PERFORMANTA
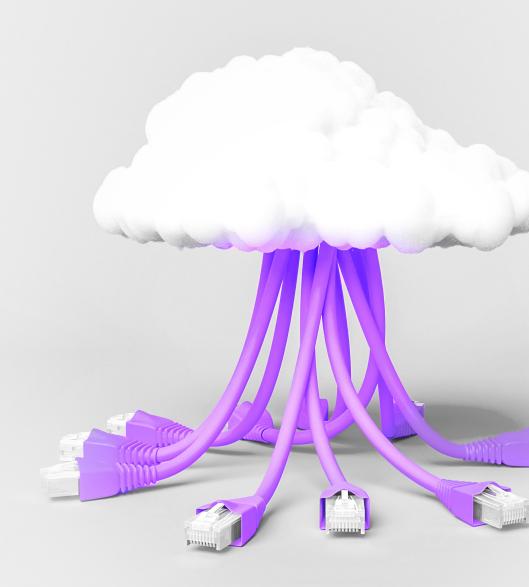
Case study

Making Identity Central To Everything:

Secure Hybrid Identity™

Executive Summary

Computer systems don't make mistakes when it comes to access. If a company can establish specific identity management rules and automated rights provisioning, it will ensure secure access to systems without inhibiting users or incurring unnecessary licensing costs. Yet hybrid environments combining on-premises and cloud systems pose challenges to such an outcome.

A large healthcare provider in the UK had adopted a leading cloud-based HR service and wanted to integrate it with their Active Directory. But standard integration options and connectors are too limited to match their granular business and identity rules. Cloud-native identity management services didn't deliver the granular customised configuration they required. This limitation blocked their goal of providing seamless access to different on-premises and cloud business systems, of which they have at least half a dozen on-premises and cloud instances.

The customer approached Performanta to solve their problem. Performanta's approach utilised our Secure Hybrid Identity™ methodology, taking the very best Microsoft technology both in cloud and on-premises to achieve the customer's goals. Over a few months, we utilised Microsoft Azure AD and Microsoft Identity Manager (MIM) to connect their HR system with Active Directory and Azure AD. The combination supports establishing specific business rules for organisational identity rights. We also developed a close relationship with the company responsible for their external client management system, providing our customer with a single touch point among their identity management service providers.

Performanta delivered identity management that operates down to the specifics of individual user roles. Leveraging the HR system, Active Directory, MIM and Azure AD to assign or remove rights automatically, the Secure Hybrid Identity™ solution provides convenient yet secure access to on-premises and cloud business systems.

Our customer now automatically provision and remove access rights to specific accounts, avoids expensive blanket licences, and can integrate new technology systems without making their environment more complex or fractured. They can expand into cloud and on-premises services, add more automation features, and maintain cohesive visibility and management of user identities.

The Challenge

A prominent healthcare practitioner embarked on a major digital modernisation project, including a cloud-based HR platform. It wished to connect the HR platform to its Active Directory system via Azure AD and Microsoft Identity Manager (MIM), facilitating more nuanced and granular management of internal user identities to bolster security and rights management, and reduce licence costs.

But the standard APIs did not provide enough customisation to enforce more specific business rules and user groups. It was a project-killing barrier for a hybrid technology estate that seamlessly delivered cloud and on-premises systems through one identity management environment.

The Solution

Our customer contracted Performanta to configure an internal identity management regime across their on-premises and cloud systems. They also required a custom API for sufficient flexible integration between the HR system and Active Directory, coordinated with MIM.

Performanta configured Azure AD and MIM to support business rules that automatically add or remove rights depending on a user's HR profile. We coded an API connector based on specifications from their systems architect, creating a seamless integration between the cloud-based HR system and the on-premises Active Directory services.

Our customer also has a sizable consumer identity service for their healthcare customers. A different provider manages that system, yet the customer prefers one point of contact and planning across both systems. Performanta established a relationship with the provider, collaborating to deliver a unified picture to our joint healthcare customer.

The Results

Both security and productivity benefit from nuanced identity management rules. Performanta utilises the best Microsoft technology and our Secure Hybrid Identity™ methodology to achieve the customer's goals across cloud and on-premises hybrid estates.

It's tricky to consolidate and narrow identity management in hybrid estates. Standard connectors often cannot cater for granular business and identity rules, and most cloud-based identity services don't offer sufficient customisation. Performanta solves the issue by configuring Azure AD in the cloud, and MIM on-premises, connecting them with the local Active Directory and cloud-based HR service via a custom-written API. Over a few months, we established the nuance, control and visibility the customer required.

Performanta's healthcare customer enjoys unprecedented control and visibility over user identities, policies and business rules. They now provide automated access rights and removal for all their business systems, managed by granular business rules and HR validations. Our customer can conveniently scale when adopting new software services and instances, adding on-premises and cloud services as required using connectors designed by Performanta. They experience substantial savings from reducing unnecessary licence costs by assigning licences to individual users, not blanket groups.

Computer systems don't make mistakes when it comes to access. Using automation and suitable business rules, our healthcare customer can dynamically and continually improve while maintaining a coherent and cohesive technology estate. By making identity central to everything, they save time and money, bolster their security, and pave the way for future digital enhancements

PERFORMANTA

www.performanta.com