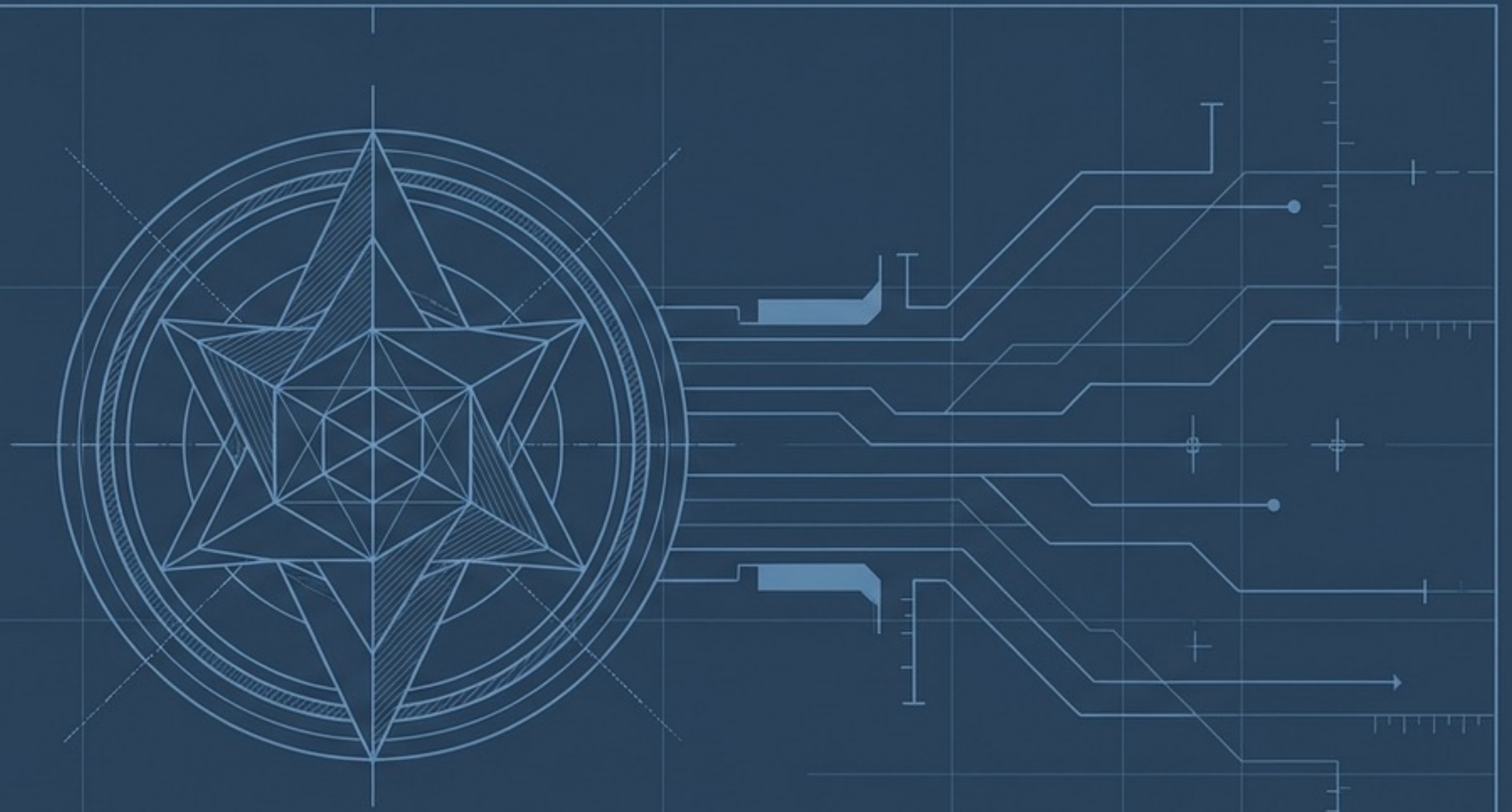


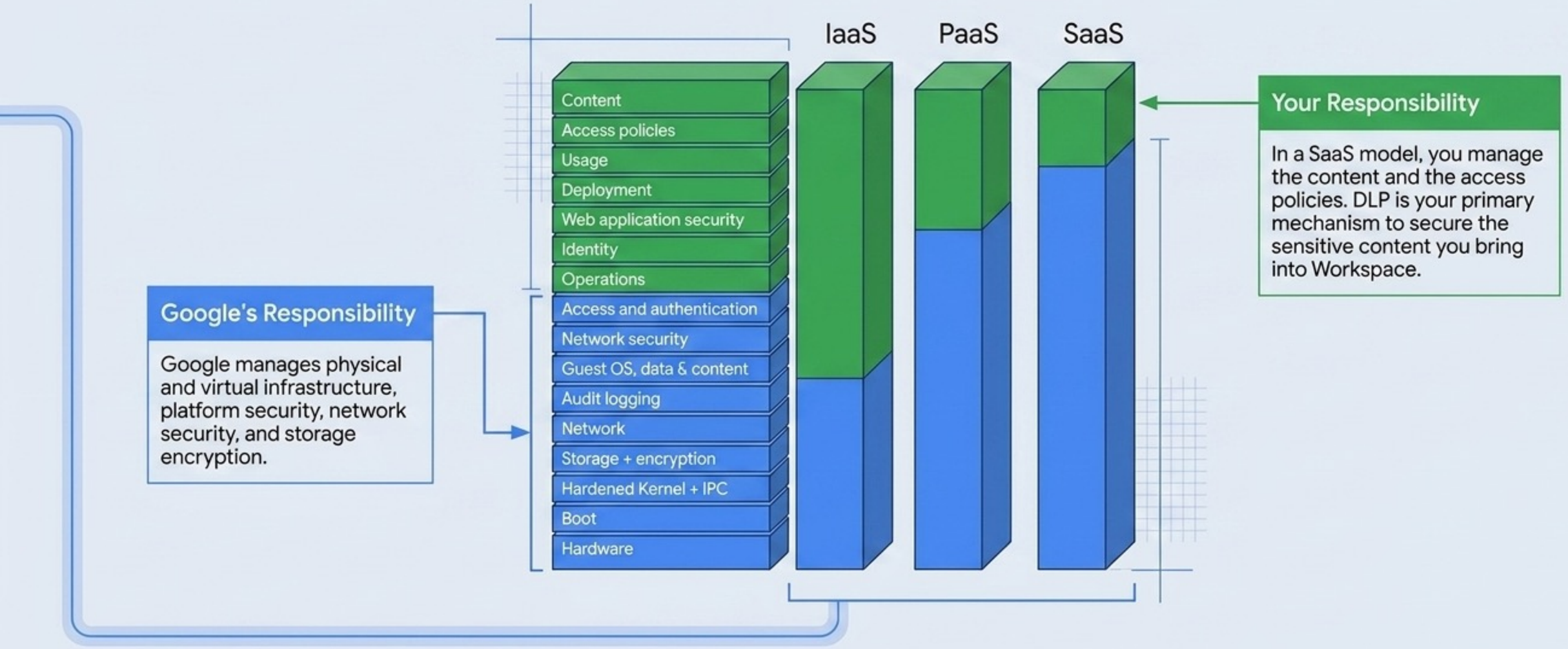
Google Workspace DLP Implementation Blueprint

