TECHNICAL SOLUTION BRIEF

Define What Runs.

Apply Control Without Disruption.

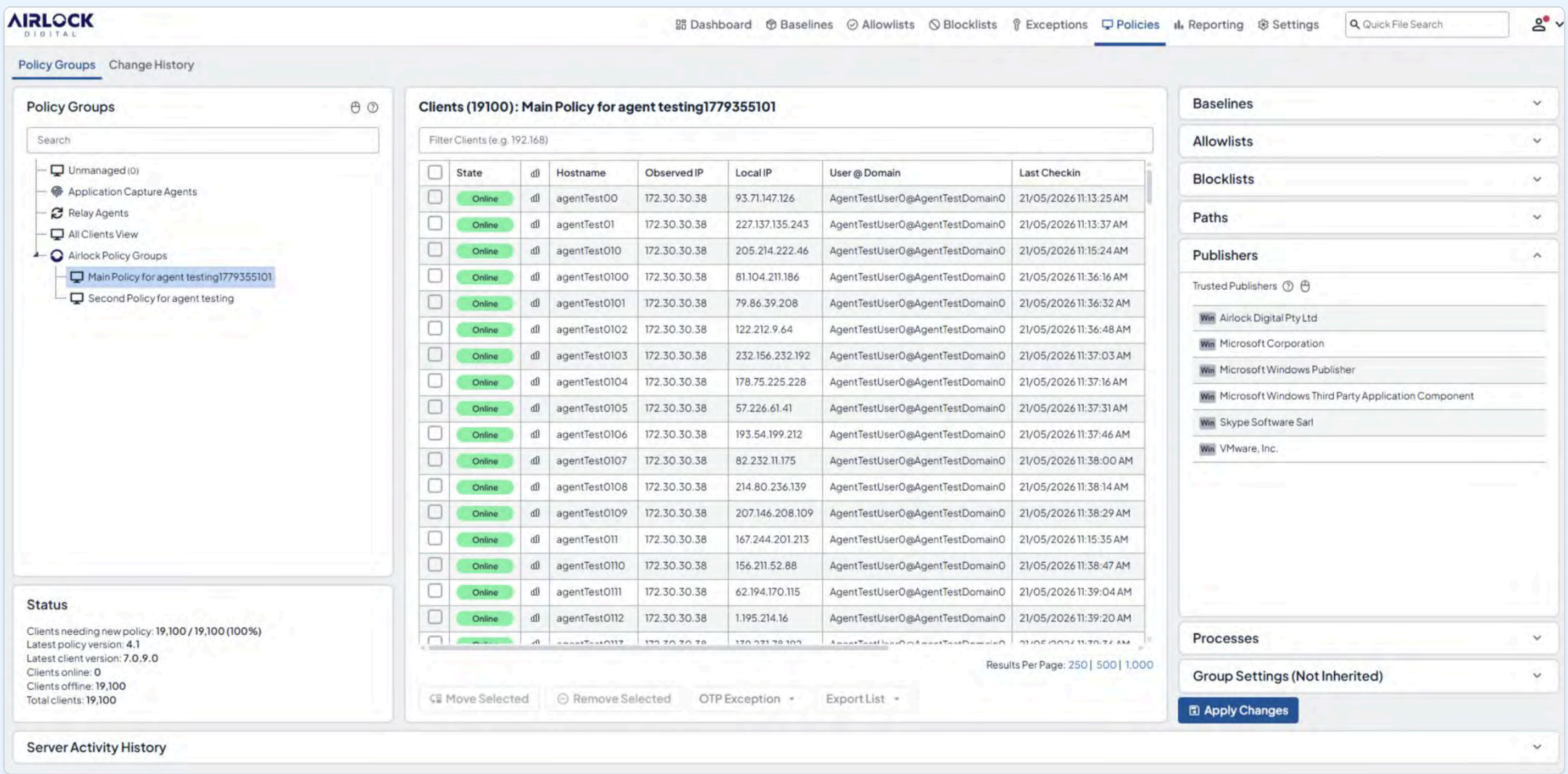
Airlock Digital helps security and IT teams control what can run across Windows, Linux, and macOS. With deep execution visibility and policy-driven control, teams can allow only trusted software to run without creating operational overhead.

