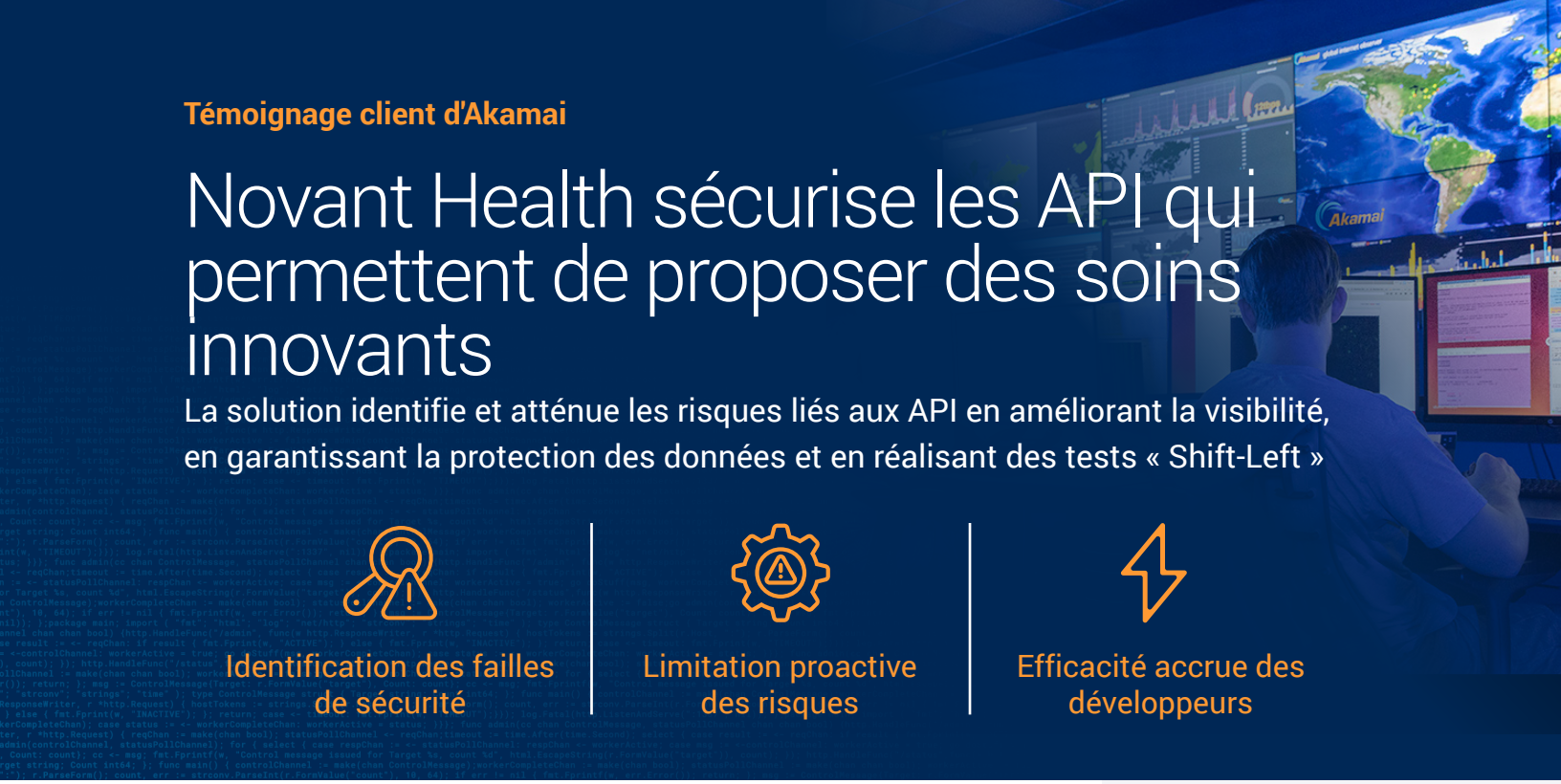
Témoignage client d'Akamai

Novant Health sécurise les API qui permettent de proposer des soins innovants

La solution identifie et atténue les risques liés aux API en améliorant la visibilité, en garantissant la protection des données et en réalisant des tests « Shift-Left »



