Le service de prévention des intrusions de Zscaler

zscaler™

Les systèmes de prévention d'intrusion (IPS) sont un élément clé d'une bonne stratégie de défense renforcée. Il est donc important de comprendre comment et où les mettre en œuvre au sein de votre organisation. Dans cet article, nous examinerons le fonctionnement des IDS/IPS, leurs différences de capacité pour ce qui est de leur rôle principal, et nous verrons quel est le lieu idéal de déploiement de ces services. Nous parlerons également de l'offre de Zscaler, dans laquelle les fonctionnalités IPS jouent un rôle clé dans la stratégie de protection renforcée contre les menaces persistantes visant l'entreprise, en même temps que d'autres techniques complémentaires.

Fonctionnement des IDS et des IPS

Les systèmes de détection d'intrusion ont été conçus pour surveiller le trafic afin de détecter toute activité non autorisée sur le réseau. Ils analysent les paquets dans leur intégralité, y compris l'en-tête et la charge utile, et les comparent aux signatures des logiciels malveillants connus. Une appliance de type IDS fonctionne généralement en dehors du flux de données direct et signale les paquets malveillants qu'il détecte. Ce peut être :

- du code malveillant
- botnet
- Virus
- des attaques ciblées
- Spywares
- des attaques d'exécutions de scripts de site à site
- des injections SQL

et bien plus encore.

Bien qu'un système de détection d'intrusion (IDS) correctement configuré soit bénéfique, il est important de noter que, même dans les meilleures conditions, la technologie IDS ne fera qu'alerter l'équipe informatique d'un problème, sans l'empêcher. Un système de prévention des intrusions est quant à lui capable de détecter les paquets malveillants et de prendre des mesures appropriées. Cela est possible parce que les IPS sont déployés inline sur le trafic du réseau proprement dit. La technologie IPS peut bloquer le trafic malveillant en réinitialisant et en bloquant la connexion ou en supprimant des paquets. Comme les paquets sont transmis au fur et à mesure de leur traitement par l'IPS, la détection doit se faire en temps réel afin de bloquer les attaques avant qu'elles n'atteignent leurs cibles. L'IPS peut également générer des journaux et des alertes destinés aux administrateurs.

L'IDS et l'IPS sont généralement installés derrière un pare-feu. Le pare-feu analyse les en-têtes des paquets et applique une politique basée sur des informations quintuples incluant le protocole, l'adresse de la source, l'adresse de la destination; le port de tri et le port de destination. Si le trafic est autorisé après analyse par le pare-feu, il passe à l'IDS/IPS, qui à sont tour analyse l'ensemble du paquet et de la charge utile.

Méthodes de détection de menaces avancées

Détection basée sur la signature (IPS)

Un IPS détecte le trafic malveillant principalement sur la base des signatures. Les signatures sont un ensemble de modèles qui identifient une vulnérabilité déclenchée ou une attaque utilisée. Les signatures représentent les éléments d'une vulnérabilité ou d'un programme malveillant qui doivent être présents dans une attaque détectée sur le réseau. Les signatures doivent être suffisamment précises pour éviter de déclencher des faux positifs, dans lesquels un trafic légitime est identifié à tort comme étant malveillant. Mais elles doivent aussi être suffisamment élargies pour bloquer les variantes d'une attaque connue afin de s'assurer qu'aucune attaque réelle ne passe.

Le trafic réseau est analysé et traité à l'avance afin de rendre la détection basée sur les signatures plus efficace et plus précise. Dans le cas du trafic HTTP, par exemple, les signatures peuvent être appliquées sur des en-têtes spécifiques, sur le contenu décodé, sur la demande ou sur la réponse du serveur. Le fournisseur de service l'IPS doit constamment surveiller les vulnérabilités et les attaques connues afin d'écrire de nouvelles signatures. Les fournisseurs d'IPS effectuent généralement des mises à jour quotidiennes de leur base de données de signatures.