Key Outcomes

- Define trusted execution using policies aligned to real software behavior
- Understand what is actually running across the environment before enforcement
- Reduce manual effort required to build and maintain policy
- Apply tightly scoped elevation without broad administrative access
- Progress to enforcement in a controlled, low-risk manner
- Operate application control consistently across IT, OT, and distributed environments

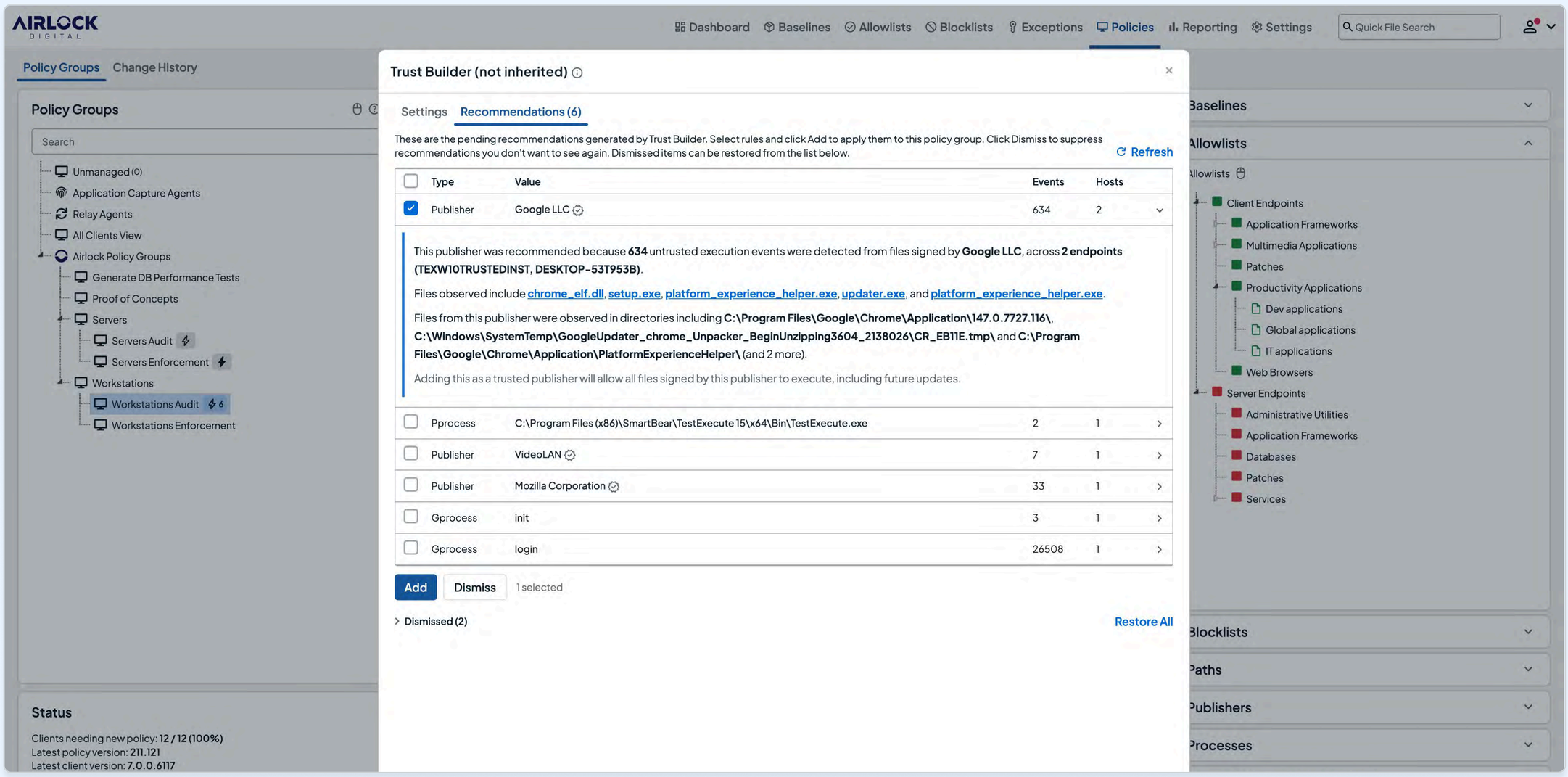
Policy-Based Execution Control

Define and enforce what software is allowed to run using flexible, policy-driven criteria. Trust decisions are based on file attributes, publishers, paths, and execution context. Policies are applied across groups with support for audit and enforcement modes, while Elevation Control enables approved applications to run with privileged access under defined conditions.



