PRÉSENTATION DE LA SOLUTION AKAMAI

Informatique confidentielle : protection des données en cours d'utilisation

Alors que les menaces ne cessent de croître en portée, en échelle et en sophistication, les équipes de sécurité parviennent généralement à relever le défi, notamment en chiffrant les données lors de leur déplacement et en limitant leur accès durant le stockage. Mais il devient de plus en plus évident que les équipes doivent également protéger les données lorsqu'elles sont en cours d'édition, de lecture ou de traitement, communément appelées *données en cours d'utilisation*.

Cette lacune dans la protection des données en cours d'utilisation prend de plus en plus d'importance avec l'évolution de l'informatique et l'essor de l'IA. La prévalence de l'informatique hybride et multicloud a multiplié les moyens de collecte et de stockage des données par les entreprises. Pendant ce temps, alors que les entreprises cherchent à tirer parti de l'IA, elles utilisent d'énormes ensembles de données, souvent leurs données les plus précieuses et les plus sensibles, sans les chiffrer ni les protéger.

Ces risques alimentent l'intérêt pour l'informatique confidentielle, une approche de la sécurité qui garantit le chiffrement et la protection de toutes les données sensibles utilisées par les applications, les processus ou les services.

Les API, une source de complexité

Les API prolifèrent parce qu'elles servent des fonctions essentielles dans deux domaines dans lesquels les entreprises placent constamment des ressources : les environnements et services cloud et les modèles d'IA. Dans le cloud, les API jouent un rôle essentiel en permettant aux technologies de communiquer et de partager des données. Dans le domaine de l'IA, les grands modèles de langage (LLM) utilisent les API pour accéder aux données et les combiner afin d'effectuer des tâches complexes telles que la compréhension linguistique et la génération de texte.

Malheureusement, les API ne reçoivent pas la même attention de la part des équipes de sécurité que les applications et l'infrastructure. Les attaquants exploitent cette faille de sécurité : 84 % des entreprises ont subi des incidents de sécurité des API au cours des 12 derniers mois.[1] Pour protéger les données sensibles avec lesquelles toutes les API liées au cloud et à l'IA entrent en contact, les entreprises ont besoin de fonctionnalités complètes de sécurité des API s'exécutant dans leurs environnements informatiques confidentiels.

Verrouillage des trois portes

Le verrouillage de vos données en transit et stockées peut toujours laisser une porte ouverte (les données en cours d'utilisation), exposant les entreprises à des risques.

Avec l'informatique confidentielle, ces données sont traitées dans un environnement jugé digne de confiance sur le plan matériel. Les API permettent aux entreprises de déployer leurs propres instances privées d'apprentissage automatique, spécialement conçues pour sécuriser le trafic des API, plutôt que d'utiliser un service d'API dans le cloud public, ce qui réduit considérablement leur surface d'attaque. L'exécution d'une solution de sécurité des API dans un environnement informatique confidentiel constitue une couche de sécurité supplémentaire. Même si une partie du système est compromise, les données de l'environnement protégé restent sécurisées. L'exécution d'une analyse d'API sur ces données dans un environnement de confiance est plus sûre et élimine le risque inhérent aux environnements traditionnels.

Cette combinaison d'IA, de sécurité des API et d'informatique confidentielle permet d'empêcher les entités non autorisées, telles que l'hyperviseur, le propriétaire de l'infrastructure du système de l'opérateur hôte ou toute personne disposant d'un accès

Avantages pour votre entreprise

Sécurité des données renforcée
Limitez l'accès aux données en cours d'utilisation grâce à des contrôles rigoureux, qui réduisent la surface d'attaque et protègent les processus sensibles pilotés par les API contre les accès non autorisés

Protection des API
Effectuez une analyse approfondie du trafic des API tout en chiffrant les données sensibles en cours d'utilisation, ce qui réduit le risque d'exposition lors de la surveillance

Conformité renforcée
Respectez les réglementations internationales strictes et en constante évolution en matière de protection des données, en garantissant la conformité aux normes sectorielles et gouvernementales

1. Akamai, Étude des impacts sur la sécurité des API, 2024

physique, de consulter ou de modifier le code ou les données pendant l'exécution, offrant ainsi une protection contre les menaces internes (par exemple, les administrateurs système malveillants ou les charges de travail exécutées sur une infrastructure non fiable) et les menaces externes (par exemple, les attaquants qui exploitent les vulnérabilités).

