



A cure for legacy access management ills

B. Braun in Germany automates identity and access management for greater security and compliance while enabling digital transformation

Key Facts

- Company**
B. Braun Melsungen AG
- Industry**
Healthcare
- Country**
Germany
- Employees**
61,583 (2017)
- Website**
www.bbraun.com

Challenges

B. Braun needed to increase security, guarantee compliance, and control access to company data, especially as it developed a hybrid IT environment.

Results

The organisation has improved security by automating account provisioning and deactivation. B. Braun has also ensured company data is protected in its hybrid environment, featuring cloud and on-premise systems.

Products

- Identity Manager
- Services

The employee landscape at organisations of all sizes and types is constantly evolving as job roles change, people leave, and new starters begin. This state of flux is a challenge for IT teams, responsible for managing access to company systems and keeping corporate data safe.

For B. Braun, one of the world’s leading providers of healthcare solutions based in Melsungen, Germany, the challenge was particularly acute. The firm manufactures 5,000 different kinds of products for the healthcare industry, including dialysis machines and specialist fibre-optic equipment for surgery. It has more than 61,000 employees worldwide — all of whom have IT user accounts that need to be carefully managed.

When outdated technology is an opportunity

B. Braun needed a more effective way to manage user accounts and protect data. Andreas Mueller, IT project manager at B. Braun, says, “We have too many manual processes, which increases the time to create or delete a user account. Overall, there was too much risk of unauthorised



“Our investment in **Identity Manager** is enabling the business to pursue its cloud-IT strategy, while ensuring **access management** is locked down.”

Andreas Mueller, IT Project Manager, B. Braun Melsungen AG, Germany

data access and therefore a failure to comply with data security regulations.”

Beyond automation, B. Braun also wanted an identity management solution that could drive digital transformation. “We’re moving some of our IT to the cloud,” says Mueller, “so we needed a solution that could talk to our on-premise infrastructure and cloud services such as Office 365.”

B. Braun hired One Identity to launch a proof of concept (POC) for Identity Manager. “Identity Manager delivered all the features we wanted,” says Mueller, “including cloud connectivity. What’s more, the technical sales team at One Identity offered to support a POC that integrated with our internal infrastructure. No other provider would go this far.”

Expert services deliver added confidence

Based on the success of the POC, B. Braun went ahead with the deployment of Identity Manager. The goal was for the solution to support both the company’s internal systems and an extranet used by B. Braun customers. Says Mueller, “For a project of this importance, we wanted to work with a services team because we didn’t have the skills in-house. We looked at several offers, but the proposal from One Identity Services gave us the most confidence. Its personnel were highly experienced in this kind of implementation.”

Services flexibility avoids runovers

During the deployment, the One Identity Services team demonstrated a high degree of flexibility as well as experience, according to Mueller. “There was a lot of back and forth between the B. Braun IT project team and stakeholders across the business. But thanks to the good planning of One Identity Services — which allocated time in its original schedule for changes to the project’s parameters — implementation stayed on track,” he says.

Getting access management right

Today, the Identity Manager solution behind B. Braun’s internal systems is about to go live for personnel in Germany and Switzerland. In the coming months, it will be rolled out worldwide. B. Braun realises that access needs to be correct in order to reduce risk and protect company data. “All the right people have access to what they need now that account creation and termination are automated with Identity Manager,” explains Mueller. “There’s complete transparency and greater protection of company data. Everyone knows the position of their requests within the workflow at any given time. There is also less chance of errors.”

Inspiring innovation, driving transformation

From a security and compliance perspective, access management is more tightly controlled. “Knowing your data is secure with One Identity frees up mental space to focus on business development and innovation,” comments Mueller. Furthermore, Identity Manager’s compatibility with cloud-based systems enables B. Braun to drive the company’s digital transformation. “Our investment in Identity Manager is enabling the business to pursue its cloud-IT strategy, while ensuring access management is locked down,” says Mueller.

Continued development

Looking ahead, B. Braun plans to enhance its password management policies with the support of One Identity. “Step by step, we’re getting our identity and access management right with One Identity. That’s great news for the company and our staff,” Mueller says.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

View all One Identity case studies at [OneIdentity.com/casestudies](https://www.oneidentity.com/casestudies)