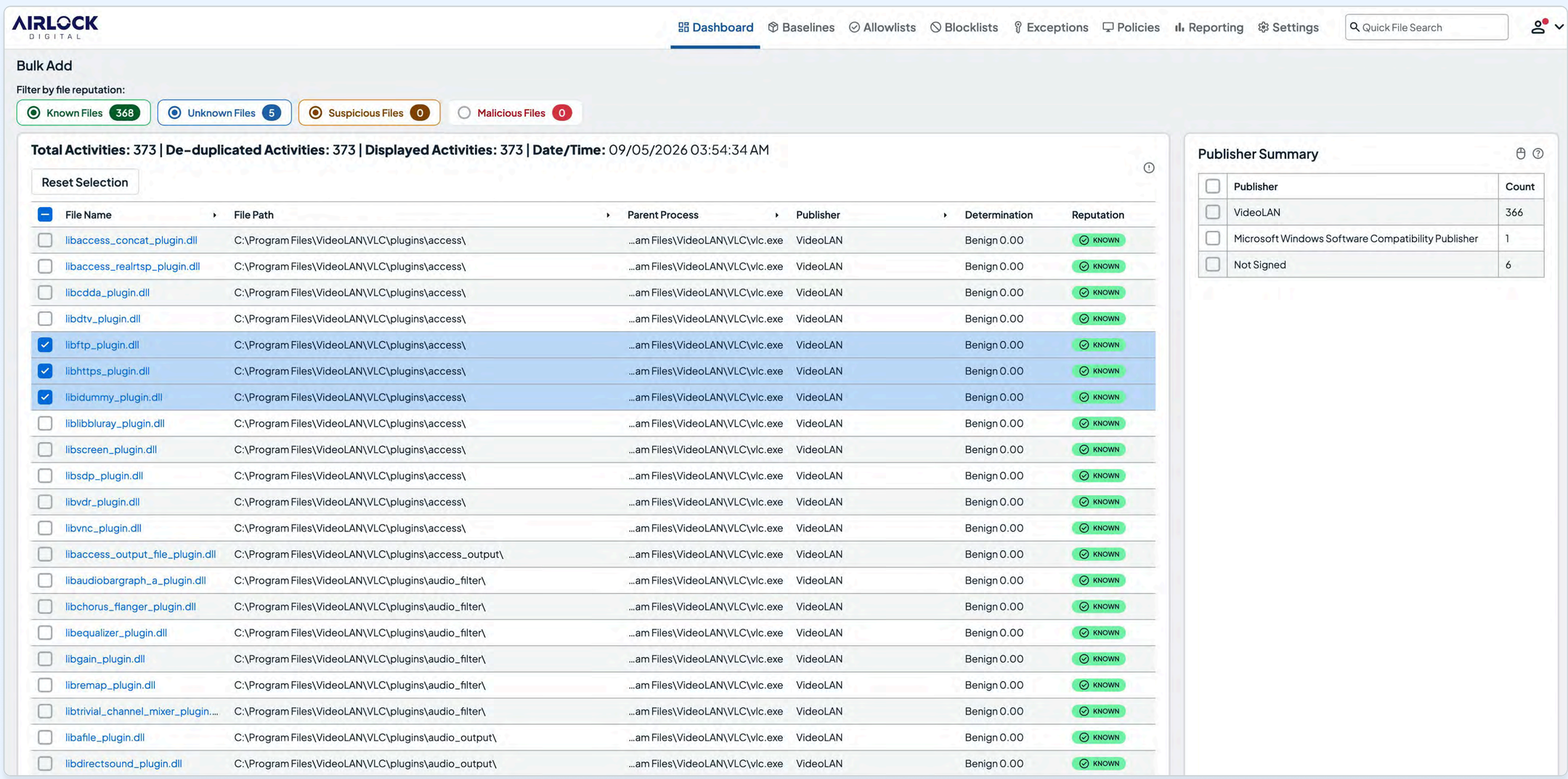
Operational Policy Management

Manage application control as an ongoing operational function. Centralized policies, role-based access, and exception workflows enable efficient management, while Trust Builder recommends or applies decision based on observed execution activity.



