PRÉSENTATION DE LA SOLUTION AKAMAI

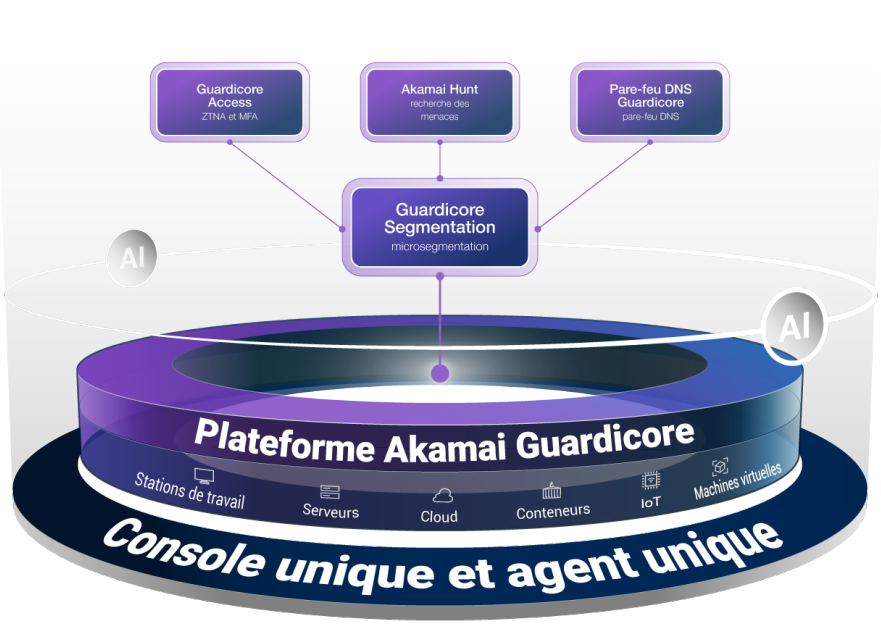
La plateforme Akamai Guardicore : sécurité Zero Trust

La mise en œuvre du modèle Zero Trust est extrêmement complexe et coûteuse pour la plupart des entreprises, en particulier lorsque ces protections doivent couvrir les ressources sur site et dans le cloud, ainsi que des collaborateurs travaillant au bureau ou à distance. La plateforme Akamai Guardicore a donc été conçue pour répondre efficacement à toutes les facettes du modèle Zero Trust avec une console et un agent uniques.

Alors que les cybermenaces deviennent de plus en plus sophistiquées et que les exigences réglementaires ne cessent de se renforcer, les entreprises sont soumises à une pression considérable pour sécuriser leurs réseaux tout en maintenant leur efficacité opérationnelle. La plateforme Akamai Guardicore offre une solution Zero Trust complète pour relever ces défis, en fournissant aux entreprises les outils et les fonctionnalités nécessaires à la mise en œuvre efficace d'un modèle de sécurité Zero Trust robuste.

Elle a été conçue pour mener à bien des projets Zero Trust en associant au sein d'une seule et même plateforme la meilleure microsegmentation, Zero Trust Network Access (ZTNA), un pare-feu DNS et la recherche des menaces. Ensemble, ces composants rationalisent les efforts du modèle Zero Trust pour réduire considérablement la surface d'attaque et renforcer la sécurité dans l'ensemble de l'entreprise.

La plateforme Akamai Guardicore



Microsegmentation

La microsegmentation est l'un des composants clés de la plateforme Akamai Guardicore. Traditionnellement, la sécurité du réseau reposait sur des défenses périmétriques qui se concentraient sur la sécurisation des limites extérieures du réseau. Cependant, avec l'évolution des cybermenaces, il est de plus en plus évident que les défenses périmétriques ne suffisent plus à se protéger contre les attaques sophistiquées.

Avantages

Infrastructure consolidée
Déployez votre infrastructure rapidement et adaptez-la sans effort, avec un impact minimal sur les performances.

Visibilité étendue et riche
Obtenez des informations complètes sur les ressources et les communications réseau.

Moteur de règles unifié
Simplifiez l'application des règles dans divers environnements à partir d'une interface utilisateur unique.

