



IMPAC + DSPM = COMPLETE DATA & CLOUD SECURITY

imPAC provides critical cloud configuration context and controls that integrate with data security platforms. Together, customers benefit from a unified approach to security that protects your most sensitive data from the inside out.

I CUSTOMER OUTCOMES:

🏠 Stop Data Breaches

- **DSPM** identifies and classifies sensitive data to stop threats across environments
- **imPAC** reveals how cloud configurations protect specific data within cloud assets
- **Result:** Complete visibility from data to infrastructure eliminates blind spots that attackers exploit

⚠️ Be Proactive Against Risks

- **DSPM** detects potential data exposure and access risks in real time
- **imPAC** prevents cloud misconfigurations through tailored policy automation
- **Together:** Stop threats before they happen by understanding data sensitivity and cloud context

🔍 Achieve Compliance Efficiently

- **DSPM** tracks data compliance and generates automated reports
- **imPAC** provides cloud configuration evidence and detailed change history
- **Result:** Continuous compliance across data and infrastructure, reducing audit prep to minutes

🔗 Unified, Scalable Security Operations

- **DSPM** monitors data access and user behavior patterns throughout databases
- **imPAC** tracks cloud configuration changes with Time Machine illustrating who changed what and when
- **Result:** Manage incidents from a centralized interface, ensuring efficient and scalable administration

I OVERALL INTEGRATION BENEFITS

- Single pane for cloud posture & sensitive data across multiple environments and providers
- Automated and self-serve policy enforcement across data classification and infrastructure
- End-to-end audit trail with full config history and data activity logs
- Real-time risk detection with complete context

