CASE STUDY

Franke gains control of identity management

Global manufacturer turns challenging environment into efficient global management system

Key Facts

Company
Franke Holding AG

Industry
Manufacturing

Country
International
(Based in Switzerland)

Employees
9,000

Website
www.franke.com

Challenges

- Gain control of identity for 9,000 employees spread across 66 legal entities, 40 countries and five continents
- On-board ever growing cloud solutions efficiently and manage via account provisioning/de-provisioning, export data as required and secure access via Single Sign On
- Automate provisioning processes to securely update employee information

Results

- Reduced security risks
- Implemented a single version of the truth of employee data
- Automated cross-domain provisioning/de-provisioning of user permissions, target systems and hardware accounts

Products

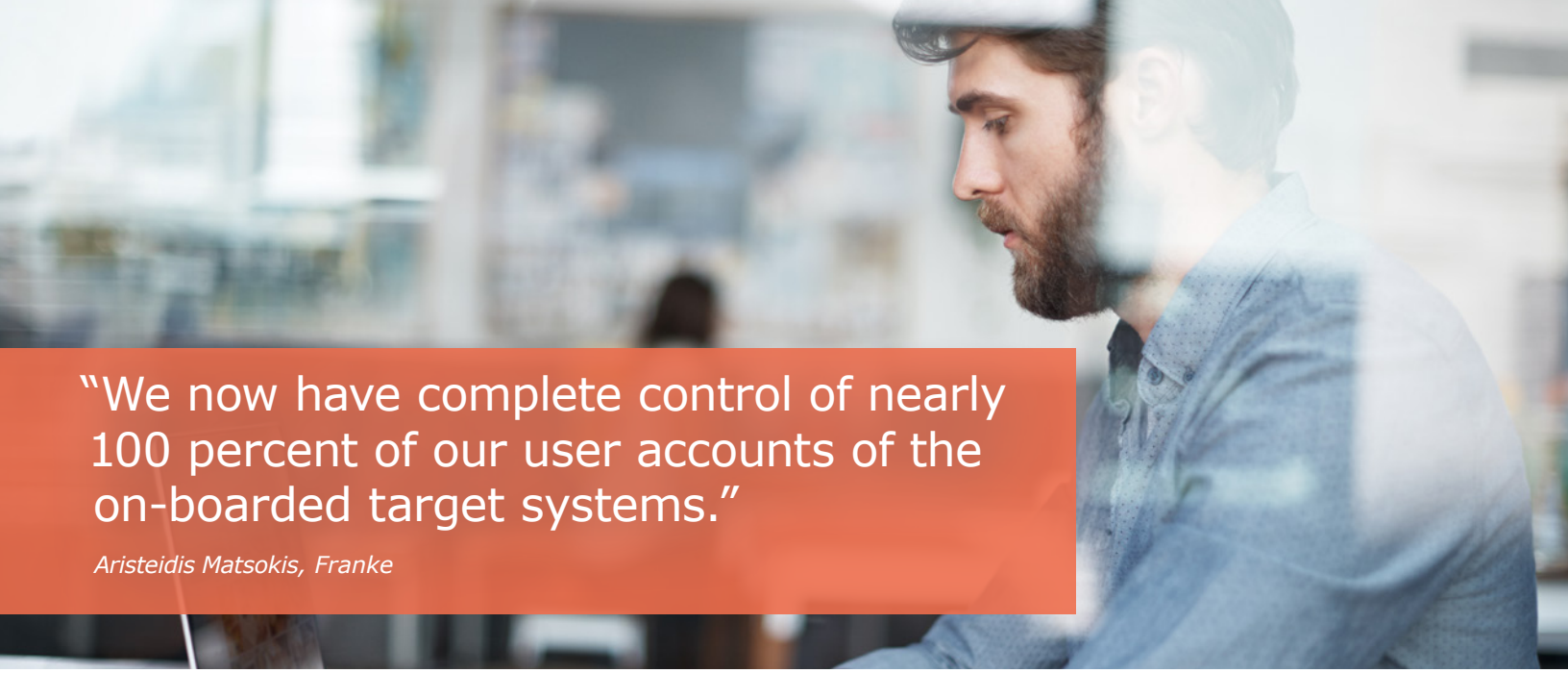
Identity Manager

Franke Holding AG, based in Aarburg, Switzerland is the global leader in commercial and residential kitchen systems. The company has a 100-year-plus history of growth and expansion. Particularly since the early 60s, the company has parlayed its leadership in the commercial sink business to enter new markets and geographies. Moreover, is a major market leader in 'Foodservice' solutions, professional 'Coffee System' solutions and 'Water' solutions.

