Identity Security Drives Frictionless Automation at **BNP Paribas Bank Polska**
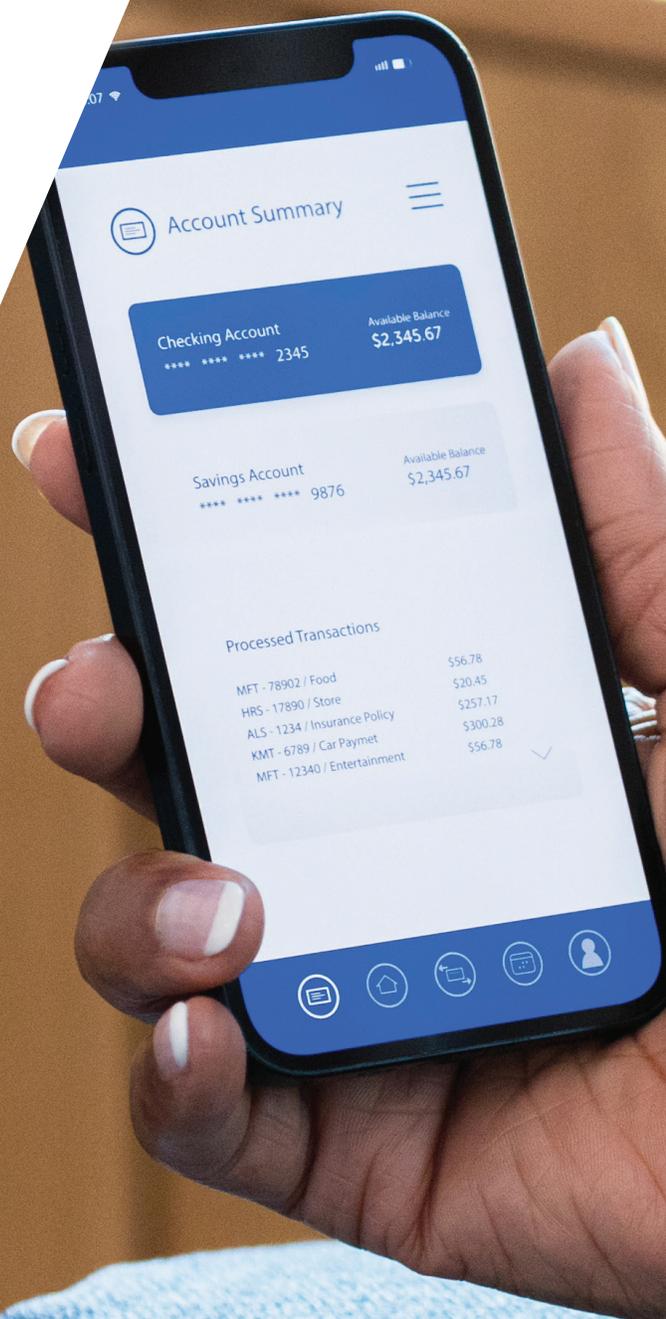
Overview

BNP Paribas Bank Polska S.A., is a part of the BNP Paribas banking group present in 65 countries, and provides wealth management services, as well as services to retail clients, and companies in the micro, SME, and corporate banking segments.

Challenge

BNP Paribas Bank Polska faced a lot of challenges related to the integrated entities that became part of the Bank as a result of mergers. The Bank needed the right tool to handle that amount of data and its interdependency. Their priority was to at least maintain, and preferably increase, the level of security while simplifying and streamlining IAM processes.

Solution

BNP Paribas Bank Polska partnered with SailPoint over a decade ago and was able to grow a mature and reliable IAM program since, applicable to every aspect of the business and impacting every employee in the organization. In particular, almost 100% of access requests are now treated automatically, with user provisioning happening on their first day of work.

BNP Paribas Bank Polska S.A. is a part of the BNP Paribas banking group present in 65 countries. In Poland, this universal Bank with global reach provides wealth management services, as well as services to retail clients, and companies in the micro, small and medium enterprises, and corporate banking segments. The Bank is also making banking processes more efficient by implementing innovative solutions in online banking.
With a nationwide footprint, BNP Paribas Bank Polska needed to ensure they have a robust IT infrastructure and a trustworthy identity solution.

"Identity and rights management in a company with over 10,000 users is really challenging," shares Paweł Mosurek, Identity and Access Management (IAM) Manager at BNP Paribas Bank Polska. "So the tool with which we design our IAM processes must be efficient and reliable. Having such a large number of employees who use hundreds of applications, systems and thousands of network IT resources makes it paramount for us to choose solutions ensuring that everything will work smoothly," adds Paweł.

BNP Paribas Bank Polska faced many challenges related to integrating entities as a result of mergers. In the IAM area, this was a huge concern. There were operations on many application system identities, so they also needed the right tools to handle that amount of data and its interdependency.

"The world and technology are constantly progressing, revealing faults and shortcomings. New opportunities are also emerging. And it's our job to keep up with this fast-paced world. Regulations sometimes can't keep up, but we have to be ready, so once they are introduced, we can say: this is achievable in the time frame intended or already been implemented," says Paweł.

