# Healthcare System Strengthens Web Application Security to Ensure Protection of Patient Data

Mount Sinai

### Profile

- Large private healthcare system based in the US
- Seven hospitals and award-winning Icahn School of Medicine (Clinical Research)

### Challenges

- Secure patient data for regulatory and compliance purposes
- Provide protection for new
- patient web applications
- Looking for a solution aligned
- with Microsoft Azure
- Ease of deployment and ongoing use

### Solution

Barracuda CloudGen WAF for Azure

### Results

- Happy customers
- Closed security gaps
- Deployed in a few hours through Microsoft Azure
- Patient data secured as application adoption grows
- Real-time Intelligence updates
- Additional grant dollars for more innovation with Sinai App Lab

**About Mount Sinai: Cutting-edge Innovation for Healthcare**

Mount Sinai is one of the largest private healthcare systems in the country, as well as among the top hospitals nationwide. With seven hospitals to its name, Mount Sinai also boasts the Icahn School of Medicine, an innovator in the medical field and an internationally recognized leader in clinical research. For Mount Sinai, innovation is key; the health system is currently providing a number of mobile applications to patients, with the goal of improving the relationship and accessibility between patients and physicians.

To help Mount Sinai connect and provide services to their patients, they created the App Lab, a team of innovators dedicated to helping patients and physicians stay better connected and track symptoms real-time using mobile devices. With leadership support and collaboration from IT and research teams, the App Lab provides cutting edge solutions for interacting with patients and collecting data on a massive scale, in real time.

**Collecting real-time Patient Data Using Mobile Devices**

Like many patients with chronic diseases, those with inflammatory bowel disease take things one day at a time, as symptoms tend to constantly flare and wane. Unfortunately, "it's very unpredictable," said Ashish Atreja, MD, Chief Technology, Innovation and Engagement Officer at Mount Sinai Health System. This presents a challenge for clinicians who typically only see each patient once or twice a year. Indeed, at Mount Sinai, physicians had "no way of tracking how the patient [was] doing once they left the offices," Atreja said.

> *We wanted to have the highest level of security and privacy for our patients. That led us to see how we could complement what Azure offers with additional security through Barracuda CloudGen WAF.*
>
> ***Doctor Ashish Atreja***
> *Chief Technology, Innovation, and Engagement Officer*
> *Mount Sinai*

Working with support from the National Institute of Health, Mount Sinai built a mobile app designed to help better manage this disease. The app, which was piloted during a clinical trial, enables patients to remotely share data about symptoms with physicians. These physicians, in turn, can then more proactively manage the disease.

## About Barracuda Security Solutions in Microsoft Azure Marketplace

Barracuda security solutions are engineered for Azure, and allow you to fully leverage the power of the cloud. Barracuda is a Gold Application Development Partner and is Microsoft Azure certified, which means solutions are well designed and pre-qualified by Microsoft. As part of the shared security responsibility model, Barracuda products complement existing Azure services by providing a comprehensive security architecture, as well as a more seamless experience across your cloud and on-premises environments—all while providing enhanced security against cyberattacks and advanced threats.

"With this mobile app, we get engaged with our patients and they enter data on a regular basis, weekly or biweekly. So we get to know which patients are on the right pill and which patients we need to pay more attention to," Atreja explained.

This is just one of six mobile apps that Mount Sinai is currently using. All of these apps allow patients to share data with their clinicians. Such data-sharing is becoming more common than ever before in the healthcare industry. In fact, there are currently 17,000 health applications available and 43 percent of these are designed for healthcare professionals, offering functionality such as remote monitoring, according to a study from research2guidance, a market research firm. As a result, clinicians can forge ahead with new care models.

"We've never had technology like this before where patients can easily enter data, but now with mobile phones and apps, we can allow that," he said. "All of our apps collect patient data . . . and then provide the data to physicians. So, we can move toward more proactive disease management."

**Facing Security Challenges**

However, the possibilities come with challenges. Mount Sinai, for example, needs to ensure that the data is shared securely, meeting all of the requirements associated with stringent HIPAA regulations. "If we do not protect security and maintain confidentiality of the patient data, then we actually are liable for penalties. We cannot just take any web application or any standard protocol and say it's safe. We have to go through an extra layer of security and governance and approval to ensure that . . . patient security and privacy and confidentiality is maintained," Atreja said.

Achieving this more sophisticated level of security, however, posed significant challenges. To start, in addition to adding mobile apps into the technology mix, Mount Sinai also was in the middle of merging complex legacy systems into its infrastructure as it transformed from a two- to seven-hospital system. What's more, the health system was generating a large volume of electronic health record and web application interfaces on premises and in the cloud. All of these systems include protected health information (PHI), which is covered under HIPAA and HITECH laws. So, it was crucial that this data remained secure in order to avoid violating federal laws.

Adding to the complexity was the fact that Mount Sinai was starting to leverage the cloud from a corporate IT standpoint with Microsoft Azure. As the health system explored moving workloads and applications to the Azure cloud, the main objective was to mimic the architecture in their on-premises environment, including the security measures and tools. It was important that the same security controls that were used on-premises were available in the cloud.

The legacy security technologies that Mount Sinai had in place were not powerful enough to protect their healthcare web apps across this hybrid infrastructure. Leaders wanted protection for coding vulnerabilities along with the highest level of security and privacy for their patients. Unfortunately, when they turned to one of its existing vendors to up the security quotient, things didn't go smoothly. "We struggled with our experience with trying to implement a web application firewall with one of our existing vendors in our physical data centers," said Kenny Liu, IT Security, Technology Specialist at Mount Sinai Health System. "We struggled trying to implement that, and in the end, we never fully implemented it because of the amount of overhead that was required for it."

As a result, Mount Sinai began to search for a solution on Azure that they could manage with a small InfoSec team. "We wanted to make sure we were doing our due diligence in terms of protecting that data in transit, at rest, and preventing it from attackers grabbing that data," Liu said.

**References**

Global Health Trends and Figures Market Report. Reseearch2Guidance. Accessed at: 500m people will be using healthcare mobile applications in 2015

### Choosing Barracuda

Based on a strong Microsoft recommendation citing the simplicity and intuitiveness of the user interface without compromising the feature set, Mount Sinai turned to the Barracuda CloudGen WAF . This solution enables the health system to protect web and mobile applications in the cloud – specifically Mount Sinai's six apps and patient portals behind the firewall, with a mix of HTTP and HTTPS.

"We realized with having the standard set of controls in place, like a network-based firewall, encrypting the data wherever possible, both at rest and in transit, and also having this additional layer of web application firewall to protect any sort of coding errors that may occur is what we needed to provide that umbrella coverage that we were looking for defending at multiple layers," Liu explained.

The Barracuda solution offered significant ease of use compared to the health system's previous experience. In fact, Mount Sinai was able to quickly get the web application firewall up and running in a matter of hours, starting with simple deployment from the Azure Marketplace, followed by hands-on Barracuda engineering help.

Using the Barracuda CloudGen WAF allowed Mount Sinai staff to see the firewall blocking malicious attacks in the logs along with enabling staff to secure encrypted traffic. They were comforted knowing that any potential coding weaknesses were not exposed to the Internet. They have reported no latency or performance degradation in applications, which allows them to make the firewall mainstream for all their upcoming mobile applications.

According to Liu, the solution does exactly what it is supposed to do as it "defends but doesn't have an impact on the performance of the apps." In the final analysis, Barracuda helps Mount Sinai securely deliver a high-touch healthcare experience using patients' mobile devices.

### About Barracuda Networks, Inc.

Barracuda Networks simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data, regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.