AIRLOCK DIGITAL

CASE STUDY

US Regional Bank

A United States regional bank used application control and allowlisting from Airlock Digital to reduce cybersecurity risk and improve compliance.

Airlock Digital for Banking & Finance

By enforcing a **Deny by Default model** and delivering real-time visibility into endpoint activity, Airlock Digital ensures financial institutions can operate securely in today's high-risk environment.

Challenge

Replace an incumbent product with a cloud-first, easy-to-use application control and allowlisting solution that complements **CrowdStrike endpoint detection and response** platform to deliver defense in depth.

Approach

The bank identified application control and allowlisting from Airlock Digital as the best fit for its requirements based on usability and performance.

Result

With the Airlock Digital solution, the bank strengthened its operational security and compliance while reducing its application control and allowlisting administration load.

Benefits to the US Regional Bank

With Airlock Digital application control and allowlisting, the bank has:

- Lowered cybersecurity risk and established trust with business teams
- Reduced near-constant administration of application control and allowlisting to 30 minutes a day
- Eliminated gaps in application control and allowlisting coverage
- Improved compliance with prescriptive and non-prescriptive security frameworks

"The difference in usability between the Airlock Digital solution and our incumbent product was like night and day."

Information Security Officer
Regional United States bank

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 Challenge

The United States regional bank has implemented a "defense in depth" cybersecurity strategy in which **application control and allowlisting complements endpoint detection and response** to minimize risk to the organization. The bank initially deployed a traditional application control and allowlisting solution but found the product's complex ruleset, lack of usability and limited functionality could not meet its long-term needs.

The Approach

"We needed a cloud-native or cloud-first solution and, as customers of CrowdStrike, evaluated Airlock Digital's application control and allowlisting solution and its integration with the endpoint detection and response platform," explained the bank's Information Security Officer. "We liked what we saw—the difference in usability between the Airlock Digital solution and our incumbent product was like night and day."

The bank ran the Airlock Digital solution side-by-side with its existing product to compare performance. "It was overwhelmingly clear that the Airlock Digital solution was the answer as a one-to-one replacement and then some, and that gave us the confidence to pull the trigger," said the bank's Information Security Engineering Manager.

The information security team deployed Airlock Digital through the CrowdStrike Falcon sensor to its thousands of endpoints, including workstations and servers, in a phased project. Once the team completed steps such as agent installation, audit and enforcement sub-policy implementation and the addition of prebuilts and publisher packages, it was able to adopt a holistic view of application usage within the organization.

The Result

Moving to Airlock Digital enabled the bank to close gaps in its application control, allowlisting, and OS hardening coverage, and adopt a proactive cybersecurity strategy. "Many teams in our organization have Microsoft Surface devices that are hybrid-joined to Microsoft's Intune endpoint management solution, but are not fully domain-joined," said the Information Security Engineering Manager. "With the Airlock Digital solution being cloud-first and deployed through CrowdStrike, we were able to bridge that gap."

The solution is light both in terms of the impact of its enforcement agent on the endpoint and the demands on team members, with information security analysts spending only about 30 minutes per day on administration and engineers logging in only when required.

In addition, the solution proved its merits during extensive penetration testing conducted by third parties in line with United States financial services regulations.

"The organization we brought in told us, based on previous versions of protection we had and what we had migrated to, 'you made us sweat'," said the Information Security Officer. "Subsequent testing confirmed that the model we went to was consistently much better."

With the information security team reporting directly to risk rather than IT or operations within the bank, deploying Airlock Digital helped build trust and address risk management. "We can now say nothing gets past us from an execution standpoint unless we review it or trust the publisher or installer," said the Information Security Officer.

This powerful cybersecurity assurance gives bankers and other team members confidence to proceed with activities that fall within the bank's broader risk framework.

While the primary reason for deploying the Airlock Digital solution was to strengthen its operational security, the institution also achieved some considerable compliance benefits.

"Allowlisting has some serious weight behind it around a number of prescriptive and non-prescriptive frameworks, so the Airlock Digital solution ticked a lot of boxes for us," said the Information Security Officer.

The Information Security Engineering Manager described the deployment of Airlock Digital application control allowlisting as a "no-brainer." "From the perspective of defense in depth, both endpoint detection and response and network detection and response are important in terms of telling you there is an attack and quarantining affected devices," he said. "However, Airlock Digital's solution integrates with CrowdStrike and allows us to prevent malware from being run to begin with!"

AIRLOCK DIGITAL