AIRLOCK DIGITAL | CASE STUDY

AIRLOCK DIGITAL

inductive automation

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

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 based on its performance in a robust proof of concept exercise

Results

- 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
- Reduce operational resource and licensing costs

> Airlock Allowlisting is evidence based and a known entity which is reliable and predictable.
>
> **- Jason Waits, CISO**
> **Inductive Automation**

About Us

Airlock Digital provides an intuitive framework that ensures software management teams can successfully implement and maintain a compliant ‘allowed applications’ list.

The framework’s intuitive design and rapid policy distribution ensures seamless deployment within customer environments.

Customer

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 (IIoT), Human-Machine Interfaces (HMI) and more.

Challenge

In 2018, Inductive Automation had implemented a broad endpoint solution to protect against cybersecurity breaches. However, the business had to dedicate extensive time and resources to managing this solution.

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 execute.

Approach

Inductive Automation purchased Airlock Digital's Allowlisting software from the CrowdStrike marketplace and commenced a proof of concept. The decision was also supported by reviews published on the widely respected Risky Business information security podcast. This exercise included rigorous stress testing and Airlock Allowlisting passed with flying colors, prompting Inductive Automation to move to full deployment.

The Airlock product'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," says Jason Waits, Chief Information Security Officer, Inductive Automation, "It has actioned support tickets and turned around feature updates in a very timely fashion."**

Airlock's Allowlisting product is across servers and end-user devices. Inductive Automation has improved its operational security by implementing policies to block nonapproved applications. Airlock Allowlisting's integration with CrowdStrike Falcon confirms parent processes for any suspicious activity, while its logs are set to Chronicle, Google's cloud-native security operations suite, for oversight.

> **"Airlock Digital provides another layer of security to protect our business," says 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!" says Jason Waits, Chief Information Security Officer, Inductive Automation.**

Results

Airlock Allowlisting's intuitive user interface and effective user experience is helping Inductive Automation improve its cyber security risk profile.

> **"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." says Dominic Calonico, Direction of Information Technology, Inductive Automation**

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 passwords for IT, security and some other power users so we don't slow down the installation of new software versions" explains Jason Waits, Chief Information Security Officer, Inductive Automation**

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

Based on its own success with Airlock, Inductive Automation has several recommendations about how to deploy the product effectively. Top among these is starting with smaller business units that are relatively static, and then expanding into more complex functions, such as Technology.

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