Apria Case Study

Headquartered in Lake Forest, California, Apria Healthcare is one of the nation's leading providers of home respiratory services and certain medical equipment, including oxygen therapy, inhalation therapies, sleep apnea treatment, enteral nutrition and negative pressure wound therapy. Apria operates over 300 locations throughout the United States and serves more than 1.8 million patients each year.

APRIA HEALTHCARE PROTECTS PATIENT DATA IN THE CLOUD AND WEB WITH NETSKOPE

Healthcare organizations balance protecting large amounts of personal and medical data with the need for quick access and easy movement by and to care providers, insurers, partners, and other affiliates. Apria Healthcare wanted to simultaneously embrace cloud across their organization to enable these initiatives and ensure their patients' personally identifiable information (PII) is protected. They explored ways to integrate the cloud into everyday processes and architecture. "The IT leadership team made a decision that we were going to be a cloud-first and mobility-first organization to support business strategies," says Jerry Sto. Tomas, Chief Information Security Officer at Apria Healthcare. "We have an IT security staff of 12 people, so we have to rely on partners to help us augment our security. To prevent data loss, combat evolving threats, and enforce data security policies across our internal, cloud, and web environment, we implemented Netskope."

PROTECTING HEALTH INFORMATION WITH NETSKOPE'S AWARD-WINNING CLOUD DLP

"As an industry with strict privacy and security regulations, we needed to implement increased cybersecurity measures to mitigate risk in the cloud" explains Sto. Tomas, "a robust Data Loss Prevention strategy was a critical part of our security program." The cloud may be changing how Apria delivers healthcare, but the sensitivity of health information hasn't changed. HIPAA requires healthcare organizations to safeguard the confidentiality, availability, and integrity of protected health information (PHI). Apria needed a modern data protection solution in place to identify PHI, eliminate access by unauthorized individuals, and to identify and control the flow of PHI in and out of cloud applications.

Netskope extends Apria's data protection policies to the cloud, ensuring that PHI and other sensitive data is not stored or shared with unauthorized individuals. "As we embraced the cloud, we needed to make sure that cloud services were secure. We want to share PHI within the organization but make sure we aren't sharing it outside," says Sto. Tomas. "We migrated our on-premise DLP policies to Netskope to increase visibility and scope of policy enforcement to the cloud and mobile devices. Now we can prevent PHI data from leaking to unsanctioned services and 3rd parties."

APRIA HEALTHCARE®

PROFILE

INDUSTRY
Healthcare

REGION
United States of America

CHALLENGES

- Inability to leverage the power of cloud due to security and compliance concerns
- Visibility and data security
- Comprehensive web classification and content filtering

BENEFITS

- Full control of SaaS and web, from one cloud-native platform
- Accelerated adoption of cloud services while enforcing security and compliance policies
- Govern web usage with comprehensive web classification and content filtering
- Protect employee and patients personally identifiable information
- Improve the ease and speed of sharing information—across multiple branches and business partners—to deliver better patient care

SOLUTIONS

- Netskope Data Loss Prevention
- Netskope for O365
- Next Gen Secure Web Gateway (SWG)

> “With Netskope Apria has implemented cloud and web data loss prevention policy enforcement without placing a burden on personnel, while also providing employees and patients the assurance that their personal information is in safe hands.”
>
> **Jerry Sto.Tomas** | Chief Information Security Officer at Apria Healthcare

SECURE ACCESS FROM MOBILE DEVICES

Most Apria workers are mobile, requiring access from anywhere. Apria has more than 300 locations with mobile drivers and remote employees working from different locations carrying devices. Mobility is an integral part of Apria’s cloud strategy. Their mobility solution is a combination of Mobile Device Management (MDM) to secure and manage IOS devices and Netskope to secure access and improve visibility. “When we first rolled out Netskope we learned that hundreds of cloud applications were being accessed by our users and gained insight into the who, what, where, context by device. We had the visibility we needed, regardless of device.” Using MDM and Netskope, Apria is able to take action like apply granular data loss prevention policies based on device type, classify devices as managed or unmanaged, and block unauthorized devices from accessing sensitive information.

IDENTITY-AS-A-SERVICE

Identity-as-a-service plays a key role in how IT teams addresses cloud security. Sto. Tomas explains, “Identity as a Service (IDaaS), Cloud Access Security Broker (CASB) and Third-party Risk Management are the fundamentals of a cloud security strategy. At Apria we use Okta to manage identities. Once users sign in through Okta for cloud service access, Netskope governs the usage of the services.”

EXPANDING THE NETSKOPE PLATFORM TO SECURE WEB ACCESS

Recently, Apria extended the Netskope Platform to enable advanced security of their web environment in addition to deep visibility and granular control for their SaaS applications. “With Netskope, we now have an integrated proxy for cloud and web along with a unified policy engine to simplify our security program and streamline administration and operations” says Sto. Tomas. Using Next Gen SWG, in addition to Netskope for SaaS, saves Apria’s security team’s time by avoiding redundant DLP and threat protection configuration steps and having to switch from one tool to the next. Unlike their legacy web proxy tool that overwhelmed security analysts with high volumes of log data, Netskope synthesizes web activity to what security teams need to focus on. This significantly cut costs for Apria without having to deploy anything new.

WHAT’S NEXT

"I need to ensure that I continue to be the enabler of the business" Sto. Tomas explains, “Netskope makes our cloud strategy possible from a security and privacy perspective.” Looking forward, Apria will continue to use Netskope to address cloud and web risk, enforce security policies, and to comply with regulation.