Identification des failles de sécurité

Limitation proactive des risques

Efficacité accrue des développeurs

Combien de vies un système de santé peut-il améliorer en proposant des soins complets à l'échelle de la communauté ? Pour Novant Health, la réponse est sans appel :

- 6,8 millions de visites en clinique
- 155 964 patients hospitalisés pris en charge
- 602 590 visites aux services des urgences
- 22 082 naissances

Ces chiffres donnent également une idée claire des personnes et des systèmes qu'un établissement de santé doit protéger contre les menaces ciblant les données sensibles à travers des violations d'API.

L'enjeu

Novant Health est un réseau intégré à but non lucratif regroupant 16 centres médicaux et plus de 1 900 médecins, sur plus de 900 sites. Avec plus de 36 000 membres d'équipe et médecins partenaires, l'organisation basée à Winston-Salem fournit des soins en Caroline du Nord et en Caroline du Sud.

Grâce à une série d'initiatives digitales, Novant prodigue des soins plus personnalisés, efficaces et efficients aux patients. Les API sont au cœur de cette innovation, en permettant un échange fluide des données patient entre les applications, les appareils et les systèmes. L'importance des API est si essentielle que Novant a créé un centre d'excellence qui rassemble les personnes, les informations et les ressources nécessaires pour garantir un développement d'API de pointe.

NOVANT HEALTH

Localisation

Winston-Salem,
Caroline du Nord, États-Unis
novanthealth.org

Secteur

Santé et sciences de la vie

Solution

API Security

Akamai

L'équipe a considéré dès le départ que la sécurité des API était une priorité absolue, après avoir étudié l'impact des attaques sur les API utilisées par les professionnels de la santé. Les statistiques du secteur qu'ils ont découvertes par la suite les ont également stupéfaits, mais pas dans le bon sens. Par exemple, le coût moyen d'une violation de données dans le domaine de la santé s'élève à 9,7 millions de dollars. De plus, 79 % des établissements de santé ont connu un incident de sécurité lié aux API au cours des 12 derniers mois.

Identification du problème

Parmi les premières mesures identifiées, le centre d'excellence des API a déterminé qu'il fallait renforcer la sécurité des API dans l'ensemble de Novant. La seule solution mise en place était un pare-feu d'application Web (WAF). Ces outils offrent une protection contre les attaques déjà connues, mais les établissements de santé actuels exigent une approche plus globale de la sécurisation des API, notamment :

- Visibilité sur le nombre d'API existant dans l'environnement informatique d'une entreprise
- Informations sur les attributs de risque de chaque API, tels que les types de données traitées
- Analyse détaillée de la stratégie de sécurité des API de l'entreprise, incluant la détection des erreurs de configuration que les pirates exploitent
- Protection contre les attaques exploitant les failles de la logique métier des API

En outre, l'équipe du centre d'excellence de Novant a identifié des lacunes majeures dans l'approche « Shift-Left » de l'entreprise (intégration de la sécurité dès les premières étapes du développement). L'équipe disposait d'outils pour tester les conteneurs Docker, mais pas d'une solution de développement d'API. Avec des données sensibles telles que les dossiers de patients en ligne, l'équipe du centre d'excellence de Novant a reconnu que la société devait trouver un fournisseur dont le personnel et les solutions étaient à 100 % dédiés à la sécurisation des API.

Prise de conscience

Le centre d'excellence de Novant a commencé à échanger avec Noname Security (désormais une entreprise d'Akamai) après avoir pris connaissance de son approche globale de la sécurisation des API. Ensemble, ils ont réalisé une analyse détaillée de la gestion de la posture de sécurité de chaque API dans l'environnement informatique de Novant. Grâce à la plateforme de sécurité de l'API Noname (qui fait désormais partie d'Akamai API Security), l'équipe a identifié une faille dans Azure qui avait des conséquences majeures en matière de sécurité.

