Akamai Customer Story

Apree Health Matures Its Security Approach

The healthcare company harnesses Akamai solutions and expertise to evolve over time, from preventing credential stuffing to automating security measures

Zero attacks in 18+ months

Reduced overhead costs

Quickly know attack vectors

Redefining the healthcare experience

Apree health – formed by the merger of Castlight Health and Vera Whole Health — is on a mission to transform the way patients access and engage with care, providers deliver care, and employers and other purchasers pay for care. As it accelerates payment and care delivery transformation using technology and a unique clinical delivery model, the company interacts with personal health information (PHI). To ensure the fast, secure sharing of that information, apree calls upon solutions from trusted partner Akamai.

Enabling a top-down security approach

Apree empowers companies and their employees by providing a health navigation platform and mobile app that helps patients find affordable, high-quality care; access their health plan details and claims; manage benefits; and even track their health. Since the company's platform and app are enabled by more than 100 API partner integrations and over 1,000 third-party customer integrations, a top-down security-minded culture rooted in best practices is essential.

As David Quisenberry, Senior Manager of Information Security for apree, explains, "The only way to enable better health outcomes is through information sharing. But that information is highly sensitive and must be protected."

apree health

apree health

San Francisco, CA
apreehealth.com

Industry

Healthcare
and Life Sciences

Solutions

- App & API Protector
- Bot Manager Premier

Akamai

Such security is critical in light of today's attack types and trends, including social engineering and API attacks enabled by bots at scale. Holistically and effectively addressing security in such an environment requires continual prioritization and iteration, while showing evidence of strong protective measures.

Unfortunately, apree lacked the right solutions to empower its security operations (SecOps) team in this way. Its basic web application firewall notified the team of potential issues, prompting SecOps to manually investigate and determine the best response. When the company experienced an onslaught of credential stuffing via its mobile app, the team was overwhelmed by the time and expense required to investigate, report on potential impacts, and take action.

According to Cat Schwan, Senior Information Security Analyst for apree, "It was like playing whack-a-mole. We couldn't improve our security posture beyond a moment in time."

Securing the API ecosystem

Apree's first priority was preventing API attacks and blocking the associated exploits. Configuring Akamai's application and API protection solutions to its needs enabled the company to do just that. With Akamai, the security team adds a layer of security at the HTTP header layer on APIs used for POST requests and for partner integrations.

At the same time, Akamai shields the company and its mobile app from the flood of bots that caused so much work and worry. As it's been 18 months since apree has experienced any credential stuffing, it has significantly reduced the overhead costs associated with addressing these exploits. Just as importantly, apree can confidently secure the sensitive data that consumers, employers, and partners entrust to it. As Schwan says, "Akamai enabled us to nip credential stuffing at the root through a defense-in-depth approach. Our API ecosystem is now very secure, which is a huge relief to our architects."

Adding to this, Quisenberry explains, "It's key that we enable fast, secure access to our app and care guides, and our engineering team is thrilled by the ability to ensure that reliably with Akamai."

> “
>
> Akamai is an industry giant, and we are a relatively small company, but we get the solutions, time, and attention we need from Akamai to strengthen our security posture in line with best practices.
>
> **– David Quisenberry,**
> **Senior Manager of Information Security, apree health**

Scaling as needed

Although preventing API attacks was the impetus for partnering with Akamai, apree has benefited in a variety of other ways, as well.

Confidence in being secure — along with the ability to scale as needed — was critical when apree (then Castlight Health) teamed with Boston Children's Hospital (BCH) and the Centers for Disease Control and Prevention (CDC) to launch a free COVID-19 vaccine finder. BCH enlisted Castlight to build out the technology infrastructure that powers the solution with updated COVID-19 vaccine data, which translated to the first ungated experience that Castlight released. Akamai's global platform made it possible to automatically ensure that the vaccine finder showed accurate, up-to-date information.

"Akamai protected our back end from unauthorized web scrapers and enabled us to handle the huge volume of traffic associated with this high-risk, high-visibility project. It also ensured the app didn't get poached," says Schwan.

Rapidly identifying and responding to threats

The application protection features that apree implemented — including DDoS attack protection, origin defense, and advanced bot detection — work in concert with its intrusion detection system for rapid threat detection and intelligence. With Akamai's solutions as part of this stack, the company can more quickly and easily understand attack vectors.

For example, when apree identified injection attacks, Akamai provided immediate protection and visibility into the threat environment. "Akamai gave us the insights we needed to prioritize our vulnerabilities and patch 98% of our virtual machines within five days," says Quisenberry.

Enabling security automation

Moreover, Akamai has proven integral as apree migrates to Google Cloud to further shore up its security foundation. According to Schwan, "Akamai has made the migration much easier as we change our environment."

An early win was ensuring more robust security of Vera Whole Health's web apps during the merger with Castlight. "It was incredibly easy to merge those apps into our environment," continues Schwan.

In fact, both Google Cloud and Akamai will enable the automation — such as when making robust API calls — that the SecOps team envisions. “The fact that Akamai enables automated change control is incredibly valuable to us, empowering our teams to set security controls and share evidence of those,” Schwan continues.

By freeing the team to focus on further maturing security measures, Akamai is helping apree confidently move into the future. “Akamai contributes the technology, telemetry, and insights we need to enable an agile, automated security architecture,” concludes Quisenberry.

> “
>
> Akamai enabled us to nip credential stuffing at the root through a defense-in-depth approach. Our API ecosystem is now very secure, which is a huge relief to our architects.
>
> **– Cat Schwan,**
> **Senior Information Security Analyst, apree health**

Apree health is on a mission to build the first end-to-end healthcare solution that redefines the care experience and transforms the way patients access and engage with care, the way providers deliver care, and the way employers and other purchasers pay for care. Apree health does this by combining best-in-class navigation and data-driven insights, the most advanced primary care model, and value-based risk models to unlock health outcomes and make life better for those it serves.

apreehealth.com