AIRLOCK DIGITAL | **CASE STUDY**

inductive automation

Overview of Case Study

How an industrial technology company deployed Airlock Allowlisting to protect its business.

About Inductive Automation

Operating for 20+ years, Inductive Automation creates industrial software that empowers a list of customers that includes 57% of the Fortune 100.

Challenge

Inductive Automation needed to implement allowlisting to complement a new endpoint protection software solution and reduce its cybersecurity risk profile.

Approach

The business selected Airlock Allowlisting (Airlock) based on its performance in a robust proof of concept exercise.

Result

Airlock's intuitive interface, effective user experience and deny by default approach is helping Inductive Automation improve its cybersecurity.

> Airlock Allowlisting is evidence based and a known entity which is reliable and predictable.

Jason Waits
CISO Inductive Automation

AIRLOCK DIGITAL

The Airlock Digital Allowlisting Solution

With Airlock Allowlisting, Inductive Automation has:

- effectively blocked known malware such as Wave browser spyware, as well as unapproved applications
- achieved seamless integration between its endpoint security and Airlock Allowlisting solutions
- customised allowlisting policies to the needs of individual business teams
- reduced operational resource and licensing costs

About Airlock Digital

Founded in 2013 in Adelaide, South Australia, pure play allowlisting and application control solution provider Airlock Digital helps organizations keep ransomware and other malware out of their environments.

AIRLOCK DIGITAL

CUSTOMER
CASE STUDY

inductive automation

The Customer

Inductive Automation specializes in web-based industrial automation software. Its core product, Ignition, enables industrial organizations to embrace digital transformation through Supervisory Control and Data Acquisition (SCADA), the Industrial Internet of Things (IoT), Human-Machine Interfaces (HMI) and more.

The Challenge

In 2019, Inductive Automation selected CrowdStrike Falcon to meet its endpoint protection requirements. The business needed to complement the endpoint solution with an allowlisting product to ensure only known applications were approved to run in its environment.

The Approach

Inductive Automation purchased Airlock Digital's Allowlisting product from the CrowdStrike marketplace and commenced a proof of concept. This exercise included rigorous stress testing and Airlock Allowlisting (Airlock) passed with flying colors, prompting Inductive Automation to move to full deployment.

Airlock's intuitive design and ease of integration with CrowdStrike Falcon ensured a straightforward deployment. The business rolled the product out to its non-technology business units in just two weeks, with the remaining in-scope endpoints completed in four weeks.

"The Airlock Digital team was extremely responsive through the deployment process and beyond," said Jason Waits, Chief Information Security Officer, Inductive Automation, "It has actioned support tickets and turned around feature updates in a very timely fashion."

With Airlock running across servers and end-user devices. Inductive Automation has improved its operational security by blocking non approved applications.

"Airlock provides another layer of security to protect our business," said Dominic Calonico, Director of Information Technology, Inductive Automation. With Airlock providing evidence-based, reliable and predictable allowlisting, Inductive Automation is well protected against security threats.

"Our penetration tester went to work and Airlock Allowlisting stopped everything he tried – he was very frustrated!" said Waits.

The Result

Airlock's intuitive interface, effective user experience and deny by default approach is helping Inductive Automation improve its cybersecurity.

"Our security team users were extremely happy with the interface, which was richer and easier to navigate than the interface of our previous allowlisting solution. They needed just two days to feel comfortable with Airlock Digital, as opposed to several weeks with the prior product." said Calonico.

As a result, the users could achieve operational efficiency faster and were able to perform their roles to a higher standard. The product has already proven its worth by blocking Wave browser spyware, mitigating the risk of a data breach and consequent exposure of sensitive data and unapproved applications.

"We allow self-service one-time pads for IT, security and some other power users so we don't slow down the installation of new software versions" explained Waits.

The benefits of Airlock are not limited to security; the product has enabled the technology team to reduce operational resource and licensing costs compared to the previous solution.

Based on its own successful deployment, Inductive Automation recommends starting with smaller business units that are relatively static before expanding into more complex functions, such as technology.

"Airlock is an integral part of our security architecture" concluded Waits. "We're now looking forward to new features such as macro allowlisting and agent self-updates that would further protect our environment."

Learn more about Inductive Automation by visiting **inductiveautomation.com**