

FICHE PRODUIT AKAMAI

Pare-feu DNS basé dans le cloud Secure Internet Access Enterprise

Avec l'adoption de l'accès direct à Internet, des applications logiciel en tant que service (SaaS), des services cloud, des politiques de travail de n'importe où, ainsi que de l'Internet des objets (IoT), les entreprises sont considérablement plus exposées aux attaques et font face à de nouveaux défis de sécurité. Protéger les entreprises et les utilisateurs contre les menaces ciblées avancées, telles que les logiciels malveillants, les ransomwares, l'hameçonnage et le vol de données, devient incroyablement plus difficile. Les complications et complexités des points de contrôle de sécurité, ainsi que les failles en matière de sécurité des solutions héritées doivent être gérées avec des ressources limitées.

Secure Internet Access Enterprise d'Akamai est un pare-feu DNS (système de noms de domaine) basé dans le cloud conçu pour aider les équipes de sécurité à s'assurer que les utilisateurs et les terminaux peuvent se connecter en toute sécurité à Internet, où qu'ils se trouvent, sans la complexité et les frais de gestion associés à d'autres solutions de sécurité héritées. Secure Internet Access Enterprise est alimenté par des renseignements sur les menaces en temps réel, basés sur les connaissances uniques d'Akamai sur Internet et le trafic DNS.

Secure Internet Access Enterprise

Reposant sur la plateforme Akamai Connected Cloud distribuée au niveau mondial et sur le service de résolution DNS récursif d'Akamai de niveau opérateur, Secure Internet Access Enterprise est un pare-feu DNS dans le cloud rapide à configurer et facile à déployer, qui ne nécessite aucune installation ni entretien de composant matériel.

Secure Internet Access Enterprise utilise en temps réel les renseignements sur la sécurité dans le cloud d'Akamai afin d'identifier et de bloquer de manière proactive les menaces ciblées, telles que les logiciels malveillants, les ransomwares, l'hameçonnage et le vol de données via DNS.

Le portail d'Akamai permet aux équipes de sécurité de créer, de déployer et d'appliquer de manière centralisée des règles de sécurité et des politiques d'utilisation acceptable (PUA) unifiées en quelques minutes pour tous les utilisateurs, où qu'ils soient connectés à Internet.

AVANTAGES POUR VOTRE ENTREPRISE



Déplace la sécurité Web vers le cloud à l'aide d'un pare-feu DNS basé sur le cloud que vous pouvez configurer et déployer à l'échelle mondiale en quelques minutes (sans interruption pour les utilisateurs), mais aussi adapter rapidement



Améliore le système de sécurité en bloquant de manière proactive les requêtes destinées à des sites contenant des logiciels malveillants et des logiciels de type ransomware, aux sites d'hameçonnage, aux serveurs commande et contrôle (C2) malveillants, et identifie les extractions de données par le biais de DNS à faible débit, le tout grâce à des informations sur les menaces uniques et actualisées en temps réel



Permet de contrôler l'utilisation du Shadow IT et des applications non sanctionnées en les identifiant et en les bloquant en fonction de leur catégorie ou score de risques



Écoute et simplifie la gestion de la sécurité en réduisant les fausses alertes de sécurité positives et les alertes des autres produits de sécurité, et en administrant les règles de sécurité et les mises à jour de n'importe où, en quelques secondes, pour protéger tous les sites



Fonctionnement

Secure Internet Access Enterprise est un service de sécurité basé sur le cloud qui peut être activé en quelques minutes pour assurer la sécurité et réduire la complexité, sans aucune incidence sur les performances. Cette protection est assurée en dirigeant simplement le trafic DNS récursif vers Secure Internet Access Enterprise au moyen de différentes méthodes, y compris les tunnels IPsec, un client léger, un redirecteur DNS géré d'Akamai ou une modification de votre résolveur DNS existant.

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 identifié 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 Web. Le DNS est par ailleurs conçu pour fonctionner de manière efficace sur tous les ports et protocoles, offrant ainsi une protection contre les logiciels malveillants qui ne visent pas les protocoles et ports Web classiques. Il est également possible de vérifier les domaines pour déterminer le type de contenu auquel un utilisateur essaie d'accéder et le bloquer s'il va à l'encontre de la PUA de l'entreprise.

Pour une protection supplémentaire, les domaines à risque peuvent être transférés vers un proxy cloud pour inspection des URL. Les URL HTTP/S demandées sont comparées aux informations en temps réel d'Akamai sur les menaces et les URL malveillantes sont automatiquement bloquées.

Secure Internet Access Enterprise s'intègre facilement aux autres produits de sécurité et outils de création de rapports, y compris les pare-feux et les solutions de gestion des informations et des événements de sécurité (SIEM), ainsi qu'aux flux de renseignements concernant les menaces externes, vous permettant ainsi d'optimiser votre investissement à tous les niveaux de votre système de sécurité.

De plus, le déploiement sur les terminaux du client léger Secure Internet Access Enterprise permet aux entreprises de protéger rapidement et facilement les ordinateurs portables ou les appareils mobiles utilisés hors du réseau.