Flexibilité modulaire
Tirez parti de composants modulaires adaptés aux besoins de votre entreprise.

Une couverture complète
Protégez toutes vos ressources sur site et dans le cloud, ainsi que les utilisateurs travaillant au bureau et à distance.

Les meilleures solutions de leur catégorie
Associez la microsegmentation de pointe et la technologie ZTNA pour une meilleure sécurité.

Akamai

La microsegmentation adopte une approche différente en divisant le réseau en segments plus petits et plus faciles à gérer, et en appliquant des règles de sécurité à chaque segment basées sur le principe du moindre privilège. Cette approche granulaire de la sécurité garantit que même si un segment est compromis, le reste du réseau est protégé. Avec Akamai Guardicore Segmentation, chaque ressource est protégée, y compris les centres de données sur site, les instances de cloud, les anciens systèmes d'exploitation, les terminaux IoT, les clusters Kubernetes et bien plus encore, sans jamais avoir à changer de console.

Zero Trust Network Access

Outre la microsegmentation, la plateforme Akamai Guardicore offre également des fonctionnalités ZTNA. ZTNA est un modèle de sécurité qui repose sur le Zero Trust, ce qui signifie qu'aucun utilisateur ou terminal ne doit être approuvé par défaut, même s'il se trouve à l'intérieur du réseau de l'entreprise. Au lieu de cela, l'accès aux ressources est accordé sur la base d'une vérification stricte de l'identité, de la posture du terminal et d'autres facteurs contextuels. Cette approche minimise le risque d'accès non autorisé et aide les entreprises à prévenir les violations de données et les menaces internes.

Pare-feu DNS

Le pare-feu DNS est un autre composant essentiel de la plateforme Akamai Guardicore. Le DNS (système de noms de domaine) est un composant fondamental d'Internet qui convertit des noms de domaine lisibles par l'homme en adresses IP. Cependant, celui-ci est fréquemment pris pour cible par les cyberattaques, car de nombreuses variantes de logiciels malveillants s'appuient sur le DNS pour communiquer avec les serveurs commande et contrôle ou pour exfiltrer des données. En déployant un pare-feu DNS, les entreprises peuvent bloquer les requêtes DNS illégitimes et empêcher les logiciels malveillants de communiquer avec des domaines malveillants, réduisant ainsi le risque de violations de données et d'autres cybermenaces.

Recherche des menaces

Enfin, la plateforme Akamai Guardicore inclut un service de segmentation adaptative qui permet aux entreprises d'identifier et de limiter de manière proactive les menaces de sécurité avant qu'elles ne dégénèrent en incidents. La recherche des menaces consiste à rechercher activement des signes de compromission au sein du réseau, tels qu'un comportement anormal ou des indicateurs de compromission (IOC). En tirant parti des outils et des techniques de recherche des menaces, les organisations peuvent garder une longueur d'avance sur les pirates informatiques et protéger leurs précieuses ressources.

En plus de ses fonctionnalités essentielles, la plateforme Akamai Guardicore offre également plusieurs avantages clés qui la distinguent des autres solutions de sécurité du marché. La plateforme fournit une infrastructure légère et consolidée qui minimise la multiplication des agents et la fatigue de la console, permettant aux entreprises de déployer et de gérer leur système de sécurité plus efficacement. En outre, la plateforme offre une visibilité étendue et riche sur les ressources et les communications réseau, permettant aux professionnels de la sécurité d'obtenir des informations complètes sur leur environnement réseau et de répondre aux menaces rapidement et efficacement.

> Dans le rapport Gartner®, Quick Answer: What Is Zero Trust Networking? Andrew Lerner, John Watts, 13 septembre 2023, « Gartner a suggéré de mettre en œuvre la microsegmentation et/ou la technologie ZTNA pour passer à un réseau Zero Trust. »*

* GARTNER est une marque commerciale et une marque de service déposée de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans le monde entier, et est utilisée dans le présent document avec son autorisation. Tous droits réservés.

Pour en savoir plus, consultez le site Sécurité Zero Trust d'Akamai.