Avantages

Avec la prolifération des menaces visant les API et l'attrait que représentent les données utilisées, les attaquants ne sont jamais loin. Les entreprises prévoyantes commencent à adopter l'informatique confidentielle pour un certain nombre de raisons :

- Limitation de l'accès aux données en cours d'utilisation en premier lieu, grâce à des contrôles rigoureux
- Analyse sécurisée du nombre croissant d'API
- Respect des nouvelles exigences strictes en matière de protection des données dans le monde entier grâce aux contrôles que l'informatique confidentielle met à leur disposition

L'informatique confidentielle est particulièrement utile aux entreprises soumises à une réglementation stricte, qu'il s'agisse d'une société de services financiers cherchant à protéger les transactions en ligne ou d'une société spécialisée dans les sciences de la vie protégeant les données de ses patients. Cette approche peut également aider un éditeur de logiciels indépendant à protéger un modèle d'IA qu'il distribue à ses clients sur plusieurs sites, de la bordure de l'Internet au cloud. En effet, toute entreprise informatique exécutant un traitement analytique en temps réel sur ses données vitales doit tenir compte de l'informatique confidentielle.

L'aide que nous et nos partenaires pouvons vous apporter

Pour être efficace, l'informatique confidentielle nécessite un ensemble intégré de solutions fonctionnant en synergie pour assurer une protection et un contrôle complets. Akamai, en collaboration avec ses partenaires Intel et IBM, assure la sécurité des données en cours d'utilisation, du matériel aux API en passant par le cloud.

Tout d'abord, Intel® Trust Domain Extensions (TDX) fournit des environnements d'exécution de confiance qui :

- Protègent contre les intrusions extérieures provenant d'acteurs menaçants et/ou d'entités non malveillantes qui ne devraient pas y avoir accès
- Améliorent la sécurité des logiciels qui contrôlent la technologie utilisée pour créer des ressources virtuelles dans le cloud, telles que les réseaux, les serveurs et le stockage
- Ajoutent une couche de sécurité indispensable autour des personnes qui administrent ces systèmes distribués, réduisant ainsi le risque d'erreurs fortuites et les cas potentiels d'activités malveillantes internes

En outre, les jetons et la vérification Intel Tiber™ Trust Authority permettent aux entreprises de limiter et de contrôler l'accès aux données non chiffrées en cours d'utilisation.

La solution Akamai API Security établit un inventaire des API utilisées dans l'entreprise, puis surveille et détecte la façon dont ces API sont utilisées. Elle détecte et empêche automatiquement les requêtes d'API malveillantes en analysant les modèles de trafic et les comportements, bloquant ainsi efficacement les menaces en bordure de réseau sans intervention manuelle. Cette solution assure une protection en temps réel contre les attaques d'API telles que les violations de données, les accès non autorisés et les abus de logique.

Ensemble, les moteurs d'apprentissage automatique à distance d'Akamai associés aux processeurs Intel Xeon® sur des IBM Cloud Virtual Servers, qui sont à leur tour sécurisés avec Intel TDX et certifiés par la solution Intel Tiber Trust Authority, offrent un environnement privé et hyperévolutif conçu pour empêcher toute menace extérieure d'accéder aux données lorsqu'elles ne sont pas chiffrées dans la phase finale de leur utilisation, qu'il s'agisse d'attaques de bot alimentées par l'IA ou d'attaques humaines.

Le moment est venu de protéger vos données en cours d'utilisation

Les entreprises ont besoin d'un environnement de confiance pour sécuriser leurs données les plus précieuses, non seulement lorsqu'elles sont stockées ou consultées, mais aussi lorsqu'elles sont en cours d'utilisation. Elles se tournent vers Akamai et ses partenaires pour obtenir une sécurité complète. Ensemble, ces entreprises informatiques de confiance garantissent la sécurité à chaque étape du cycle de vie des données.

Découvrez comment notre partenariat dans le domaine de l'informatique confidentielle peut vous aider à protéger vos données sensibles.
En savoir plus sur la solution Akamai API Security.