A strategic flowchart for planning, deploying, and actioning Data Loss Prevention.

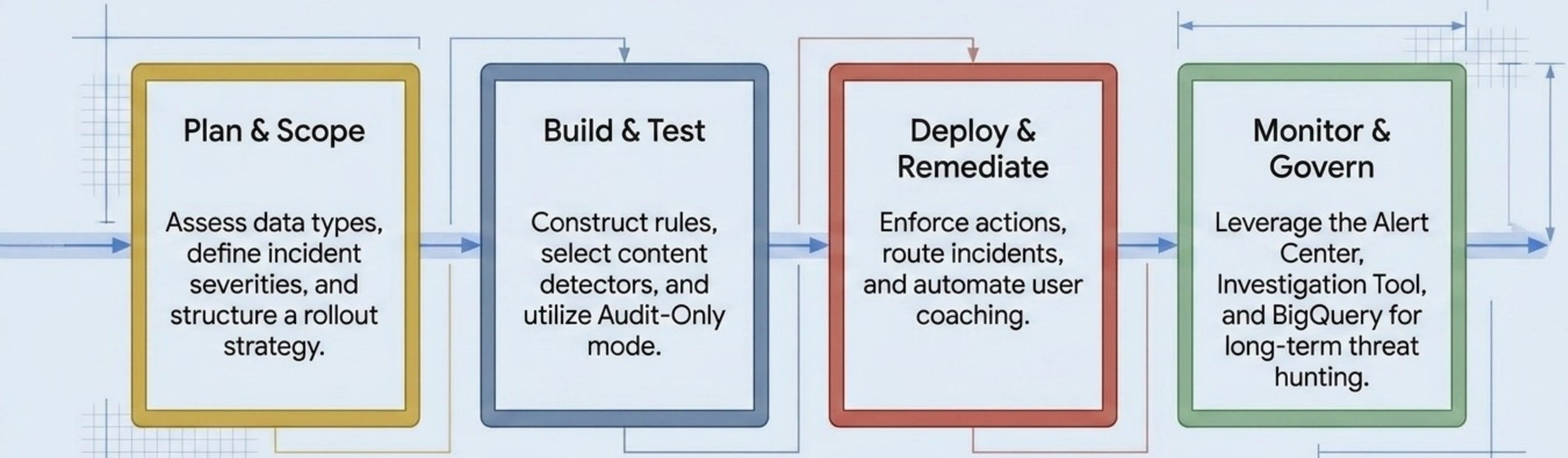
Designed for Workspace Enterprise Standard & Plus

