Enterprise Threat Protector
Passerelle Web sécurisée basée dans le cloud

Les entreprises, en adoptant l'accès Internet direct (DIA), les applications SaaS, les services cloud, la mobilité et le travail à distance, ainsi que l'Internet des objets (IoT), augmentent considérablement leur exposition aux attaques et se trouvent confrontées à de nouveaux défis en matière de sécurité. La protection de l'entreprise et des utilisateurs contre les menaces ciblées avancées telles que les logiciels malveillants, les ransomware, l'hameçonnage et le vol de données devient plus difficile et ce, de façon exponentielle. 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.

Enterprise Threat Protector est une passerelle Web sécurisée (SWG) basée dans le cloud conçue 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. Enterprise Threat Protector est alimentée par des renseignements sur les menaces en temps réel, basés sur les connaissances uniques d'Akamai sur Internet et le trafic DNS (système de noms de domaine), et plusieurs moteurs de détection de logiciels malveillants.

Enterprise Threat Protector

Reposant sur la plateforme mondiale Intelligent Edge Platform et sur le service de résolution DNS récursif de niveau opérateur d'Akamai, Enterprise Threat Protector est une passerelle Web sécurisée basée sur le cloud facile à configurer et à déployer, qui ne nécessite aucune installation ni aucun entretien de composant matériel.

Enterprise Threat Protector comporte plusieurs niveaux de protection qui utilisent en temps réel Akamai Cloud Security Intelligence, ainsi que plusieurs moteurs de détection des logiciels malveillants statiques et dynamiques afin d'identifier les menaces ciblées (logiciels malveillants, ransomware, hameçonnage, vol de données via DNS) et de les bloquer de manière proactive. 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 employés, où qu'ils soient connectés à Internet.

Comment procéder ?

Enterprise Threat Protector comporte plusieurs niveaux de protection : DNS, URL et analyse de la charge utile en ligne, qui assurent la sécurité et réduisent la complexité, sans nuire aux performances. Cette protection complète peut être atteinte en dirigeant simplement le trafic Web vers Enterprise Threat Protector à l'aide d'un client léger ou en transférant le trafic Web depuis un autre proxy Web grâce au chaînage de proxy.

Enterprise Threat Protector : Passerelle Web sécurisée basée dans le cloud

Inspection DNS : 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 de manière proactive les menaces de manière précoce dans la chaîne d'attaque et avant l'établissement de la connexion Web. Le DNS est également conçu pour fonctionner de manière efficace sur tous les ports et protocoles, ce qui les protège des logiciels malveillants qui ne passent pas par des protocoles et des 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 politique d'utilisation acceptable (PUA) de l'entreprise.

Inspection de l'URL : Les URL HTTP et HTTPS sollicitées sont vérifiées à l'aide des informations en temps réel d'Akamai sur les menaces et les URL malveillantes sont automatiquement bloquées.

Analyse de la charge utile : Les charges utiles HTTP/S sont analysées en ligne ou hors ligne à l'aide de plusieurs moteurs avancés de détection de logiciels malveillants. Ces moteurs utilisent de nombreuses techniques, y compris la détection des signatures, la détection des menaces sans signature, l'apprentissage automatique et des environnements de test, qui offrent une protection « zero day » complète contre les fichiers potentiellement malveillants, tels que les exécutables et les documents. En outre, le moteur de détection d'hameçonnage « zero day » d'Akamai catégorise et bloque les pages d'hameçonnage nouvellement créées au point de demande, même si la page n'a jamais été vue auparavant.

Enterprise Threat Protector s'intègre facilement aux autres produits de sécurité et outils de création de rapports, y compris les pare-feu et SIEM, ainsi qu'aux flux de renseignements concernant les menaces externes, vous permettant ainsi d'optimiser votre investissement à tous les niveaux du système de sécurité de votre entreprise.