Renseignements sur la sécurité dans le cloud d'Akamai

Secure Internet Access Enterprise est basé sur les 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 menaces actuelles 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 11 000 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'apprentissage automatique et les algorithmes propriétaires. Les nouvelles menaces identifiées sont immédiatement ajoutées au service Secure Internet Access Enterprise, afin d'offrir une protection en temps réel.

Akamai Connected Cloud

Le service Secure Internet Access Enterprise 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 (SLA), et assure une fiabilité optimale pour la sécurité Web d'une entreprise.

AVANTAGES POUR VOTRE ENTREPRISE



Réduit les risques et améliore la sécurité des terminaux utilisés en dehors du réseau, en toute simplicité et sans utiliser de VPN, grâce au client léger Secure Internet Access Enterprise qui permet de renforcer les politiques de sécurité et les PUA



Veille à la conformité de votre PUA de manière rapide et uniforme en bloquant l'accès aux domaines et catégories de contenu indésirables ou inappropriés



Augmente immédiatement la résilience et la fiabilité grâce à Akamai Connected Cloud et la plateforme DNS de niveau opérateur d'Akamai

Portail de gestion dans le cloud

La configuration et la gestion continue de Secure Internet Access Enterprise s'effectuent sur le portail cloud Akamai Control Center, ce qui vous permet d'y accéder à tout moment, où que vous soyez.

La gestion des règles est simple et rapide, et des modifications peuvent être globalement implémentées en quelques minutes pour assurer la protection de tous vos sites et utilisateurs. Il est possible de configurer des alertes par e-mail en temps réel et des rapports programmés pour prévenir les équipes de sécurité des principaux événements liés à une règle donnée afin qu'elles puissent prendre rapidement des mesures pour identifier et résoudre les menaces potentielles. Un tableau de bord en temps réel fournit un aperçu du trafic, des menaces et des événements PUA. Vous pouvez consulter des informations détaillées sur chaque activité grâce à des analyses individuelles sur les éléments du tableau de bord. Ces informations détaillées sont importantes pour analyser et corriger les incidents de sécurité.

Toutes les fonctionnalités du portail sont accessibles depuis les API et vous pouvez exporter les journaux de données vers un SIEM, ce qui permet à Secure Internet Access Enterprise de s'intégrer de manière simple et efficace à vos autres solutions de sécurité et outils de création de rapports.

Fonctionnalités

Sécurité
Blocage des logiciels malveillants, des ransomwares et des domaines et URL de hameçonnage
Blocage des requêtes C2 malveillantes
Identification de l'extraction de données via DNS
Inspection des domaines proxy à risque pour les adresses URL HTTP et HTTPS demandées
Création d'une liste personnalisée de domaines pour l'inspection des adresses URL HTTP et HTTPS
Analyses rétrospectives des journaux de trafic client pour identifier et alerter sur les menaces nouvellement découvertes
Création de listes d'autorisation/exclusion personnalisées
Intégration de flux supplémentaires de renseignements sur les menaces
Personnalisation des pages d'erreur
Requêtes à la base de données sur les menaces d'Akamai pour obtenir des informations sur les domaines et URL malveillants
Application de la sécurité pour les terminaux hors réseau (Windows, MacOS, iOS, Android, Chrome)
Politique d'utilisation acceptable (PUA)
Création de PUA basées sur des groupes
Surveillance ou blocage des utilisateurs sur le réseau et hors réseau ayant commis des violations de PUA
Application de la protection SafeSearch sur Google, Bing et YouTube

Courtier de sécurité d'accès au cloud (en ligne)
Identification et blocage des applications de Shadow IT
Blocage des applications en fonction du score de risques ou du groupe d'applications
Application des locataires SaaS
Rapport, surveillance et administration
Intégration d'IDP et d'Active Directory
Vue d'ensemble des activités de l'entreprise avec tableaux de bord personnalisables
Analyse détaillée de tous les événements PUA et menaces
Journalisation et visibilité complètes de toutes les demandes de trafic et des menaces et événements PUA
Service Log Delivery pour tous les journaux ; conservation des journaux pendant 30 jours et exportation possible via une API
Configuration, listes de sécurité personnalisées et événements disponibles via une API
Intégration à d'autres systèmes de sécurité, tels que les SIEM, via une API
Alertes de sécurité en temps réel par e-mail
Programmation de rapports quotidiens ou hebdomadaires par e-mail
Gestion déléguée
Plateforme Akamai Connected Cloud
Adresses VIP IPv4 et IPv6 dédiées par client pour le service DNS récursif
Disponibilité à 100 % garantie par un accord de niveau de service (SLA)
Routage DNS Anycast pour des performances optimales
Application de DNSSEC, DoH et DoT pour une sécurité accrue
Attribution de terminaux d'entreprise
Attribution en ligne à l'aide d'un redirecteur DNS
Attribution hors ligne à l'aide de Security Connector
Attribution basée sur le client pour les ordinateurs portables et les terminaux mobiles (Windows, MacOS, iOS, Android, Chrome)

Pour en savoir plus sur Secure Internet Access Enterprise et pour tester une version gratuite, [rendez-vous sur akamai.com](https://akamai.com).