SecOps Playbook

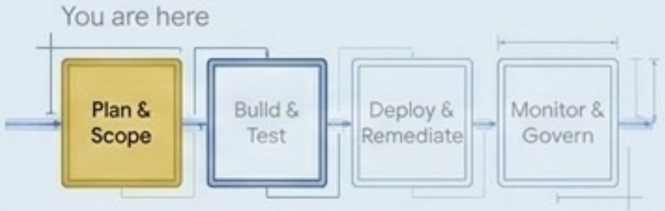
The Foundation: Shared Responsibility



The Phased Implementation Lifecycle



Phase 1: Strategic Prerequisites



Identify Datasets

What needs scanning? Target specific data types like PII, Financials, Intellectual Property, or custom internal code.

Define Severity

What dictates a low vs. high severity incident? Establish the baseline for your organizational response.

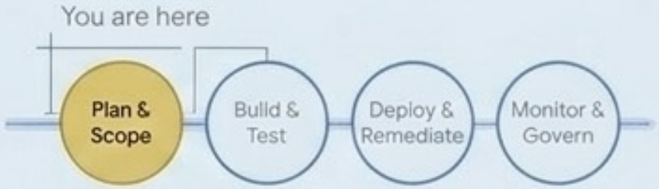
Determine Scope

Which Organizational Units (OUs) or Groups need these rules? (Avoid sweeping domain-wide rules initially).

Review Templates

Can existing Workspace templates cover the requirement? Evaluate pre-built frameworks before building from scratch.

Phase 1: The Phased Rollout Strategy



Step 1: IT & Security Only

Apply rules to a micro-group (e.g., SecOps). Ensure triggers fire correctly and logs populate as expected.

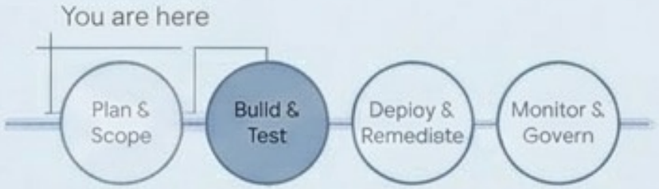
Step 2: Early Adopters (5-10%)