Détection des anomalies (IPS)

Les systèmes de prévention des intrusions étant de plus en plus utilisés, les hackers ont trouvé des moyens de contourner la détection basée sur les signatures. Si le hacker détourne le prétraitement du trafic en générant un trafic qui sera mal analysé par l'IPS, mais correctement interprété par la cible, les signatures seront appliquées à la mauvaise partie du trafic réseau et ne pourront pas provoquer une action de l'IPS. Au nombre des techniques de contournement les plus courantes, on peut citer le codage multiple de l'URL, l'utilisation d'espaces blancs inhabituels pour séparer les en-têtes HTTP, ou l'utilisation de techniques de codage inhabituelles (ASCII à 7 bits). La technologie IPS détecte les anomalies afin d'éviter ces techniques de contournement. Le trafic anormal peut alors être signalé et bloqué inline.

Analyse comportementale (Sandboxing)

Bien qu'un IPS puisse fournir une défense solide contre les menaces entrantes, les auteurs d'attaques ont trouvé des moyens de contourner leur détection. En "empoisonnant" un fichier et y apportant en permanence de légères modifications, un pirate peut contourner les détections IPS basées à la fois sur la signature et sur les anomalies. Comme le fichier qui transporte la charge utile malveillante a été légèrement modifié, le hachage du fichier qui en résulte change également. Le hachage de fichier est un calcul mathématique effectué sur un fichier connu qu'un IPS utilise pour déterminer s'il a déjà vu le fichier par le passé. L'analyse comportementale, approche courante dans la technologie de Sandboxing, consiste à effectuer une analyse approfondie du comportement d'un fichier pour déterminer si le comportement du fichier lors de son exécution sur le système cible sera malveillant. Bien qu'il ne soit pas l'objet de cet article, le Sandboxing est une technologie que vous voudrez intégrer à votre stratégie de défense afin de combler vos failles de sécurité existantes.

Le fonctionnement détermine la forme

Si les fonctionnalités de base de l'IDS/IPS sont largement utilisées, la méthode d'activation de cette fonctionnalité, le lieu où elle est déployée et la manière dont les informations sont utilisées varient grandement. Il existe encore des fournisseurs de services IDS/IPS "purs" qui sont généralement déployés dans des data centers pour protéger les serveurs ou le trafic agrégé des utilisateurs en direction d'Internet. Dans de nombreux cas, cependant, la technologie IDS/IPS est inclue dans d'autres produits.

Appliances UTM (Unified Threat Management)

L'UTM (Unified Threat Management) a été l'une des premières catégories de produits à intégrer la fonctionnalité IDS/IPS combinant le pare-feu, les fonctionnalités IDS/IDP et l'antivirus de passerelle dans une seule appliance. Gartner définit le marché de l'UTM comme étant celui de produits de sécurité réseau multifonctionnels utilisés par les petites et moyennes entreprises[1];

Lorsque les entreprises envisagent de protéger leurs bureaux distants ou leurs filiales, leur choix se porte souvent en premier sur un UTM, car obtenir une seule appliance semble être moins coûteux. Ce n'est malheureusement pas toujours le cas, car le coût de l'achat d'appliances s'est avéré extrêmement élevé dans plusieurs filiales. Ajoutez-y les coûts nécessaires pour installer et déployer les appliances, vous assurer que les politiques interagissent avec les dispositifs en amont et en aval, que les politiques sont cohérentes entre les filiales, que vous gérez les mises à jour et la maintenance, puis que vous mettez en corrélation les journaux pour obtenir une image complète de l'entreprise, et même le plus petit UTM devient hors de prix.

