ENTERPRISE DEFENDER

Sécurité Zero Trust en bordure de l'Internet

Le périmètre réseau défendable n'existe plus, du moins sous sa forme connue. L'utilisation actuelle d'une approche de sécurité et d'accès qui était pertinente il y a 20 ans est, dans le meilleur des cas, inappropriée, et dans le pire, extrêmement risquée. Et ce n'est pas qu'une théorie. C'est devenu une évidence à la lumière de l'ampleur et de l'énorme quantité d'atteintes à la protection des données observées au cours des cinq dernières années, lesquelles s'expliquent en majorité par des intrusions dans le périmètre suite à des abus de confiance. Il est temps d'adopter la sécurité Zero Trust, où la confiance dans le réseau d'entreprise n'est plus inhérente, et les décisions relatives à la sécurité et aux accès sont appliquées de manière dynamique en fonction de l'identité, du terminal et du contexte de l'utilisateur.

ENTERPRISE DEFENDER

Basé sur l'Akamai Intelligent Edge Platform, Enterprise Defender associe la prévention des programmes malveillants à l'accès adaptatif aux applications, à la sécurité et à l'accélération dans un service de sécurité simple à utiliser en bordure de l'Internet. Enterprise Defender permet aux entreprises d'adopter une stratégie de sécurité Zero Trust sans matériel ni équipement. Abonnez-vous simplement à Enterprise Defender pour réduire les risques et la complexité tout en améliorant l'expérience utilisateur.

FONCTIONNEMENT

Enterprise Defender s'appuie sur l'Akamai Intelligent Edge Platform pour sécuriser toutes les applications et tous les utilisateurs de l'entreprise, en offrant une sécurité optimale et en réduisant la complexité sans affecter les performances. Il vous permet d'assurer un accès sécurisé aux applications que vous contrôlez, tout en limitant les risques associés à l'accès de vos utilisateurs aux applications que vous ne contrôlez pas.

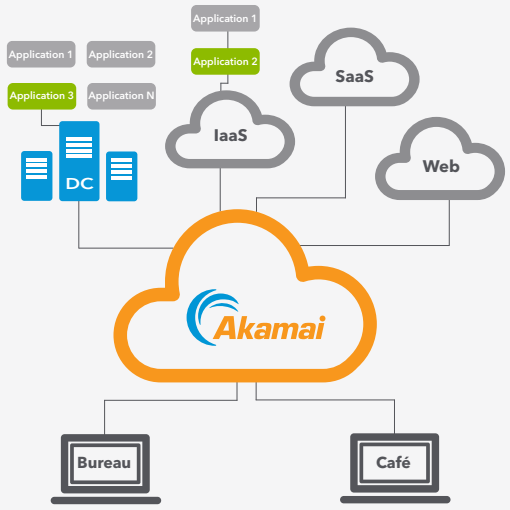
Enterprise Defender inclut les fonctionnalités suivantes dans un service d'abonnement mensuel par utilisateur facile à utiliser :

Prévention contre les programmes malveillants : Akamai identifie, bloque et atténue de manière proactive les menaces ciblées telles que les logiciels malveillants, les ransomware, l'hameçonnage, les vols de données via DNS et les attaques zero day de niveau complexe. Akamai offre 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 et aux applications que vous ne contrôlez pas, quel que soit l'endroit d'où ils se connectent, sans la complexité associée aux approches héritées.

Accès sécurisé aux applications : Akamai garantit que seuls les utilisateurs et terminaux autorisés ont accès aux applications internes dont ils ont besoin, et non à l'ensemble du réseau de l'entreprise. Aucun utilisateur non autorisé ne peut accéder directement aux applications, car celles-ci ne sont pas visibles sur Internet et restent inaccessibles au grand public. Enterprise Defender intègre à un seul service la protection des chemins d'accès aux données, l'authentification unique, l'accès basé sur l'identité, la sécurité des applications, la visibilité des opérations de gestion et le contrôle centralisé.

Web Application Firewall (WAF) : Akamai offre une protection étendue pour les applications Web essentielles contre les attaques applicatives Web et DDoS les plus importantes et les plus sophistiquées. Notre WAF propose des mesures de protection destinées aux sites Web, mises à jour par la meilleure équipe de recherche sur les menaces du secteur, pour aider les entreprises à faire face aux menaces de sécurité en constante évolution.

