Securing privileged access for robotic process automation (RPA)

PROSEGUR

Prosegur uses RPA to transform its business while reducing the risk from privileged account access using One Identity Safeguard

Customer:
Prosegur

Industry:
Security

Country:
Spain

Website:
www.prosegur.com

Challenge

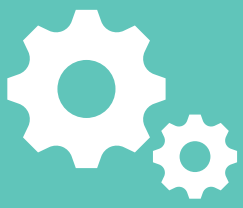
Prosegur wanted to monitor and record privileged access for digital workers but the potential solution it identified was unable to integrate via an application programming interface (API).

Solution

It overcame the issue with One Identity Safeguard for privileged access management, automating control of privileged access to reduce risk, improve security and ensure compliance.

Reduces the risk of digital-worker accounts being compromised

Enhances security through automated password control



Gains easy integration with RPA solution using Safeguard RESTful API

Ensures compliance using detailed auditing trails

Prosegur, headquartered in Madrid, delivers a wide range of private security services. These include residential alarms, security guards to patrol locations, and security vehicles to collect cash takings and fill cashpoint machines. It has a global presence and employs more than 160,000 people worldwide.

Adopting robotic process automation (RPA)

Prosegur is migrating rules-based administration tasks to digital workers through RPA—allowing its people to focus on higher-value tasks. To support this shift, Prosegur selected the Blue Prism RPA platform for best practices in optimizing the speed of the transition and reducing costs.

In just two years, Prosegur has scaled its digital workforce across 14 business areas—including HR, finance, legal, marketing, IT and operations. The program has given 350,000 hours back to the business.

RPA software interacts directly with business applications, mimicking the way applications and humans use credentials and entitlements. This means it can introduce risks when digital workers perform business processes that require access to privileged credentials.

Therefore, it was a top priority for Prosegur to manage privileged credentials in a secure manner, reducing the risk of breach through compromised access. "Ensuring Blue Prism could securely gain access to privileged credentials was critical to the security of our RPA initiative," says Prasanna Kumar, IT architect at Prosegur.

The need for automation

When Prosegur first implemented its RPA solution, it didn't have the functionality to automate control and secure the process of granting privileged access. The company ran a proof of concept (POC) with a leading privileged access management (PAM) solution but was unable to integrate the RPA solution using the available API. Kumar and his colleagues decided to run another POC—this time, using One Identity Safeguard. "We solved our API issues straightaway," he says. "We found the One Identity API easy to work with. Plus, the support from One Identity is amazing. Our POC for Safeguard our RPA solution were a complete success."

Reduced risk

With Safeguard, Prosegur has lowered the risk of providing privileged access to digital workers. When a digital worker needs access to a privileged credential, an API call is made to the Safeguard vault to retrieve it. Safeguard provides a full audit trail of which digital worker has access to what applications and when. In addition, Safeguard also manages access to the RPA solution by developers who need privileged access in order to test the workflows they have created.

> **"Through automation we save around a week setting up user accounts for our digital workers with Safeguard and around a day making changes to the passwords."**
>
> **Prasanna Kumar,**
> IT architect, Prosegur

> **"We found the One Identity API easy to work with. Plus, the support from One Identity is amazing."**
>
> **Prasanna Kumar,**
> IT architect, Prosegur

Enhanced security

Prosegur saves time setting up user accounts for digital workers and generating passwords, which can now be rotated in line with the demands of each department.

Says Kumar, "Through automation we save around a week setting up user accounts for our digital workers with Safeguard and around a day making changes to the passwords. We can use the time to focus on our compliance strategy and ensure the organization meets the regulations."

Compliance through detailed auditing trails

Prosegur can control, monitor and record digital-worker access to compile a detailed auditing trail. This helps ensure Prosegur stays compliant with the European Union's General Data Protection Regulation (GDPR). Kumar says, "We can see what's going on in our environment at any point in time. Now that privileged access is under control with One Identity Safeguard, we can accelerate our RPA program."

About One Identity:

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com.