Avantages pour votre entreprise

- **Déplace la sécurité Web vers le cloud** à l'aide d'une passerelle Web sécurisée basée 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 nettement le système de sécurité** en bloquant de manière proactive les requêtes DNS 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 aux domaines vecteurs de vol de données via DNS, le tout grâce à des informations sur les menaces uniques et actualisées en temps réel.
- **Bloque les charges utiles malveillantes pour une meilleure protection « zero day »** en analysant les fichiers et le contenu Web demandés pour arrêter les menaces avant qu'elles atteignent et compromettent les terminaux des points de terminaison.
- **Permet de contrôler l'utilisation des applications informatiques fantômes et non sanctionnées** en les identifiant et en les bloquant en fonction de leur score de risques et en limitant leurs fonctionnalités.
- **Empêche les pertes de données** en identifiant et en bloquant le téléchargement de données sensibles ou confidentielles telles que celles régies par PII, PCI ou HIPAA.
- **Réduit le temps et la complexité de la gestion de la sécurité** en réduisant les fausses alertes de sécurité positives, en diminuant le nombre d'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.
- **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 Enterprise Threat Protector qui permet de renforcer les politiques de sécurité et les PUA.
- **Veille à la conformité de votre politique d'utilisation acceptable de manière rapide et uniforme** en bloquant l'accès aux domaines et catégories de contenu indésirables ou inappropriés.
- **Augmente la résilience et la fiabilité** grâce à la plateforme Intelligent Edge Platform d'Akamai.

Enterprise Threat Protector : Passerelle Web sécurisée basée dans le cloud

De plus, le déploiement du client Enterprise Threat Protector sur les terminaux gérés permet également aux entreprises d'ajouter rapidement une couche additionnelle de protection proactive lorsque les ordinateurs portables ou les terminaux mobiles sont utilisés en dehors du réseau.

Moteur Cloud Security Intelligence d'Akamai

Enterprise Threat Protector est basée sur la solution Cloud Security Intelligence d'Akamai. Cette dernière lui fournit des informations en temps réel concernant les menaces et les risques qu'elles représentent pour les entreprises.

Les informations sur les menaces d'Akamai sont conçues pour fournir une protection contre les menaces actuelles et pertinentes qui pourraient influencer votre entreprise et minimiser le nombre de 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 l'Intelligent Edge Platform d'Akamai, qui gère jusqu'à 30 % du trafic Web mondial et traite chaque jour jusqu'à 2 200 milliards de requêtes DNS. Les informations d'Akamai sont complétées par des centaines de flux de menaces externes, et 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. Lorsque de nouvelles menaces sont identifiées, elles sont immédiatement ajoutées au service Enterprise Threat Protector, ce qui permet d'offrir une protection en temps réel.

Akamai Intelligent Edge Platform

Le service Enterprise Threat Protector est basé sur l'Intelligent Edge Platform d'Akamai, une plateforme rapide, intelligente et sûre. Distribuée dans le monde entier, cette plateforme 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.

Portail de gestion dans le cloud

La configuration et la gestion continue d'Enterprise Threat Protector 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 vous pouvez envoyer des modifications dans le monde entier en quelques minutes pour vous assurer que vos sites et vos utilisateurs sont protégés de manière instantanée. 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 afficher des informations détaillées sur toutes les activités en analysant chaque élément 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 Enterprise Threat Protector de s'intégrer de manière simple et efficace à vos autres solutions de sécurité et outils de création de rapports.

Enterprise Threat Protector : Passerelle Web sécurisée basée dans le cloud

Principales fonctionnalités

- **Menaces catégorisées par Akamai :** renseignements en temps réel sur les menaces basés sur la visibilité d'Akamai sur 2 200 milliards de requêtes DNS, le trafic CDN et les journaux d'autres services de sécurité Akamai.
- **Menaces catégorisées par le client :** les équipes de sécurité peuvent intégrer rapidement des flux de renseignements sur les menaces, ce qui rentabilise vos investissements actuels en matière de sécurité.
- **Analyse de la charge utile en ligne et hors ligne :** cinq moteurs de détection de logiciels malveillants avancés permettent d'identifier et de bloquer les menaces avancées complexes et d'améliorer la protection « zero day ».
- **Prévention des pertes de données :** bloquer ou surveiller les téléchargements de fichiers contenant des données PII, PCI, DSS ou HIPAA.
- **Visibilité et contrôle des applications :** identifier et bloquer l'utilisation des applications non approuvées en fonction du score de risques ou limiter les fonctionnalités de l'application.
- **Inspection TLS :** inspecter les requêtes et les charges utiles chiffrées par TLS.
- **Protection en dehors du réseau :** protéger les ordinateurs portables et les terminaux mobiles utilisés en dehors du réseau.
- **Politiques d'utilisation acceptable :** appliquer la politique d'utilisation acceptable de l'entreprise et assurer son respect en limitant les catégories de contenu auquel il est possible ou non d'accéder.
- **Analyse, rapports et journalisation :** Des tableaux de bord en temps réel fournissent des informations sur le trafic, la sécurité et les alertes PUA, tandis que les journaux peuvent être exportés ou intégrés dans un SIEM.
- **DoT et DNSSEC :** Déployez DNS sur TLS et DNSSEC pour assurer la sécurité de bout en bout du trafic DNS.