Accélération des applications : Akamai aide les entreprises à diffuser des applications rapides, fiables et sécurisées de manière économique. Les entreprises peuvent ainsi relever les défis liés à la diffusion d'applications professionnelles sur Internet en plaçant les fonctionnalités de diffusion d'applications au sein de l'Akamai Intelligent Edge Platform, à proximité immédiate des utilisateurs, du cloud et des charges de travail sur site, partout dans le monde.



Accès aux applications, accélération et contrôles de sécurité en bordure de l'Internet

Tenez les utilisateurs à l'écart du réseau de votre entreprise

Authentification unique et multifactorielle pour les applications d'entreprise

Blocage de l'accès aux domaines, URL et contenus malveillants partout dans le monde

ENTERPRISE DEFENDER

AVANTAGES POUR VOTRE ENTREPRISE

- **Arrêter la propagation des logiciels malveillants et les mouvements latéraux**
  Dans les réseaux traditionnels basés sur le périmètre, les logiciels malveillants pénètrent généralement en profondeur en raison d'un manque de segmentation et d'une mauvaise visibilité du réseau. Avec Enterprise Defender, l'association de contrôles d'accès plus granulaires pour des applications spécifiques et d'une prévention proactive des menaces complique la propagation des logiciels malveillants ou l'accès des pirates à d'autres charges de travail.

- **Réduire la complexité et rationaliser les opérations**
  La sécurité basée sur le cloud, telle qu'Enterprise Defender, permet aux équipes de remplacer les équipements matériels ou virtuels coûteux à gérer et à entretenir par un simple service de sécurité en bordure de l'Internet.

- **Réduire à la fois les dépenses d'investissement et d'exploitation pour la sécurité**
  L'amélioration de la sécurité est invariablement associée à une augmentation des coûts. Avec Enterprise Defender, ce n'est pas le cas. Au contraire, une sécurité améliorée associée à la simplicité du cloud permet aux responsables des technologies de sécurité de l'information et aux équipes de sécurité de renforcer plusieurs contrôles de sécurité disparates et de réduire les coûts de gestion.

- **Augmenter la visibilité et diminuer le temps de détection des violations**
  Lorsqu'on entend parler de violations, on entend souvent : « les acteurs malveillants n'ont pas été détectés pendant *n* mois » et « une fois le périmètre franchi, les acteurs malveillants ont pu se déplacer sans être détectés sur le réseau. » Avec Enterprise Defender, la combinaison d'une journalisation des accès aux applications plus granulaire et de contrôles de sécurité DNS offre une meilleure visibilité et accélère la détection des violations.

- **Empêcher les vols de données internes**
  Laisser les données tomber entre les mains d'acteurs malveillants peut avoir de graves conséquences pour l'entreprise, qu'il s'agisse d'amendes pour ne pas avoir pris suffisamment soin des données personnelles ou de la perte de revenus causée par le vol de propriété intellectuelle ou de plans stratégiques. Avec Enterprise Defender, empêchez les vols de données internes avec des contrôles d'accès adaptatifs basés sur le « moindre privilège » et une visibilité et une sécurité basées sur le DNS.

- **Favoriser la transformation digitale des entreprises**
  Les équipes informatiques et de sécurité peuvent devenir partenaires dans la transformation digitale. Avec la sécurité basée sur le périmètre, les équipes ont acquis une réputation de gardiens paranoïaques. Une fois qu'elles ont autorisé l'accès au périmètre de l'entreprise pour prendre en charge un nouveau service cloud, partenaire ou modèle client, elles ouvrent une porte ou une connexion à l'ensemble du réseau d'entreprise. Avec Enterprise Defender, ce n'est pas le cas : l'accès n'est accordé qu'à un nombre limité d'applications, en fonction du contexte d'identité et de sécurité, sans jamais accorder l'accès à l'ensemble du réseau. De plus, vous pouvez établir une culture d'entreprise actuelle et mobile en bloquant l'accès aux domaines, URL et contenus malveillants, que vos utilisateurs se trouvent au bureau ou dans un café local.