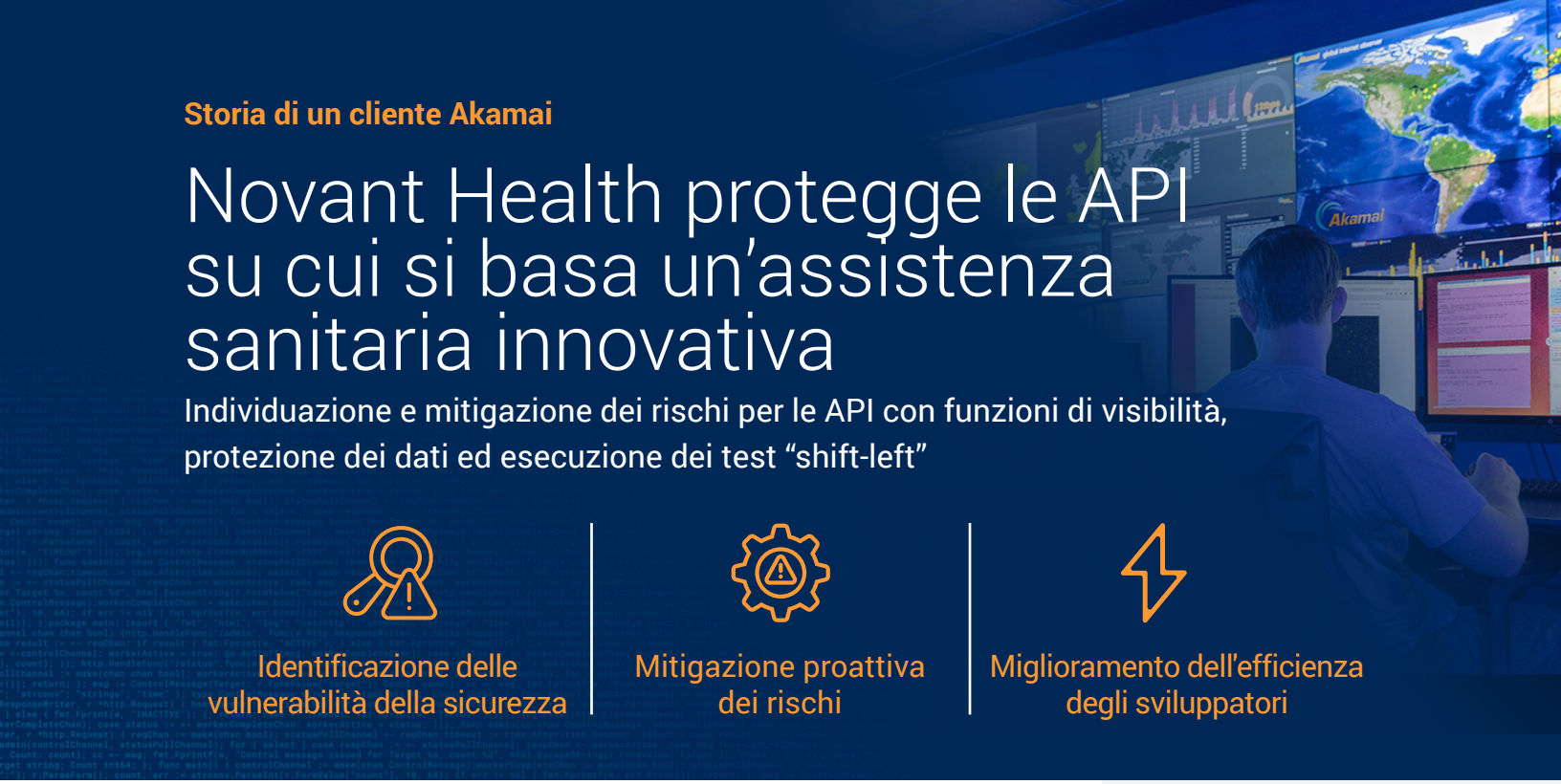
Storia di un cliente Akamai

Novant Health protegge le API su cui si basa un'assistenza sanitaria innovativa

Individuazione e mitigazione dei rischi per le API con funzioni di visibilità, protezione dei dati ed esecuzione dei test "shift-left"



Identificazione delle vulnerabilità della sicurezza

Mitigazione proattiva dei rischi

Miglioramento dell'efficienza degli sviluppatori

Quante vite può migliorare un sistema sanitario tramite un'assistenza completa e incentrata sulle comunità? Per Novant Health, la risposta è sbalorditiva, se consideriamo, tra l'altro, queste cifre:

- 6,8 milioni di accessi ospedalieri
- 155.964 pazienti ricoverati assistiti
- 602.590 accessi in pronto soccorso
- 22.082 nascite

Cifre come quelle riportate qui sopra offrono anche una chiara visione delle risorse di cui una struttura sanitaria ha bisogno per proteggersi dai criminali che prendono di mira i propri dati sensibili tramite la violazione delle API.

