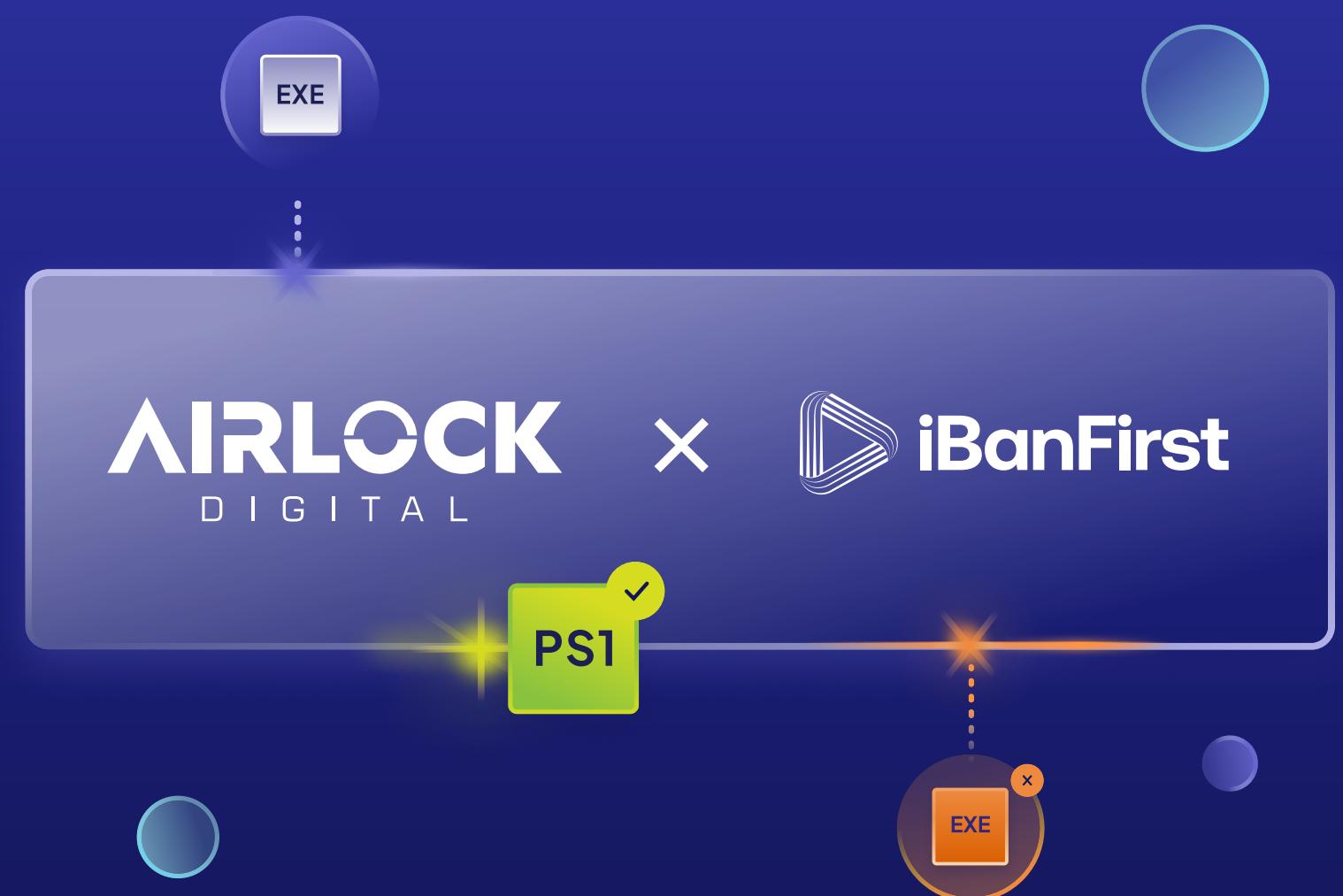# AIRLOCK DIGITAL

CASE STUDY

iBanFirst

iBanFirst chose application control and allowlisting from Airlock Digital to reduce threats, improve control, and help ensure compliance.

About iBanFirst

iBanFirst is a European-headquartered fintech that specializes in enabling medium sized businesses to undertake cross-border payments and transactions.

Learn more about iBanFirst by visiting **www.ibanfirst.com**.

Challenge

iBanFirst wanted to reduce its attack surface and implement a second line of defense that built on its endpoint detection and response (EDR) solution.

Approach

iBanFirst elected to implement application control and allowlisting from Airlock Digital after reviewing it in the **CrowdStrike Marketplace** and evaluating its performance, ease of use and functionality.

Result

With Airlock Digital, iBanFirst has implemented effective, easy-to-manage application control and augmented its endpoint detection and response capabilities.

