FICHE PRODUIT AKAMAI

Pare-feu DNS Akamai Guardicore

Visibilité et contrôle complets du trafic DNS pour les charges de travail

Le DNS (système de noms de domaine) est essentiel aux services Internet. Cependant, il ne sait pas faire la différence entre les requêtes inoffensives et les requêtes malveillantes. Par conséquent, les entreprises ont mis en place des pare-feux DNS pour inspecter les requêtes DNS, bloquer les domaines nuisibles et résoudre ceux qui sont sécurisés. Toutefois, puisque l'utilisation du DNS s'étend aux charges de travail, aux serveurs et à d'autres terminaux connectés, le manque de visibilité et de contrôle sur ce trafic DNS introduit d'autres risques en matière de sécurité.

Une segmentation unifiée et un pare-feu DNS

Akamai Guardicore Segmentation associée au pare-feu DNS Akamai Guardicore offre une défense puissante pour votre réseau. En bloquant les requêtes DNS malveillantes et en isolant les segments de réseau critiques, cette intégration réduit considérablement votre surface d'attaque et empêche la propagation des menaces. Cette approche à deux niveaux améliore la sécurité, garantit la conformité, préserve l'efficacité opérationnelle et constitue ainsi une solution essentielle pour protéger votre réseau de manière fiable.

Fonctionnement du pare-feu DNS Akamai Guardicore

Le pare-feu DNS Akamai Guardicore peut être activé en quelques minutes afin d'assurer la sécurité et de réduire la complexité sans affecter les performances. Chaque domaine sollicité est vérifié à l'aide des informations en temps réel d'Akamai sur les menaces et les requêtes envoyées à tout domaine malveillant sont automatiquement bloquées. L'utilisation du DNS en tant que couche de sécurité initiale bloque activement les menaces dans la chaîne d'attaque de manière précoce, avant l'établissement de toute connexion IP. Le DNS est par ailleurs conçu pour fonctionner de manière efficace sur la plupart des ports et des protocoles, offrant même une protection contre les logiciels malveillants qui ne visent pas les protocoles et ports Web classiques.

Lorsqu'une requête DNS est bloquée, un incident est créé. Il fournit aux équipes de sécurité et de recherche de menaces des informations détaillées sur la raison pour laquelle la menace a été bloquée, la source et la destination de la requête qui peuvent être visualisées dans une carte, et des détails précis sur les indicateurs de compromission.

Avantages pour votre entreprise

Protection complète contre les menaces
En filtrant le trafic DNS sur le périmètre du réseau et en appliquant la microsegmentation au niveau du réseau interne, les entreprises peuvent se défendre efficacement contre les logiciels malveillants, l'hameçonnage, les serveurs commande et contrôle et les tentatives d'exfiltration de données.

Recherche des menaces plus efficace
Les incidents aident les équipes de sécurité à mieux détecter, analyser et réagir face aux menaces émergentes, en minimisant l'impact des violations et en renforçant les défenses globales en matière de cybersécurité.

Amélioration de la visibilité et du contexte
L'association du pare-feu DNS et de la microsegmentation offre une meilleure visibilité des modèles de trafic DNS afin d'identifier les menaces potentielles et les violations des règles.

Gestion simplifiée
L'intégration d'un pare-feu DNS avec microsegmentation rationalise la gestion de la sécurité en fournissant une création, une application et une surveillance unifiées des règles. La complexité et les frais d'exploitation sont ainsi réduits et les entreprises peuvent donc gérer efficacement leur infrastructure de sécurité.

Renseignements sur la sécurité dans le cloud d'Akamai

Le pare-feu DNS Akamai Guardicore fonctionne grâce aux renseignements sur la sécurité dans le cloud d'Akamai, qui lui fournissent des informations en temps réel sur les menaces et les risques pour les entreprises. Les informations sur les menaces d'Akamai sont conçues pour protéger contre les dangers actuels préjudiciables pour votre entreprise et diminuer les fausses alertes positives sur lesquelles vos équipes de sécurité doivent enquêter. Ces informations sont fondées sur les données recueillies 24 h/24 et 7 j/7 par Akamai Connected Cloud, qui gère jusqu'à 30 % du trafic Web mondial et traite chaque jour jusqu'à 14 000 milliards de requêtes DNS. Les informations d'Akamai sont complétées par des centaines de flux de renseignements sur les menaces externes. L'ensemble de ces données est analysé et traité en continu en utilisant les techniques d'analyse comportementale avancée, l'intelligence artificielle et les algorithmes propriétaires. Les nouvelles menaces identifiées sont immédiatement ajoutées à l'ensemble de données sur les menaces, afin d'offrir une protection en temps réel.

Akamai Connected Cloud

Le service de pare-feu DNS Akamai Guardicore repose sur Akamai Connected Cloud, plateforme la plus distribuée au monde au service du Cloud Computing, de la sécurité et de la diffusion de contenu. Akamai Connected Cloud offre une disponibilité à 100 %, garantie par un accord de niveau de service, et assure une fiabilité optimale pour la sécurité DNS d'une entreprise.

Rendez-vous sur le site Sécurité Zero Trust d'Akamai pour en savoir plus.