Automating identity and privileged access management

BEC protects customer data with user-friendly software, saving time and resources whilst reducing risks.

Customer:

BEC Financial Technologies

Industry:

IT services

Country:

Denmark

Website:

bec.dk/en/about-bec/

Challenge

Danish IT services provider BEC wanted to strengthen protection around its core systems and customer data without impeding the productivity of its developer and governance teams.

Solution

- One Identity Safeguard
- One Identity Manager
- One Identity Privileged Access Management (PAM)

Protects systems and data against unapproved log-ins

Locks down passwords for privileged users

Provides predefined reports out of the box

Simple and easy to use interface saves time and resources

BEC is a Danish IT services provider with more than 50 years' experience developing and operating technology for financial companies. It offers consultancy, technology and operational services, and develops innovative solutions in close cooperation with its clients These include small, large, traditional and niche financial companies.

The integral role BEC plays with its clients means it needs to operate with strict data protection and governance standards in place. It was using its own systems for managing identity and access control, but wanted to raise levels of protection.

"We identified that there were areas of compliance we could improve on by raising the level of automation involved," says Bethina Luckow, Manager of identity governance and administration. "We wanted to get rid of all remaining outdated systems because the fewer manual processes that are in place, the fewer the mistakes that are made."

> "Our top priorities are **security** and **compliance**, along with **protecting** our customers' **sensitive financial information**. We wanted to adopt **higher levels of automation** in how we achieved those goals"
>
> Bethina Luckow, Manager of Identity Governance and Administration, BEC

Building higher levels of protection

BEC considered a range of different options and chose One Identity partner Intragen to implement One Identity Manager and One Identity Safeguard. Having the software in place made it easy to set up and provide access to different systems for designated users.

The next stage was to implement an even higher level of protection with a system for managing privileged user access. This would enable BEC to manage and report on access to IT systems whilst locking down passwords for valid and approved reasons only.

BEC looked at available PAM solutions that would meet its stringent requirements, which were for a system that would be highly automated and reliable, whilst providing a user-friendly interface and a high level of security.

Since BEC had already set up One Identity Manager, it made sense to choose One Identity Privileged Access Management (PAM) as an additional, integrated layer of security, says Luckow. "It was a no-brainer for us to implement One Identity PAM because all of the information we needed to input was already in One Identity Manager and could be automatically added."

Preventing breaches

"Having the PAM in place is an extremely effective way of protecting sensitive data and systems," Luckow adds. A systems breach resulting in compromised data is something BEC needs to be particularly wary of. One Identity PAM guards against unapproved log-ins by providing just the right amount of access to mitigate such scenarios..

> "We identified that there were areas of **compliance** we could improve on by **raising** the level of **automation** involved. We wanted to get rid of all remaining outdated systems, because the fewer manual processes in place, the fewer the mistakes that are made"
>
> Bethina Luckow, Manager of Identity Governance and Administration, BEC

As well as limiting access, One Identity Manager and PAM enable BEC to automatically create regular reports. "Previously, compliance reporting was more difficult and we had to do more manual work, which meant we only worked on reports when we had to," explains Luckow. "Now we can use predefined reports out of the box as well as build our own. If you can provide reports automatically every month by email they are also more likely to be accessed and read."

A further benefit is that One Identity Manager and PAM are highly resilient, Luckow says, "There have never been any incidents where we couldn't connect to our systems, which is really important for the successful operation of our business."

Simple yet powerful

Above all, One Identity Manager and PAM are simple and easy to use without taking up time and resources better used to support customers, whilst also playing a vital role in keeping data safe from unauthorised users. "PAM holds the keys to our most privileged data and accesses," concludes Luckow.

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, future-ready solutions for identity governance, access management and privileged management.

intragen