

Témoignage de client d'Akamai

Aflac renforce ses activités digitales contre les attaques d'API

Bénéficiaire d'une visibilité totale et de la capacité de corriger les vulnérabilités avec API Security



Le manque de visibilité était une préoccupation majeure chez Aflac

Les entreprises de services financiers doivent innover à un rythme effréné à mesure que les utilisateurs continuent de s'éloigner des expériences physiques au profit des interactions digitales. Aflac ne fait pas exception à la règle. Cependant, pour atteindre ses objectifs de transformation digitale, Aflac a dû adopter une approche distribuée plutôt que centralisée pour déployer de nouvelles applications. Si cette approche a été bénéfique du point de vue de la gestion des ressources, elle a néanmoins ajouté de la complexité à un scénario de gestion des actifs déjà délicat.

En outre, la société dépendait fortement de ses passerelles d'API existantes pour fournir une visibilité sur son parc d'API. C'était là aussi une question importante pour les dirigeants. Même si les passerelles d'API sont des composants de la pile de diffusion, elles ne sont pas conçues pour fournir les contrôles de sécurité et l'observabilité nécessaires pour protéger correctement les API. En outre, les API mises en œuvre en dehors d'une passerelle présentaient encore plus de problèmes de visibilité et de sécurité.

« Nous savions que l'empreinte de nos API était importante, et nous voulions être totalement sûrs que chaque API était prise en compte, que nous avions une visibilité totale sur leur fonctionnement et qu'elles étaient continuellement testées pour évaluer les risques de sécurité. Cet aspect était essentiel à notre stratégie de lutte contre le risque d'exploitation dans un contexte d'empreinte technologique en expansion », précise M. Goldsworthy.



Columbus, Géorgie
aflac.com

Secteur
Services financiers

Solution
Akamai API Security

Impacts majeurs

- Visibilité complète des API
- Protection en temps réel
- Identification précoce des vulnérabilités



Protéger les clients et leurs applications existantes

Outre l'obtention d'une vue d'ensemble complète du parc d'API, Aflac devait également assurer la défense de ses API contre les attaques. Compte tenu de sa réputation à toute épreuve et de sa portée mondiale, l'entreprise était bien consciente qu'elle pouvait devenir une cible. Elle avait besoin d'une [solution de sécurité des API](#) globale lui assurant non seulement de la visibilité, mais aussi la capacité de corriger les vulnérabilités et les attaques pour éviter de se retrouver à la une des journaux.

« Noname (désormais une entreprise Akamai) est la solution de sécurité API la plus avancée et la plus complète parmi toutes celles que nous avons testées. Elle dépasse même nos attentes initiales. Non seulement Noname offre la technologie nécessaire pour répondre à nos besoins actuels, mais j'ai également été satisfait des réponses apportées sur leur feuille de route pour relever les défis de sécurité émergents », ajoute M. Goldsworthy.

Aflac choisit un leader du marché

Après avoir évalué la plateforme Noname (désormais intégrée à Akamai API Security), Aflac a décidé qu'il s'agissait de la solution la plus complète pour protéger ses API, dont beaucoup résident dans son environnement AWS. La solution fournit à la fois la détection des API et la protection de l'exécution des API, ce qui permet à l'entreprise d'avoir une visibilité complète sur tous les types d'API dont elle dispose, y compris HTTP, RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC et gRPC.

Le module de détection des API fournit également des informations sur les types de données qui transitent sur les API de l'entreprise. Aflac peut ainsi savoir quelles API sont en mesure d'accéder aux données sensibles et identifier toute anomalie au niveau de l'accès aux données.

Cela signifie également que l'entreprise dispose d'une protection en temps réel pour contrecarrer toute attaque d'API. La solution utilise la détection automatisée de l'IA et de l'apprentissage automatique pour effectuer une analyse du trafic en temps réel et fournir des informations contextuelles sur les fuites de données, la falsification de données, les violations de politiques de données, les comportements suspects et les attaques de sécurité des API.

Akamai API Security fonctionne hors bande et tire parti de la mise en miroir du trafic VPC pour copier le trafic d'API depuis AWS Application Load Balancer dans l'environnement d'Aflac. Cette approche permet de surveiller le trafic sans impacter les performances. Les données sont ensuite transmises aux moteurs distants Akamai déployés sur des instances EC2 pour une analyse plus approfondie. La plateforme extrait également des informations à partir des passerelles d'API d'Aflac, en envoyant des journaux d'exécution et des journaux d'accès à Amazon CloudWatch. Les nombreux types d'intégrations qu'Akamai propose dans l'écosystème AWS permettent à Aflac de bénéficier du support requis pour répondre en toute confiance à ses obligations en matière de sécurité des données.



Noname (désormais une entreprise Akamai) est une entreprise visionnaire qui révolutionne la manière dont les entreprises abordent la sécurité des API. Elle continue d'innover et de résoudre de nouveaux défis de sécurité à un rythme remarquable. Elle apporte en permanence des solutions, car elle est à l'écoute de ses clients et s'investit dans leur succès.

– DJ Goldsworthy
Vice-président,
Opérations de sécurité et
gestion des menaces,
Aflac



Comment Aflac prévoit de se développer avec Akamai API Security

L'entreprise Aflac étudie déjà la manière dont elle prévoit d'étendre sa couverture de sécurité des API à l'échelle mondiale, notamment au Japon. L'Asie est un marché en plein essor pour l'entreprise, et elle veut s'assurer que ses clients sur les marchés émergents bénéficient du même niveau de sécurité. Cela lui permettra non seulement de se démarquer sur le marché, mais aussi de renforcer sa réputation en tant qu'entreprise axée sur le client.

L'entreprise implémente également le module de test de la solution Akamai API Security, ce qui permet aux entreprises d'identifier les vulnérabilités pendant le développement et de les corriger avant qu'elles n'atteignent la phase de production. Fidèle à l'approche « shift-left », le module de test fournit une batterie de tests de sécurité des API que les opérations de sécurité peuvent exécuter à la demande ou dans le cadre d'un pipeline d'intégration continue/diffusion continue (CI/CD) afin de s'assurer que les API sont implémentées en toute sécurité. Aflac perçoit les capacités de test d'Akamai API Security comme un avantage stratégique qui lui permettra d'améliorer les tests et d'enrichir les outils de sécurité de ses applications existantes avec une solution complète de test de sécurité des API.

« Aflac se réjouit qu'un véritable leader du marché sécurise son parc d'API. Nous avons confiance en la plateforme Noname Security (désormais intégrée à Akamai API Security), en son équipe et en sa vision. La valeur d'Akamai n'est plus à démontrer, et compte tenu de son impressionnante capacité d'innovation, nous avons hâte de voir ce que l'avenir de notre partenariat nous réserve », conclut M. Goldsworthy.



Aflac Incorporated, une entreprise du classement Fortune 500, fournit une protection financière à des millions de souscripteurs et de clients par l'intermédiaire de ses filiales aux États-Unis et au Japon. Lorsqu'un souscripteur ou un assuré tombe malade ou se blesse, Aflac verse rapidement des prestations en espèces pour les réclamations admissibles, directement à l'assuré (sauf indication contraire). Depuis plus de soixante ans, les polices d'assurance volontaire d'Aflac offrent aux souscripteurs la possibilité de se concentrer sur leur rétablissement, en toute sérénité sur le plan financier.