Execution Visibility and Validation

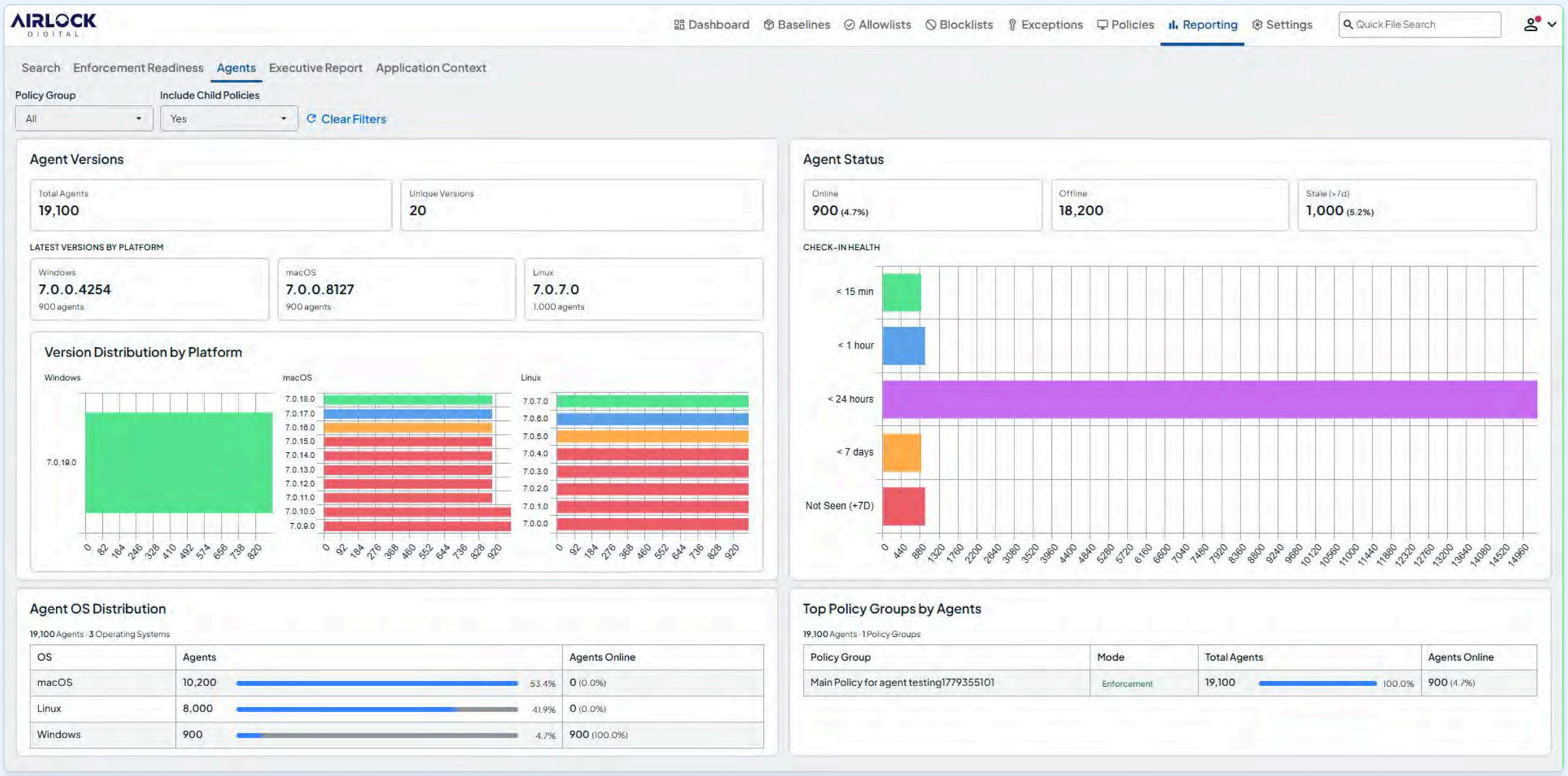
Analyze real execution activity to validate behavior before enforcing policy. Search, reporting and telemetry provide visibility into what is running, while audit and enforcement modes support staged rollout. Application Context groups related components based on execution behavior.



