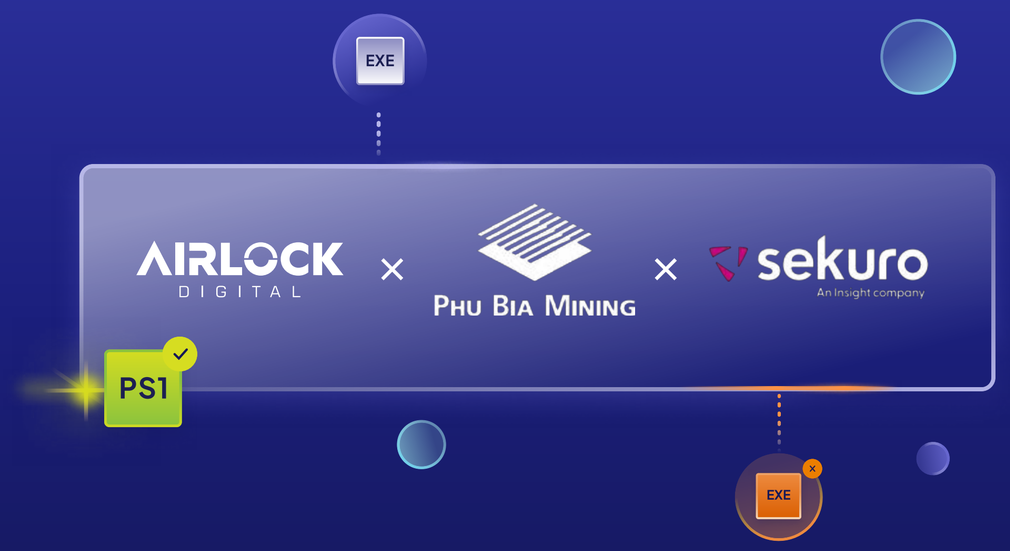
AIRLOCK DIGITAL

CASE STUDY

PanAust & Sekuro

With Airlock Digital and Sekuro, a multinational resources organization gains control over endpoint executions and aligns with Essential Eight mitigation strategies.



About PanAust

Australian-incorporated PanAust is a copper and gold producer in Laos, with operations also extending into Papua New Guinea and Chile.

Challenge

Reduce phishing malware and align with the Essential Eight application control mitigation strategy

Approach

Collaborate with leading Airlock Digital partner Sekuro to implement an enterprise-class application control solution that can be extended seamlessly from IT to a profit-generating OT environment

Result

Working with Sekuro, PanAust has seamlessly deployed Airlock Digital to align with the Essential Eight application control strategy and stop malware execution.

The Airlock Digital Application Control Solution

With the Airlock Digital solution, PanAust has:

- Established a sound base to move to larger frameworks including the NIST Cybersecurity Framework and/or ISO 27001
- Minimized the number of malware incidents raised by its Managed Detection and Response (MDR) team
- Eliminated unauthorized browser extension installations
- Used multiple trust options to determine the applications and files to trust, reflecting organizational usage patterns
- Completed a smooth implementation of application control with leading partner Sekuro

“While we targeted Essential Eight Maturity Level Two, we realized that, with Airlock Digital, there wouldn’t be much more work needed to achieve Maturity Level Three. Working with Sekuro made the implementation considerably easier.”

Scott Brownlee
Cybersecurity Superintendent
PanAust

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

Headquartered in Brisbane, Australia, PanAust is a copper and gold producer in Laos, with additional operations in Papua New Guinea and Chile. The organization has about 4,000 team members, about 1,700 of which are computer users, and engages contractors and consultants across its operations.

The Challenge

PanAust needed to implement security controls that stopped phishing malware from compromising teams across various geographic regions.

The organization decided to align with the Australian Signals Directorate's Australian Cyber Security Centre's Essential Eight mitigation strategies for internet-connected IT networks, as they were easy to communicate to non-technical teams within the business.

"We see the Essential Eight as the foundation of a strong, risk-based cyber security program that will allow us to leverage bigger frameworks such as NIST and/or ISO 27001 in the future," said Scott Brownlee, Cybersecurity Superintendent, PanAust.

The Approach

PanAust established separate alignment projects for each Essential Eight mitigation strategy. This entailed reviewing its environment against the supporting Essential Eight Maturity Model to identify the right maturity level that each project should target.

The organization identified Maturity Level Two, which targets malicious actors that invest time and employ common social engineering techniques, as the right target for its application control alignment strategy.

PanAust needed a trusted advisor to help navigate market options and identify the most economical, effective and efficient application control solution for its needs.

The advisor also needed a deep understanding of PanAust's broader security strategy to align the project with the organization's priorities.

Following a comprehensive market evaluation, PanAust turned to leading Airlock Digital partner Sekuro to guide its application control procurement and instill confidence that the selected solution could meet the needs of the business.

Sekuro's commitment to best of breed cybersecurity technologies, existing relationships across PanAust and commitment to application control best practice set the organization apart from its competitors through the assessment.