> Akamai a permis à Novant Health de combler une importante vulnérabilité et ainsi de bénéficier d'une meilleure visibilité sur l'une des ressources les plus fréquemment ciblées par les cybercriminels. Les découvertes de failles de sécurité exploitables dans notre écosystème d'API ont déjà fait leurs preuves. La protection des données est la première priorité de Novant Health. Akamai est en phase avec ces valeurs et est devenu un véritable pilier de notre système de sécurité des données.
>
> – Justin P. Byrd
> Vice-président, plateforme de données et intégration, Novant Health

Akamai

La solution de gestion de la posture de sécurité des API de la plateforme a révélé que certaines requêtes d'API dans l'environnement cloud de Novant étaient envoyées *en contournant* l'outil WAF, au lieu d'être traitées par celui-ci. Les cybercriminels contournaient le WAF à l'aide d'une « porte ouverte » que le WAF ne pouvait pas sécuriser et attaquaient en permanence les API de Novant, exposant la société à son insu.

Les informations fournies par Akamai se sont révélées à la fois choquantes et très utiles. Pour développer et gérer des API en toute sécurité, Novant Health avait besoin d'un espace de travail dans le cloud entièrement protégé. Le vice-président de Novant Justin P. Byrd et son équipe ont été impressionnés par la volonté de l'équipe d'Akamai de se retrousser les manches et d'appliquer sa solution de gestion de la posture de sécurité des API pour identifier et combler les failles de sécurité découvertes.

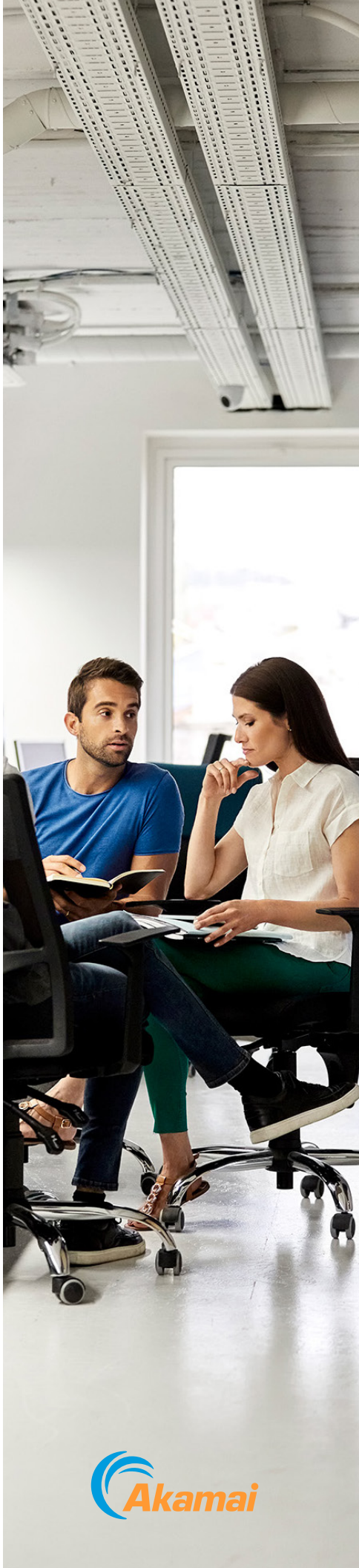
En s'appuyant sur ses découvertes initiales, l'équipe du centre d'excellence peut désormais utiliser les fonctionnalités automatisées de la solution de gestion de la posture de sécurité des API d'Akamai, qui vérifient en permanence les erreurs de configuration et les risques cachés des API pour permettre à la société de les éliminer de manière proactive. Cela passe notamment par l'identification des API et des utilisateurs internes capables d'accéder aux données sensibles.

Pour une organisation comme Novant, qui gère des données de santé issues de millions d'interactions avec les patients, il est essentiel de savoir quelles API interagissent avec des informations sensibles, afin de renforcer et de conserver la confiance des patients, des fournisseurs et des organismes de réglementation.

Sécurité et valeur métier

L'autre priorité du centre d'excellence de Novant, qui compte dans ses rangs des responsables techniques expérimentés, était d'intégrer la sécurité aux tests d'API de l'entreprise. La vitesse de développement d'une API est essentielle, et c'est d'autant plus vrai pour une organisation comme Novant, où les API jouent un rôle crucial dans la prise en charge des patients. Cependant, cette pression pour accélérer le développement favorise également l'apparition de vulnérabilités ou de défauts de conception lors d'un développement à marche forcée.

