netskope | omada

Solution Story

How Data Security Puts the “Care” in “Healthcare”

Data loss prevention from Netskope is helping Omada Health deliver against its duty of care towards patients, customers, and employees.

Obesity affects 41.9% of adults in the U.S. and accounts for approximately $147 billion in annual healthcare costs[1]. Lying at the heart of multiple comorbid and chronic medical conditions such as type 2 diabetes, some forms of cancer, and heart disease[2], it is one of the most significant healthcare challenges facing the country.

KEEPING AMERICA FIT AND WELL THROUGH VIRTUAL HEALTHCARE

Since its founding in 2011, Omada Health has been on a mission to nurture lifelong health by tackling many of the most pervasive chronic conditions, such as prediabetes, diabetes, hypertension and musculoskeletal conditions.

The company achieves this goal through innovative virtual care programs combining smartphone apps, behavior science, and rigorous clinical protocols to help its members make long-lasting improvements to their health. Omada Health's users benefit from human-led, data-empowered care through a fully dedicated, 1:1 coaching model, including behavioral health support. Bill Dougherty, Chief Information Security Officer (CISO) at Omada Health, explained the company's business model: "Our customers are organizations that own the risk of individual's health decisions, such as insurance companies and large employers. Our proposition is twofold: we help improve the lives of their individuals and make them demonstrably happier, while also cutting healthcare costs by reducing long-term risk, because conditions like type 2 diabetes and hypertension can be hugely expensive. It's a win-win. By providing personalized care to individuals on behalf of our customers, people get healthier and more productive as a result."

THE DATA DUTY OF CARE

From a security perspective, Omada Health is responsible for protecting the data of its customers and its patients, as well as ensuring its own corporate data is safe. Healthcare data is extremely sensitive and is regulated by the stringent Health Insurance Portability and Accountability Act (HIPAA), a set of standards that outlines the lawful use and disclosure of protected health information (PHI).

As Dougherty explains, the company's business model exacerbates this central challenge of caring for data: "We hold health information on our patients and health information from our customers. We are obliged to treat these two datasets differently because in the latter instance we're effectively acting as business associates of our customers, so we have to enforce our customers' rules on the data rather than our own. We hold multiple forms of PHI that we must manage separately. And then of course on top of that we have the usual personally identifiable information [PII], corporate data, and financial data that come with their own requirements for control and protection. It's an extraordinarily complex environment."

[1] CDC, 2023: https://www.cdc.gov/nccdphp/dnpao/state-local-programs/fundingopp/2023/hop.html#:~:text=Poor%20diet%20and%20low%20levels,in%20annual%20health%20care%20costs.

[2] Forbes, 2023: https://www.forbes.com/health/body/obesity-statistics/

PROTECTING A CLOUD-FIRST BUSINESS

Adding yet more complexity to this challenge is the fact that Omada Health operates entirely in the cloud through a remote workforce. Having no enterprise servers of its own, the company uses only Software as a Service (SaaS) applications accessed from many hundreds of endpoints. "After the COVID-19 pandemic, we went remote-first and decided to never go back to the office. Today we have 700 employees, and they all work from home. It's the perfect model for us, but it does mean we need to double down on controlling what users do on our devices and mitigating against data exfiltration," explains Dougherty.

Simply locking down all data is not an option. Omada Health needs to find a balance between ensuring appropriate data use by employees and giving them the right level of access to work effectively. The challenge facing Dougherty and his team was that none of their existing security tools had the capability required to write rules and block inappropriate data sharing. If Omada Health was to ensure the levels of data loss prevention and control its customers demand, it would need to look elsewhere.

DATA LOSS PREVENTION THE NETSKOPE WAY

Today, Omada Health has deployed Netskope Data Loss Prevention (DLP) agents across all its endpoints. Thanks to the Netskope DLP, Omada Health can consistently discover, monitor, and protect sensitive data across endpoint and SaaS application, providing comprehensive coverage and unified data protection policies for every location where data is stored, used, or transferred.

"If I look at my universe of vendors, five or six of them say that they can provide DLP," says Dougherty. "But in fact, only Netskope provides the set of services we need to monitor and act at the edge. Because its solution is agent-based, the Netskope DLP can act in real time and just outright block inappropriate data sharing. It's ideally suited to our cloud-only architecture and remote-first operating model. Our control points cannot be in the network, because we don't have a network, so it has to be in the endpoint and at the edge."

With the Netskope DLP solution, Omada Health can set clear, granular policies around where and when employees can upload data, which map to the type of data in question. PHI, for instance, is governed by tighter controls than marketing data. Other policies control access to websites. The solution also provides forensic data so Dougherty's team can follow up on risky behaviors and help educate employees on best practice.

PROTECTING EMPLOYEES

In line with Omada's overall mission to care for all stakeholders, its DLP system helps it protect its workers from inadvertent data breaches that could damage the company's brand and lead to them losing their jobs. "Preventing mistakes is often hard to do," says Dougherty. "I can predict malicious behavior, but it's harder to predict a mistake. Netskope enables us to write rules that will protect us from both. That means we can fulfill our duty of care towards our customer and member data while also protecting our employees."

Dougherty prioritizes being upfront with employees and educating them on the controls the security team puts in place. “Once employees recognize that we are trying to protect them as much as the company and our data, they understand why DLP is so important,” says Dougherty. “In an increasingly sophisticated threat landscape they want to know we have their back.”

For Dougherty, the role of security is to say “yes” to employees, to enable them to work effectively and in a way that suits them, but to do so safely. To that end, the security team uses the Netskope DLP to send live alerts to users once a rule has been triggered. These alerts are structured to be informative and helpful, so that the employee in question understands why the system is blocking their activity. “On top of that, we’re very big on staff security training. We want our people to be as productive as possible, and in the modern world that means understanding the company’s security posture,” adds Dougherty.

A CARE-CENTRIC SECURITY MODEL

Security at Omada Health is always top of mind. “Trust is the foundation of the Omada programs, and implicit in that trust is a duty to be good stewards of the data”, says Dougherty. Health data is core to the company’s ability to provide personalized care programs and ultimately helps people live healthier lives. A data breach would not only impact current members , but would damage the company’s reputation and impact its ability to continue its mission to nurture lifelong health for future members.

Omada Health’s security posture also protects its business. A data breach is an existential threat to the company given the costs associated with losing a record. According to IBM and the Ponemon Institute, the average cost per record involved in a data breach is $165[3]. Given that Omada Health has already helped almost 1 million patients, and holds records on many more, the monetary loss of an extensive data breach would be devastating. Caring for data is therefore mission-critical to the company and its customers.

DEFENSE IN DEPTH

Asked if Dougherty has any lessons to share with his peers, he notes that effective DLP is an integral part of a layered defense posture. He explains: “Endpoints are the frontline of defense. They’re the doorway into the network and applications. The closer you move your policies and controls to the endpoint the better protected you will be. Netskope is one of the solutions we rely upon every day to keep our data safe.”

[3] IBM, 2023: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.