CASE STUDY

# Privileged access management you can count on

Workers Savings Bank improves security, reduces privileged access approval time to just seconds and boosts administrative efficiency with a solution from One Identity



**Key Facts**

**Company**
Delavska hranilnica

**Industry**
Banking and finance

**Country**
Slovenia

**Employees**
300

**Website**
www.delavska-hranilnica.si

## Challenges

To reduce risk from internal and external threats, simplify compliance, and speed productivity, Delavska hranilnica wanted to increase insight and control over privileged accounts.

## Results

- Improved security and simplified compliance
- Gained highly detailed control over who accesses what, when and why
- Sped approvals and password changes from at least 15 minutes to just seconds
- Accelerated and expanded insight
- Replaced command-line processes with point-and-click tools

## Products

One Identity Safeguard

Statistics show that "insiders" pose the biggest IT security risks. While organizations look to increase insight and control over employees' IT access, there are also increasing requirements for managing privileged accounts. These profiles are prized by hackers because they provide carte-blanche access to systems.

Delavska hranilnica (Workers Savings Bank) in Slovenia takes a proactive approach when it comes to security, especially privileged access management (PAM). This is why it sought an easier, more effective way to manage privileged access. Any profile or password change was extremely time-consuming. Administrators had to use a Linux command line to manually reconfigure software agents on individual devices. To save time and reduce complexity, multiple administrators were sharing privileged accounts and passwords — a common practice in global organizations. However, this approach, along with some technology limitations, restricted insight about the behavior of individual privileged users. Gathering any information about privileged users' access also meant that someone had to manually sort through system log files and compile a report.

ONE IDENTITY

> "It was **mind-blowing** to see the change. Safeguard is so easy to use, and we have **better visibility and control.**"
>
> *Janko Zorman, Chief Information Officer, Delavska hranilnica*

## A better solution in days

Delavska hranilnica evaluated leading enterprise PAM solutions, looking for one that would provide improved controls, insight and reporting — plus simplify regulatory compliance. The bank found that it could address its challenges with One Identity Safeguard. For help with its implementation, the bank engaged One Identity partner ADM Adria. The initial deployment took just two days. Janko Zorman, chief information officer at Delavska hranilnica, says, "ADM Adria was the right partner for us because it has the know-how to deploy the Safeguard solution efficiently and with best practices. After we implemented the solution, it was mind-blowing to see the change. Safeguard is so easy to use, and we have better visibility and control over privileged access. We also love that Safeguard is a turnkey solution that's agentless."

## Improved security

Today, the bank is better protected against external and internal threats. "We are more secure today with One Identity Safeguard," Zorman explains. "We make changes based on very granular and defined processes that are integrated with our Active Directory. Privileged users also have their own passwords, which we can change after every session."

## Increased administrative efficiency

IT employees manage Safeguard from a GUI console, which they can access remotely. With the Favorites capability, staff can set up orchestrations that give them one-click access to privileged accounts. And they no longer have to manage separate software agents. "Our efficiency is up by at least 20 percent," says Zorman. "In a few clicks, engineers can add a new system, user, group or workflow — and they don't need advanced skills to do so."

## Almost instant external access

Granting privileged access to people working outside corporate intranets is also faster today. Zorman explains, "External users such as remote vendors can gain access to systems or get a new password almost instantly now that we use Safeguard. Before, it usually took at least 15 minutes. There's no need to enable or disable VPNs anymore. The whole process is more user-friendly for everyone." External users can connect to systems through Safeguard using the program of their choice, such as PuTTY or Microsoft Remote Desktop.

## Faster insight and simplified compliance

When administrators access Safeguard, they can quickly see a comprehensive view of privileged accounts, including which users made what changes, to which systems, when and why. In addition to saving time, this improved insight greatly simplifies compliance with regulations such as GDPR. "In seconds, we can get the information we need and generate reports using Safeguard," Zorman explains. "A few weeks back, a sales representative tried to sell us a different PAM solution. I explained to him that we have Safeguard, and that he should start selling it instead. It would be better for him."

## 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**



ONE IDENTITY