Airlock Allowlisting Solution Blocks Ransomware and Reduces Operational Overhead for IT and Cybersecurity Teams

Airlock pro-actively blocks malware, ransomware and zero-day attacks to help meet government cybersecurity standards including ACSC Essential Eight and NIST 800-171

Adelaide, Australia – 24 March 2021: Australian cybersecurity pioneer Airlock Digital continues to enhance its industry-leading allowlisting solution to more effectively block malware, ransomware and zero-day attacks, help comply with cybersecurity standards, and reduce the allowlisting operational effort for IT and cybersecurity teams.

Allowlisting – also referred to as application whitelisting or application control – is documented in a number of government cybersecurity standards and/or regulations worldwide, including the ACSC Essential Eight Strategies to Mitigate Cyber Security Incidents, U.S. Top 10 Mitigations, NIST 800-171, CMMC, Center for Internet Security Basic Six, Canadian Top 10 IT Security Actions, and New Zealand Critical Controls.

Many cybersecurity solutions exist today that can block the execution of files on endpoint systems. Almost none offer the granular centralised control, the workflow support, or the operational flexibility required to cost-effectively support allowlisting in dynamic, enterprise computing environments.

“There are many security products that can allow or block files. That isn’t the challenge,” says Airlock Digital Co-Founder, David Cottingham. “The challenge is how you instrument the allowlisting process to operationalise pro-active security controls.”

Airlock reduces the support burden of allowlisting, utilising easy-to-use workflows that prevent disruption to users. If a required application is blocked, IT teams, including non-cybersecurity staff, can simply and easily grant permissions to users with a range of one-time password (OTP) options.

In addition to one-time use and mobile OTP, the latest Airlock version 4.7 release provides a new codeless self-service capability, helping to maintain user productivity without compromising on security. Codeless self-service allows privileged users to self-administer temporary access to applications and scripts restricted to the general user base.

“Codeless self-service aims to reduce friction and enables users to handle exceptions as quickly as possible, reducing overall business impact and work disruption,” says Cottingham. “Ultimately, organisations can choose how they want exception management to be used, in line with the organisation’s appetite for risk.”

With the latest product enhancements, Airlock Digital has embraced a user-centric approach to allowlisting. Airlock offers the ability to control access for individual users or groups, in addition to devices, to give organisations additional flexibility and more streamlined workflows. This makes allowlisting with Airlock more practical to implement at scale and allows integration with privileged access management (PAM) solutions. Additional, more granular blocklisting criteria have been included to apply blocklist rules to specific enterprise security groups and operating system versions, ensuring that only appropriately privileged users can execute files across specific device types.

“By having more granular criteria for blocklisting rules, you can now easily operationalise your security policies,” says Daniel Schell, Co-Founder and Chief Technology Officer for Airlock Digital. “Based on Active Directory group membership, security administrators can easily block applications such as TeamViewer across the environment in a couple of clicks, while still allowing access for users that may need it.”

Airlock’s enhancements continue to add to its value as a strategic cybersecurity tool for achieving proactive endpoint protection. Another immediate benefit – simply achieved by blocking the execution of malware and restricting the ability to execute risky code – is reducing the number of security events that Security Operations Centre (SOC) teams must deal with.

Airlock also provides full visibility over all files running across endpoints, including their history and associated network activity, and can share this data with Security Information and Event Management (SIEM) platforms. With the latest release, Airlock cloud customers gain the ability to pull SIEM logs from the cloud via a REST API, removing the need to use a custom solution or expose ports to the Internet.

About Airlock Digital

Australian based cybersecurity company, Airlock Digital, delivers forward thinking endpoint protection solutions which enable organisations to implement rapid, scalable allowlisting and execution control. Through first-hand understanding of the operational challenges in cybersecurity, intimate industry experience, and an intuitive solution set, Airlock Digital is positioned as the leading, commercial allowlisting vendor. Airlock operates worldwide with offices in Australia and the United States.

The Airlock allowlisting solution enables organisations to reduce cyber risk and significantly uplift their endpoint security posture. Through industry leading workflows that are easy to use, Airlock enables organisations of all maturity levels to maintain a long-term effective allowlisting strategy without end user disruption. Airlock’s innovative, feature-rich allowlisting is used to protect hundreds of thousands of endpoints across the globe.

Contact us for more information at info@airlockdigital.com.

Contacts

Chris Bowes
04 0335 2232
mailto: chris.bowes@bowespr.com