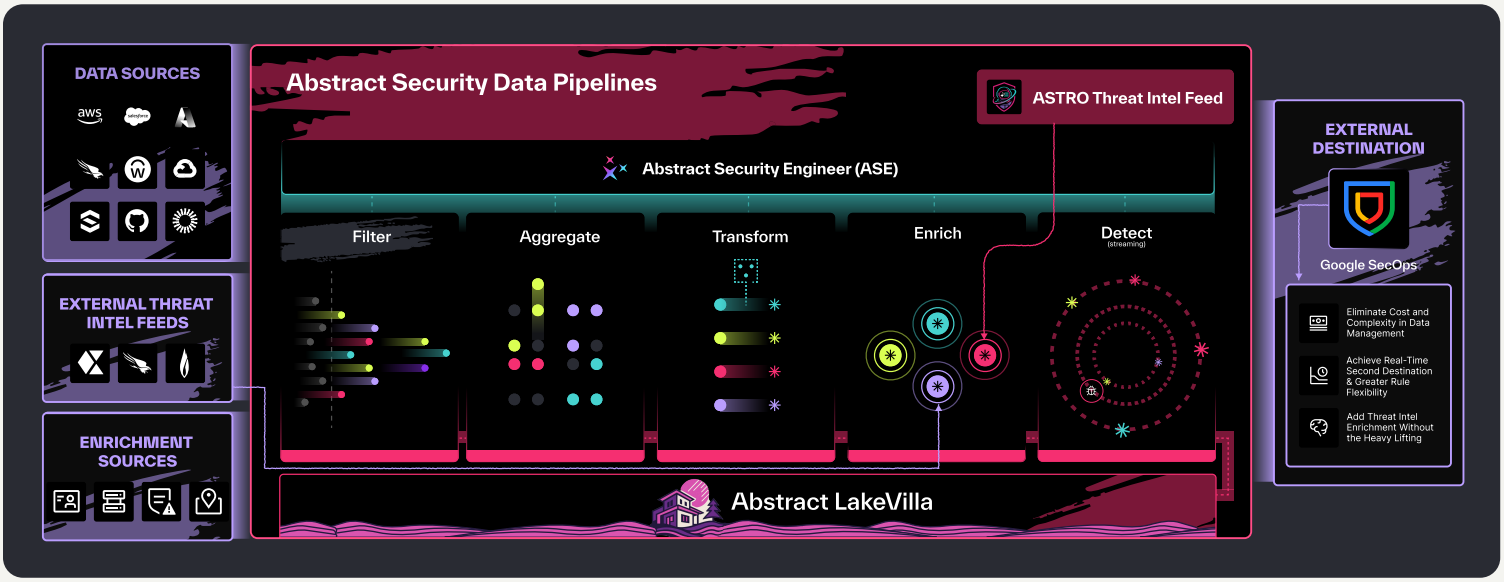
abstract security

Abstract + Google SecOps: Better Together

Google SecOps delivers scalable visibility and analytics across Google Cloud and endpoints, backed by curated threat intelligence and tight integration with the broader Google ecosystem. Abstract Security builds on this strength by simplifying SaaS and cross-cloud ingestion, reducing data management costs, and adding real-time, identity-aware detections. **The result is faster insights, broader coverage, and lower overhead for teams that rely on Google SecOps.**



Top 3 Reasons To Use Abstract With Google SecOps

01. Easier Data Onboarding Across the Modern Stack

- **Google SecOps** centralizes endpoint and cloud telemetry at scale.
- **Abstract** extends this by connecting SaaS and identity sources through API-native integrations with built-in reliability.
- **Together:** Security teams onboard diverse data sources quickly, without custom pipelines or manual upkeep.

02. Faster, More Flexible Detections

- **Google SecOps** provides real-time analytics for single-event rules across cloud and endpoint data.
- **Abstract** enables multi-event, cross-cloud, and identity-aware detections with sub-second latency.
- **Together:** Teams respond to threats earlier with broader, more flexible detection logic.

03. Richer Threat Context for Investigation

- **Google SecOps** delivers curated intelligence from VirusTotal, Mandiant, and OSINT feeds.
- **Abstract** complements this with real-time enrichment from additional third-party sources like Flashpoint and Recorded Future.
- **Together:** Analysts investigate faster with more complete context, reducing mean time to respond.

Building on Google SecOps with Abstract Security

Capability	Google SecOps	Abstract Security
Data Management Complexity	Ingests endpoint and cloud telemetry via HTTP, Syslog, and BindPlane agents.	Simplifies onboarding with SaaS-native API integrations and no-code pipelines that reduce setup and management overhead.
Ingestion Reliability	Provides reliable ingestion through BindPlane and agents.	Strengthens reliability with built-in checkpointing and automated retry controls, ensuring consistent, lossless delivery.
Cost Reduction in Data Volume	Stores full data volumes for analysis and compliance.	Reduces data volumes by up to 80% before ingestion and provides optional cost-efficient long-term retention, lowering spend without sacrificing visibility.
Detection Rule Capacity	Supports detection rules with defined thresholds per account and per rule.	Adds streaming support for both single- and multi-event rules with sub-second latency, accelerating response to complex threats.
Real-time Detection Latency	Enables real-time detection for single-event rules across cloud and endpoint data.	Supports real-time streaming for both single and multi-event rules with sub-second latency, enabling faster, more complex detection in real-time.
Detection Logic Complexity & Speed	Runs streamlined detection logic across Google Cloud and endpoint sources.	Expands flexibility with identity-aware, cross-cloud correlation logic in real time, surfacing sophisticated threats earlier.
Threat Intel Enrichment	Provides curated intel from VirusTotal, Mandiant, and OSINT feeds.	Complements this with real-time enrichment from additional third-party sources like Flashpoint and Recorded Future, applied in-stream without added overhead.

Ideal Use Case:

Google SecOps is ideal for organizations seeking scalable visibility and analytics across Google Cloud and endpoint environments, with curated threat intelligence and strong ecosystem integration. Abstract Security complements this by adding seamless SaaS and identity ingestion, in-stream cost optimization, and real-time, identity-aware detections. Together, they deliver broader coverage, lower overhead, and faster insights without disrupting existing workflows.

Simplified Data Ingestion Framework

- Google SecOps ingests endpoint and cloud telemetry through HTTP, Syslog, and BindPlane agents, providing strong coverage across Google-native environments. Abstract Security enhances this by adding SaaS- and identity-native API integrations with built-in reliability, eliminating custom scripts and simplifying onboarding across diverse sources.

Efficient Data Volume Management

- Google SecOps stores ingested data in full fidelity for analysis, compliance, and investigations. Abstract Security complements this by reducing volumes by up to 80% before ingestion and providing optional cost-efficient retention. Teams maintain complete visibility while lowering storage and processing costs.

Expanded Detection Capacity and Flexibility

- Google SecOps supports real-time analytics for single-event rules across cloud and endpoint data. Abstract Security extends this with unlimited rule capacity and multi-event, cross-cloud, and identity-aware streaming detections. This combination helps teams scale detections broadly while catching complex threats earlier.

Real-Time Detection Capabilities

- Google SecOps processes single-event rules in real time to support fast response. Abstract Security complements this with streaming detections for both single- and multi-event logic at sub-second latency. Together, teams reduce time-to-detection from minutes to seconds.

Integrated Threat Intelligence Enrichment

- Google SecOps provides curated threat intelligence through sources like VirusTotal, Mandiant, and OSINT. Abstract Security enriches telemetry in-stream with additional feeds such as Flashpoint and Recorded Future. This layered approach ensures investigations include broader context without added manual effort.