Therefore, the Bank distinguished several key principles of their IAM program:

- Processes must be understandable and simple for the end-user.

- The system must not make work harder for people.

- IAM team's job is to help users to make things work more efficiently, faster, and more conveniently. It shouldn't be a complex process everyone will complain about and figure out how to get around.

- And most importantly, all the activities mentioned above must be safe too - as this is the primary goal of cybersecurity solutions.

SailPoint's Trusted Partner for Over a Decade

Initially, BNP Paribas Bank Polska selected SailPoint solution as it held a top-ranked position as a leader in Gartner Identity Governance and Administration report. "When we analyzed our needs, environment, and architecture, SailPoint's IdentityIQ seemed like a natural choice. It is a platform that fits well with our IT architecture. It is a very flexible product that can be adapted to our needs," Paweł remembers.

By now, SailPoint has been a BNP Paribas Bank Polska trusted partner for over 10 years. During this time both the product and the approach to the IAM have significantly evolved. Nowadays, the company has reached such maturity in identity and access management that each of its employees identifies it with the processes and capabilities that SailPoint provides. "It's a kind of natural evolution that we've gone through and continue to go through in order to achieve our goals, but without losing along the way something that's very important today, namely cyber security," says Paweł.

"The priority for us was to at least maintain, and preferably increase, the level of security while simplifying and streamlining IAM processes," he adds.

With such a large workforce, the diversity of its operations and the number of IT assets, BNP Paribas Bank Polska has good reasons to be proud of where they are today in its IAM journey.

BNP Paribas Bank Polska currently manages approximately 600 production applications and 300 applications for test and development environments in IdentityIQ. These applications are built with approximately 120,000 managed individual rights.

Paweł's team also relies primarily on Microsoft Active Directory technology which according to Paweł, is the most appropriate technology for integrating and managing users and accesses from the SailPoint tools level. These 5 applications are fundamental to SailPoint integration at the company:

1. Active Directory
2. MS SQL
3. Lotus
4. I5OS (AS400)
5. Connectors enabling management in the Cloud (Azure, IBM, GCP)

Automation At Scale in Fast-Paced Banking Environment

Currently, in the Bank, the process of onboarding a new employee is fully automatic, and at the same time, within IAM processes, the time it takes to equipthe user with access to the relevant systems and roles is less than one day. In most cases, an employee becomes active on day one.

For IT department users, Paweł's team creates additional domain accounts with different password policies and rights based on policies consistent with NIST best practices. The user can manage all this in a friendly and clear interface.

For several years now, BNP Paribas Bank Polska has been dynamically developing the area of certification of rights and access to IT systems.

The ability to automatically create different types of certification campaigns is vital to the overall business. "You already know the scale of our organization, and the fact is that there are two employees dedicated to the certification process who dedicate approximately 15% of their work time to this task. We perform manager certification for every employee and owner certification for approximately 400 IT assets per year," shares Paweł.

"Our processes are almost 100% automated, which is important because IAM is not just IdentityIQ. It's also a multitude of other tasks performed by a small team of excellent specialists. But without automation, even they would not be able to cope with the scale we are facing. Fortunately, SailPoint and our integrator give us virtually endless possibilities for automation," he adds.

Every employee of the organization is impacted by Identity Security. Every month, users perform about 4,000 resets and password changes using mechanisms embedded in IdentityIQ. In the SailPoint tool, BNP Paribas Bank Polska has several connectors dedicated to their individual

> " **We can simplify many actions and automate them while maintaining appropriate security and ensuring proper reporting, including audits. The number of tasks performed by SailPoint automation per month is approximately 40,000 events.**
>
> **Paweł Mosurek**
> Identity and Access Management (IAM) Manager, BNP Paribas Bank Polska

solutions. One connector is ensuring that users do not need to call the Helpdesk when they want to reset the password or enable or disable the application account. The number of requests generated by users per month averages about 800, of which 90% are executed automatically.

As Paweł looks ahead, Privileged Access Management (PAM) stands out as a priority for his team. The Bank is currently extending the capabilities of SailPoint Identity IQ by enhancing it with a PAM module. Paweł intends to use, among others, Identity IQ for privileged access certification using this integration and the PAM module.

As Paweł's team has accumulated quite a lot of experiences and observations over the years in the area of rights and identity management, they've established some best practices.

- For each organization, exact IAM steps are likely to relate to specific needs and circumstances. Still, we can define some universal golden rules.

- Ready-made studies carried out by entities dealing with rights and identity issues, such as National Institute of Standards and Technology, have proven to be very helpful in defining such good practices.

- IAM and PAM should not be treated as a project, but rather as a program planned out and scheduled.

- It is not possible to implement everything at once. The expected maturity must be reached systematically step by step, along the way achieving milestones that should be clearly defined at the beginning of the program.

- Support and commitment of the senior management are vital. The signal must come from there that the IAM plan is in line with the company's broader mission.

- Keeping in mind the end-users are crucial. As they are the ones who will be using the system the most, it needs to be user-friendly, natural, and helpful for them.

"And, of course, we need to remember that this is a security matter and be aware this is not for fun. Today, information is the most valuable asset in the world, and as such, it must be protected in a controlled manner," says Paweł.

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.