FICHE PRODUIT AKAMAI

Akamai Guardicore Segmentation

Arrêter les mouvements latéraux avec une visibilité granulaire et des commandes de microsegmentation

L'infrastructure informatique d'entreprise ne cesse de s'éloigner des centres de données traditionnels sur site pour évoluer vers des architectures de cloud et de cloud hybride, où cohabitent toutes sortes de plateformes et différents modèles de déploiement d'applications. Bien que cette transformation digitale aide de nombreuses entreprises à améliorer leur agilité, à réduire leurs coûts d'infrastructure et à permettre le travail à distance, elle se traduit également par une surface d'attaque plus vaste et plus complexe sans périmètre bien défini. Chaque serveur, machine virtuelle, instance sur le cloud et point de terminaison constitue désormais un point d'exposition potentiel aux cyberattaques. De plus, avec la prévalence de menaces telles que les ransomwares et les vulnérabilités Zero Day, les hackers deviennent de plus en plus aptes à se déplacer latéralement vers des cibles de grande valeur quand (et non si) ils trouvent un moyen d'y entrer.

Akamai Guardicore Segmentation constitue le moyen le plus simple, le plus rapide et le plus intuitif d'appliquer les principes Zero Trust au sein de votre réseau. Conçue pour stopper les mouvements latéraux, cette solution visualise l'activité au sein de vos environnements informatiques, met en œuvre des stratégies de microsegmentation précises et détecte rapidement les éventuelles violations.

Principales fonctionnalités de la solution

Une segmentation granulaire, alimentée par l'IA

Les recommandations optimisées par l'IA, les modèles de remèdes aux ransomwares et autres cas d'utilisation courants, et les attributs précis de charge de travail (processus, utilisateurs, noms de domaine, etc.) permettent de mettre en œuvre des politiques en seulement quelques clics

Visibilité en temps réel et historique

Cartographiez les dépendances et les flux d'application aux niveaux des utilisateurs et des processus en temps réel ou sur une base historique

Prise en charge de plateforme étendue

Couvrez les systèmes d'exploitation récents ou anciens sur les serveurs dédiés physiques (bare metal), les machines virtuelles, les conteneurs, l'Internet des objets et les instances cloud

Étiquetage flexible des actifs

Ajoutez un contexte riche avec une hiérarchie d'étiquetage personnalisable pour favoriser la visibilité et l'application des règles, et une intégration aux outils d'orchestration et aux bases de données de gestion de configuration pour un étiquetage automatisé

Méthodes de protection multiple

Intégrez des fonctionnalités de renseignement sur les menaces, de défense et de détection des violations afin de réduire le temps de réponse aux incidents

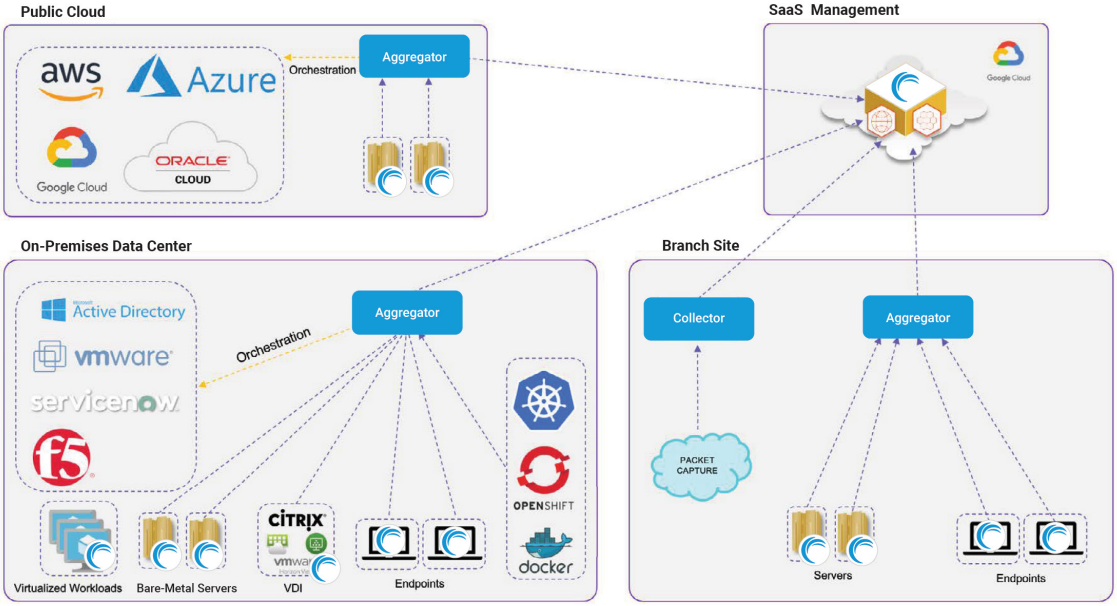
AVANTAGES POUR VOTRE ENTREPRISE

- Protège contre les ransomwares
- Met en œuvre le modèle Zero Trust
- Accélère la conformité
- Cloisonne les applications critiques
- Sécurise les migrations vers le cloud
- Protège les télétravailleurs
- Protège les points de terminaison
- Va plus loin que les pare-feux internes

