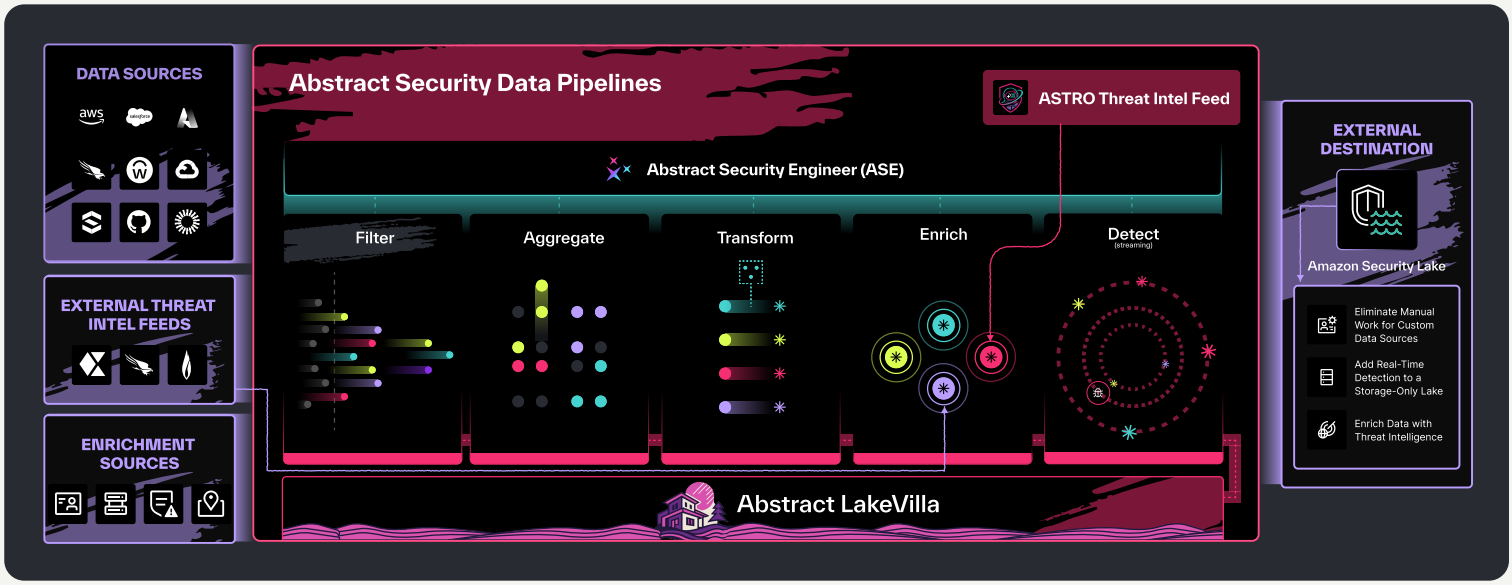
abstract security

Abstract + AWS Security Lake: Better Together

Centralizing security data at scale requires durability, standardization, and analytics flexibility—exactly what AWS Security Lake provides. Abstract Security builds on that strength with no-code onboarding, real-time detections, and in-stream enrichment, helping teams cut noise and surface insights instantly. **Together they create a seamless "collect, detect, retain" cycle that simplifies operations, controls costs, and accelerates time-to-value.**



Top 3 Reasons to Use Abstract Security with AWS Security Lake

01. Simplify Data Onboarding

- **AWS Security Lake** ingests data from across accounts, services, and custom sources in OCSF format.
- **Abstract** makes this even easier with prebuilt, no-code SaaS, Syslog, and API integrations that automatically transform and route data.
- **Together:** Teams connect data sources in minutes, not weeks, without managing custom pipelines or folder structures.

02. Accelerate Detection and Response

- **AWS Security Lake** centralizes and stores high-fidelity security data for analysis, compliance, and long-term value.
- **Abstract** adds real-time streaming detections at the edge, before data lands in the lake.
- **Together:** Security teams detect and act on threats in seconds, while Security Lake retains both enriched and raw data for deep investigation.

03. Enrich Data with Threat Intelligence

- **AWS Security Lake** standardizes data for consistent analysis across AWS and partner services.
- **Abstract** enriches that data in motion by applying third-party threat intelligence feeds and context.
- **Together:** Analysts investigate faster and more accurately with enriched insights stored directly in Security Lake.

