

Understanding Application Control (Allowlisting)

What is Application Control (Allowlisting)?

Application control, also known as allowlisting, is an invaluable addition to your security tech stack. Why? Because, against an increasingly hostile threat landscape, it empowers you to control what code runs in your environment.

Application control (allowlisting) is recognized as a critical cybersecurity control by bodies such as:

- The National Institute of Standards and Technology (NIST)
- The United States Department of Defense
- The Canadian Centre for Cyber Security, and
- The Australian Cyber Security Centre

How Does Application Control (Allowlisting) Work?

An allowlist is a list of files and applications you trust to run in your environment.

With all other files, including ransomware, malware and unauthorized software unable to execute, your organization and its people can focus on growth, innovation and success.

Here's what allowlisting can do for your organization. You can:

- Permit only trusted files and applications block untrusted applications, scripts and installers
- Prevent unknown code and never-before-seen, file-based attacks
- Allow only authorized people to run approved applications and files
- Enforce your security policies and harden your operating systems

We make 'deny by default' for file execution realistic and scalable, by putting you in control of what you trust

You can secure your organization without slowing down your users.

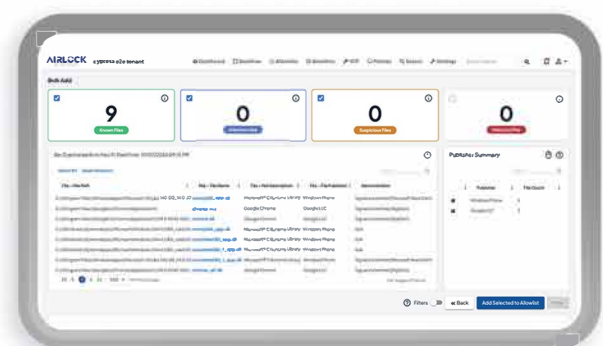
When those users do need to access applications outside policy, our exception process is quick, simple and secure.

Your security team enforces a proactive standard rather than being forced to scramble to respond to alerts.

And because you set the rules for your environment, cybercriminals find it harder to target your organization and have a lower chance of success.

With our solution, whether you're running the latest or certain legacy Windows, Linux or macOS versions, you can still determine which files can run and which can't.

You can also verify, monitor and record all file executions, so your security team can run queries and make timely, accurate decisions about your environment.


AIRLOCK
DIGITAL

AVAILABLE FOR
Windows™ | Linux® | MacOS™

What Does Airlock Digital's Application Control (Allowlisting) Solution Do?

Airlock Digital's application control (allowlisting) solution does not rely on signature or behavior-based detection to stop unknown and untrusted files from executing.

