PLATFORM COMPARISON: IMPAC LABS VS. WIZ

1. INTRODUCTION: THE CONTROL GAP IN CLOUD SECURITY

Cloud security today is no longer only about visibility – its about taking control of your dynamic environment. This is the foundational gap between Wiz and imPAC.

While Cloud Native Application Protection Platforms (CNAPPs) like Wiz offer valuable insights into cloud risks and risk detection, they lack the automation capabilities and controls needed for effective, proactive governance – continuously, at scale, with context.

2. GAPS IN WIZ'S APPROACH

In short, Wiz shows you everything that might be wrong…but without context or correlation, it's hard to know what matters, what's accurate, and what to act on.

- **Wiz evaluates assets in isolation –** imPAC models complete asset chains and relationships (e.g., S3 buckets → IAM roles → encryption keys).
- **Wiz operates on point-in-time snapshots –** imPAC continuously ingests and tracks real-time changes that can be tailored to your scope and frequency.
- **Wiz lacks remediation logic –** imPAC enables automated remediation flows through our Compose module.
- **Wiz cannot ingest external signals for smarter control –** imPAC supports DSPM, vulnerability, and GRC integrations to enrich context.
- **Wiz focuses on detection –** imPAC enforces policy and proves compliance with built-in audit trails that streamline incident investigations and auditor requests.

3. IMPAC LABS IS BUILT FOR CONTROL, NOT JUST DETECTION

imPAC Labs takes a fundamentally different approach to control risk in real time: automate, rather than alert. At our core is a federated automation framework with three pillars:

- Unified Asset Models: Holistic configuration visibility, including depth and relationship context (asset chains technology).
- Common Enforcement Point: Smarter guardrails using Compose applications that can be built tailored to your environments to detect and fix issues.
- Centralized Audit Trail: Continuous compliance evidence generation with Time Machine and Vault ensuring you see who changed what, why, and when.

Customers using imPAC have automated configuration control to:

- Monitor sensitive assets tagged by DSPMs like Varonis and BigID for complete data & cloud security protection.
- Detect and auto-remediate insecure configurations across interconnected assets (e.g., public EC2s using high-risk IAM roles).
- Provide continuous proof of control for audit requirements (NIST, PCI, SOC2).
- Reduce mean time to remediation (MTTR) and maintain strong security posture
- In one case, a customer implemented automated ransomware protections in hours and began reporting posture to their board within a day.

4. WIZ VS. IMPAC: COMPETITIVE COMPARISON

Feature Comparison Matrix

Capability	Wiz	imPAC	Why it Matters
Unified Asset Model	Partial (based on snapshots)	✅ Deep, contextual, and real-time	Understand true posture with full config & asset chain visibility
Policy Enforcement Engine	Detection-focused, manual remediation	✅ Automated, policy-driven guardrails via Compose	Move beyond alert fatigue with real, scalable control
Historical Change Tracking	Basic	✅ Full attribute-level tracking via Time Machine	Track drift, investigate incidents, and support audits effortlessly

Capability	Wiz	imPAC	Why it Matters
Contextual Risk Prioritization	Limited to static rules and snapshots	✅ Dynamic, context-aware enforcement using asset metadata & relationships	Prioritize what actually matters with real-world context
Federated Signal Integration	Fragmented integrations, manual effort	✅ Federated signal ingestion with Connect (DSPM, CNAPP, IAM, etc.)	Use insights from your stack to drive smarter enforcement & confluence
Audit Readiness	Report-based, limited historical proof	✅ Centralized, non-tamperable audit trail via Vault	Simplify and accelerate audits with continuous, verified evidence
Remediation Workflows	Requires manual ticketing (e.g., Jira), limited automation	✅ No-code Compose apps automate enforcement and remediation	Reduce MTTR and reliance on manual triage/ticketing systems
Noise & False Positives	High alert volume, limited tuning	✅ Context and confluence reduce false positives and prioritize real risk	Focus your team to prioritize what actually reduces risk

5. CUSTOMER VALUE COMPARISON

Value Driver	Wiz	imPAC
Alert Triage & Dashboarding	✅	✅
Real-Time Prevention	❌	✅
Unified View of Config Risk	⚠ (surface-level)	✅
Customization & Flexibility	⚠ (limited tuning)	✅ Fully composable policy engine
Audit Automation	⚠	✅ Continuous and automated
Cost & Efficiency Optimization	⚠ (alert mgmt focus)	✅ Faster fixes, fewer people, smarter prioritization