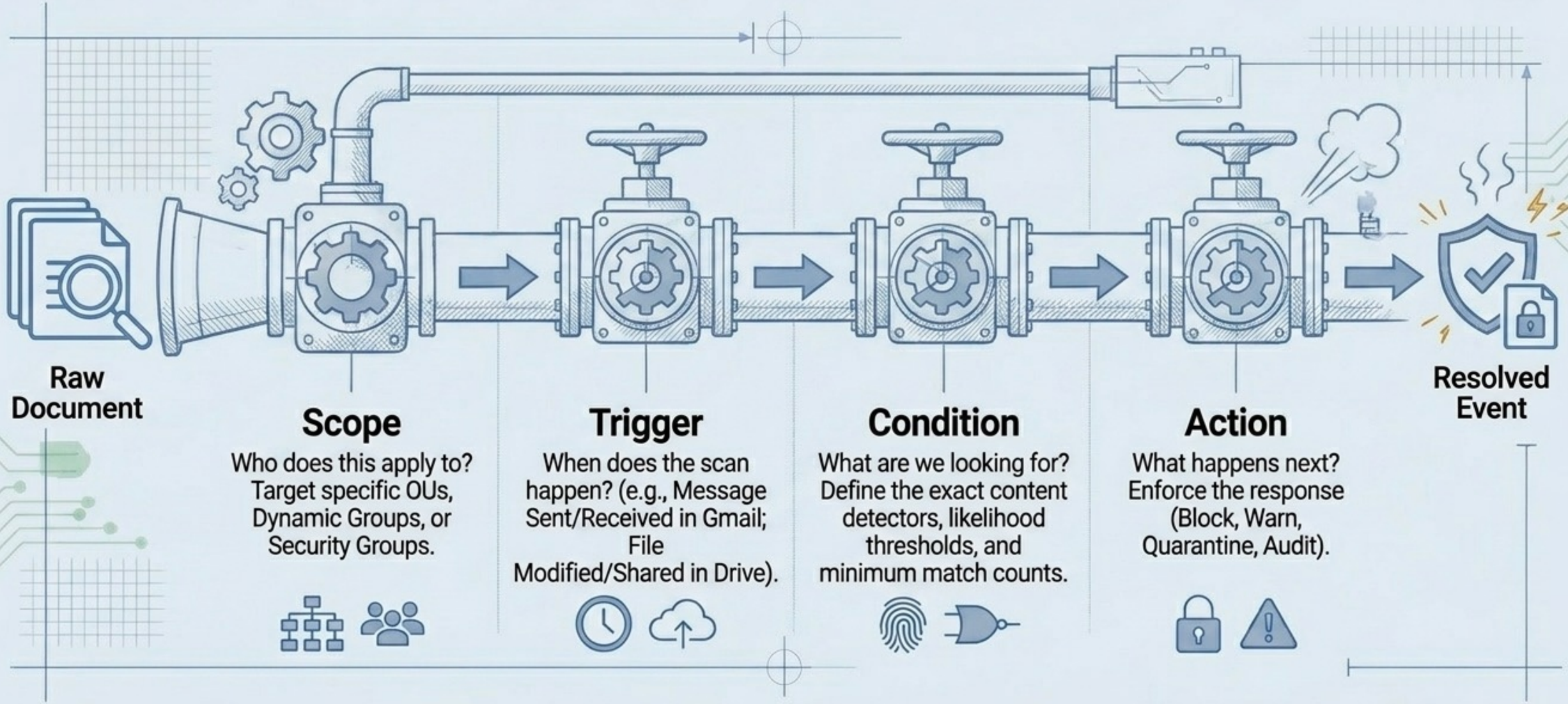
Deploy to a specific department or dynamic group. Gather feedback on daily workflow interruptions and false positive rates.

Step 3: Full Production

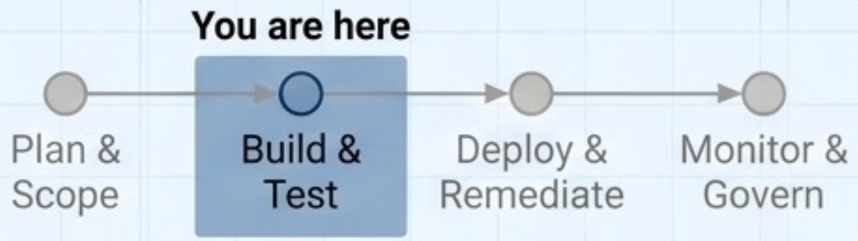
Roll out to target OUs. Live enforcement is active, and the incident remediation plan is fully operational.

Phase 2: Anatomy of a DLP Rule





Phase 2: Defining Conditions: Content Detectors



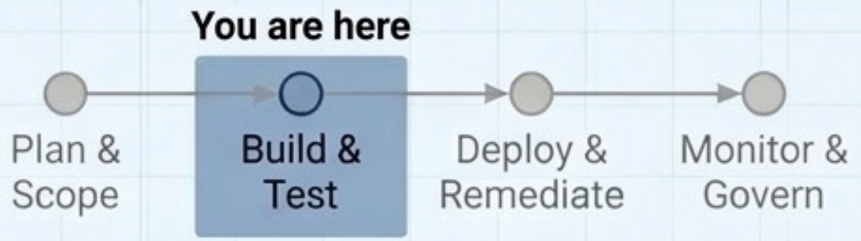
Predefined Classifiers

- **Mechanism**: Google's pre-trained machine learning models.
- **Capabilities:** Automatically detects 40+ global data types including SEC filings, tax forms, passports, and global VINs.
- **Trade-off:** Zero setup required, but cannot detect internal company jargon.