L'environnement Akamai

L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Nos solutions complètes sont gérées via l'Akamai Control Center qui en assure la visibilité et la gestion. Elles sont prises en charge par des experts des services professionnels qui peuvent vous aider à mettre en place votre service, mais aussi vous suggérer des solutions adaptées à l'évolution de votre stratégie.

Pour en savoir plus sur Enterprise Threat Protector et vous inscrire pour bénéficier d'une évaluation gratuite, rendez-vous sur akamai.com/etp.

Enterprise Threat Protector : Passerelle Web sécurisée basée dans le cloud

Sécurité	Intelligence	Standard	Advanced
Blocage des logiciels malveillants, des ransomware, et des domaines et URL de hameçonnage	✓	✓	✓
Blocage des logiciels malveillants et requêtes de commande et de contrôle (C2)	✓	✓	✓
Identification de l'extraction de données via DNS	✓	✓	✓
Inspection des domaines proxy à risque pour les adresses URL HTTP et HTTPS demandées	✓	✓	✓
Autorisation de l'ensemble du trafic Web pour les DNS et l'inspection d'URL		✓	✓
Analyse en ligne et hors ligne de la charge utile HTTP et HTTPS à risque à l'aide de plusieurs moteurs d'analyse et de détection des logiciels malveillants			✓
Test cloud pour l'analyse dynamique de la charge utile hors ligne*			✓
Analyse en ligne en temps réel des pages Web pour détecter les pages d'hameçonnage « zero day »			✓
Analyse en ligne ou hors ligne* en temps réel des fichiers téléchargés depuis des sites de partage de fichiers			✓
Création d'une liste personnalisée de domaines pour l'inspection des adresses URL HTTP et HTTPS	✓	✓	✓
Création d'une liste personnalisée de domaines pour l'analyse en ligne/hors ligne* de la charge utile			✓
Analyse rétrospective 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	✓	✓	✓
Pages d'erreur personnalisables	✓	✓	✓
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)	**Intelligence**	**Standard**	**Advanced**
Création de PUA basées sur des groupes		✓	✓
Surveillance ou blocage des utilisateurs sur le réseau et hors réseau ayant commis des violations de la PUA	✓	✓	✓
Application de la protection SafeSearch sur Google, Bing et YouTube	✓	✓	✓

Enterprise Threat Protector : Passerelle Web sécurisée basée dans le cloud

Prévention intégrée des fuites de données (DLP)	Intelligence	Standard	Advanced
Dictionnaires standard pour les dictionnaires personnalisés IIP, PCI et HIPAA			✓
Blocage ou surveillance des actions de règle			✓
Rapports			✓
Visibilité et contrôle des applications (AVC)	**Intelligence**	**Standard**	**Advanced**
Identification et blocage des applications informatiques fantômes	✓	✓	✓
Blocage des applications en fonction du score de risques ou du groupe d'applications	✓	✓	✓
Blocage/autorisation des opérations d'application		✓	✓
Application des locataires SaaS	✓	✓	✓
Rapports, surveillance et administration	**Intelligence**	**Standard**	**Advanced**
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 OUVERTE	✓	✓	✓
Intégration à d'autres systèmes de sécurité, tels que les SIEM, via une API OUVERTE	✓	✓	✓
Alertes de sécurité en temps réel par e-mail	✓	✓	✓
Programmation de rapports quotidiens ou hebdomadaires par e-mail	✓	✓	✓
Gestion déléguée	✓	✓	✓
Akamai Intelligent Edge Platform	**Intelligence**	**Standard**	**Advanced**
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	✓	✓	✓
DNSSEC appliqué pour une sécurité accrue	✓	✓	✓

Enterprise Threat Protector : Passerelle Web sécurisée basée dans le cloud

Attribution de terminal d'entreprise	Intelligence	Standard	Advanced
Attribution en ligne à l'aide d'un redirecteur DNS	✓	✓	✓
Attribution hors ligne à l'aide d'Enterprise Security Connector	✓	✓	✓
Attribution basée sur le client pour les ordinateurs portables et les terminaux mobiles (Windows, MacOS, iOS, Android, Chrome)	✓	✓	✓

* Le test cloud est un module complémentaire en option requis pour les analyses hors ligne de gros fichiers.

Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multiclouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et sur mobile, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques mondiales font confiance à Akamai, visitez www.akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse www.akamai.com/locations. Publication : 10/20.