The partner worked closely with PanAust to identify Airlock Digital as the preferred solution to deploy application control across about 2,000 endpoints. "While we targeted Essential Eight Maturity Level Two, we realized that, with Airlock Digital, there wouldn't be much more work needed to achieve Maturity Level Three. This would give us the ability to defend against adaptable and capable threat actors aiming to perform targeted intrusions," said Brownlee.

"In addition, we have an operational technology (OT) environment that is the profit generation engine of our business, and we plan to extend application control to its endpoints.

"With Airlock Digital, we could do that without running two separate products or modifying our security strategy to allow the connection of all our IT and OT endpoints to a single solution."

Expert deployment with Sekuro

Through the engagement, Sekuro demonstrated its flexibility in accommodating PanAust's requirements.

"I wanted our team members to configure and implement Airlock Digital themselves as they would have to own and manage the solution," explained Brownlee. "Working with Sekuro made the implementation considerably easier, as its consultants applied considerable skill and experience to help ensure a smooth deployment across our complex, decentralized environment."

During initial workshops with PanAust, Sekuro created a project plan and task list to guide the project end to end. This covered deployment of the Airlock Digital agent, initial configuration and monitoring of trusted executions.

The Airlock Digital partner also provided an initial point of contact for any queries PanAust had about the solution console and configuration.

The advice and engagement with Sekuro proved integral in aligning the implementation with Essential Eight Maturity Level Two requirements.

Smooth policy management workflows

Seamless policy management workflows offered by Airlock Digital enabled PanAust to easily assign common security policies to non-IT Windows servers, Linux servers, and workstations across the organization. IT workstations and Windows servers were allocated to a separate policy group to support specialist software needs.

AIRLOCK DIGITAL

The IT team captured configuration images on its various types of hardware, added them to a baseline, and maintained the endpoints in audit mode to build its application control policies.

“Airlock Digital gave us the flexibility to work through what we wanted to allow and what we didn’t at our own pace,” said Brownlee. “We spent a few hours each week for a few weeks until we reached a point at which we were comfortable with what we’d added to our allowlists.”

The team then transitioned Airlock Digital to enforcement mode site by site over four months, allowing policies to be enforced and preventing untrusted applications and files from running. The lightweight Airlock Digital agent minimized impact on system resources while enforcing policies in real-time.

Extensive engagement with the business helped build internal support for the application control project. These included including ‘hyper care’ periods in which extra resources were available to help allowlist additional applications required by teams.

Starting at smaller sites, IT was able to capture most applications needed by the business before moving to bigger locations, ensuring a smooth deployment.

The Result

With Airlock Digital and Sekuro, PanAust has aligned with the Essential Eight application control mitigation strategy to Maturity Level Two.

This is a critical step in the organization’s broader Essential Eight alignment strategy and its establishment of a platform from which to comply with the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework and the ISO 27001 international standard for Information Security Management Systems.

Minimizing malware incidents

PanAust has minimized the number of malware incidents raised by its Managed Detection and Response team after adding Airlock Digital to its security stack. “Prior to Airlock Digital and USB control, we would see malware every one or two weeks,” said Brownlee. “Now, we haven’t seen a genuine malware alert for months.”

Brownlee nominates the browser extension control feature of Airlock Digital, which enables PanAust to allow only trusted extensions to run, as critical to reducing the organization’s attack surface. “That is a big benefit for us, because browser extensions can be installed by users without administrator involvement,” said Brownlee. “With Airlock Digital, we can stop unauthorized browser extension installations and lower our cybersecurity risk accordingly.”

Using multiple trust options to reflect usage

The application control solution provides multiple options when determining the applications and files to trust, ensuring PanAust’s policies fully reflect the usage patterns of teams across the organization.

The IT team turns first to Trusted Installer to allow and automate the deployment of applications through Microsoft Endpoint Configuration Manager, followed by publisher, which enables it to trust software from approved third parties, and hash for code that is unsigned or considered not appropriate for deployment through Trusted Installer.

With many field-based reviewers and users of mining industry software (such as specialist blast-modeling, water level, vibration and topology products), PanAust is a prolific user of Airlock Digital’s One Time Password (OTP) feature for temporary execution of applications not on its allowlist.

PanAust now plans to extend its application control deployment to its OT environment and, with each site being comparatively static, plans to take a highly granular approach to the applications allowed to run in each location. Airlock Digital support for legacy and current operating system versions is integral to the project, as the environment features applications certified to run only with certain firmware and operating systems.

Without the compatibility offered by Airlock Digital, upgrading to newer operating systems would be expensive and impractical.

In addition, with the environment featuring restricted traffic flows, the organization can use a single on-premises policy node that requires only limited connectivity with the Airlock Digital cloud-hosted portal to ensure the continued operation of application control.

“Airlock Digital is a very effective tool in our security arsenal,” concluded Brownlee.

AIRLOCK DIGITAL

Lessons Learned

“We recommend getting your house in order before deploying Airlock Digital. Cleaning up your application list and standardizing your corporate applications makes that process a lot easier. Having a trusted partner like Sekuro can contribute considerably to the success of your project.”

Scott Brownlee, Cybersecurity Superintendent, PanAust