CASE STUDY

Omada Health Meets HIPAA Compliance and Drives Operational Efficiency

About Omada Health

Omada Health is leading the digital revolution in chronic disease prevention and management. Specializing in the prevention and treatment of obesity-related chronic diseases, Omada also offers a hypertension program, and recently launched a mental health application focused on anxiety and depression.

Operating under HIPAA, Omada is highly regulated and places a premium on data and systems security. As Bill Dougherty, VP of IT and Security, puts it: “As the leading provider of digital care, protecting the health information of our participants is of the utmost importance. Trust and safety are a core part of our brand.”

Omada’s Challenges

Omada’s key challenges center on the need to meet rigorous compliance standards, provide exacting data and systems security, and manage continued hyper growth of over 50% per year in their customer base.

Omada’s customer base of large employers and insurance companies is extremely sensitive about security risk and HIPAA compliance, requiring Omada to constantly prove how secure their code and systems are and demonstrate 24/7 monitoring of their systems. In addition, since Omada is adding participants in their program at the rate of tens of thousands each month, the company needs technology that will scale rapidly and smoothly to accommodate this growth.

Before adopting F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, Omada worked with a vendor that only analyzed log files and provided an outsourced Security Operations Center (SOC). The combination of poor data and outsourced analytics forced Omada to spend countless hours each day sifting through hundreds of false positives along with escalated alerts that weren’t actionable.

omada

Founded
2011

Headquarters
San Francisco, CA

Industry
Hospital and Healthcare

Employees
~500

When Omada decided to switch vendors, they had a host of demanding requirements. Specifically, they wanted a platform that would gather data from across their infrastructure, including logs, system calls, and behavioral analysis based on a contextual understanding of their environment, while providing the ability to create customized rules as needed. They also wanted technology backed by a SOC that would analyze their security telemetry, escalate important alerts, provide actionable recommendations on remediation, help them improve operational efficiency, and proactively reduce their risk profile.

The Benefits of Adopting Distributed Cloud AIP

When Omada adopted the Distributed Cloud AIP, along with Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights services, they began seeing an immediate ROI.

Omada's security and operations specialists state that Distributed Cloud AIP's platform is more comprehensive and reliable than the previous vendor. According to Dougherty, Distributed Cloud AIP has a "really nice technology stack for solving intrusion detection that filters down to actionable information quickly and is backed by a Security Operations Center that I can depend on." He went on to say that the UI is "clean and easy to understand, pushing the right information to my fingertips so I get an actionable snapshot of where I'm at with the ability to dig down."

Using Distributed Cloud AIP, Omada recoups two to four hours of at least one security analyst's time per day. And since they only receive high priority, trustworthy, actionable information, the engineers save time as well: When a problem is escalated, they know it's something that needs to be acted on, and they have specific recommendations on how to remediate the issue.

According to Omada, most other vendors don't back up their technology with any kind of analyst service or a SOC that's watching it. And without that, Dougherty says, "The responsibility is placed back on the customer to determine which alerts represent real threats, and which are false positives. The only way we can run a lean and efficient staff is to rely on strong partners like [Distributed Cloud AIP]. There's just no other way."

Summing up, Dougherty points to Distributed Cloud AIP as a total solution: "We like dealing with [Distributed Cloud AIP] because they offer a complete solution. They back up their technology with security insights and expertise through its [Distributed Cloud AIP Insights and Distributed Cloud AIP Managed Security Services]—while most of their competitors rely on partners to provide services."

> *"We like dealing with [Distributed Cloud AIP] because they offer a complete solution. They back up their technology with security insights and expertise through their [Distributed Cloud AIP Insights and Distributed Cloud AIP Managed Security Services]—while most of their competitors rely on partners to provide services."*
>
> **Bill Dougherty, Omada Health, VP of IT and Security**

Expanding Omada's Partnership

As Omada plans their future growth, the company intends to expand their partnership with Distributed Cloud AIP based on the cybersecurity company's demonstrated history of enriching its platform and services to incorporate new technologies, optimize operational efficiency, and refine the security analytics it provides to customers. In Dougherty's view, this will support Omada as their team size doubles over the next year and their server counts grow by 30-40%. Dougherty is also confident that Distributed Cloud AIP's platform will be there to support him with container security monitoring as Omada accelerates the adoption of containers.

Omada Recommends Distributed Cloud AIP

When asked if he would recommend Distributed Cloud AIP as a partner, Dougherty stated that he already has based on the company's "comprehensive intrusion detection-based technology stack that gets to actionable information quickly and is backed by an Operations Center that I can depend on."

As Omada continues to mature and scale their technical infrastructure, they plan to leverage Distributed Cloud AIP to strengthen security and compliance, optimize operations, and achieve their goal of providing a "digital care program that empowers people across the chronic disease spectrum to set and reach their health goals by offering one dynamic program for multiple conditions."

About Omada Health

Named one of Fast Company's "50 Most Innovative Companies in the World," Omada employees include individuals from Google, IDEO, Harvard, Stanford, and Columbia. Their approach has been embraced by major employers across the country, including Costco and Iron Mountain, as well as leading health plans, such as Kaiser Permanente and Humana. Founded in 2011, Omada is headquartered in San Francisco, and has approximately 500 employees.

Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.