With that expansion, which includes mergers and acquisitions, came a nearly unmanageable set of IT and HR systems, each with its own way to collect, store and share user identity information. Eventually, the holding company found itself managing 66 legal entities, 32 different HR systems and 9,000 employees located in 40 countries on five continents.

Franke needed to research, assess and implement an identity and access management (IAM) solution and therefore, teamed-up with IT services

ONE IDENTITY



> "We now have complete control of nearly 100 percent of our user accounts of the on-boarded target systems."
>
> *Aristeidis Matsokis, Franke*

partner, Devoteam. The manufacturer's goal was to gain control of their enterprise and manage their identity and access processes with a single source of truth. They needed an identity solution that could consolidate all employee/user data, and then simplify and automate time-consuming provisioning and de-provisioning tasks across all target systems. They needed their solution to do this regardless if the apps are on premise or in the cloud or in the server room down the hall or on the other side of the globe.

"Before, we used to have many applications, and no one was really taking care of the lifecycle of the accounts and those applications," said Aristeidis Matsokis, business process specialist at Franke. "It was easy to create the account in the applications because someone would complain that they needed access. But when a person changed role or moved outside the company, no one was really taking care of the account."

Due to the complexity of Franke's organization and IT systems, the account might get closed — or it might 'get orphaned,' which means it's still open but the user associated with the account has left the company or has moved to a new role. Either way, they no longer need access to the application. When that happens, the orphaned account, with its access to the application and all the data, becomes a vulnerability.

"Franke is continually adding cloud solutions as well as new target systems," said Yves Kronenburg, senior consultant at Devoteam. "With the ability of users to access applications remotely, when these accounts don't get locked, it's a big issue."

In the process of assessing this type of vulnerability, Franke and Devoteam — with the help of Identity Manager — found many orphaned accounts. By locating and disabling these accounts, as well as reducing the number of access points, Franke was able to greatly reduce its security risk and show that reduction in a measureable way.

Solution

With Devoteam's guidance and support, Franke implemented Identity Manager. Once it was up and running, the partners were able to use Identity Manager to consolidate employee data — for employees with access to at least one IT system — to a single system. Target systems (on-prem and cloud apps, mostly) are now provisioned/de-provisioned automatically or via approval when an employee moves roles, changes names or moves to a position at another Franke subsidiary regardless of the target systems interface, e.g. FTP upload, REST or SOAP. For example, today Franke is in position to connect to any new cloud system via FTP and provision/de-provision in a required frequency e.g. hourly with a 30 minute internal effort.

A self-service portal has enabled users and managers to reset passwords, and to request and get resource-access approval without taking up IT team time, which was a huge improvement over users or managers opening IT tickets or sending emails to get access. Additionally, resource and hardware accounts are disabled or delegated via a tiered set of approval workflows. Plus, the attestation process for employees and contractors is streamlined as they now can verify the appropriateness of

> "With the ability of users to access applications remotely, when these accounts don't get locked, it's a big issue."
>
> *Yves Kronenburg, Devoteam*

their access on their own and re-certify as required.

Identity Manager has simplified and accelerated access audits. So, now managers can see who has access to what — and when, by whom and why the access was granted.

Today, Franke has a clear view of its user permissions and activities worldwide. One example of the impact that Identity Manager has had on the manufacturer includes a recent domain-name change by one of its subsidiaries. The changeover took just minutes to complete with user data propagated to a broad range of systems, including Active Directory, SAP, Lotus Notes, Google, SuccessFactors, Concur and more. Prior to the implementation, a domain-name change would require manual tasks, which means the process would be prone to errors, support teams for every target system would have to dedicate time and attention to the domain-change effort and the whole process would have taken much longer – weeks or months.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.

Learn more: OneIdentity.com

CaseStudy-IM-Franke-US-CW-28245

ONE IDENTITY