Conoscere la posta in gioco

Novant Health è un sistema integrato no profit che è costituito da 16 centri sanitari e da più di 1.900 medici dislocati in oltre 900 sedi. Con più di 36.000 dipendenti e collaboratori medici, l'organizzazione, che ha sede a Winston-Salem negli Stati Uniti, fornisce assistenza sanitaria nella Carolina del Nord e nella Carolina del Sud.

Tramite una serie di iniziative digitali, Novant rende l'assistenza sanitaria ai pazienti più efficace, personalizzata ed efficiente. Le API sono il fulcro di queste innovazioni perché consentono di scambiare facilmente i dati dei pazienti tra vari sistemi, applicazioni e dispositivi. In effetti, le API sono talmente importanti per Novant tanto che l'azienda ha realizzato un centro di eccellenza (COE) riunendo le persone, le competenze e le risorse necessarie per garantire il miglior livello di sviluppo dei prodotti per le API.

NOVANT HEALTH

Sede

Winston-Salem,
Carolina del Nord
novanthealth.org

Settore

Settore scientifico-sanitario

Soluzione

API Security

Akamai

Il team ha giustamente considerato la sicurezza delle API come la massima priorità fin dall'inizio, sapendo come gli attacchi alle API influiscano sulle aziende sanitarie. Anche i dati statistici di settore emersi nel loro percorso sono sbalorditivi, ma non in senso positivo. Ad esempio, il costo di una violazione di dati sanitari si aggira sui 9,7 milioni di dollari. Inoltre, il 79% delle aziende sanitarie ha riscontrato un problema di sicurezza delle API negli ultimi 12 mesi.

Individuare il problema

Come primo obiettivo aziendale, il COE ha stabilito la necessità di migliorare la sicurezza delle API in tutta l'organizzazione di Novant. L'unica soluzione messa in atto dall'azienda consisteva in un WAF (Web Application Firewall). Gli strumenti di questo tipo offrono una protezione da attacchi già noti, tuttavia oggi le aziende sanitarie richiedono un approccio più completo per la protezione delle API, che include, tra l'altro, i seguenti aspetti:

- Visibilità sul numero di API presenti nell'ambiente IT di un'organizzazione
- Informazioni sugli attributi di rischio delle API, come, ad esempio, i tipi di dati gestiti
- Analisi approfondite del sistema di sicurezza delle API di un'organizzazione, inclusi gli errori di configurazione sfruttati dai criminali
- Protezione dagli attacchi che sfruttano i difetti presenti nella logica aziendale delle API

Inoltre, il team COE di Novant ha identificato i principali problemi riscontrati nelle attività condotte dall'organizzazione per eseguire test "shift-left" o per integrare la sicurezza nelle fasi iniziali dello sviluppo. Inoltre, il team aveva messo in atto gli strumenti necessari per l'esecuzione di test sui container Docker, ma aveva bisogno di una soluzione per lo sviluppo delle API. Sapendo di poter mettere a rischio i suoi dati sensibili, come i dati sanitari dei pazienti, il team COE di Novant si è reso conto di aver bisogno di un vendor in grado di fornire persone e prodotti focalizzati al 100% sulla protezione delle API.

Scoprire i momenti eccezionali

Il COE di Novant ha avviato una serie di incontri con Noname Security (ora acquisita da Akamai) dopo aver appreso il suo approccio completo alla protezione delle API allo scopo di condurre un'analisi approfondita della gestione del sistema di sicurezza delle API presenti nell'ambiente IT di Novant. Utilizzando la piattaforma di sicurezza delle API di Noname (ora parte di Akamai API Security), il team ha identificato una vulnerabilità di Azure con notevoli implicazioni in termini di sicurezza.