Appliances "nouvelle génération"

La fonctionnalité IDS/IPS est souvent considérée comme partie intégrande du pare-feu de nouvelle génération (NGFW). Bien que la signification du terme demeure quelque peu floue, la plupart des gens s'accordent à dire qu'un NGFW est un dispositif qui applique unilatéralement la politique et que son inspection ne se limite pas aux informations d'en-tête des paquets réseau fournies par les firewalls traditionnels. Les NGFW peuvent être installées devant les serveurs de l'entreprise pour assurer une protection contre l'accès illégitime aux ressources de l'entreprise. Ils sont particulièrement utiles dans les data centers, où il y a des possibilités d'attaques entrantes ou internes. Les appareils NGFW peuvent également être installés à l'intérieur du réseau local pour protéger les clients et les serveurs contre les attaques internes, et peuvent être placés aux points de sortie pour protéger les utilisateurs accédant à l'internet. Mais comme les appareils NGFW doivent couvrir tous les ports et protocoles, leur déploiement dans les filiales est généralement inutile et certainement trop coûteux, puisque la grande majorité du trafic dans la filiale est en HTTP/HTTPS.

[1] Le carré magique de Gartner pour les appliances UTM (Unified Threat Management)

L'offre de protection contre les menaces avancées basée sur le cloud de Zscaler

Si le data center demeure le site central dont la sécurité doit être assurée, d'autres sites, tels que les bureaux distants ou les filiales peuvent présenter des défis. Dans la plupart des cas, l'essentiel du trafic dans les bureaux distants ou les filiales se fait sur le Web, et la seule défense qui semble peu coûteuse est un système UTM. Si se procurer un seul appareil peut sembler moins cher, en acheter en grande quantité pour couvrir l'ensemble des filiales ne l'est certainement pas. De nombreuses filiales se retrouvent ainsi avec des systèmes de détection et de prévention des intrusions incohérents ou non-conformes aux normes. De plus, à moins qu'il ne passe par l'IPS du data center via des tunnels VPN induisant des latences ou des liaisons MPLS coûteuses, le trafic lié aux utilisateurs distants n'est généralement pas du tout examiné. Les hackers le savent très bien.

Bien qu'il y aura toujours des groupes ciblant les plus grandes organisations, ils savent qu'ils seront confrontés aux systèmes de sécurité les plus robustes. Toutefois, les plus grandes organisations ont des filiales et des bureaux distants ayant des défenses moins robustes, et une fois qu'un utilisateur sur l'un de ces sites a cliqué sur un e-mail de phishing ou téléchargé involontairement un programme malveillant sur son appareil suite à une attaque "zero-frame", il devient le chemin menant le hacker vers le siège de l'entreprise.

Zscaler est la solution. Basé sur le cloud, le moteur de protection avancée contre les menaces de Zscaler combine le meilleur de la protection IPS avec un certain nombre d'autres fonctionnalités telles que les antivirus ou antimalware, la mise en liste noire et le Sanboxing. Les filiales et les utilisateurs n'ont qu'à simplement diriger leur trafic HTTP et HTTPS sortant vers un ZIA Public Service Edge (anciennement Zscaler Enforcement Node - ZEN), et Zscaler géolocalise chaque connexion vers le ZIA Public Service Edge le plus proche basé dans l'un de ses centaines de data centers. Zscaler examine ensuite chaque octet de trafic ainsi que chaque réponse. Nul besoin d'acheter du matériel, de mettre à jour des logiciels, ni de maintenir ou de coordonner les versions. Zscaler a été conçu dès le départ pour éliminer les problèmes de traitement, de performance et d'évolutivité inhérents aux appareils basés sur le périmètre de sécurité.

