FICHE PRODUIT AKAMAI

Secure Internet Access ThreatAvert

Protéger les ressources réseau essentielles et identifier les logiciels malveillants qui affectent les abonnés

Les fournisseurs de services sont bien conscients que la sécurité du réseau a une incidence directe sur leur image de marque, car elle influe directement sur la satisfaction des abonnés. La plupart des menaces exploitent le DNS et de nouvelles menaces ont été mises au point afin de cibler spécifiquement les infrastructures DNS critiques. Les fournisseurs doivent repenser la façon de protéger les abonnés et les ressources du réseau, en particulier lorsque les menaces deviennent de plus en plus dynamiques et changeantes dans un monde entièrement connecté.

Le service Secure Internet Access ThreatAvert d'Akamai évalue les recherches DNS en temps réel pour détecter et interrompre les activités malveillantes. Secure Internet Access ThreatAvert cible les menaces qui entraînent des pannes réseau ou des ralentissements nuisant à l'expérience de l'abonné, ou qui sont en mesure de contourner d'autres protections réseau, notamment :

- les attaques DDoS sur les DNS, qui submergent les résolveurs en leur adressant des volumes massifs de requêtes
- les bots porteurs de logiciels malveillants, qui dérobent de précieuses données personnelles ou mettent en danger les terminaux des utilisateurs
- les tunnels DNS, qui volent des services en transportant d'autres protocoles à l'intérieur du DNS

Secure Internet Access ThreatAvert est basé sur le principal résolveur DNS CacheServe d'Akamai, équipé d'informations sur les menaces dynamiques d'Akamai. CacheServe est la référence majeure en matière de fiabilité : des années d'investissement dans l'optimisation des performances et de nombreuses améliorations logicielles garantissent résilience et disponibilité même en cas de pics majeurs dans le trafic DNS. Les informations sur les menaces d'Akamai sont le fruit du travail de l'équipe Akamai Data Science qui traite chaque jour plus de 100 milliards de requêtes DNS en temps réel partout dans le monde.

La sécurité DNS intégrée aux serveurs DNS

Les requêtes DNS constituent un bon indicateur d'activité malveillante, car la résolution de l'adresse d'une ressource malveillante (serveur de commande et de contrôle, téléchargement de logiciel malveillant, site d'exfiltration, etc.) est la première étape de l'activation de la plupart des activités malveillantes. Les résolveurs DNS sont l'endroit idéal où disséminer les processus d'information permettant de cibler les menaces, car ils voient toutes les requêtes émises sur un réseau de fournisseur. L'activité malveillante peut être détectée en comparant les requêtes entrantes aux entrées figurant sur des listes de menaces dynamiques.

AVANTAGES POUR VOTRE ENTREPRISE

- Solution légère, adaptable à des millions d'abonnés, couvrant tous les terminaux
- Les récents développements en science des données offrent une couverture des menaces plus sophistiquée et plus étendue
- Les informations sur les menaces actualisées en continu permettent d'ajuster la protection selon l'évolution des attaques
- Faciles à lire, les rapports en temps réel présentent instantanément l'état des menaces en fournissant un lien vers des informations plus détaillées
- Collecte efficace et gestion évolutive des données télémétriques et sur les menaces

Akamai

Secure Internet Access ThreatAvert s'intègre au plan de contrôle DNS, avec des coûts, des efforts opérationnels et un impact sur le réseau nettement inférieurs à ceux des solutions dédiées de traitement par paquets, qui s'intègrent au niveau du trafic de données.

Il s'agit d'un outil léger et efficace, et le trafic réseau ne subit pas de latence supplémentaire. Comme il est basé sur le réseau, chaque terminal est couvert, et les clients et les hôtes ne doivent procéder à aucune installation ni mise à jour de logiciel de sécurité.

Précision, profondeur et couverture des menaces améliorées

Les développeurs de logiciels malveillants innovent en permanence pour optimiser le retour sur investissement de leurs exploits. De fait, la plupart des menaces sont soigneusement conçues pour échapper à la détection et évoluent rapidement pour être en mesure de poursuivre leur action. La surface d'attaque a également augmenté en incluant une quantité impressionnante d'objets connectés. Les pirates informatiques emploient donc des méthodes d'attaque très variées pour atteindre leurs objectifs.

