ENTERPRISE THREAT PROTECTOR

Protection contre les menaces avancées dans le cloud

Les entreprises, en adoptant l'accès Internet direct (DIA), les applications SaaS, les services cloud, la mobilité et l'Internet des objets (IoT), augmentent considérablement leur exposition aux attaques et se trouvent confrontées à de nouveaux défis. La protection de l'organisation et des utilisateurs contre les menaces ciblées avancées telles que les logiciels malveillants, le 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. Enterprise Threat Protector (ETP) est une plateforme Secure Internet Gateway (SIG) qui permet aux équipes de sécurité de s'assurer que les utilisateurs et les terminaux peuvent se connecter en toute sécurité à Internet où qu'ils se trouvent, sans la complexité associée 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 concernant Internet et le trafic DNS (système de noms de domaine).

ENTERPRISE THREAT PROTECTOR

Reposant sur l'Intelligent Edge Platform™ d'Akamai et sur le service de résolution DNS récursif de niveau opérateur également conçu par Akamai, Enterprise Threat Protector est une solution SIG facile à configurer et à déployer, qui ne nécessite aucune installation ni entretien de composant matériel.

Enterprise Threat Protector utilise en temps réel Akamai Cloud Security Intelligence ainsi que la plateforme Akamai éprouvée et distribuée dans le monde entier afin d'identifier les menaces ciblées (programmes 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.

FONCTIONNEMENT

Enterprise Threat Protector utilise plusieurs niveaux de protection : DNS, URL et analyse de la charge utile en ligne ; offrant une sécurité optimale et réduisant la complexité, sans aucun impact sur les performances.

Inspection DNS : en dirigeant simplement votre trafic DNS récursif externe vers Enterprise Threat Protector, tous les domaines demandés sont vérifiés à l'aide des informations d'évaluation du danger des domaines en temps réel d'Akamai. Les utilisateurs sont bloqués de manière proactive et ne peuvent accéder aux domaines et services malveillants tandis que les demandes vers des domaines et services sécurisés sont résolues. Cette validation a lieu avant que la connexion IP soit établie, les menaces peuvent donc être contrées plus tôt dans la chaîne d'attaque. Le DNS fonctionne également sur tous les ports et protocoles, ce qui les protège des programmes 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 domaines qui sont considérés comme à risque selon les informations sur les menaces d'Akamai sont automatiquement transmis à un proxy cloud sur l'Intelligent Edge Platform™d'Akamai. L'URL demandée est vérifiée selon les informations sur les menaces URL d'Akamai et les URL malveillantes sont automatiquement bloquées. Le proxy inspecte les URL HTTP et HTTPS.

Analyse de la charge utile en ligne : les ressources HTTP et HTTPS provenant de domaines considérés comme risqués sont ensuite analysées en temps réel en utilisant 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 et l'apprentissage automatique, qui offrent une protection « zero day » complète contre les fichiers potentiellement malveillants, tels que les exécutables et les documents, ainsi que d'autres logiciels malveillants qui sont intégrés directement dans la page Web demandée, tels que les fichiers JavaScript malveillants dont l'emplacement est brouillé.

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 que les 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.

De plus, le déploiement de l'outil léger Enterprise Client Connector sur les ordinateurs portables gérés permet également aux entreprises d'ajouter rapidement une couche additionnelle de protection proactive lorsque ceux-ci sont utilisés en dehors du réseau.

AVANTAGES POUR VOTRE ENTREPRISE

- **Améliore le système de sécurité** en bloquant de manière proactive les requêtes destinées à des sites contenant des programmes malveillants et des logiciels de type ransomware, aux serveurs CnC malveillants et aux domaines et URL vecteurs de vol de données/hameçonnage via DNS, le tout grâce à des informations sur les menaces uniques et actualisées en temps réel.
- **Bloque les charges malveillantes pour une meilleure protection « zéro day »** en analysant les fichiers et le contenu Web demandés en temps réel pour arrêter les menaces avant qu'elles atteignent et compromettent les terminaux des points de terminaison.
- **Améliore la performance de DIA** en autorisant uniquement le trafic suspect pour l'inspection des URL et l'analyse de la charge utile.
- **Renforce instantanément la protection sans complexité ni installation matérielle** en choisissant une solution entièrement hébergée dans le cloud que vous pouvez configurer et déployer à l'échelle mondiale en quelques minutes (sans interruption pour les utilisateurs), mais aussi adapter rapidement.
- **Réduit les risques et améliore la sécurité des ordinateurs portables utilisés en dehors du réseau, en toute simplicité et sans utiliser de VPN**, grâce à l'outil léger Enterprise Client Connector qui permet de renforcer les politiques de sécurité et les PUA.
- **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 emplacements.
- **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 du DNS** grâce à l'Intelligent Edge Platform d'Akamai.

ENTERPRISE THREAT PROTECTOR

CLOUD SECURITY INTELLIGENCE (CSI) 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 un grand nombre 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.

INTELLIGENT EDGE PLATFORM D'AKAMAI

Le service Enterprise Threat Protector est basé sur l'Intelligent Edge Platform d'Akamai, une plateforme de niveau opérateur sûre, fiable et rapide. Distribuée dans le monde entier, elle offre une disponibilité de 100 % garantie par un accord de niveau de service (SLA) et assure une fiabilité optimale pour le service DNS récursif d'une entreprise.