Les défis liés aux appliances IPS

Offrir des fonctionnalités IPS grâce à une appliance basée sur le périmètre de sécurité entraîne un certain nombre de problèmes qui vont bien au-delà du coût de déploiement et de maintenance d'un dispositif matériel ou logiciel. Ces défis sont communs aux dispositifs de sécurité basés sur le périmètre, en particulier ceux qui se trouvent en dehors du périmètre du data center. Voici quelques unes de ces difficultés:

Une technologie limitée

Les performances d'un IPS dépendent de la quantité de décodage de protocole et de recherches de modèle que l'appliance doit effectuer. La technologie IPS n'est pas conçue pour gérer de très grandes listes noires d'URL ou d'adresses IP. Il ne prend pas non plus en charge les antivirus et les technologies d'analyse de fichiers plus avancées, telles que le Sandboxing évoqué précédemment. Aujourd'hui, l'IPS est intégré dans des systèmes UTM plus complets pour offrir une sécurité plus étendue. Mais comme nous l'avons déjà dit, les systèmes UTM ne constituent pas une solution efficace pour les utilisateurs des sites distants ou des filiales.

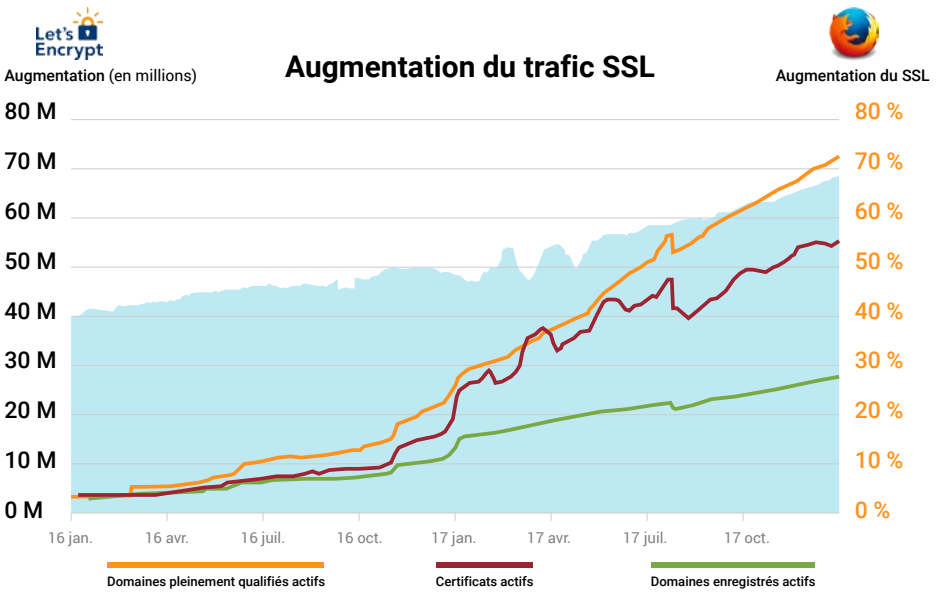
Performance

La performance des appliances IPS dépend du nombre de signatures activées et de la quantité de contenus à inspecter. Dans le cas du trafic HTTP où la taille de la response est généralement beaucoup plus grande que celle de la requête, l'activation des signatures HTTP de serveur à client ralentit considérablement les performances des appliances IPS; en fait, la plupart des appliances IPS désactivent par défaut l'analyse des réponses lorsqu'ils atteignent le volume maximal qu'ils disent pouvoir prendre en charge.

Cette pratique a malheureusement pour conséquence la baisse spectaculaire du niveau de sécurité. Une analyse complète de la réponse HTTP est nécessaire pour détecter de nombreux types de menaces, y compris les attaques de navigateur, les kits d'attaque, et bien plus encore. En outre, la majorité du trafic généré par les botnet est dynamique et les adresses IP et les domaines concernés changent constamment. Dans ce genre de cas, le trafic malveillant peut être bloqué plus efficacement en inspectant la réponse plutôt que la demande, car cela permet de visualiser des éléments tels que le téléchargement de la configuration, la liste des IPS ou des domaines auxquels se connecter, etc.