> "Akamai ha colmato una lacuna significativa per Novant Health, offrendo all'azienda una maggiore visibilità su una delle risorse maggiormente prese di mira dai criminali. I risultati emersi finora relativamente alla vulnerabilità della sicurezza presenti nel nostro ecosistema delle API hanno già confermato il loro valore. Per Novant Health, la protezione dei propri dati è la massima priorità e Akamai si allinea a questa visione offrendo le funzionalità di base che servono all'azienda per il suo sistema di sicurezza dei dati.
>
> - Justin P. Byrd
> Vicepresidente, Data Platform and Integration, Novant Health

Akamai

La soluzione di gestione della sicurezza delle API offerta dalla piattaforma ha mostrato come alcune richieste effettuate alle API nell'ambiente cloud di Novant stavano entrando *nello* strumento WAF anziché tramite di esso. I criminali hanno bypassato la soluzione WAF tramite una "porta aperta" che lo strumento WAF non poteva proteggere e hanno attaccato ripetutamente le API di Novant, lasciando l'azienda vulnerabile e ignara della situazione.

Le informazioni fornite da Akamai sono risultate sbalorditive e si sono rivelate estremamente utili fin da subito. La capacità di sviluppare e gestire le API in modo sicuro da parte di Novant Health si basa sul fatto di disporre di uno spazio di lavoro nel cloud completamente protetto. Justin P. Byrd, vicepresidente di Novant, e il suo team sono rimasti favorevolmente colpiti da come i membri del team di Akamai si siano rimboccati le maniche per applicare la soluzione di gestione della sicurezza delle API in modo da poter individuare e mitigare le falle nella sicurezza non ancora scoperte.

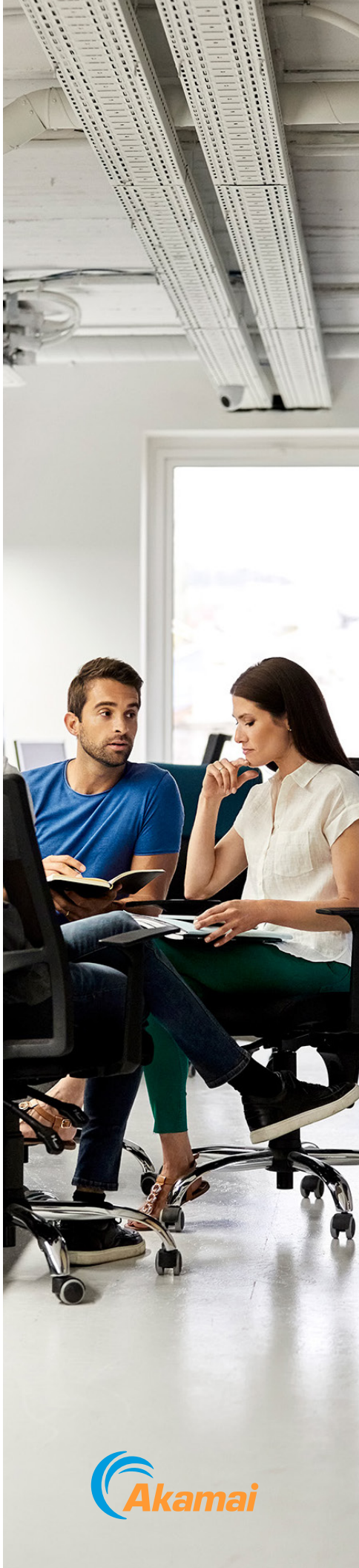
Basandosi sulle scoperte iniziali, il team COE ora può utilizzare le funzionalità automatizzate offerte dalla soluzione di gestione della sicurezza delle API di Akamai per controllare continuamente le API alla ricerca di errori di configurazione e rischi nascosti in modo da consentire all'organizzazione di intraprendere le misure adeguate per mitigarli in modo proattivo, come la capacità di identificare le API e gli utenti interni che possono accedere ai dati sensibili.

Per un'organizzazione come Novant, che si occupa della gestione di dati sanitari relativi a milioni di interazioni dei pazienti, il fatto di sapere quali API interagiscono con le informazioni sensibili è fondamentale per costruire e sostenere la fiducia con pazienti, provider ed enti di controllo.

Conseguire vantaggi per la sicurezza e le aziende

Per il COE di Novant, che include responsabili della progettazione con un'esperienza pratica, un'altra priorità è stata quella di integrare la sicurezza nei test condotti sulle API dell'organizzazione. La velocità dello sviluppo è fondamentale per tutte le API, specialmente per un'organizzazione come Novant, in cui le API svolgono un ruolo cruciale nell'assistenza ai pazienti. Tuttavia, la pressione necessaria per velocizzare lo sviluppo rende anche più semplice per una vulnerabilità o un difetto di progettazione passare inosservati nella corsa degli sviluppatori verso la fase di produzione.