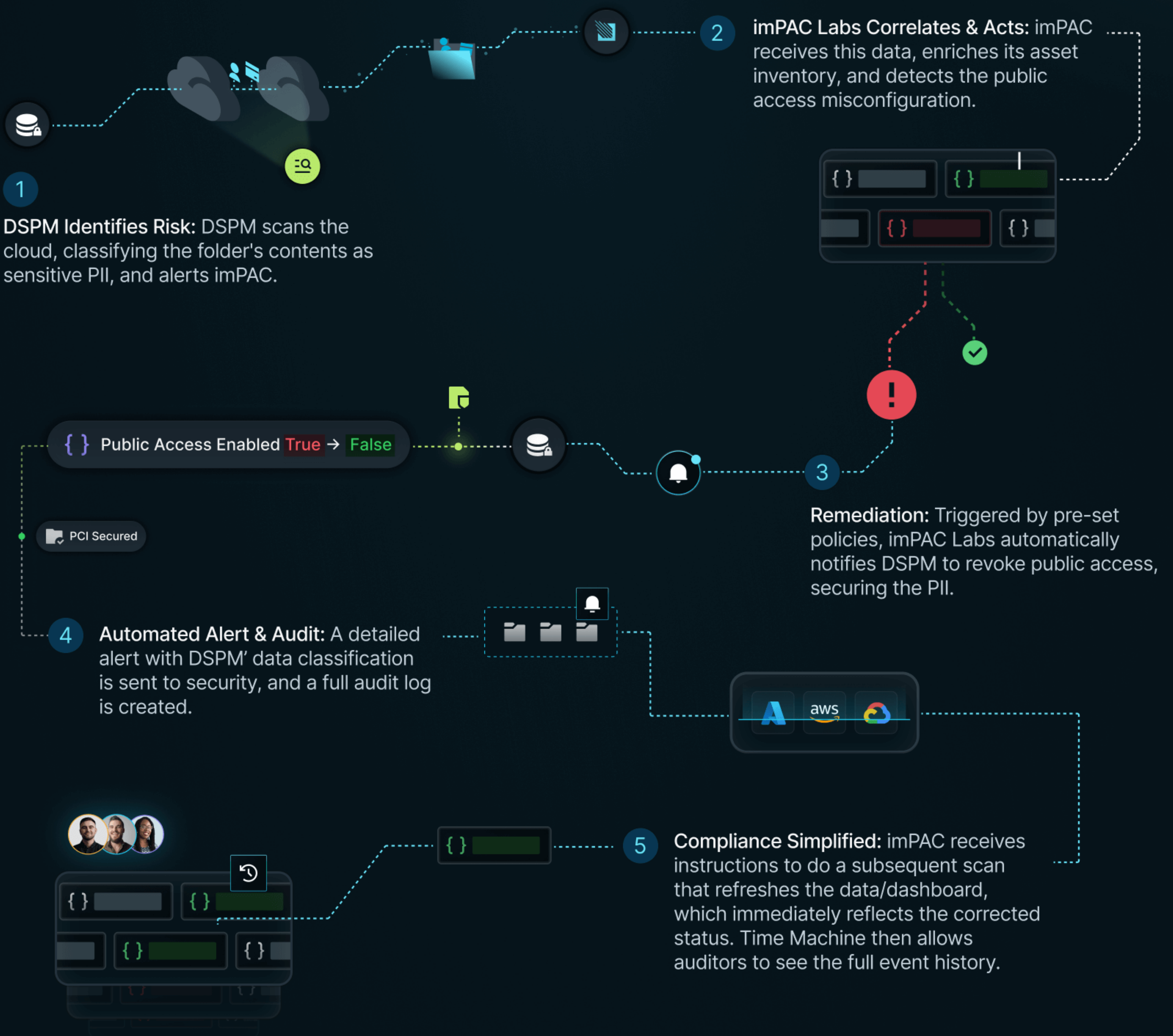




IMPAC + DSPM IN ACTION: AUTOMATED PII PROTECTION

Imagine a shared cloud folder holding sensitive customer PII. A configuration error could make this information publicly accessible, resulting in a compliance nightmare. But by integrating DSPM capabilities with imPAC, you're always protected end to end.

HERE'S HOW IT WORKS



THE RESULT?

Sensitive data is secured instantly, compliance is maintained, and security teams are freed from manual intervention. This is the power of imPAC Labs working seamlessly with a DSPM: automated security and compliance control with audit-ready evidence.

CONTINUOUS CLOUD SECURITY & COMPLIANCE

imPAC Labs delivers comprehensive cloud security through AI that maps every cloud asset, tracks every configuration change, and orchestrates tailored cloud defenses

CORE PLATFORM CAPABILITIES



SEE IT: UNLOCK UNMATCHED VISIBILITY

- Gain comprehensive insight into AWS, Azure, and GCP environments via read-only [agentless] access
- Access high-fidelity asset data with built-in risk scoring and AI-anomaly detection to reveal critical resources
- Check critical resource relationships via **Asset Chains** (e.g., AWS S3 buckets → IAM roles → encryption keys)



FIX IT: AUTOMATE SECURITY CONTROLS

- Create custom dashboards to validate your environment (e.g., check against compliance frameworks like PCI)
- Automate security processes by building natural language policies that can be deployed in minutes
- Cut through alert fatigue and false positives with targeted controls tailored to your business and context

Runs	Added	Removed	Modified
3	+ 98	- 186	114
+ Added			
- Removed			
Modified			
	astro-archive-vault	S3 Bucket	2 Changes
	nebula-vault-storage	EC2 Security Group	2 Changes
	galactic-repository	IAM User	2 Changes
	astro-archive-vault	Provider	1 Changes
	Nova-Entitled-Vault	S3 Bucket	2 Changes
	orion-repository	KMS	2 Changes
	stellar-storage-hub	Lambda	3 Changes

PROVE IT: DEMONSTRATE YOUR SECURITY POSTURE

- Maintain complete configuration history, track all asset changes, and compare cloud states with **Time Machine**
- Verify cloud asset security and ensure continuous compliance posture with self-evidencing logs
- Eliminate manual processes and streamline audits with automated evidence collection

BUSINESS IMPACT

⌘ Hours not months

- Map full cloud asset inventory in under 1 hour
- Leverage pre-built controls from day one
- Avoid complex integrations and engineering

🔔 Do more with less

- Consolidate multiple point solutions into one platform
- Break down org silos with a unified security view
- Scale security operations without adding headcount

🛡️ Move beyond compliance

- Build a strong, proactive security foundation
- Understand asset relationships to protect your entire cloud
- Catch misconfigurations before they become breaches