Absence de décryptage SSL

Dispositifs transparents, de nombreux IPS ont du mal à effectuer le décryptage SSL intermédiaire (en anglais "man-in-the-middle", MiTM). Le décryptage HTTPS est gourmand en processeur et limite fortement les performances que peuvent offrir les appliances IPS matériels. Ce problème devient d'autant plus important lorsque le volume du trafic SSL augmente. Selon le rapport de transparence de Google, plus de 90% du trafic transitant par Google est désormais crypté[2]. De plus, des sites de certificats SSL gratuits comme LetsEncrypt ont permis aux pirates de pouvoir mettre sur pieds le SSL sur des sites web malveillants. Comme de plus en plus de menaces et de pirates ont migré vers le SSL, il est nécessaire que la stratégie de défense d'une entreprise inclue de forts moyens d'inspection pour l'ensemble du trafic SSL.



[1]Rapport de transparence de Google: https://transparencyreport.google.com/https/overview?hl=en

Trafic asynchrone

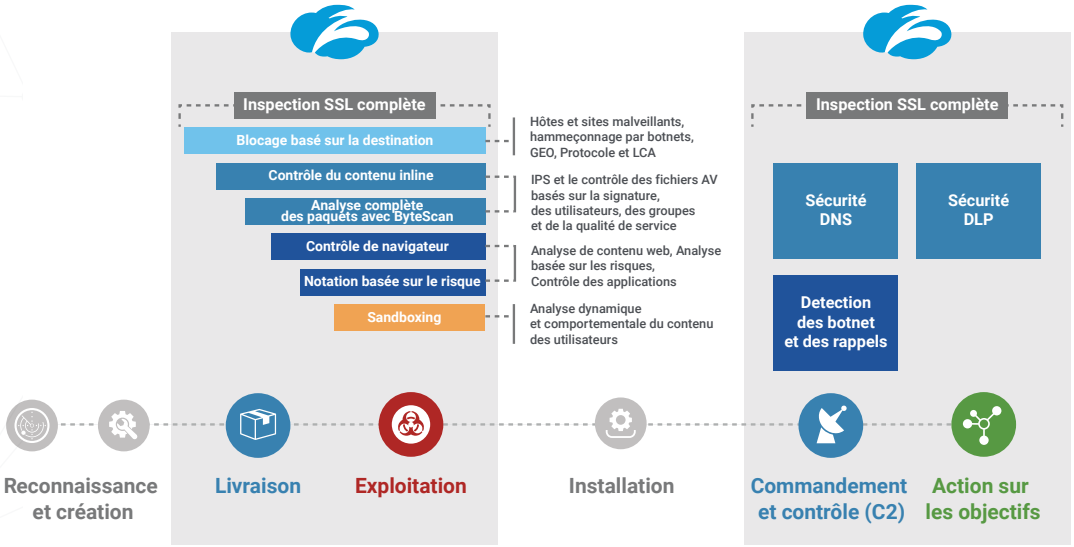
Dans de nombreux réseaux, le trafic d'un utilisateur peut souvent sortir et entrer à partir de différents points d'accès au sein du réseau. Appelée trafic asynchrone, cette méthode de routage emmène souvent les IPS et d'autres dispositifs d'inspection à passer à côté de menaces pertinentes. Pour détecter efficacement les menaces, un IPS ou tout autre dispositif d'inspection doit souvent mettre en corrélation les côtés client et serveur du modèle de communication de l'utilisateur afin d'effectuer correctement la détection des signatures. Comme il est généralement impossible de placer une seule appliance IPS sur plusieurs passerelles, les trafics entrant et sortant séparés de l'utilisateur ne peuvent être correctement suivis et inspectés par l'appliance. Certaines attaques ne sont donc pas détectées.

Pertes de paquets mal gérées

L'IPS protège le trafic au niveau de la couche 4, mais des applications telles que les navigateurs Web fonctionnent au niveau de la couche 5 et au-delà. Certaines plateformes IPS ne fournissent pas de réinitialisation TCP lorsque les paquets sont perdus. Les tentatives de connexion en boucle de nombreuses applications seront donc réinitialisées, entraînant une augmentation du trafic sur le réseau.

