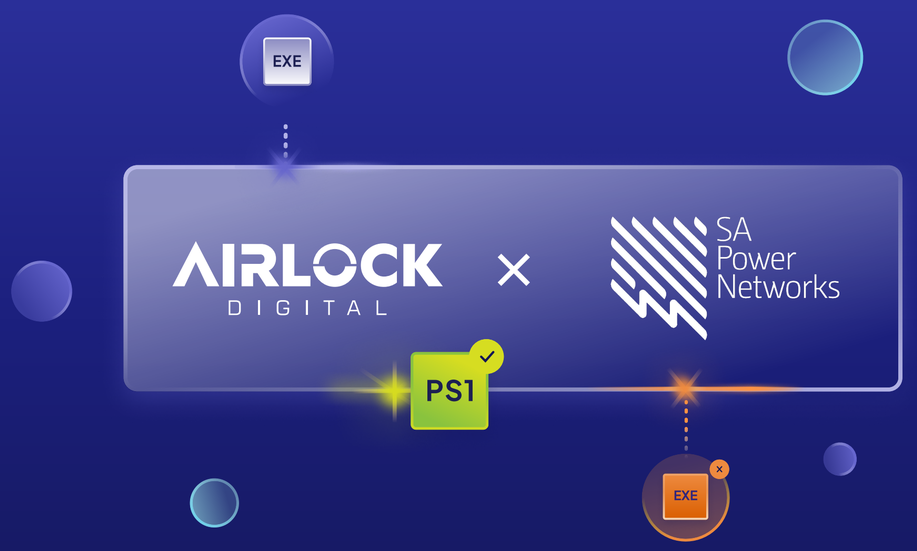
AIRLOCK DIGITAL

CASE STUDY

SA Power Networks

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



About SA Power Networks

As South Australia's sole electricity distributor, SA Power Networks delivers power, manages the grid and supports the state's rapid shift to renewable energy through innovation in technology like rooftop solar and EV charging. They maintain safety, reliability, and a 24/7 fault service, modernizing their infrastructure to handle new energy demands for their 1.7 million customers. SA Power Network employs 2,900 employees.

Learn more about SA Power Networks by visiting **www.sapowernetworks.com.au**.

Challenge

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

Approach

SA Power Networks conducted a thorough procurement exercise and selected Airlock Digital for application control and allowlisting because of its integration with their existing CrowdStrike endpoint detection and response product, as well as the solution's ease of management, transparency, and minimal user impact.

Result

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

Benefits to SA Power Networks

With Airlock Digital application control and allowlisting, 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 from potentially downloading maliciously modified versions of end-user software
- Reduced EDR system alerts
- Improved the organization's patch management regimen

"With Airlock Digital's solution and support, we are upgrading cybersecurity across SA Power Networks."

Lindbergh Caldeira
Cyber Security Operations Manager SA Power Networks

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

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

The Challenge

SA Power Networks needed to mature its endpoint cybersecurity strategy, 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 organization pursue external projects.

The Approach

SA Power Networks undertook a comprehensive procurement process to select an application control and allowlisting solution. Through this exercise, they 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 organization began 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 cybersecurity analyst to complete the deployment; Airlock Digital’s intuitive design ensured 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 Airlock Digital application control and allowlisting deployed across its in-scope endpoints, SA Power Networks achieved a range of improvements. AT the top of the list is a defense-in-depth endpoint cybersecurity strategy that helps reduce the organization’s attack surface and achieve DISP Level 1 compliance.

SA Power Networks recorded only a handful of endpoint detection and response system alerts on endpoints with Airlock Digital deployed, reducing the workload of its Security Operations Center 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 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’ cybersecurity team 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 vulnerability management software detected third-party software not installed through authorized 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 cybersecurity across SA Power Networks to better protect our systems from ransomware, malware and other cyber threats,” concluded Caldeira.

AIRLOCK DIGITAL