AIRLOCK DIGITAL

2018 AIRLOCK APPLICATION WHITELISTING

Airlock vs AppLocker Comparison

AIRLOCK PARTNER
TRAINING MATERIAL

How Does It Stack Up?
Airlock vs AppLocker

Not all application whitelisting solutions are created equal. Airlock was designed from the ground up to be the most secure and easy to manage application whitelisting solution on the market. Many organisations attempt to deploy Microsoft® AppLocker to achieve a higher level of security only to encounter the shortfalls.

01 Centralised Reporting

Airlock performs comprehensive out of the box reporting. Providing realtime dashboards and flexible search functionality to make environment management and monitoring easy.

02 User Permissions

Airlock performs Application Whitelisting in the SYSTEM user context and has the ability to catch file loads before Anti-Virus platforms. All users on the system have Application Whitelisting enforced.

03 Emergency Exclusions

Supports the use of One Time Pad (OTP) codes, which are provided to users in the event they need to run files that would otherwise be blocked. Users are not required to be connected to the company network. Codes temporarily disable whitelisting enforcement (not monitoring) for a defined time period.

01 Centralised Reporting

AppLocker provides no centralised monitoring or reporting capabilities. Monitoring can be added seperately using Windows Event Forwarding in combination with a third party Security Information and Event Management (SIEM) solution to correlate and display events.

02 User Permissions

AppLocker relies heavily upon user permissions in order to provide security. By default, all domain and local administrative users are exempt from application whitelisting. Files executing below the administrative user context (SYSTEM), such as drivers, are not logged or blocked by AppLocker.

03 Emergency Exclusions

AppLocker has no ability to temporarily 'opt-out' users from Application Whitelisting. Computers must be removed from AppLocker policy while the computer is connected to the organisations network. Often this process also requires the user to logoff and back on the computer for changes to take effect.

04 Policy Update Speed

Airlock has an configurable client poll time that defines when the server is queried for policy updates. This process is seamless and enables whitelisting policy distribution to an entire network in under three minutes, with no user action required.

05 Folder Exemptions

Airlock has been designed to perform the most effective method of application whitelisting possible using purely file cryptographic hash values. Comprehensive folder exemption support is included within Airlock, however none are required for effective operation.

06 Whitelisting Bypasses

Airlock monitors target systems for all attempts to map files on disk into executable memory, making it extremely effective in preventing all application whitelist bypass techniques. Airlock is under continual development with active research and verification into all known and emerging bypass techniques.

07 Event Troubleshooting

Airlock presents customisable block notifications to users every time a block event occurs. Airlock's Enforcement agent GUI makes reviewing, exporting and troubleshooting application whitelisting activity easy.

04 Policy Update Speed

AppLocker relies upon group policy replication to deliver updated policy to clients. This can take hours in many cases for computers to receive and update policy. To force policies to apply faster users must either reboot or log off and back onto their computer to recieve new rules.

05 Folder Exemptions

AppLocker excludes two major system directories by default to make operation 'easier'. These locations are C:\Windows* and C:\Program Files* any files located in these directories (including subdirectories) with default rules in place are allowed to run unrestricted. Creating a significant security gap.

06 Whitelisting Bypasses

Microsoft states that AppLocker is not considered a 'security boundary'[1] and does not patch AppLocker bypass techniques. AppLocker bypass techniques are commonplace and easy to use, with numerous methods contained (and frequently updated) in attack frameworks such as Metasploit[2] and Crackmapexec[3].

07 Event Troubleshooting

Troubleshooting block events using AppLocker can be a time consuming task, requiring administrators to dig through Windows Event Logs to identify AppLocker activity. AppLocker only presents block messages to users if they attempt to open a file from the explorer shell, not if an application performs a file load request, often causing confusion.

1 https://github.com/kasif-dekel/Microsoft-Applocker-Bypass#microsfts-response
2 https://www.rapid7.com/db/modules/exploit/windows/local/applocker_bypass
3 https://github.com/byt3bl33d3r/CrackMapExec

08 Disabling the Whitelist

Airlock can be configured to allow or deny administrative users from disabling the application whitelist. Unique passwords can be configured to prevent Airlock services from being tampered with or disabled. Airlock logs are protected against deletion or tampering by all users.

09 Hash Based Whitelisting

Airlock makes pure hash based application whitelists a reality in continually changing enterprise environments. Airlock supports large policy sets containing greater than 1+ million hash values that are easy to configure and manage.

10 Application Libraries (.DLL)

Airlock performs efficient whitelisting on all executable code (including .DLL files), regardless of file type or extension. Airlock's easy to use workflows make the task of managing tens of thousands of file exceptions easy. Airlocks Enforcement agent is lean, with next to zero impact on system resources.

08 Disabling the Whitelist

Users that have administrative access to a system can easily temporarily stop or entirely disable the AppLocker service. Administrators have the ability to delete AppLocker event logs from their system.

09 Hash Based Whitelisting

AppLocker stores configuration information in a Group Policy Object (GPO). GPO's do not support storing and processing the large number of hash values required to whitelist a typical operating system (30,000+). Hash values are supported, but must be used in combination with less secure path and publisher rules to permit system operation.

10 Application Libraries (.DLL)

"Each application can load several DLLs, and AppLocker must check each DLL before it is allowed to run. Therefore, creating DLL rules might cause performance problems on some computers. Denying some DLLs from running can also create application compatibility problems. As a result, the DLL rule collection is not enabled by default."[4]

Airlock Digital was founded in 2013 with one goal: Enable organisations to implement and maintain application whitelisting, simply and securely, in dynamic computing environments.

The founders of Airlock Digital have spent years implementing application whitelisting technologies in enterprise organisations and deeply understand real-world whitelisting challenges. Airlock Digital was born out of necessity to address these challenges, as a new approach to application whitelisting was needed.

4 https://technet.microsoft.com/en-us/library/ee460950(v=ws.11).aspx