Asegurar el acceso privilegiado para la automatización robótica de procesos (RPA)

PROSEGUR

Prosegur utiliza RPA para transformar su negocio mientras reduce el riesgo de los accesos privilegiados utilizando One Identity Safeguard

Cliente:
Prosegur

Sector:
Seguridad

País:
España

Sitio web:
www.prosegur.com

El problema

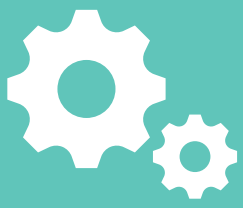
Prosegur quería monitorizar y grabar los accesos privilegiados de los trabajadores digitales, pero la solución que tenía en mente no se podía integrar mediante una interfaz de programación de aplicaciones (o API).

La solución

La empresa salvó esta dificultad con Safeguard, la solución de One Identity para la gestión de accesos privilegiados. Safeguard le permitió automatizar la supervisión de estos accesos con el objetivo de minimizar el riesgo, reforzar la seguridad y garantizar el cumplimiento normativo.

Reduce el riesgo de que las cuentas de los trabajadores digitales se vean comprometidas

Refuerza la seguridad gracias a la automatización del control de contraseñas



Se integra fácilmente con soluciones de RPA mediante la API RESTful de Safeguard

Garantiza el cumplimiento normativo gracias a los registros de auditoría detallados

Con sede en Madrid, Prosegur ofrece una amplia gama de servicios de seguridad privada, entre los que se cuentan alarmas residenciales, vigilantes de seguridad o vehículos blindados para el transporte de efectivo y la reposición de cajeros automáticos. Está presente en diferentes países y cuenta con más de 160.000 empleados en todo el mundo.

Adopción de la automatización robótica de procesos (RPA)

Prosegur está digitalizando las tareas administrativas basadas en reglas mediante RPA, permitiendo así a sus trabajadores centrarse en aquellas que aportan más valor a la empresa. Con el objetivo de reducir costes y de facilitar y agilizar la transición, Prosegur eligió la plataforma de RPA de Blue Prism.

En solo dos años, la multinacional ha multiplicado el número de trabajadores digitales en 14 áreas de negocio, como las de recursos humanos, finanzas, aspectos jurídicos, marketing, servicios informáticos y operaciones. El programa ha permitido ahorrar 350.000 horas.

El software de RPA interactúa directamente con las aplicaciones empresariales, reproduciendo la forma en la que las aplicaciones y las personas utilizan las credenciales y los permisos. Esto puede conllevar ciertos riesgos cuando los trabajadores digitales se embarcan en procesos que requieren acceso a credenciales privilegiadas.

Por eso, para Prosegur era fundamental poder gestionar las credenciales privilegiadas de forma segura y proteger los accesos para reducir el riesgo de infiltraciones. «Garantizar que Blue Prism pudiese acceder de forma segura a las credenciales privilegiadas era de vital importancia para nuestra iniciativa de RPA», explica Prasanna Kumar, arquitecto informático de Prosegur.

La necesidad de automatizar

La primera vez que Prosegur implementó una solución de RPA, esta no ofrecía las funciones necesarias para automatizar el control ni garantizar que los accesos privilegiados se concedían de forma segura. La empresa realizó una prueba de concepto (POC) con una de las principales soluciones de gestión de acceso privilegiado (PAM), pero no fue capaz de integrar la solución de RPA mediante la API de la que disponía. Kumar y sus compañeros decidieron hacer otra POC, utilizando, en esta ocasión, Safeguard de One Identity. «Los problemas relativos a la API desaparecieron de un plumazo —comenta—. Trabajar con la API de One Identity nos resultó muy sencillo y, además, la asistencia que brindan es magnífica. La prueba de concepto con Safeguard y la solución de RPA fueron todo un éxito».

Reducción del riesgo

Gracias a Safeguard, Prosegur ha logrado reducir el riesgo que supone conceder acceso privilegiado a los trabajadores digitales. Cuando estos necesitan acceso a una credencial privilegiada, se hace una llamada de API a Safeguard para recuperarla.

> **«Gracias a Safeguard y a la automatización, nos ahorramos en torno a una semana en la creación de cuentas de usuarios para nuestros trabajadores digitales y un día en modificar las contraseñas».**
>
> **Prasanna Kumar,**
> arquitecto informático de Prosegur

> **«Trabajar con la API de One Identity nos resultó muy sencillo y, además, la asistencia que brindan es magnífica».**
>
> **Prasanna Kumar,**
> arquitecto informático de Prosegur

Safeguard proporciona un registro de auditoría completo que ilustra quién tiene acceso a qué aplicaciones en qué momento. Y no solo eso: también gestiona el acceso privilegiado a la solución de RPA cuando los desarrolladores necesitan probar los flujos de trabajo que han diseñado.

Seguridad reforzada

Ahora, Prosegur tarda menos en crear cuentas de usuario para sus trabajadores digitales y generar contraseñas, y puede intercambiarlas de acuerdo con las necesidades de cada departamento.

Kumar mantiene que «gracias a Safeguard y a la automatización, nos ahorramos en torno a una semana en la creación de cuentas de usuarios para nuestros trabajadores digitales y un día en modificar las contraseñas, y podemos dedicar este tiempo a nuestra estrategia de cumplimiento y a garantizar que la empresa se rige por la normativa».

Cumplimiento garantizado con registros de auditoría detallados

Prosegur puede controlar, supervisar y grabar los accesos de los trabajadores digitales para mantener un registro de auditoría detallado, lo que le ayuda a garantizar que cumple el reglamento general de protección de datos (RGPD) de la Unión Europea. En palabras de Kumar, «Podemos ver lo que pasa en nuestro entorno en todo momento. Ahora que gracias a Safeguard de One Identity ya no tenemos que preocuparnos por los accesos privilegiados, nos será más fácil acelerar nuestro programa de RPA».

Acerca de One Identity

One Identity, una empresa de Quest Software, ayuda a las organizaciones a adoptar una estrategia de seguridad centrada en las identidades, ya sea en sus propias instalaciones, en la nube o en un entorno híbrido. Nuestra amplia cartera de soluciones integradas de gestión de identidades abarca, entre otros servicios, la administración de cuentas y de accesos privilegiados y el control y la gestión de identidades. Al centrarse en las identidades y autorizar solo los accesos oportunos para cada tipo de usuario, sistema y datos, estas soluciones permiten a las empresas aprovechar todo su potencial y garantizar la seguridad. Encontrará más información en OneIdentity.com.