Benefits to iBanFirst

With Airlock Digital application control and allowlisting, iBanFirst has:

- Reduced application control and allowlisting administration down to one to two hours a week

- Aligned with financial services-specific compliance requirements and broader cybersecurity rules and standards

- Implemented best-in-class application control and allowlisting to reduce the organization's attack surface

- Minimized disruption and secured workforce support for a critical cybersecurity control

> "Airlock Digital builds stakeholder trust in our ability to mitigate threats such as ransomware and malware."

Florent Gilain
Chief Information Security Officer
iBanFirst

About Airlock Digital

Airlock Digital is the global leader in application control and allowlisting, trusted by organizations worldwide to protect against ransomware, malware and other cyber threats. Our deny by default solution enables customers to run only the applications and files they trust, with all others blocked from executing. This approach minimizes attack surfaces and helps organizations align their cybersecurity strategies with government frameworks and standards. Scalable and easy to implement, our solution is used across financial services, government, healthcare, manufacturing and other industries. By securing endpoints running legacy and new versions of Windows, macOS and Linux, we extend protection across IT and operational technology environments. Airlock Digital is a pillar of modern cybersecurity strategies, delivering robust protection to organizations of all sizes.

The Customer

The mission of European-headquartered fintech iBanFirst is to make cross-border payments and transactions between 180+ countries both fast and reliable. Serving predominantly medium-sized businesses, the organization has around 350 employees across 12 countries in Europe, and processes 2 billion-plus euros worth of transactions monthly. It provides executives and finance teams with access to currency markets and enables them to hold, collect, and send funds in 30+ currencies, while providing the ability to develop custom hedging strategies.

The Challenge

iBanFirst needed comprehensive, high-standard cybersecurity to stops threats before they start and maintain the confidence of its 10,000+ customers. Four years ago, the business created the position of Chief Information Security Officer to modernize its security architecture and appointed experienced cybersecurity and infrastructure specialist Florent Gilain to the role. In developing and executing a strategy for iBanFirst, Florent initially opted for a defensive security feature available to the organization through its existing technology investments. However, deploying this feature to protect the organization's servers took several months, and the security provided did not meet iBanFirst's requirements.

The Approach

Having implemented **CrowdStrike** to provide endpoint detection and response, Florent started looking at opportunities to augment the product's functionality with a second line of defense. "We wanted a solution that would allow us to control what executed on our laptops in order to reduce our attack surface," he explained. "For example, we needed to restrict users to Chrome or Edge, with no unauthorized browsers allowed to run. In addition, we wanted to control the execution of extensions and apply several CIS-benchmark hardening guides for systems, browsers and other elements of our architecture.

"We found only application control and allowlisting with Airlock Digital would allow us to do that."

The simplicity of its allowlisting processes, the flexibility and budget-friendliness of running a cloud-based solution, and a logging feature that enables the security team to track what attempts to execute also contributed to Florent's decision to implement Airlock Digital.

The Result

iBanFirst now relies on Airlock Digital to protect its laptops and servers running Windows, about 500 assets in total. "We achieved some quick early wins on our servers via the ease with which we were able to determine trust and create and enforce policies with Airlock Digital," said Florent. The business was also able to move its Windows laptops into enforcement in just three months.

The project was so successful the iBanFirst cybersecurity team won silver and the special jury prize at a prestigious event, Cybernight, organized by Republik Cyber, for "delivering a transformative solution that significantly strengthens security."

Securing buy-in across the organization for Airlock Digital as a critical security control was straightforward thanks to clear communication to users from the information security team, and the solution's **one-time password functionality**. This enabled iBanFirst to provide time-limited exceptions for users who require time-limited access to non-allowlisted applications, minimizing disruption to productivity including when offline.

The combination of effectiveness, ease of use, and manageability offered by Airlock Digital is epitomized by the fact iBanFirst's three-person security team spends just one to two hours per week working with the solution to review executions. Meanwhile, the organization relies on the solution to align with critical cybersecurity frameworks and regulations, such as the **European Union's Digital Operational Resilience Act** (DORA), which aims to strengthen the security and resilience of financial institutions. "Airlock Digital's application control and allowlisting solution helps limit the propagation or lateralization of a cyber-attack, which minimizes the risk of disruption to customer services and supports the objectives of DORA and other finance sector cybersecurity rules," said Florent. "We expect the solution to play an important role in our program to become ISO27001-compliant in line with requests from our customers.

"Just as iBanFirst extends trust beyond borders with our payment solution, Airlock Digital builds stakeholder trust in our ability to mitigate threats such as ransomware and malware," he concluded.

AIRLOCK
D I G I T A L