

Airlock Digital application control

Canonical:

<https://agentic.blueapache.com/technical-excellence/airlock-digital/airlock-digital-solutions-with-blueapache/>

Description:

We help you implement application control that reflects the software your business needs to run.

Details:

We help you select and implement Airlock Digital application control so your organisation can decide which software is trusted to run. We combine the platform with our endpoint, security and implementation expertise, shaping the deployment around your applications, your people and the responsibilities your IT team wants to retain.

Application control is an operational discipline as well as a security control. A useful deployment needs to recognise legitimate business software, handle updates and give staff a clear route to request an exception. We work through those requirements with you before introducing enforcement.

Control what runs across your environment

Airlock Digital uses application allowlisting to permit trusted code and restrict execution outside the approved policy. Its controls extend beyond installed applications to executables, libraries, installers and scripts. Trust can be defined using attributes such as file hashes, publishers, paths and process relationships.

That gives us several design choices. A tightly controlled server may need a different policy from a developer workstation or a shared frontline device. We help you assess those differences and choose how policies should apply across the selected endpoint groups. Supported Windows, macOS and Linux environments can be considered, with compatibility checked against your actual operating systems and applications.

We also consider how application control fits alongside your existing endpoint detection, identity protection and patching. Restricting execution and investigating suspicious activity address different parts of endpoint security; we plan how those capabilities work together.

Plan the move from visibility to enforcement

We help you turn a broad application-control requirement into a practical implementation scope:

- Identify the devices, business applications, scripts and software distribution tools that matter to your operations.
- Review execution activity in audit mode to understand what would be affected by a policy.
- Define trust rules and assign ownership for approving new software and changes.
- Pilot enforcement with a representative group, including applications that run infrequently but are business critical.
- Agree how exceptions, software updates and support requests will be handled as deployment expands.

The audit stage matters because observing an application is not the same as deciding it should be trusted. We work with application owners and your IT team to make that decision, rather than treating every observed file as automatically approved.

Keep application control workable after deployment

Software estates change. New applications arrive, publishers release updates and staff move between roles. We help you plan the approval and review processes needed to keep the policy useful over time. That includes identifying who can approve an exception, how changes are recorded and when a temporary exception should be reviewed.

For example, a finance application update may introduce new executables or scripts. The rollout plan should account for those changes before the update reaches users. The same principle applies to engineering tools, remote support utilities and applications used only at month end.

Choose how to work with us

Through our TECHNOLOGY offering, you can engage us for product selection and implementation while your internal team retains operational ownership. If application control is part of a wider security or endpoint requirement, we can also discuss how responsibilities fit within a CONTROL co-managed engagement or an OUTCOME managed service. We define the Airlock-specific scope with you, including deployment, policy administration and ongoing support.

Questions about application control

Can our IT team manage Airlock after implementation?

Yes. We can structure the project around your team's ownership, covering the selected deployment, policy approach and operational handover. We agree which responsibilities remain with you and where you want our continued assistance.

Will allowlisting stop staff using legitimate software?

An enforced policy can block software that has not been approved. We address that through application discovery, audit-mode review, piloting and an agreed exception process. Your business workflows are part of the design.

Does buying Airlock complete our security programme?

We treat application control as one part of your wider security approach. We consider it alongside patching, identity, detection and response, backup and the way your people use technology.

Talk with our team about application control

Related expertise

- NinjaOne endpoint management
- Huntress endpoint and identity security