Building on AWS Security Lake with Abstract Security

Capability	AWS Security Lake	Abstract Security
Data Collection	Flexible pipelines for bringing in data in OCSF format	Simplified onboarding with no-code SaaS, API, and Syslog integrations that automatically transform and route data
Data Normalization	Standardizes ingested data to OCSF for consistent analytics	Normalizes before ingestion, ensuring clean, structured data flows directly into Security Lake
Detection Engine	Centralized storage and analytics for downstream detection tools	Adds real-time, streaming detection at the edge with thousands of pre-built rules, delivering alerts in seconds while Security Lake retains full context for investigation
Threat Intelligence	Supports integration with downstream analytics and enrichment services	Enriches streaming data in-line with third-party threat feeds, storing enriched events in Security Lake for faster investigations
Cost Efficiency	Provides scalable, durable storage of high-fidelity data	Reduces data volumes by up to 80% before ingestion, giving teams flexibility to retain critical data in Security Lake while routing less urgent data to cost-efficient storage options

Ideal Use Case:

Built for scale, AWS Security Lake centralizes security data in a standardized format and connects seamlessly with a broad analytics ecosystem. Abstract Security builds on that foundation with no-code onboarding, real-time detections, and in-stream enrichment—helping teams move faster from collection to action.

Simplified Data Ingestion Framework

- AWS Security Lake provides a flexible framework for ingesting security data in the OCSF standard, giving organizations the freedom to build custom pipelines that fit their environment. This ensures consistency and interoperability across analytics and security tools.

  Abstract Security complements this flexibility with prebuilt, no-code SaaS, HTTP, Syslog, and API integrations that automatically convert logs into OCSF and route them into Security Lake. Teams can quickly connect diverse data sources without building or maintaining custom ingestion pipelines, accelerating time-to-value and reducing operational overhead.

  Together, Security Lake and Abstract let organizations choose the best approach: custom pipelines where they need control, and out-of-the-box integrations where they want speed and simplicity.

Real Time and Flexible Detections

- AWS Security Lake provides a centralized, standardized data store that integrates with a broad ecosystem of analytics and detection tools. This makes it an excellent foundation for custom detection pipelines or partner-driven solutions.

  Abstract Security extends this by adding a built-in, real-time detection engine that processes data as it streams in. With thousands of prebuilt rules and support for complex, multi-event logic, Abstract delivers sub-second detections while Security Lake retains the enriched and raw data for long-term analytics, auditing, and compliance.

  Together, AWS Security Lake and Abstract Security combine breadth and immediacy: scalable storage and partner flexibility from AWS, with instant, out-of-the-box detections from Abstract that accelerate time-to-insight and response.

Efficient Data Volume Management

- AWS Security Lake stores all ingested data in its full fidelity on Amazon S3, providing durable, long-term retention and enabling a wide range of analytics through services like Athena, OpenSearch, and QuickSight. This ensures organizations can always access complete datasets for compliance, investigations, and advanced use cases.

  Abstract Security enhances this model by reducing data volumes by up to 80% before they reach Security Lake. By filtering, normalizing, and enriching data in-stream, Abstract helps teams control storage and query costs while still ensuring critical signals are preserved. Teams can also choose to retain critical data in Security Lake while routing less urgent data to cost-efficient storage options, giving them flexibility without sacrificing visibility.

  Together, AWS Security Lake and Abstract Security provide both breadth and efficiency: organizations can store everything they need at scale, while also keeping costs predictable and queries fast.

Integrated Threat Intelligence Enrichment

- AWS Security Lake ensures that security data is stored in a standardized format and made accessible to a wide ecosystem of analytics and enrichment tools. This gives organizations flexibility to apply the threat intelligence workflows that best fit their environment.

  Abstract Security enhances this approach by enriching data in real time, directly in the streaming pipeline. By automatically applying indicators from leading threat intelligence providers, Abstract ensures that enriched events are routed into Security Lake alongside raw telemetry. Security teams can then query and investigate data that already includes contextual threat intelligence, accelerating detection and response.

  Together, AWS Security Lake and Abstract Security give organizations a complete picture: the durability and openness of AWS for broad analytics, and the in-stream enrichment of Abstract for immediate, actionable insights.