AIRLOCK DIGITAL

Cross-Platform and Distributed Enforcement

Policies are defined centrally and enforced locally, ensuring consistent control regardless of connectivity or environment type.



Supported Environments

Windows™
Desktop & Servers

Linux®
Servers & Workloads

macOS™
Desktop & Endpoints

OT / ICS
OT-Adjacent Environments

Air-Gapped
Disconnected Environments

Remote Endpoints
Mobile & Teleworkers

Distributed Sites
Branch & Edge

Hybrid
Cloud & On-Prem

Built for Security and IT Teams

Endpoint Security Teams

Enforce control over what executes across endpoints. Validate behavior before enforcement, reduce unknown execution, and shift from reactive investigation to proactive control at execution time.

IT Operations Managers

Deploy and manage application control within existing operational workflows. Use staged rollout, centralized policy management, and controlled exceptions to minimize disruption while improving control over software execution.

Airlock Digital: Features & Capabilities at a Glance

Policy-Based Execution Control	Define and enforce trusted execution policies using file attributes, publishers, paths, hashes, parent-child relationships, execution context, and behavioral controls.
Audit-Mode Execution Visibility	Observe and analyze execution activity prior to enforcement, enabling validation of expected behavior and lower-risk policy development.
Executable, Script, and Installer Control	Apply execution policy consistently across executables, scripts, installers, browser extensions, libraries, and software update workflows.
Application-Level Privilege Elevation	Apply administrative-equivalent privileges to approved applications and processes—not users—through policy-defined conditions and metadata-driven controls.
Trust Builder (Policy Automation & Acceleration)	Accelerate policy creation using execution-pattern analysis, trust recommendation workflows, rule consolidation, and policy automation based on observed activity.
Application Context	Build application-level visibility from real execution activity by grouping files, libraries, dependencies, and runtime relationships into recognizable applications.
Execution-Aware Policy Validation	Validate allowlist and blocklist behavior against real execution activity using Contextual Repository data, including rule match visibility and policy decision explanation.
Centralized Policy Workflow and Approval Management	Manage approvals, exceptions, reviews, and policy rollout workflows through centralized administrative processes with audit visibility.
Policy Change Tracking and Auditability	Maintain traceability of policy modifications, trust decisions, administrative actions, and enforcement history for governance and compliance purposes.
Policy-Scoped Access Control	Restrict visibility and management capabilities based on assigned policy scope, enabling enforced operational separation across teams and environments.
Staged Policy Deployment and Enforcement	Transition from monitoring to enforcement using phased deployment models that support operational validation and controlled rollout.
Broad Operating System (OS) Support	Support Windows, Linux, macOS, OT-adjacent, remote, legacy, and distributed environments with centrally managed policies enforced locally.
Offline and Air-Gapped Enforcement	Continue enforcing policy and securing endpoints in disconnected, low-connectivity, and air-gapped environments without dependency on continuous cloud connectivity.
Real-Time Execution Prevention	Prevent unauthorized software, malicious binaries, ransomware, scripts, and high-risk system tools from executing through policy enforcement and deny controls.
Resource-Efficient Endpoint Operation	Minimal impact on endpoint performance, even with high-security settings, making it suitable for both resource-constrained and high-availability environments.
Cloud or On-Premises Deployment	Deploy within cloud-hosted, hybrid, or fully on-premises environments to align with operational, regulatory, and security architecture requirements.
Integration with Security and IT Operations	Integrate with identity, EDR, SIEM/logging, alerting, ITSM/workflow platforms to reinforce a layered security approach and enhance detection capabilities.
Execution Reporting and Alerting	Provide reporting, alerting, and execution telemetry for operational monitoring, policy validation, compliance tracking, and incident response activities.

Discuss Your Application Control Strategy

Work with Airlock Digital to define what runs in your environment, validate enforcement readiness, and implement application control without disruption.

www.airlockdigital.com

AIRLOCK DIGITAL