

Chugai Pharma Europe Combines SSO, MFA and VPN-less Remote Access with Idaptive



Chugai Pharmaceutical Co Ltd. is Japan's leading biopharmaceutical company. A member of the Roche Group, Chugai's mission is to add exceptional value through the creation of innovative medical products and services for the benefit of the medical community and human health around the world. Chugai Pharma Europe Ltd (CPE), is a subsidiary of Chugai Pharmaceutical Co Ltd, responsible for the European input to Chugai's global product development pipeline. CPE is an integral part of developing product candidates through to Market.

THE CHALLENGE

Leverage a comprehensive solution to provide SSO, MFA and EMM for Chugai's distributed infrastructure. Protect the company's IP as well as the confidential information of patients participating in clinical trials.

At Chugai Pharmaceutical Co Ltd, three different tools were used to provide single sign-on (SSO), enterprise mobility management (EMM) and multi-factor authentication (MFA) across the company's European and US divisions – Chugai Pharma Europe, Ltd. With a limited IT staff in each location, management of these separate solutions created unnecessary strain and considerable expense. Looking to simplify IT processes and save money, the company first considered expanding its relationship with its existing SSO provider.

"We have a mix of cloud and traditional on-premises web apps and we needed to provide secure access to all of them," says David Howell, IT Associate Director at Chugai Pharma Europe Ltd. "The SSO solution we were using was very effective for cloud-based apps, but lacked any capabilities to address our on-premises applications. And while they also provided an EMM component, there wasn't the level of control we needed."

The company was also looking to replace its existing MFA tool with a solution that leveraged users' mobile devices. "We were really looking for a solution that could address all of our identity management needs across the board," says Howell. "It would be much easier to manage, easier to support and less expensive in terms of user licenses."

Last, the company was specifically interested in a cloud-based solution. "Provider-hosted solutions mean lower infrastructure costs to us because we're not running the services on premises," says Howell. "So, we needed a cloud-based solution that included SSO, MFA and EMM to protect Chugai's intellectual property as well as the personal information of patients participating in our clinical trials."

THE SOLUTION

Chugai (Europe and North America) selected Idaptive to replace three disconnected tools already in use in the company. Key to the decision was Idaptive's ability to manage both web and on-premises app access.

Chugai discovered Idaptive because it was included in the Gartner Magic Quadrant, along with several competitive solutions. "I studied the Gartner material to understand industry and analyst perspectives," says Howell. "I looked at several of solutions, but when I took EMM and MFA into consideration, and the fact that Idaptive would cover both cloud and on-prem apps, I really didn't need to look any further."

During the evaluation process, Howell was particularly impressed by Idaptive's on-premises App Gateway, which delivers secure remote access to internal web apps like SharePoint without the need for a VPN. "Traditionally we've granted access to internal resources through VPNs, which works for laptops because they're easily installed and relatively simple to use," he says. "But we were challenged with providing that same access for the mobile devices used in the field."



With the Idaptive App Gateway, companies can encrypt and tunnel secure connections to on-premises applications without a VPN or the need to open ports in the firewall. Whether apps are in the cloud or on-premises, users get secure one-click access, and IT gets policy-based control and visibility without having to configure endpoint devices.

“The Idaptive App Gateway allows us to provide mobile access to on-premises systems like annual leave and finance right out of the box without any network changes – it was just a matter of clicking a check box in the app and then setting up a DNS connection,” says Howell. “Configuring additional policies like MFA requirements was also straightforward. It gave us a quick and easy deployment that also allowed us to phase out some of the VPNs we were using.”

THE RESULTS

The company has replaced three costly products with a single, cost-effective solution to fully address SSO, MFA and EMM requirements. Strain on IT resources has been alleviated. Centralized identity management has simplified policy enforcement across all apps and devices. Patient data is protected.

After a detailed testing phase, Chugai rolled out Identity Service to a pilot group of users in the UK. “We had a quick meeting with Idaptive Professional Services where they created our account, talked us through the various settings and trained us to configure apps and policies,” says Howell. “They walked me through the first cloud connector set up and the rest we did ourselves. With just a basic understanding of SAML and WS-Federation, it’s a fairly simple process.”

“The first app we implemented was Office 365 because it was the most fundamental to the company,” says Howell. “We provisioned a couple of additional internal apps and then rolled it out to the rest of the organization by letting Idaptive claim federation for the additional domains. It took about two hours for the changes to be replicated throughout the organization and we began seeing users register through the Idaptive dashboard without any issues.”

“One huge benefit is the Idaptive integration between PowerShell and Office 365 that makes quarantining and un-quarantining devices from Exchange ActiveSync incredibly simple. You basically just integrate it, the user registers their phone, and the device is automatically un-quarantined. With our previous solution we spent a lot of time doing this manually.

“Today, with Idaptive, we’ve got one centralized identity management solution that covers our single-sign-on needs across all apps and addresses our EMM and MFA requirements as well,” says Howell. “That has saved us money and IT resources, and allows us to build very specific policies around application access.”

“There are so many benefits to centralization. It’s really quite complicated to integrate three separate tools and enable cross communication. We don’t worry about that anymore.”

Now that the UK and Germany roll-outs are complete, the company will soon begin implementation in the US and France. “Beyond that, we’re currently doing demonstrations at the head office in Tokyo, where they’re interested in how we’ve achieved centralized identity management,” says Howell.

Idaptive delivers Next-Gen Access, protecting organizations from data breaches through a Zero Trust approach. Idaptive secures access to applications and endpoints by verifying every user, validating their devices, and intelligently limiting their access. Idaptive Next-Gen Access is the only industry-recognized solution that uniquely converges single sign-on (SSO), adaptive multi-factor authentication (MFA), enterprise mobility management (EMM) and user behavior analytics (UBA). With Idaptive, organizations experience secure access everywhere, reduced complexity and have newfound confidence to drive new business models and deliver kick-ass customer experiences. Over 2,000 organizations worldwide trust Idaptive to proactively secure their businesses. To learn more visit www.idaptive.com.

Ready to learn more?

Please contact us at
hello@idaptive.com