Fonctionnement

Akamai Guardicore Segmentation collecte des informations détaillées sur l'infrastructure informatique d'une entreprise grâce à une combinaison de capteurs basés sur des agents, de collecteurs de données basés sur le réseau, de journaux de flux de cloud privé virtuel provenant de fournisseurs de cloud et d'intégrations permettant une fonctionnalité sans agent. Un contexte pertinent est ajouté à ces informations par le biais d'un processus d'étiquetage flexible et hautement automatisé qui inclut l'intégration aux sources de données existantes, telles que les systèmes d'orchestration et les bases de données de gestion de configuration.

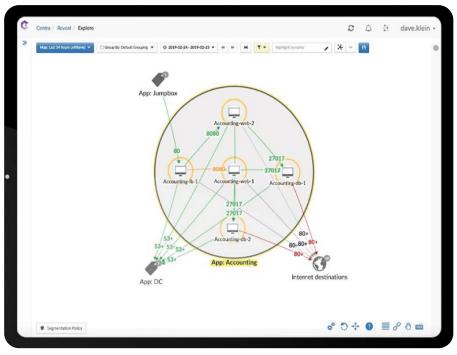
Topologie de l'infrastructure



La plupart des clients utilisent la gestion SaaS,
mais des options de gestion sur site sont également disponibles.

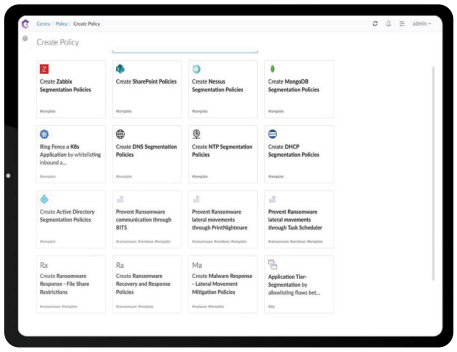
Cartographie du réseau

Le résultat est une carte dynamique de l'ensemble de l'infrastructure informatique qui permet aux équipes de sécurité de visualiser l'activité avec une granularité au niveau des utilisateurs et des processus en temps réel ou sur une base historique. Ces informations détaillées, associées aux flux de travail de politiques reposant sur l'intelligence artificielle, rendent la création de politiques de segmentation rapide, intuitive et basée sur un contexte de charge de travail réel.



Modèles

La création de politiques est simplifiée par des modèles prédéfinis pour les cas d'utilisation les plus courants. L'application des politiques est complètement dissociée de l'infrastructure sous-jacente, de sorte que les politiques de sécurité peuvent être créées ou altérées sans modification complexe du réseau et sans interruption de service. En outre, les politiques suivent la charge de travail, peu importe où elle se trouve : dans les centres de données sur site ou dans les environnements de cloud public. Nos capacités de segmentation sont complétées par un ensemble sophistiqué de fonctionnalités de défense contre les menaces et de détection des violations, ainsi que par Akamai Hunt, notre service managé de recherche des menaces.