Custom Detectors

- **Mechanism:** Regex and Wordlists.
- **Capabilities:** Highly specific matching (e.g., internal "Project X" codenames, custom employee ID formats).
- **Trade-off:** Requires manual creation, exact matching parameters, and ongoing maintenance.

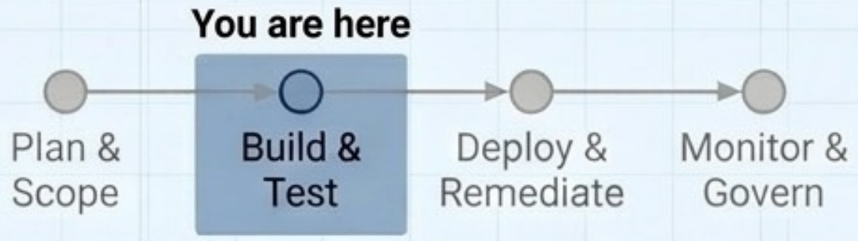
Phase 2: App-Specific Enforcement Actions



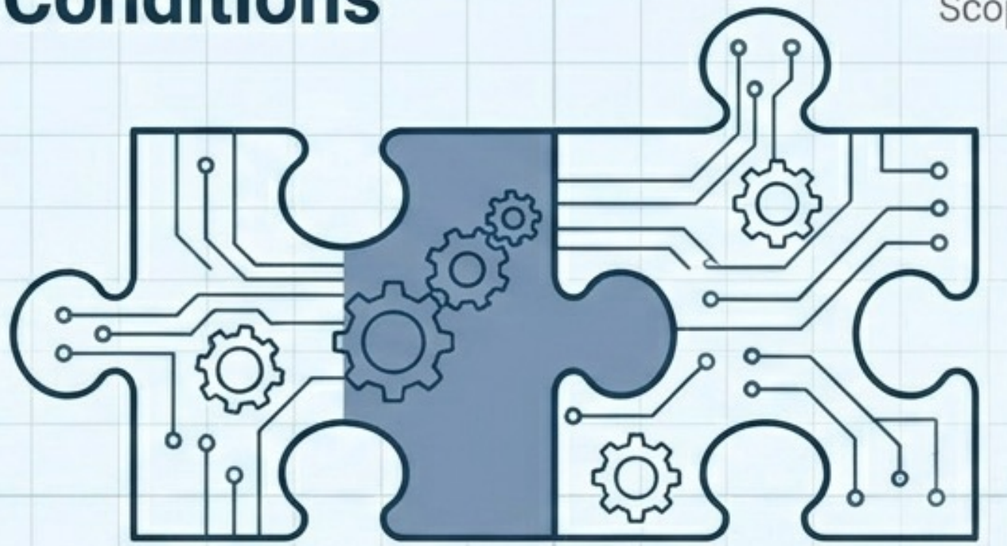
- Quarantine message for admin review.
- Reject message from being sent.
- Modify message (automatically append classification labels or notes).
- Deliver with a prominent warning.

- Disable download, print, and copy for viewers/commenters.
- Block external sharing completely.
- Warn users before sharing sensitive files.

Phase 2: Advanced Logic: Context-Aware Conditions



Content
(DLP Engine)



Context
(Access Controls)