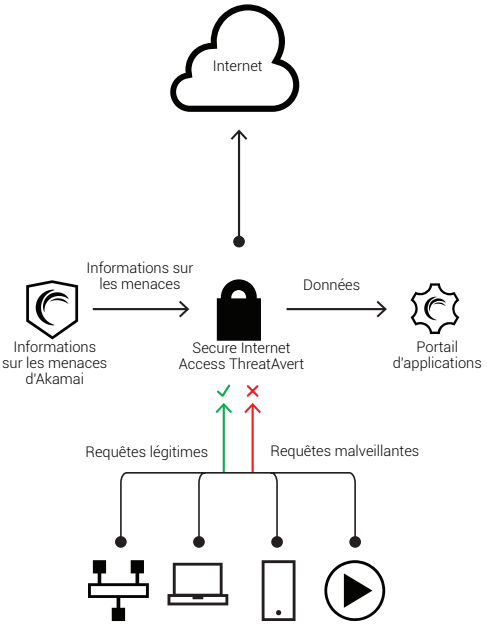
Comprenant la subtilité et la diversité de l'écosystème des menaces, l'équipe Akamai Data Science a élaboré, mis en œuvre et intégré des systèmes clés permettant d'analyser les requêtes DNS en temps réel. Les données relatives aux menaces provenant de listes de réputation, de « pots de miel » et d'autres sources tierces sont incorporées dans le processus. L'étendue et la profondeur de la couverture des menaces, ainsi que son exactitude et son agilité, sont le résultat d'investissements dans les domaines suivants :

- des algorithmes (en attente de brevet) permettant de détecter instantanément un comportement anormal (comme les attaques DDoS sur les DNS), de corréler des menaces disparates et d'identifier de nouveaux algorithmes de génération de domaine basés sur des bots
- des techniques avancées de mise en liste blanche garantissant une protection systématique des requêtes DNS légitimes
- un personnel de recherche expérimenté dans le domaine de la sécurité connaissant parfaitement les logiciels malveillants et les données DNS
- un réseau mondial et des centres de données assurant le traitement en temps réel des flux de données

Règles de précision bloquant le trafic malveillant et protégeant le bon trafic

Des règles de précision sont incorporées aux flux d'informations sur les menaces d'Akamai pour gérer le trafic DNS indésirable. Un ensemble étendu de fonctionnalités permet d'assurer un filtrage précis afin de cibler les requêtes malveillantes et de protéger les requêtes légitimes (et d'y répondre) :

- Les règles de précision peuvent être appliquées à des requêtes entrantes ou à des réponses sortantes
- Les filtres ou les limites de débit peuvent être définis selon l'adresse IP, le type de requête, le FQDN ou d'autres paramètres de requête
- Les filtres ou les limites de débit peuvent utiliser plusieurs paramètres de requête avec des opérateurs logiques : QTYPE AND FQDN, IP AND FQDN, etc.



L'important flux de données traité par les experts d'Akamai fournit une vue d'ensemble des activités malveillantes sur Internet, ainsi que des attaques localisées.

- Les filtres ou limites de débit peuvent être corrélés avec les listes de menaces dynamiques provenant des informations sur les menaces d'Akamai ou avec des listes fournies par des opérateurs
- Des règles et des listes de menaces peuvent être associées comme suit : CORRESPONDANCE avec LISTE DE BLOCAGE et ABSENCE de la LISTE BLANCHE
- Plusieurs actions de règles déterminent le traitement des requêtes : abandon, synthèse de réponse, réponse tronquée, NXD, NOERROR, etc.
- Ces règles peuvent être combinées et imbriquées, ce qui les rend encore plus efficaces

Les règles de précision peuvent également être configurées manuellement pour résoudre des problèmes ponctuels dans un réseau de fournisseur.

Gestion évolutive des données, télémétrie et rapports étendus

Secure Internet Access ThreatAvert intègre une architecture de gestion des données basée sur des solutions ouvertes testées et approuvées par les plus grands réseaux du monde, et qui permettent de bénéficier d'une excellence opérationnelle avec la portée et la vitesse du Web. Des données en direct provenant des systèmes de Secure Internet Access ThreatAvert sur l'ensemble du réseau sont agrégées et mises à la disposition des processus de génération de rapports (voir ci-dessous) et d'autres systèmes. Cette architecture résiliente assure une disponibilité permanente au service d'une expérience utilisateur sans interruption. Des applications dédiées ou des connecteurs optionnels vers des systèmes de Big Data ouverts (comme Splunk et Hadoop) peuvent être utilisés pour obtenir d'autres informations opérationnelles, de sécurité et d'activité.

Les rapports de Secure Internet Access ThreatAvert offrent une évaluation instantanée de la stratégie de sécurité avec un tableau de bord exécutif couvrant les requêtes DNS bloquées, la bande passante DNS économisée, les logiciels malveillants les plus présents sur le réseau, les abonnés infectés et les mises à jour des informations relatives aux menaces. Un tableau de bord de sécurité supplémentaire fournit des graphiques représentant de manière détaillée les attaques DDoS et les logiciels malveillants. Des couches successives de détails sur les logiciels malveillants et les clients infectés sont également à portée de clic. Des tableaux de bord et des rapports personnalisés peuvent être créés en quelques minutes pour afficher les données de sécurité dans un format défini par l'utilisateur de manière adaptée à ses besoins opérationnels particuliers. Les rapports basés sur des balises permettent au personnel en charge des opérations de configurer les vues de sa topologie Secure Internet Access ThreatAvert de manière adaptée à ses besoins spécifiques.