# DSPM CONTEXT MEETS CLOUD CONTROL WITH VARONIS + IMPAC

### Sensitive Data Aware. Policy Enforced.

Bring data classification and context from Varonis directly into your cloud configuration control plane, turning visibility into action.

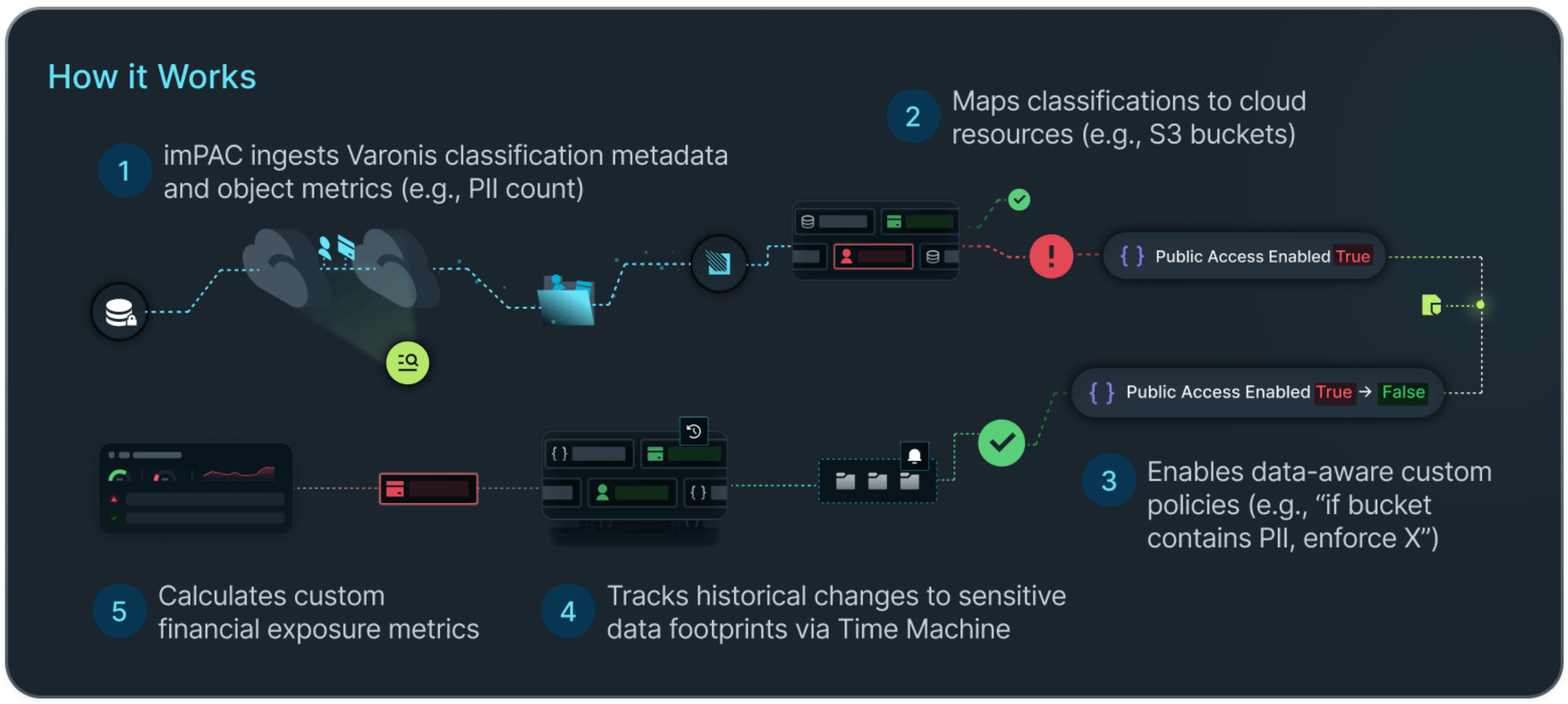
By ingesting Varonis tags (like PII and financial data sensitivity) and object-level metadata, imPAC enriches your cloud asset model with deep **data awareness** and makes it instantly actionable via **policy-based controls.** Teams can now detect, govern, and prove security for sensitive data across cloud environments without relying on disjointed tools.

### See the data. Understand the risk. Enforce the control.

When a bucket contains PII or financial records, imPAC helps you automatically enforce encryption, backup, and access control policies. No guesswork required.

### Context from Varonis includes:

- PII classification, object count, and sensitivity tags
- PII frequency per asset and other similar metrics
- Audit timelines for sensitive data growth or cleanup




### Business Impact

**Data insight into policy:** Enforce encryption, backups, tagging, and isolation.

**Enforce data residency:** Ensure PII and financial data live in approved regions only.

**Track change over time:** Visualize when sensitive data appeared or was removed.

**Quantify risk:** Custom exposure formulas provide board-ready insights.