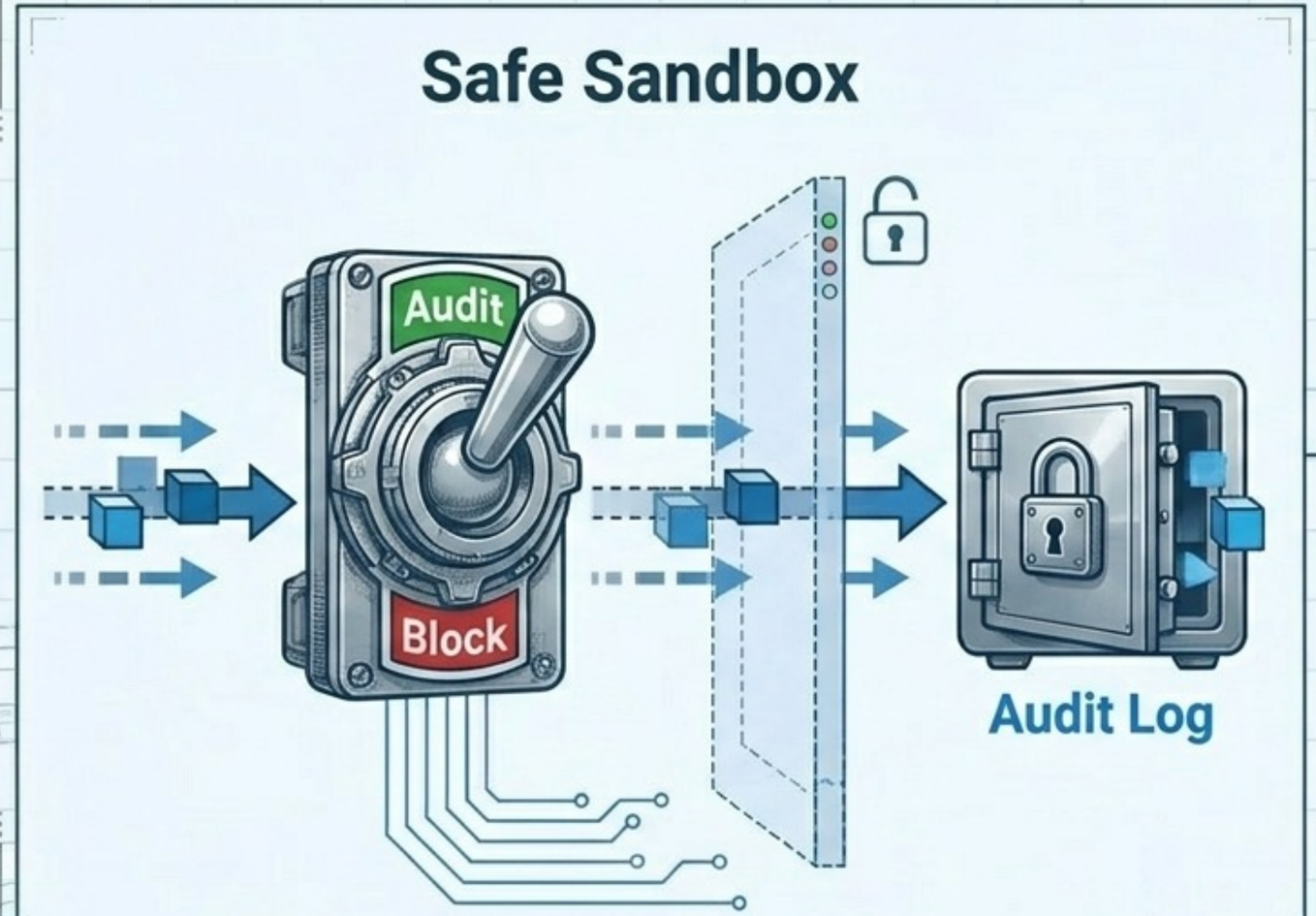
- **The Concept:** Combine **What the data is** with **How it is being accessed**.
- **The Mechanism:** DLP rules can be configured to execute only when specific Context-Aware Access (CAA) attributes are met.

Example Policy:
Block the download of a Drive document containing financial data ONLY IF the user is attempting access from an unauthorized mobile OS (iOS/Android) or from outside the corporate IP range.

Phase 2: The Audit-Only Testing Imperative

You are here

Plan & Scope → **Build & Test** → Deploy & Remediate → Monitor & Govern



The Standard: Always deploy new or modified rules in Audit-only mode first.

The Rationale: This evaluates potential business impact and identifies false-positive rates without blocking legitimate user workflows.

Next Steps: Route these audit logs to the Security Investigation Tool for baseline review before flipping the switch to live enforcement.

Phase 3: Incident Response Matrix

Incoming DLP Alert

Severity?

Low Severity

1. Audit file/email
2. T/F Classify as true/false positive
3. Send automated coaching email to user
4. Monitor for recurrence

High Severity

1. Trigger Alert Center
2. Immediately revoke file access via Investigation Tool
3. Escalate to SecOps team
4. Audit user permissions & isolate account

Phase 3: Setting User Expectations

You are here

Plan & Scope — Build & Test — **Deploy & Remediate** — Monitor & Govern

The Strategy: Automated remediation relies on end-user education. Turn blocks into coaching moments.