Protection complète à grande échelle

Tout environnement

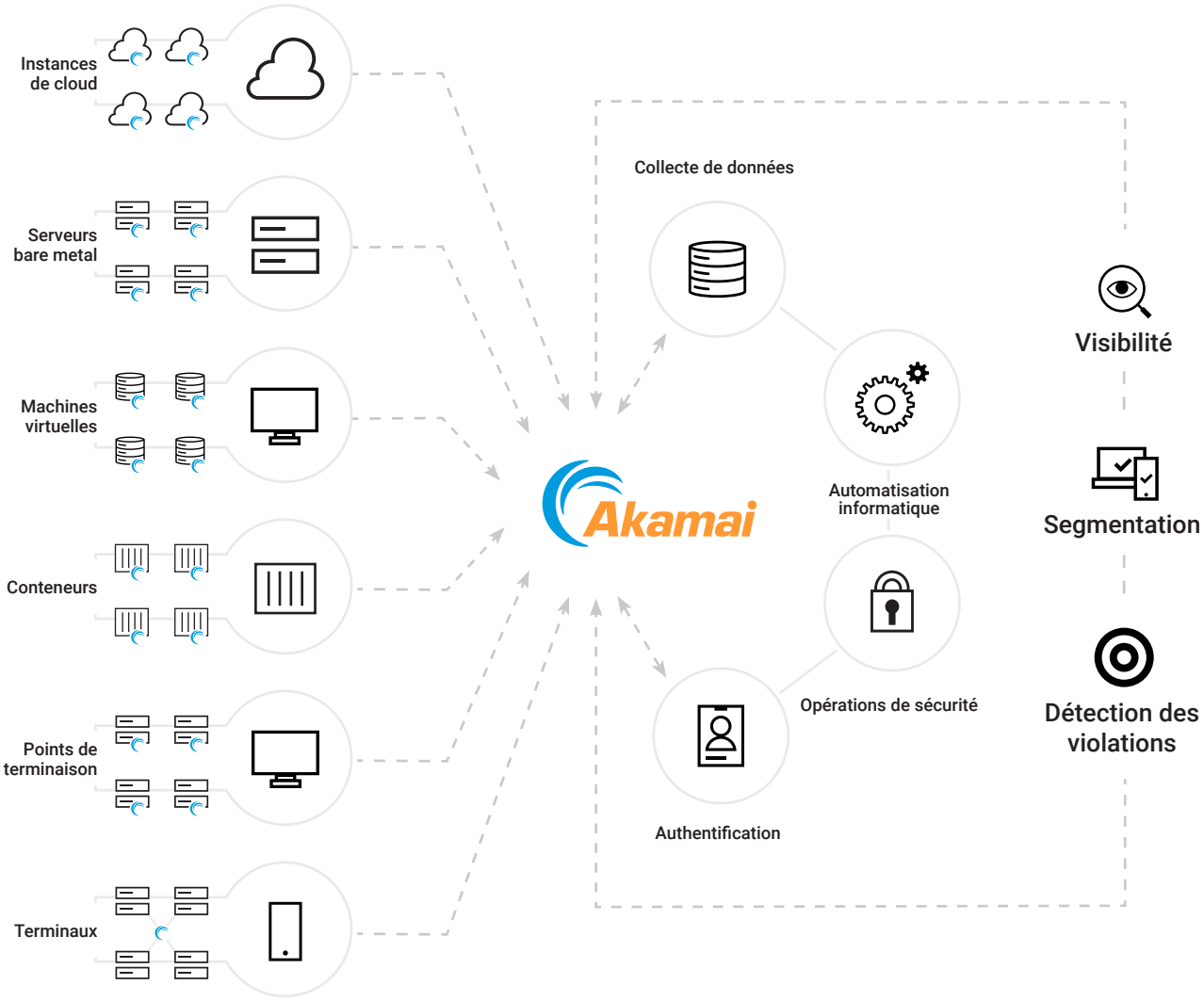
Protégez les charges de travail dans des environnements informatiques complexes grâce à une combinaison de charges de travail sur site, de machines virtuelles, de systèmes existants, de conteneurs et d'orchestration, d'instances de cloud public/privé et d'IoT/OT

Sécurité simplifiée

Simplifiez la gestion de la sécurité grâce à une plateforme unique qui permet la visualisation et la segmentation du réseau, la défense contre les menaces, des fonctionnalités de détection des violations et une application guidée des règles pour les initiatives Zero Trust

Évolutivité et performances de l'entreprise

Commencez par une protection ciblée de vos ressources digitales les plus critiques, puis faites-la évoluer pour couvrir l'ensemble de votre entreprise sans complexité, sans changements d'infrastructure ni goulets d'étranglement



Plateformes et technologies prises en charge

- Akamai Guardicore Segmentation est conçu pour s'intégrer à votre infrastructure existante.
- Notre prise en charge de systèmes d'exploitation s'étend en permanence, proportionnellement aux besoins de nos clients.
- Consultez la page de nos partenaires technologiques pour une liste complète de nos intégrations.

Systèmes d'exploitation

Linux

Apple

Microsoft

Unix

Fournisseurs de cloud public

Hyperviseurs

Orchestration de l'hypervision

Passerelles de sécurité

Orchestration des conteneurs et moteurs

Navigateurs pour la console Web

Exigences minimales de mémoire et de système

Management Server 32 GB RAM, 8 vCPUs, 530 GB	**Aggregator** 4 GB RAM, 4 vCPUs, 30 GB
Deception Server 32 GB RAM, 8 vCPUs, 100 GB	**ESC Collector** 2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

Pour en savoir plus sur Akamai Guardicore Segmentation ou pour demander une démonstration personnalisée du produit, consultez notre site à l'adresse akamai.com/guardicore.

 | Assistance | | Publication : 07/23