PRÉSENTATION DE LA SOLUTION AKAMAI

API Security pour le secteur de la santé

Découvrez comment la solution Akamai API Security aide les prestataires de soins de santé à identifier les menaces ciblant les API et à s'en défendre.

Les API permettent aux prestataires de soins de santé d'améliorer et de rationaliser les soins aux patients en facilitant un échange fluide de données entre les systèmes, les appareils et les personnes. Cependant, ces données sont souvent sensibles, telles que des dossiers de patients et des polices d'assurance, ce qui fait des API une cible de grande valeur pour les pirates.

Vos API sont-elles en danger ? Examinez les conclusions suivantes de l'étude 2024 des impacts sur la sécurité des API :

- Près de 85 % des établissements de santé ont connu des incidents de sécurité des API en 2024, contre 79 % en 2023.
- Seuls 24 % de ces établissements disposant d'un inventaire complet de leurs API savent lesquelles échangent des données sensibles, contre 40 % en 2023.

Dans le même temps, les responsables informatiques et de la sécurité de plusieurs secteurs d'activité déclarent dépenser en moyenne plus de 943 000 dollars américains pour traiter les incidents de sécurité des API et s'en remettre.

Les API permettent un échange de données fluide, offrant aux établissements de santé les avantages d'une interopérabilité et d'une efficacité accrues. Cependant, les API élargissent également la surface d'attaque : le risque augmente en parallèle de la multiplication des API dans les applications, les environnements cloud et les modèles d'IA. Les établissements de santé déploient par inadvertance des API mal configurées, mal testées et conçues sans contrôle d'accès, ce qui facilite le vol de données et la perturbation des opérations par les pirates.

Akamai API Security aide les fournisseurs à découvrir le nombre d'API dont ils disposent et les types de données qui transitent par ces API, et leur offre les moyens de protéger ces données à tout moment. Malheureusement, de nombreux professionnels de santé considèrent les API comme un outil de sécurité traditionnel des applications. Cependant, les équipes de sécurité des applications et de DevOps doivent réfléchir séparément aux questions de sécurité uniques que les API leur posent à chacune. En tant que technologie fondamentale permettant la mise en place de soins de santé modernes, les API présentent de nouveaux risques que les outils traditionnels ne peuvent pas gérer.

Pour mettre en place un programme robuste de gouvernance et de sécurité des API, les entreprises doivent collaborer avec le fournisseur de sécurité des API approprié. Dans le secteur de la santé, les flux de données non surveillés présentent des risques importants. Pourtant, de nombreuses entreprises ne disposent toujours pas d'un inventaire complet de leurs API. Akamai API Security aide les institutions à bénéficier d'une visibilité totale sur leur environnement d'API en identifiant toutes les API actives et en analysant les types de données qu'elles gèrent. À partir de là, notre solution assure une protection continue grâce à la gestion des ressources, à l'analyse des données sensibles, à la détection des anomalies, aux tests de sécurité des API, à l'intégration CI/CD et à une correction à la fois manuelle et automatisée, qui s'intègrent de manière transparente aux flux de travail tiers.

Défis

- Les API élargissent la surface d'attaque
- Près de 85 % des établissements de santé ont connu des incidents de sécurité des API en 2024

Comment Akamai API Security répond aux menaces qui ciblent les API

La solution d'Akamai est spécialement conçue pour aider les établissements de santé à protéger leur environnement API.

Détection complète des API

Identifiez et inventoriez les API de votre environnement, notamment RESTful, GraphQL, SOAP, XML-RPC et GRPC. Détectez les API non gérées ou obsolètes qui ne sont pas couvertes par votre passerelle d'API et gagnez en visibilité sur leurs attributs et leurs métadonnées.

Comprendre le comportement des API et détecter les menaces

Tirez parti de l'analyse basée sur l'IA pour identifier automatiquement les risques de sécurité tels que les fuites de données, les accès non autorisés, les erreurs de configuration et les activités suspectes. Gardez une longueur d'avance sur les menaces grâce à une surveillance continue et à la détection des anomalies.

Protéger les API et corriger les failles de sécurité

Bloquez les attaques en temps réel, corrigez les erreurs de configuration de la sécurité et mettez automatiquement à jour les règles de pare-feu pour arrêter le trafic malveillant. Intégrez en toute transparence la solution aux écosystèmes de sécurité existants, tels que les WAF, les systèmes de gestion des tickets et les plateformes SIEM, afin d'améliorer vos capacités de réponse.

Tester les API de manière proactive avant le déploiement

Assurez-vous que les API sont soigneusement testées dans le cadre du cycle de développement, ce qui permet de détecter les défauts de logique métier, les erreurs de configuration et d'autres vulnérabilités avant qu'elles n'atteignent la production. En intégrant rapidement les tests de sécurité, les entreprises peuvent gérer les risques de manière proactive et renforcer leurs défenses API.

Akamai API Security

De la détection des API et de l'analyse des risques aux tests et à la conformité des API

Pour en savoir plus, rendez-vous sur notre page API Security ou contactez l'équipe commerciale d'Akamai.