Le centre d'excellence recherchait des fonctionnalités de test d'API fiables pour évaluer les mesures de sécurité mises en œuvre dans chaque API. Cela implique de réaliser des tests complets pour identifier les vulnérabilités dans des variables telles que les mécanismes d'authentification, les contrôles d'autorisation, l'intégrité des données et les protocoles de chiffrement.



Bien sûr, la réussite du déploiement d'un nouvel outil de sécurité dépend non seulement de sa fonctionnalité, mais également de la participation des principales parties prenantes. Les développeurs comprennent l'importance de la sécurité, mais se méfient généralement des ralentissements qu'un outil inconnu peut entraîner dans leur quête de vitesse.

C'était le cas chez Novant Health, du moins au début.

Au fil de sa collaboration avec Akamai, l'équipe de Novant a déterminé un ensemble de fonctionnalités qui pourraient aider les développeurs à travailler de manière sécurisée tout en gagnant en efficacité. Par exemple, les tests actifs d'Akamai API Security permettent de détecter en amont les erreurs qui peuvent entraîner des problèmes importants et chronophages par la suite.

En outre, la solution a également permis au centre d'excellence de proposer des moyens rapides pour améliorer l'efficacité des développeurs, ce qui a agréablement surpris les membres de l'équipe, qui n'ont pas réalisé que la solution permettait également d'effectuer des contrôles d'assurance qualité non liés à la sécurité. Par exemple, ils peuvent désormais déterminer si les spécifications d'une API reflètent ses performances réelles. Les développeurs, peu enthousiastes au départ, n'ont pas tardé à comprendre à leur tour les avantages qu'offrent la solution en matière de sécurité et d'efficacité et se sont réjouis de travailler avec Akamai API Security.

« Dès le premier jour, Akamai a été un conseiller de confiance qui nous a aidés à découvrir, à protéger et à tester nos API à chaque étape, de la programmation à la production. Notre centre d'excellence peut désormais montrer à l'ensemble de l'entreprise comment conjuguer sécurité et efficacité », explique Justin P. Byrd. « Ce partenariat ne se limite pas aux produits. Les membres de l'équipe de Noname [désormais une société d'Akamai] comprennent notre domaine et les facteurs économiques qui motivent le développement d'API ».

La direction de Novant abonde également en ce sens, louant la capacité d'Akamai API Security à « détecter les anomalies avant qu'elles ne deviennent un problème » et à renforcer la stratégie de sécurisation des API en phase de développement de l'entreprise.

Tirer parti des gains d'API Security

Aujourd'hui, Novant utilise Akamai API Security pour fournir une « protection automatique » à ses API et à chacune de ses initiatives digitales. Grâce aux avantages dont bénéficie Novant en matière de découverte, d'inventaire, d'évaluation et de test des API, l'équipe du centre d'excellence applique désormais la protection complète de la plateforme aux nouvelles API que la société développe. L'équipe est convaincue que chaque API respectant les meilleures pratiques créée par les développeurs de Novant sera automatiquement protégée.

À l'avenir, l'équipe du centre d'excellence envisage d'étendre l'utilisation d'Akamai API Security à d'autres équipes au sein de l'entreprise. Dans l'optique de développer un modèle de collaboration inter-entreprises pour la protection des API, le centre d'excellence envisage de nouer un partenariat avec l'équipe de sécurité de Novant Health et l'équipe de structure de l'entreprise pour utiliser Akamai API Security.

NOVANT HEALTH

Novant Health est un réseau intégré à but non lucratif regroupant 19 centres médicaux et plus de 2 000 médecins sur plus de 900 sites, ainsi que de nombreux centres de chirurgie ambulatoire, des centres de soins, des programmes de rééducation, des centres d'imagerie médicale et des programmes de sensibilisation à la santé des communautés. Les quelque 40 000 membres de l'équipe et médecins partenaires de Novant Health répondent aux besoins médicaux des patients et des communautés de Caroline du Nord et de Caroline du Sud.

Akamai