes avancées modernes (APT).

Solution

- Les solutions ETM de Blue Coat identifient et contrôlent intelligemment le trafic SSL/TLS et alimentent plusieurs dispositifs de sécurité avec les flux chiffrés et/ou déchiffrés, afin d'offrir une analyse et une prévention complètes contre les menaces.
- Blue Coat SSL Visibility Appliance augmente de manière significative l'efficacité des solutions de sandboxing et de protection contre les logiciels malveillants en détectant et en isolant les APT, tout en préservant et en étendant le retour sur investissement, par l'amélioration de la visibilité et de l'analyse de menaces précédemment cachées.

3. Protection inadéquate contre les intrusions qui ne bloque pas les attaques

Problèmes

- La plupart des solutions de détection et prévention des intrusions (IDS/IPS) ne voient pas et n'inspectent pas le trafic SSL/TLS, les rendant ainsi moins efficaces en termes de sécurisation des réseaux modernes.
- Étant donné la croissance rapide des communications malveillantes Commande et contrôle (C&C) utilisant le SSL, les technologies IDS/IPS sont incapables de voir le trafic entrant et sortant contenant des logiciels malveillants et des APT dangereux.

Solution

- Les solutions Blue Coat ETM permettent aux IDS/IPS de trouver et d'éliminer les menaces avancées cachées au sein du trafic SSL/TLS sans altérer les performances.
- La solution Blue Coat SSL Visibility Appliance préserve et augmente le retour sur investissement de vos solutions IDS/IPS, en apportant une nouvelle visibilité et une analyse du trafic réseau précédemment caché et des menaces potentielles.

4. Faibles capacités de recherche de preuves sur le réseau incapable de surveiller et de bloquer les attaques sophistiquées

Problèmes

- Les outils de recherche de preuves réseau ne peuvent pas voir, analyser ou répondre aux menaces cachées dans le trafic SSL/TLS, entraînant d'importants angles morts dans la sécurité et une faible réponse aux incidents.

Solution

- Les solutions Blue Coat ETM permettent une identification rapide du réseau suspect et du comportement de l'attaquant, et la résilience des actifs du réseau compromis indépendamment de l'utilisation du SSL/TLS.
- La solution SSL Visibility Appliance de Blue Coat préserve et augmente le retour sur investissement de vos solutions de sécurité réseau et recherche de preuves, en apportant une nouvelle visibilité, une analyse complète et une réponse plus rapide par rapport au trafic réseau précédemment caché et aux menaces avancées.

5. Déchiffrement SSL décentralisé ajoutant de la complexité et des coûts

Problèmes

- L'intégration d'un nouvel outil de gestion du trafic SSL/TLS nécessite souvent l'ajout de dispositifs de sécurité dupliqués ou de matériel supplémentaire, afin de répondre aux besoins de performance du réseau.
- Cette situation peut être onéreuse et complexe car elle nécessite une refonte complète de l'infrastructure de sécurité réseau.

Solution

- La solution Blue Coat SSL Visibility Appliance peut évoluer pour gérer le trafic chiffré sur différents segments réseau, avec des dispositifs actifs et passifs sur chaque segment.
- Grâce à l'utilisation de politiques intelligentes, la solution Blue Coat SSL Visibility Appliance propose un trafic SSL inspecté, déchiffré ou non aux appliances de sécurité existantes telles que les DLP, NGFW, IPS, d'analyse des logiciels malveillants, de recherche de preuve, et plus encore.
- Les appliances de sécurité existantes bénéficient d'une nouvelle visibilité très utile sur les flux SSL/TLS, et sur les menaces potentielles cachées, sans altérer la performance réseau, et sans nécessiter de mise à niveau significative et coûteuse de matériel.

6. Inspection et déchiffrement du trafic SSL qui vous ralentit vraiment

Problèmes

- Les dispositifs de sécurité capables de voir et d'inspecter le trafic SSL comme les NGFW et les IPS souffrent d'une dégradation significative de leurs performances, pouvant aller jusqu'à 80 %, une fois que le trafic SSL est « activé ».*
- L'enquête duGartner confirme ce fait et indique que « moins de 20 % des entreprises possédant un pare-feu, une IPS ou une appliance de gestion des menaces unifiée (UTL) déchiffrent le trafic SSL entrant ou sortant. »*

Solution

- Blue Coat SSL Visibility Appliance prend en charge jusqu'à 9 Gbit/s de données SSL et 800 000 sessions SSL simultanées, pour répondre aux besoins des entreprises les plus exigeantes.
- La conception « Déchiffrer une fois et en alimenter plusieurs » s'adapte pour proposer intelligemment du trafic chiffré et déchiffré aux différents outils de sécurité comme les NGFW et les IPS, réduisant ainsi de manière significative le temps de configuration et d'exploitation.
- Blue Coat SSL Visibility Appliance préserve et augmente le retour sur l'investissement de vos solutions NGFW/IPS, en les améliorant grâce à une nouvelle visibilité et une analyse du trafic et des menaces précédemment cachés.

7. Se conformer aux demandes croissantes concernant la conformité et la confidentialité des données

Problèmes

- L'inspection et le déchiffrement de certains types de trafic SSL/TLS vont à l'encontre des réglementations concernant la conformité et la confidentialité des données.
- Ne pas inspecter ni déchiffrer le trafic SSL/TLS entraîne un risque dû aux logiciels malveillants et innovants qui se cachent dans le trafic chiffré
- Une approche de déchiffrement « tout ou rien » est irréaliste et irréalisable

Solution

- Les solutions Blue Coat ETM permettent une inspection et un déchiffrement sélectifs, basés sur un moteur de politiques complet. De cette manière, vous pouvez déchiffrer le trafic inconnu et suspect, tout en autorisant le « bon » trafic de confiance à passer dans son état chiffré.
- Le service Blue Coat Host Categorization utilise l'incomparable base de données Global Threat intelligence pour obtenir une analyse et une catégorisation mises à jour des menaces, du trafic et des sites internet, vous assurant ainsi une sécurité réseau réactive, utilisant les dernières normes de sécurité.
- Les solutions Blue Coat ETM vous assurent la confidentialité et la conformité des données afin que tout le monde soit satisfait, qu'il s'agisse des équipes RH, juridique et de conformité.

Résolvez vos problèmes de sécurité avec Blue Coat ETM

Lors de la préparation de votre stratégie ETM, gardez à l'esprit que toute solution que vous mettez en œuvre doit vous offrir une visibilité complète sur le trafic SSL/TLS, tout en complétant (et non en remplaçant) votre infrastructure sécurité existante. Cette solution doit associer de manière économique une politique simple de contrôle et une croissance rapide de plusieurs composantes : croissance de l'entreprise, croissance de l'adoption dans l'entreprise et, bien sûr, la croissance rapide des flux chiffrés C'est pourquoi Blue Coat ETM s'adapte simplement et efficacement pour résoudre les problèmes causés par le trafic SSL/TLS.

Pour en savoir plus sur les fonctionnalités de base et les bénéfices de Blue Coat ETM sur **bluecoat.com/uncoverssl**

Copyright © 2016, Blue Coat Systems, Inc. Tous droits réservés. Blue Coat et le logo Blue Coat sont des marques déposées de Blue Coat Systems, Inc.