L'IPS cloud de Zscaler

Zscaler intègre la technologie IPS à sa politique de détection des menaces avancées. En plus de la mise en liste noire, de l'analyse heuristique (Page Risk), des antivirus, du Sandboxing, et bien d'autres encore, l'IPS est l'un des nombreux types d'inspection utilisées. Comme Zscaler protège les utilisateurs et non les serveurs, l'IPS ne recherche pas les attaques de serveur telles que les injections SQL, le déni de service ou l'exécution de code à distance, qui sont les types de menaces auxquelles on s'attend à être confronté dans les data centers. L'IPS de Zscaler se concentre plutôt sur la détection des menaces visant les utilisateurs via le HTTP et le HTTPS, ce qui en fait la solution idéale pour les filiales et les bureaux distants, ainsi que pour les utilisateurs mobiles. Grâce à ses performances, à son évolutivité et à ses services de sécurité intégrés, Zscaler peut aussi facilement ajouter une couche de sécurité à tout déploiement, où qu'il soit.



La plateforme Zscaler Cloud intègre la protection IPS dans une pile de sécurité complète. Bénéficiez d'une protection complète contre tous les types de menaces, y compris en SSL, sans les limites de performances du matériel ni les efforts d'intégration complexes.

Catégories basées sur les signatures couvertes par Zscaler Cloud IPS

Protection contre les botnets

- Serveur de commande et de contrôle
- Trafic de commande et de contrôle

Protection contre le contenu actif malveillant

- Contenus et sites malveillants
- Contrôles ActiveX vulnérables
- Attaques de navigateur
- Vulnérabilités de format de fichier
- Blocker les URLs malveillantes

Protection contre la fraude

- Sites de phishing connus
- Suspicions de site de phishing
- Spyware ou adware
- Webspam

Protection contre les communications non autorisées

- Tunneling IRC
- Tunneling SSH
- Anonymiseurs

Protection contre l'exécution de scripts de site à site

- Vol de cookies
- Demandes potentiellement malveillantes

Protection contre les destinations suspectes

Protection contre le partage de fichiers P2P

Protection contre les anonymiseurs P2P

Protection contre la VoIP P2P

Cryptominage

Zscaler utilise sa technologie propriétaire ByteScan pour scanner tout le trafic, aussi bien de client à serveur que de serveur à client. Aussi bien les requêtes que les réponses sont analysées pour rechercher les vulnérabilités et les signatures d'attaques sur l'ensemble du trafic Web. Zscaler est en mesure d'examiner à la fois la demande et la réponse beaucoup plus volumineuse pour vous donner une vision complète des menaces. Toutes les signatures sont comparées en temps réel à la requête et à la réponse liées à chaque transaction. Qu'il provienne d'un navigateur Web ou d'une application s'exécutant sur l'appareil client, tout le trafic Web passe par l'IPS de Zscaler.

Détection basée sur la signature

Tout le trafic HTTP et HTTPS entrant et sortant est analysé pour en extraire l'URL, les en-têtes, les données POST, le corps de la réponse, etc. L'équipe de sécurité de Zscaler publie chaque année plus de 2.000 nouvelles signatures couvrant les vulnérabilités des navigateurs et des applications, y compris celles du programme Microsoft Active protections Program (MAPP), ainsi que les programmes de divulgation d'autres fournisseurs. Au nombre des signatures figurent également celles des kits d'attaque, du trafic de commande et de contrôle, de l'exécution de scripts de site à site, etc.

Peut-être plus important encore, avec Zscaler, les signatures sont mises à jour et ajoutées de manière transparente plusieurs fois par jour dans l'ensemble du cloud Zscaler. C'est loin d'être le cas pour les IPS basées sur les appliances, pour lesquels les mises à jour de signatures peuvent être effectuée au mieux une fois par jour. Comme autre avantage, lorsque Zscaler détecte une menace, il la bloque pour tous les utilisateurs. Cela signifie que chaque utilisateur est protégé dès la première fois qu'une menace est détectée.