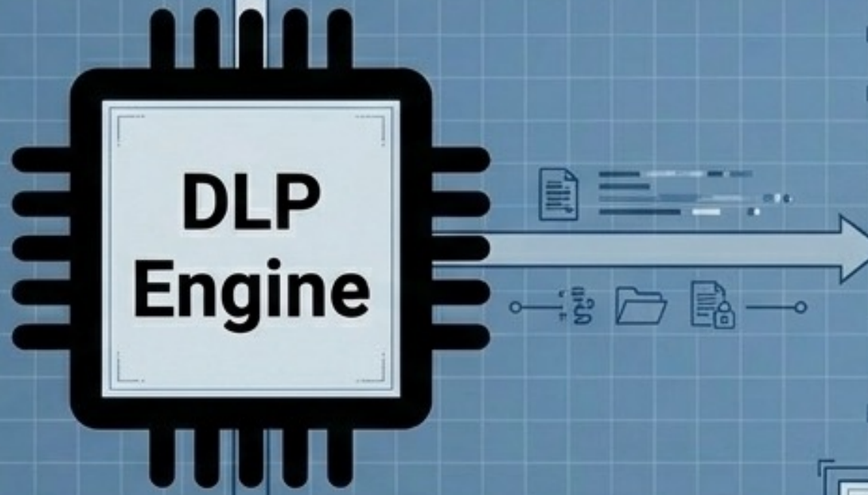
The Execution: Utilize custom remediation messages to explain exactly why a specific action was intercepted.

The Outcome: Significantly reduces IT helpdesk tickets regarding blocked sharing attempts.

Phase 4: The Security Monitoring Ecosystem

You are here

Plan & Scope — Build & Test — **Deploy & Remediate** — Monitor & Govern



Alert Center

Built for high-level summaries and immediate administrative notifications of high-severity rule breaches.

Investigation Tool

Built for granular auditing, querying Rule Log Events, viewing sensitive content snippets, and executing bulk-action file permission revocations.

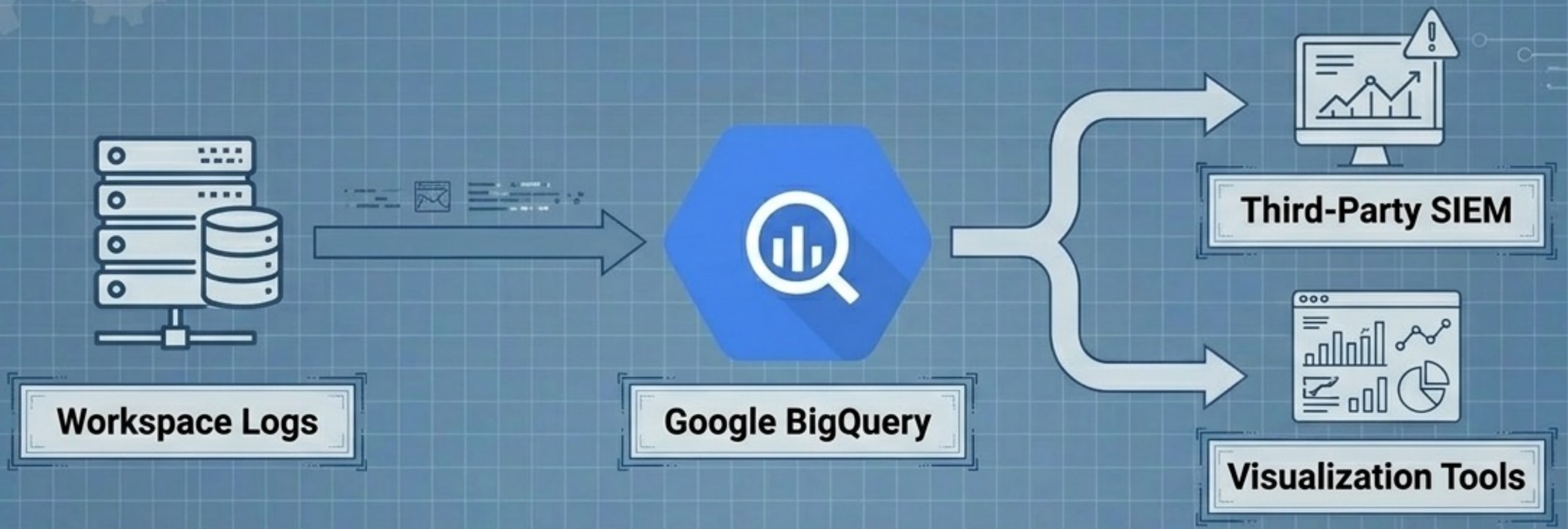
Data Protection Insights

Built for macro-level dashboards showing external file-sharing footprints and proactive recommendations for new rules.

