datawiza

/ CASE STUDY

Datawiza AMaaS Gives Medical Device Innovators Simple, Secure Path to Doctor, Patient, and Manufacturer Interactions

Consumer convenience is coming to healthcare. We're now accustomed to the ease of ordering and customizing our meals, groceries, rides, sneakers and more. Now, from 3D printing to remote patient monitoring, the field of personalized medical devices is exploding. Manufacturers can now supply patients with a variety of wearables, hearing aids, orthotics, implants and orthodontics that are tailored specifically to a patient's unique physiology and requirements. Manufacturers are also increasing their reliance on IoT technologies to enable real-time monitoring of patients using sensors attached to the new devices, such as alert bracelets, blood pressure monitors and even pacemakers. According to Precedence Research, the global wearable medical device market is expected to reach $89.45 billion by 2027, with a CAGR of 25.6% from 2020 to 2027, while according to Markets and Research, the global 3D printing medical devices market is expected to grow by more than $1.5 billion from 2020 to 2024, with a CAGR of 13%.

Along with these technologies, manufacturers have developed new ways to engage with doctors and patients, including online portals that allow for the ordering and customizing of devices, tracking updates and repairs, and educating teams on new products and techniques. The goal is to increase self-service for a more powerful, personalized and friction-free experience that enables doctors to help more patients while delivering better healthcare outcomes, shortening and improving the effectiveness of the supply chain.

For many of these companies, the new devices and ways of engagement have introduced new communication and network technology requirements. Many must also ensure compliance with ever-evolving privacy regulations because they are now collecting huge amounts of personalized doctor and patient information and must verify every time that the people accessing their systems are who they say they are and can access only the information they are authorized to access. Further, because their customer bases may be national or global, these companies must rely on distributed cloud technologies to ensure access and performance – without compromising security.

TODAY'S CHALLENGE

- HIPPA requirements add complexity to self-service web portals
- Insecure, difficult-to-use legacy authentication solutions
- High resource requirements to support OAuth SSO across multiple portals
- Expensive, hard-to-find security expertise

DATAWIZA ACCESS MANAGEMENT AS A SERVICE

- Painless SSO authorization for all apps in a hybrid environment
- Migration from legacy authentications to Okta with zero engineering effort
- Comprehensive, centralized, fine-grained policy management in a single console
- Turnkey solution built by security experts

The Challenge of Legacy Infrastructures

One manufacturer recently found itself in this exact situation. Several years ago, the company built a self-service ordering and customization customer portal using Apache Tomcat®, an open source Java-based development platform, and relied on Basic Auth, the simple authentication scheme built into the HTTP protocol, to authenticate users onto the system. The portal gave doctors control over ordering the company's custom-designed solutions, which included uploading sensitive patient information.

Recently, to meet new competitive demands and evolving customer requirements, the manufacturer wanted to add new video content to the portal but had to use a separate development platform. This raised several concerns. First, with HTTP Basic Auth, credentials are vulnerable. If not properly protected -- which is common since most developers are not security experts -- credentials can easily be intercepted, and once they are, cybercriminals can access all the resources in the associated account. Given the increasing sophistication and frequency of cyberattacks, the manufacturer wanted to integrate the portal with Okta for secure identity management (IM) in the cloud. The company also wanted to migrate to a modern and more secure authentication protocol, OAuth, which uses a token instead of the actual password when users log in. Tokens are more secure because they can specify access rules for the account, such as an expiration date or which applications can use the token.

Second, the manufacturer wanted to develop a separate platform using WordPress instead of Apache Tomcat to host training videos for how to use the company's products. Because WordPress has its own built-in authentication system, users would have to log in a second time when they wanted to access the video content. The company recognized that this would frustrate users and reduce usage, so it was eager to find a painless solution for single sign-on (SSO) while accommodating the company's rapid growth projections.

The options for solving these challenges were not appealing. Rewriting the Tomcat application using a more open platform was time and cost prohibitive. Another option, having the company's small development team use Okta's SDK to connect the Tomcat-based application to Okta, would still require a couple of months to accomplish, given the team's lack of experience with Okta or deep security expertise. Further, all that effort would not solve the SSO challenge since the available third-party plugins to allow WordPress to integrate with Okta would not work with Tomcat.

Fortunately the company found Datawiza.

Datawiza access management as a service

Datawiza access management as a service (AMaaS) enables companies to move to a modern authentication protocol and establish SSO across siloed on-premises and cloud applications without any coding.

The Datawiza Access Broker, a lightweight cloud-native proxy, connects applications and databases to SSO applications such as Okta and Microsoft Azure AD. The Datawiza Cloud Management Console provides comprehensive, centralized, fine-grained policy management, visibility and analytics across the entire environment. Datawiza consolidates access management across all data sources in hybrid multi cloud deployments for continuous, real-time trust and risk management, and companies can manage all types of data access, including remote workers, contractors, partners and customers. The system propagates a single identity definition update across all datastores and applications, simplifying access management while increasing security and reducing frustration for users who get immediate access to the content they need using a single login ID and password.

For the medical device manufacturer, Datawiza AMaaS acts as a smart bridge between the Tomcat-based portal application and Okta, allowing the company to migrate to Okta with zero engineering effort. Datawiza also establishes SSO across the Tomcat and WordPress platforms, allowing doctors to log in once to access all the information they need. A particular advantage of using Datawiza as a bridge, or broker, between multiple applications and the identity management solution is that as the applications evolve or the IM solution changes, Datawiza maintains the unified access management environment without any effort from the company.

Another way that Datawiza AMaaS has future-proofed the company's infrastructure is that it allows the company to create different access policies for different users or groups of users. For example, the company may eventually want to make different types of information available to different staff levels within a medical practice, or it may want to offer premium content for an additional fee.

Datawiza enables the company to easily add fine-grained authorization on top of its existing identity management services. As this company rapidly grows its business and expands its services, this capability is critical to support their self-service requirements.

Datawiza AMaaS ensures the company can continue to innovate and introduce new solutions without worrying that it will ever break its secure, unified SSO access management environment. It increases security by verifying every time that users are who they say they are and can access only the information they are authorized to access. And it provides all of this – rapid scaling, new applications, fine-grained authorization, new security protocols – without any recoding.

About Datawiza

The cloud-delivered Datawiza Platform offers Access Management as a Service (AMaaS) to secure applications and APIs based on the Zero Trust architecture, providing consolidated and continuous risk and trust assessment. Unlike other access management products (e.g., legacy web access managers) that are complex and siloed in hybrid environments, Datawiza offers large enterprises and SMBs a comprehensive, centralized and easy-to-deploy solution that allows every company to simplify access management, save time and increase security. Datawiza was founded in 2018 by security expert Dr. Canming Jiang, a veteran of Shape Security, now part of F5, and cloud expert Cunhao (Alex) Gao, a veteran of Google and Amazon. For more information, visit datawiza.com.