Détection des anomalies - IPS proxy

Les ZIA Public Service Edge (anciennement Zscaler Enforcement Node, ZEN) sont des proxy, non des appareils transparents. Les ZIA Public Service Edge reçoivent une demande des clients et créent une nouvelle demande au serveur de destination. Pour remplir cette fonction, les ZIA Public Service Edge doivent pouvoir analyser correctement l'ensemble de la demande. Les techniques de contournement visant à tromper les dispositifs de sécurité en leur faisant mal interpréter les demandes ne fonctionnent pas sur une architecture proxy comme celle de Zscaler. Si un ZIA Public Service Edge ne peut pas analyser une demande, la demande n'est pas transmise au serveur de destination. Tenter de contourner les décodeurs de protocole de Zscaler empêche les demandes malveillantes d'être transmises.

Prévention

Les ZIA Public Service Edge envoient des pages de notification HTML conviviales aux utilisateurs et aux applications lorsque le trafic malveillant est bloqué. L'utilisateur peut donc comprendre qu'une demande a été bloquée et pourquoi, et peut alors prendre des mesures. Toutes les attaques sont bloquées, enregistrées et signalées en temps réel. Les administrateurs peuvent facilement corréler les attaques ou examiner l'activité de l'utilisateur avant les attaques. Les expertises sont ainsi considérablement plus facile à effectuer.

Inspection SSL

En tant que proxy, Zscaler peut décrypter le trafic SSL et scanner entièrement le trafic HTTPS afin de faire correspondre les signatures. Tout le trafic Web, qu'il soit chiffré ou non, passe par le même niveau de protection de sécurité. Zscaler élimine ainsi la grande difficulté liée à "l'angle mort" du SSL, sans qu'aucun impact sur les performances ne soit ressenti au niveau des appareils. L'inspection SSL est activée et désactivée en fonction des catégories d'URL, ou des applications et des emplacements dans le cloud.

Haute performance, faible latence sur l'ensemble du trafic

Zscaler a développé son propre moteur IPS pour une utilisation à grande échelle. La détection basée sur les signatures, tant pour la demande que pour la réponse, est toujours activée, et il n'y a pas de latence supplémentaire lorsque la politique sur les menaces avancées est activée. De plus, les défis liés à l'inspection du trafic asynchrone ne posent plus de problème, car le cloud Zscaler couvre facilement toutes les voies de connexion qu'un utilisateur peut emprunter pour accéder à Internet. Les clients de Zscaler n'ont donc pas à choisir entre vitesse et sécurité; ils bénéficient en permanence d'une grande vitesse et d'une grande couverture.

Conclusion

L'IPS a un rôle à jouer dans la protection des utilisateurs contre certains types de menaces. Zscaler s'appuie sur ByteScan et la détection basée sur les signatures, ainsi que sur une pile de sécurité entièrement intégrée qui comprend le Sandboxing et l'inspection SSL afin de bloquer le plus d'attaques et de trafic malveillant visant les utilisateurs. En activant le déchiffrement SSL, tout le trafic peut bénéficier du même niveau d'inspection de sécurité. Sans les limites imposées par le matériel et avec la capacité d'évoluer de manière élastique pour répondre aux demandes de trafic d'une organisation, la suite de techniques de protection contre les menaces avancées de Zscaler peut largement dépasser le niveau de protection fourni par les autres solutions de type IPS disponibles sur le marché.

Pour en savoir plus sur **Zscaler Cloud IPS, Zscaler Cloud Sandboxing,** ou la suite complète des offres de **protection avancée contre les menaces de Zscaler,** visitez notre site Internet, ou contactez nous **pour une démo.**

Zscaler, Inc.
110 Rose Way Orchard
San José, Californie
+1 408 533 0288
www.zscaler.com