Il COE ha cercato affidabili funzionalità di test delle API per valutare le misure di sicurezza implementate in ogni API, tra cui l'esecuzione di test completi per identificare le vulnerabilità presenti in variabili, come, ad esempio, meccanismi di autenticazione, controlli delle autorizzazioni, integrità dei dati e protocolli di crittografia.



Ovviamente, quando si implementa un nuovo strumento di sicurezza, il successo dipende non solo dalle funzionalità offerte, ma anche dal coinvolgimento delle parti interessate. Gli sviluppatori comprendono l'importanza della sicurezza, ma, considerando le loro esigenze di velocità, sono, di solito, sospettosi nel caso di rallentamenti che si possono verificare con uno strumento non consueto.

All'inizio, questo è stato il caso di Novant Health.

Collaborando maggiormente con Akamai, il team di Novant ha stabilito una serie di funzionalità in grado di aiutare gli sviluppatori a svolgere il loro lavoro in modo sicuro ed efficiente. Ad esempio, il modulo Active Testing di Akamai API Security potrebbe rilevare in modo proattivo gli errori che avrebbero la capacità di trasformarsi in problemi significativi e dispendiosi in termini di tempo nelle fasi successive del processo.

Inoltre, la soluzione ha anche consentito al COE di fornire agli sviluppatori brevi note per migliorare l'efficienza: una piacevole sorpresa per i membri del team COE che non si erano resi conto del fatto che la soluzione includeva anche controlli di qualità non relativi alla sicurezza. Ad esempio, ora il team può stabilire se le specifiche di un'API corrispondono a ciò che viene effettivamente fornito dalle API create. Non c'è voluto molto tempo prima che gli sviluppatori (all'inizio reticenti) facenti parte del team COE si rendessero conto dei vantaggi conseguiti in termini di sicurezza ed efficienza fino a diventare entusiasti di utilizzare Akamai API Security.

"Fin dall'inizio, Akamai ha fornito consigli affidabili su come scoprire, proteggere e testare le nostre API in tutte le loro fasi, dalla creazione del codice alla produzione. Il nostro centro di eccellenza, in tal modo, può mostrare all'intera organizzazione come conseguire nello stesso tempo sicurezza ed efficienza", ha spiegato Byrd. "Questa partnership non riguarda solo i prodotti: i membri del team di Noname [ora acquisita da Akamai] comprendono il nostro mondo e i fattori aziendali alla base dello sviluppo delle API".

I dirigenti di Novant si sono mostrati anche concordi nel riconoscere la capacità di Akamai API Security di capire le situazioni prima che possano diventare problemi, aiutando a cementare la sicurezza delle API nelle attività "shift-left" dell'organizzazione.

Basarsi sui vantaggi in termini di sicurezza delle API

Oggi, Novant utilizza Akamai API Security per proteggere automaticamente le proprie API e le attività digitali che si basano su di esse. Basandosi sui vantaggi riscontrati da Novant per individuare, inventariare, valutare e testare le API, il team COE applica ora la protezione completa della piattaforma alle nuove API sviluppate dall'azienda. Il team ritiene che, poiché gli sviluppatori di Novant creano le API in base alle best practice più appropriate, tutte le API verranno automaticamente protette.

Per il futuro, il team di COE prevede di espandere l'utilizzo di Akamai API Security ad altri team all'interno dell'azienda. Puntando a realizzare un modello collaborativo interaziendale per la protezione delle API, il COE si propone di instaurare una partnership con il team addetto alla sicurezza di Novant Health e il team della struttura basilare dell'organizzazione per l'utilizzo di Akamai API Security.

NOVANT HEALTH

Novant Health è un sistema integrato no profit che è costituito da 16 centri sanitari e da più di 2.000 medici dislocati in oltre 900 sedi, nonché numerosi ambulatori, poli ospedalieri, programmi di riabilitazione, centri di diagnostica per immagini e consultori. Novant Health si avvale di quasi 40.000 dipendenti e collaboratori medici per assistere i suoi pazienti e le comunità in cui opera nella Carolina del Nord e nella Carolina del Sud.

Akamai