

AIRLOCK DIGITAL – ADDRESSING ASD’S NUMBER 1 CYBER MITIGATION STRATEGY, EVEN EASIER WITH REPUTATIONAL FILE LOOKUPS

Application whitelisting implemented in days not months, adds ReversingLabs support to allow administration by non-cyber security specialists

Adelaide, South Australia, December 1, 2017 – Airlock Digital, headquartered in Adelaide, South Australia, today announced that its application whitelisting solution now includes integrated file reputational lookups to streamline administration and allow non-cyber security specialists to easily assess the threat level of unknown files. The Airlock solution is specifically built around the Australian Signals Directorate’s (ASD) controls for application whitelisting, the number one cyber threat mitigation strategy in the Australian Information Security Manual (ISM). Airlock leads the industry in ease of use with inbuilt workflows enabling application whitelisting to be implemented in days, not months. “Airlock already makes application whitelisting easy to deploy and maintain in dynamic environments,” said Daniel Schell, Co-Founder of Airlock Digital. “Adding reputation lookup through our ReversingLabs partnership makes management of the whitelist even easier by providing additional context to the trust decision making workflow.” “Despite being recognised as the most effective strategy by the ASD, organisations have resisted application whitelisting because of perceptions it is onerous to administer, resource intensive to implement and reliant on a supplied list of known good files,” said Richard Rundle, CEO and Co-Founder of Airlock Digital. “With Airlock, these perceptions are no longer the reality.” Airlock improves implementation time by interrogating a customer’s existing environment to allow security and operations teams to quickly populate whitelists and create security policies. Integrated file reputational lookups – provided in partnership with global file classification leader, ReversingLabs – makes ongoing administration of the solution simple and easy. “The inclusion of reputational lookups from a trusted source significantly reduces the time for administrators to make decisions about whether to trust new files,” said Rundle. “Not all people administering endpoint and server protection are security specialists, so the risk levels posed by unknown files has to be easy to understand. With ReversingLabs, we add confidence to the process.” “Airlock’s expanded capabilities represent another breakthrough in ease of use which opens up new opportunities for the company’s rapidly growing base of channel partners,” said Scott Hagenus, CMO of emt Distribution – Airlock Digital’s Australian and New Zealand distributor. “Traditional blacklisting technologies have proven ineffective against the myriad of attacks we see today, as seen by the frequency and reach of ransomware attacks,” said Hagenus. “Airlock addresses the barriers that have restricted the uptake of application whitelisting. By minimising the impact on operations, more organisations can enjoy protection by the number one cyber mitigation strategy, and resellers can more easily support them.” In addition to integrated file reputational lookups, Airlock now boasts increased performance with a single instance able to manage in excess of 20,000 devices, restriction of access to specific networks, increased collection and reporting on file metadata, and support for AppX digital signatures making granular trust of Windows Store applications possible. “As an Australian cyber security vendor, we understand the vital roles the ASD, the Australian Cyber Security Centre and AusCERT play in helping protect and defend the Australian economy from cyber threats,” said Airlock Digital Co-Founder, David Cottingham. “We’ve taken notice, understand the value and have built a solution from the ground up to meet the cyber security challenge head on – and we continue to investigate and research successful breaches, so we can learn from them.” For a full list of new features and enhancements to Airlock visit www.airlockdigital.com About Airlock Digital Airlock Digital was born out of necessity to address the challenges faced by enterprise and government organisations when implementing application whitelisting technologies and policies. The founders of Airlock Digital spent years implementing application whitelisting technologies in enterprise organisations and deeply understand real-world whitelisting challenges. A new approach to whitelisting was needed – Airlock makes application whitelisting work. # # # If you would like more information about this topic, please contact Glenn Mahney at +61 8 8273 3030 or email at glenn@airlockdigital.com.

Contacts

Chris Bowes
02 9387 2332
[mailto: chris.bowes@bowespr.com](mailto:chris.bowes@bowespr.com)