PORTAIL DE GESTION DANS LE CLOUD

Toute la configuration et la gestion continue d'Enterprise Threat Protector s'effectue sur le portail cloud Luna d'Akamai, 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.

PRINCIPALES FONCTIONNALITÉS

- **Menaces catégorisées par Akamai :** les informations en temps réel sur les menaces dont dispose Akamai, basées sur sa visibilité de 15 à 30 % du trafic Web mondial, sont combinées à 2 200 milliards de requêtes DNS quotidiennes sur le cloud DNS récursif d'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 en temps réel :** trois moteurs de détection de logiciels malveillants avancés permettent d'identifier et de bloquer les menaces avancées complexes et d'améliorer la protection « zero day ».
- **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 et création de rapports :** les tableaux de bord fournissent des informations en temps réel sur la totalité du trafic Web sortant de l'entreprise ainsi que sur les menaces et les événements PUA.
- **Informations concernant la sécurité :** comprendre rapidement pourquoi Akamai a ajouté un domaine ou une URL à ses listes d'informations sur les menaces.
- **Consignation :** les journaux de trafic sont conservés pendant 30 jours et peuvent facilement être exportés au format CSV ou intégrés à un SIEM pour être analysés.
- **DNSSEC :** DNSSEC est activé sur toutes les requêtes DNS envoyées à Enterprise Threat Protector.

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 le Luna 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 une évaluation gratuite, rendez-vous sur akamai.com/etp.

Akamai

ENTERPRISE THREAT PROTECTOR

SÉCURITÉ	Guest Wi-Fi	Intelligence	Advanced Threat
Blocage des logiciels malveillants, ransomware et domaines dédiés au hameçonnage		X	X
Blocage des logiciels malveillants et requêtes de commande et de contrôle (CnC)		X	X
Identification de l'extraction de données via DNS		X	X
Inspection des domaines proxy à risque pour les adresses URL HTTP et HTTPS demandées		X	X
Analyse en ligne en temps réel de la charge utile HTTP et HTTPS à risque à l'aide de plusieurs moteurs en ligne d'analyse et de détection des logiciels malveillants			X
Analyse en ligne en temps réel des fichiers téléchargés depuis des sites de partage de fichiers			X
Création d'une liste personnalisée de domaines pour l'inspection des adresses URL HTTP et HTTPS		X	X
Création d'une liste personnalisée de domaines pour l'analyse en ligne de la charge utile			X
Analyse rétrospective des journaux de trafic client pour identifier et alerter sur les menaces nouvellement découvertes		X	X
Création de listes d'autorisation/exclusion personnalisées		X	X
Intégration de flux supplémentaires de renseignements sur les menaces		X	X
Pages d'erreur personnalisables	X	X	X
Requêtes à la base de données sur les menaces d'Akamai pour obtenir des informations sur les domaines et URL malveillants		X	X
Sécurisation des ordinateurs portables hors réseau (Windows et MacOS)		X	X
POLITIQUE D'UTILISATION ACCEPTABLE (PUA)	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Surveillance ou blocage des utilisateurs sur le réseau et hors réseau ayant commis des violations de la PUA	X[1]	X	X
Application de la protection SafeSearch sur Google, Bing et YouTube	X	X	X
RAPPORT, SURVEILLANCE ET ADMINISTRATION	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Vue d'ensemble des activités de l'entreprise avec tableaux de bord personnalisables	X[2]	X	X
Analyse détaillée de toutes les menaces et événements PUA	X[2]	X	X
Journalisation et visibilité complètes de toutes les demandes de trafic et les menaces et événements PUA	X[2]	X	X
Service Log Delivery pour tous les journaux ; conservation des journaux pendant 30 jours et exportation possible via une API	X[2]	X	X
Configuration, listes de sécurité personnalisées et événements disponibles via une API ouverte	X[2]	X	X
Intégration à d'autres systèmes de sécurité, tels que les SIEM, via une API ouverte	X	X	X
Alertes de sécurité et PUA en temps réel par e-mail	X[2]	X	X
Programmation de rapports quotidiens ou hebdomadaires par e-mail	X	X	X
Gestion déléguée	X	X	X
INTELLIGENT EDGE PLATFORM™ D'AKAMAI	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Adresses VIP IPv4 et IPv6 dédiées par client pour le service DNS récursif	X	X	X
Disponibilité de 100 % garantie par un accord de niveau de service (SLA)	X	X	X
Routage DNS Anycast pour des performances optimales	X	X	X
DNSSEC appliqué pour une sécurité accrue	X	X	X
CONNECTEURS D'ENTREPRISE	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Connecteur de sécurité client pour la protection des ordinateurs portables hors réseau (Windows et OSX) et signalement du nom de la machine pour les événements sur le réseau et hors réseau		X	X
Mise à jour automatique du connecteur de sécurité client		X	X
Identification des adresses IP et des noms de machine pour les terminaux des points de terminaison via le connecteur de sécurité client		X	X

1. La version Wi-Fi public d'ETP n'inclut pas l'application hors réseau de la PUA.
2. La version Wi-Fi public d'ETP n'inclut pas les contrôles de sécurité. Les alertes, analyses, tableaux de bord et journaux n'incluent que l'activité et les événements PUA.