Phase 4: Advanced Telemetry & Log Exporting

You are here

Plan & Scope — Build & Test — **Deploy & Remediate** — Monitor & Govern

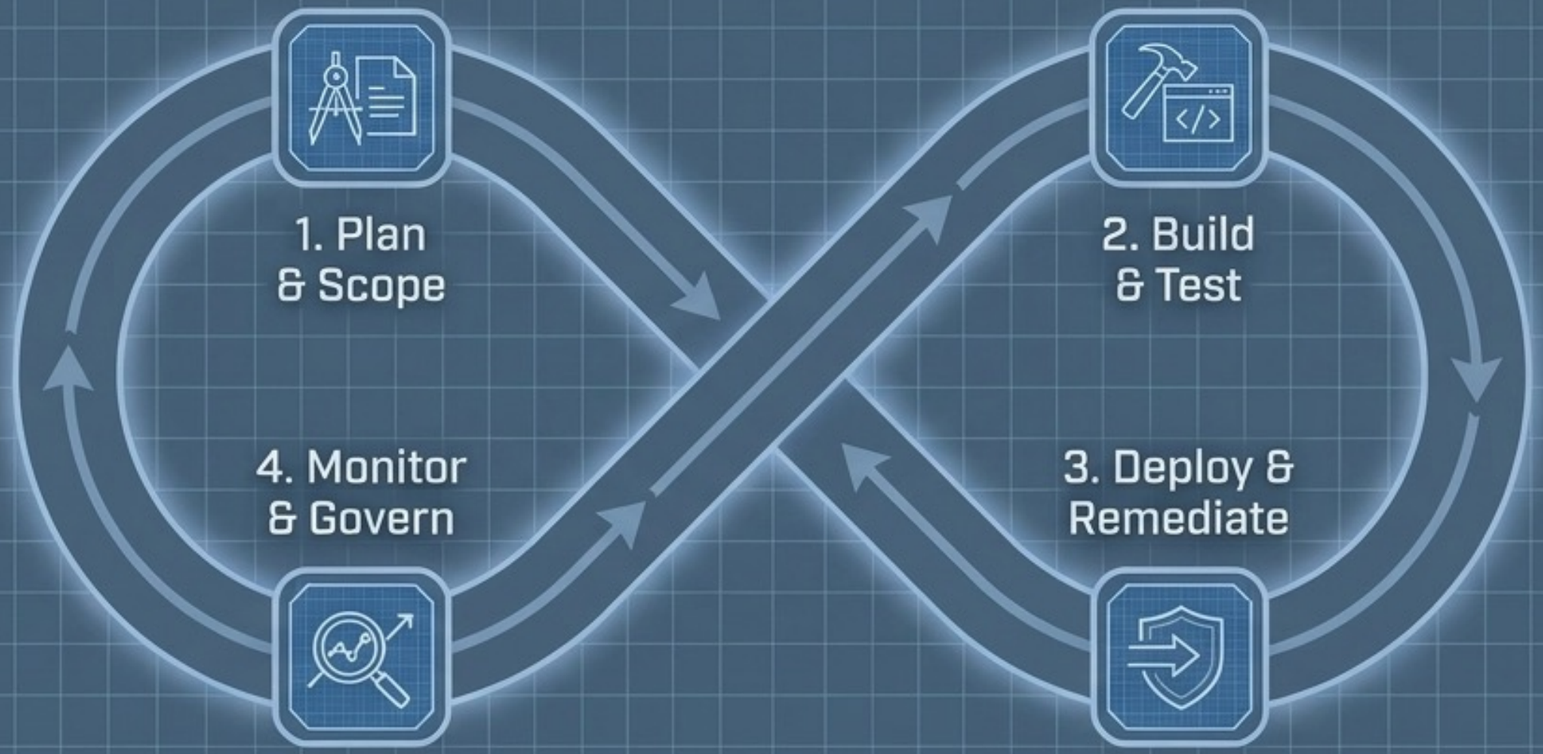


The Challenge: Native Workspace tools retain logs for a limited time and isolate data from organizational SIEMs.

The Solution: Configure automated service log exports directly to Google BigQuery.

The Capability: Enables custom SQL querying of Rule Log Events, long-term data retention, and seamless integration with external security tools.

Synthesis: The DLP Governance Cycle



Synthesis

Data Loss Prevention is not a set-and-forget toggle switch; it is a living operational ecosystem.

Ongoing Operations

Sustained security requires continuous governance—reviewing false positive rates, updating custom wordlists, and auditing organizational scope.

Action

Access the Security Center today to run your baseline Data Protection Insight report.