AIRLOCK DIGITAL | **CASE STUDY**

SA Power Networks **Empowering South Australia**

Overview of Case Study

How SA Power Networks used Airlock Digital's application control and allowlisting solution to reduce its attack surface and access new business.

Challenge

SA Power Networks needed to improve its cyber security maturity to reduce its expanding attack surface and comply with the Defence Industry Security Program (DISP), which mandates application control and allowlisting as a key control priority.

Approach

SA Power Networks conducted a thorough procurement exercise and selected Airlock Digital's application control and allowlisting based on the solution's ease of management, integration with the CrowdStrike endpoint detection and response product running in its environment, transparency, and minimal user impact.

Result

By implementing the Airlock Digital solution, SA Power Networks has significantly enhanced its cyber security maturity and achieved DISP compliance Level 1, allowing it to pursue external projects.

> With Airlock Digital's solution and support, we are upgrading cyber security across SA Power Networks.
>
> **Lindbergh Caldeira**
> Cyber Security Operations Manager
> SA Power Networks

The Airlock Digital Application Control and Allowlisting Solution

With Airlock Digital's application control and allowlisting solution, SA Power Networks has:

- eliminated up to five days' monthly effort for its desktop support team to investigate unknown software
- moved in-scope endpoints seamlessly into enforcement
- prevented users potentially downloading maliciously modified versions of end-user software
- reduced EDR system alerts
- improved the organisation's patch management regime

About Airlock Digital

Airlock Digital is the global leader in application control and allowlisting, trusted by organisations worldwide to protect against ransomware, malware and other cyber threats.

AIRLOCK DIGITAL

CUSTOMER
CASE STUDY

SA Power Networks Empowering South Australia

The Customer

SA Power Networks is the sole electricity distributor for South Australia and supplies power to 1.7 million people across about 900,000 homes and business. Its primary role is to build, maintain and upgrade a 90,000-kilometre distribution network.

The Challenge

SA Power Networks needed to mature its endpoint cyber security strategy to reduce its exposure to cyber threats and achieve Level 1 compliance with the Defence Industry Security Program (DISP). Attaining this compliance level would help the organisation pursue external projects.

The Approach

SA Power Networks undertook a comprehensive procurement process to select an application control and allowlisting solution. Through this exercise, the organisation identified the key benefits of the Airlock Digital solution as: ease of management, integration with the CrowdStrike endpoint detection and response product running in its environment, transparency, and minimal user impact. SA Power Networks signed up with Airlock Digital in September 2023 and ramped up deployment in early 2024. By April, the organisation started moving its in-scope endpoints into enforcement mode.

"When compared with the products of its competitors, the Airlock Digital solution was clearly the leader in this area. The Airlock Digital team was supportive during the evaluation process and the ease of deployment made them the obvious pick for a larger deployment of application control," said Alex Duffy, Cyber Security Advisory Manager, SA Power Networks.

IT consultancy The Missing Link worked with an SA Power Networks cyber security analyst to complete the deployment, with the Airlock Digital solution's intuitive design ensuring a seamless project. "Today, that analyst is our Airlock Digital subject-matter expert and is charged with ensuring a measured balance between security and user experience," said Lindbergh Caldeira, Cyber Security Operations Manager, SA Power Networks.

The Result

With the Airlock Digital application control and allowlisting solution deployed across its in-scope endpoints, SA Power Networks has achieved a range of improvements. Top of the list is a defence-in-depth endpoint cyber security strategy that helps reduce the organisation's attack surface and achieve DISP Level 1 compliance.

The organisation has recorded only a handful of endpoint detection and response system alerts on endpoints with Airlock Digital deployed, reducing the workload of its Security Operations Centre analysts.

"While our endpoint detection and response solution is excellent at blocking malicious threats, there are sporadic false positives requiring investigation and validation by our analysts. Mitigating these false positives reduces alert noise and allows our team to focus on our other technology investments," said Caldeira.

With the transition to enforcement mode, SA Power Networks has closed an unapproved software detection loophole and implemented a secure operational process to manage user software requests.

"We now work closely with our users to understand their requirements and, through the integration of VirusTotal and the CrowdStrike product into the Airlock Digital solution, validate that the software they are installing is authentic and not a malicious version," said Caldeira.

SA Power Networks' cyber security team also now collaborates with its desktop support team to quickly add any new software to its patching regimen and set up appropriate update schedules. Previously, if the organisation's vulnerability management software detected third-party software not installed through authorised processes, the desktop support team had to properly identify the software and undertake any investigations and remediation required. This process could take up to five days per month to complete.

"With Airlock Digital's solution and support, we are upgrading cyber security across SA Power Networks to better protect our systems from ransomware, malware and other cyber threats," concluded Caldeira.

Learn more about SA Power Networks here
www.sapowernetworks.com.au

Find out how Airlock Digital can help.
Visit our website to request a personalized demo
airlockdigital.com