AIRLOCK DIGITAL

A Checklist for Endpoint Security Readiness

When developing a strong endpoint security strategy, it's helpful to understand your current state as well as potential changes to your future requirements. A proactive posture will allow for modern application control at scale, while meeting compliance standards and ensuring the flexibility needed to secure the enterprise.

Use the checklist below to assess your endpoint security needs.

Consideration	Key Questions
1 **Agent Efficiency**	• How much CPU, memory, and disk impact can my environment tolerate from endpoint agents? • Will our IT or security team be able to manage the agent footprint of the product I am evaluating at scale? • Do our existing security policies or SLAs limit the resources available to run security agents?
2 **OS & Legacy Coverage**	• Are we running any unsupported or legacy operating systems that still require protection? • Do we need to maintain visibility and control over both modern and older endpoints? • How much variation is there across our endpoint fleet in terms of OS and system requirements?

Consideration	Key Questions
3 **Trust Mechanism Diversity**	• Can we use a single modality for assigning trust (e.g. hash), or do we need the ability to trust applications based using multiple approaches (e.g. publisher, path, hash, or parent process?) • Is flexibility in assigning trust important to support different workflows or levels of assurance? • How do we currently verify that trust decisions are accurate and reflect organizational risk tolerance?
4 **Security Stack Integration**	• Do we need to feed relevant application control data into our existing SIEM tool? If so, what specific data? • Do we need to integrate our application control solution with our existing EDR/XDR tool? • Do we want to automate certain application control processes via our other enterprise tools, such as our ITSM?
5 **Deployment Flexibility**	• Do we have regulatory or architectural reasons to prioritize on-prem, cloud, or hybrid deployment? • Do we require SaaS or private cloud options due to policy, scalability, or vendor management needs? • Will a cloud-based deployment help reduce operational burden or complexity for our team?
6 **Offline & Air-Gapped Support**	• Do we have users or systems that frequently operate without reliable connectivity? • Do we operate in environments with limited or no external network connectivity (e.g. OT, field units)? • Can our security policies enforce control over systems that are disconnected from central management?

Consideration	Key Questions
7 **Software Deployment Tool Compatibility**	• What software deployment tools do we rely on to manage applications across the organization? • How critical is seamless integration between application control and our deployment workflows? • Have we experienced friction in past deployments due to poor integration with deployment tools?
8 **Exception Management**	• How frequently do users require exceptions to run new or unknown applications? • Is the current process for managing exceptions manual, slow, or prone to error? • Would a secure, self-service exception process improve user productivity and reduce burden on the IT team?
9 **Browser Extension Control**	• Do we have visibility and control over browser extensions in our environment? • Do malicious or unauthorized browser extensions represent a security risk in our organization? • Do we require consistent control over browser extensions across Chrome, Edge, Firefox, and Brave?
10 **Bulk Trust Assignment**	• How often do we need to apply trust to large numbers of files across systems or environments? • Is it a bottleneck today to manually approve trusted files in bulk • What tools or processes do we have in place to baseline known good files across environments?

Consideration	Key Questions
11 Blocklisting Capabilities	• Do we need to block known malicious or unauthorized files across the enterprise? • Given our organization, is it important to be able to block files using a mix of methods-hash, path, or metadata such as filename, domain security group, etc. • Have we experienced incidents due to misuse of legitimate tools (LOTL attacks) or shadow IT?
12 User Management & Access Control	• Do we need to delegate responsibilities across multiple security or IT teams? • Does our organization require integration with domain security groups or SAML for access control? • Is Role-Based Access Control (RBAC) important to align policy management with team responsibilities?

For more information about choosing the right solution for your organization, download:
Modern Application Control: Enterprise Buyer's Guide. 12 Key Considerations for Enterprise Buyers.

This guide provides in-depth perspective and guidance to align with your security strategy.

Want to discuss your application control needs with an enterprise endpoint expert?
Visit **www.airlockdigital.com/book-a-meeting** today to talk with a team member in your region.