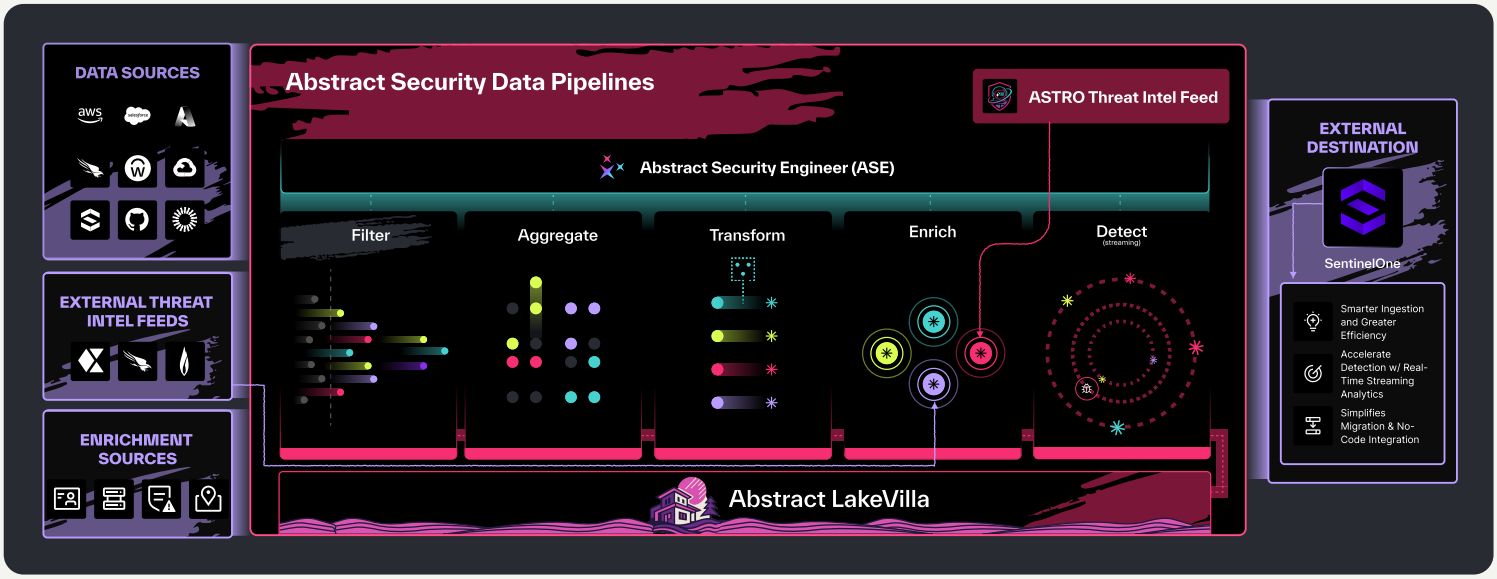
abstract security

Abstract + SentinelOne: Better Together

Abstract Security amplifies the power of SentinelOne's Singularity™ AI SIEM by optimizing data pipelines, streamlining ingestion, and enabling real-time threat detection at scale. Together, Abstract and SentinelOne bring clarity, speed, and intelligence to modern security operations empowering organizations to move at machine speed while staying ahead of emerging threats.

By combining Abstract's AI-driven, streaming-first data platform with SentinelOne's market-leading autonomous threat protection, security teams gain deeper visibility, faster detection, and simpler operations all without additional complexity.



Top 3 Reasons to Use Abstract with SentinelOne

01. Smarter Ingestion, Greater Efficiency

- **SentinelOne** ingests structured and unstructured data with OCSF and AI-driven analytics.
- **Abstract** filters, normalizes, and enriches telemetry at the source with SaaS-native connectors and built-in reliability.
- **Together:** Security teams reduce noise, cut ingestion costs, and deliver higher-value data into Singularity™ for stronger analytics.

02. Accelerate Detection with Real-Time Streaming Analytics

- **SentinelOne** provides autonomous detection with Purple AI and real-time analytics once data is ingested.
- **Abstract** applies streaming detections and threat enrichment in motion, surfacing suspicious activity before it lands in the SIEM.
- **Together:** Teams gain faster insight, shorter MTTD/MTTR, and more complete context for SentinelOne's AI-powered analysis.

03. Simplified Migration and No-Code Integration

- **SentinelOne** supports flexible onboarding for endpoints, cloud workloads, and identity data sources.
- **Abstract** adds prebuilt connectors, drag-and-drop pipelines, and native OCSF normalization to simplify migrations and cross-platform integration.
- **Together:** Organizations adopt Singularity™ more quickly, modernize without disruption, and unlock value across legacy and new environments.

Building on SentinelOne with Abstract Security

Capability	SentinelOne Singularity™ AI SIEM	Abstract Security
Data Ingestion	Ingests structured/unstructured data with OCSF and agentic AI	SaaS-native connectors with built-in normalization and filtering
Detection Speed	Autonomous threat detection with Purple AI and real-time analytics	Streaming-first detection with enriched context before routing to Singularity.
Noise Reduction	AI-driven analytics to filter data post ingestion	Filters irrelevant data before ingestion to optimize SIEM outcomes
Threat Detection	Autonomous AI driven threat detection capabilities on data that is ingested	Augments Singularity's threat detection capabilities with thousands of OOTB detection rules applicable on streaming data
Storage	Always-hot storage for fast queries	Detections in seconds by applying on streaming data

Ideal Use Case:

SentinelOne's Singularity™ AI SIEM provides powerful, autonomous threat detection and response across endpoints, cloud workloads, and identities. Abstract Security complements this with an AI-enhanced data pipeline purpose-built for security operations offering precision control, faster ingestion, and enriched context in every event. Now organizations can build a high-performance security operations platform that is intelligent, agile, and scalable, ideal for navigating today's fast-paced threat landscape.

Smarter Ingestion, Greater Efficiency

- SentinelOne's Singularity™ AI SIEM ingests massive amounts of security data, but post-ingestion filtering and enrichment can drive up storage and compute costs. Abstract optimizes at the source, applying normalization, enrichment, and precision filtering in-stream so only high-value events reach Singularity. The result is cleaner data, lower overhead, and more predictable storage strategies.

Accelerate Detection with Real-Time Streaming Analytics

- Singularity provides powerful autonomous detection and AI-driven analytics across environments. Abstract amplifies this by running detections and enrichment in real time, surfacing threats earlier and reducing mean time to detect and respond from minutes to seconds. Analysts gain high-fidelity alerts with less noise and broader visibility across endpoints, cloud, and SaaS.

Simplified Migration and Future-Ready Operations

- Migrating to Singularity or expanding its use often requires manual setup and engineering effort. Abstract speeds adoption with prebuilt connectors, OCSF-native transformations, and a drag-and-drop interface that simplifies onboarding SaaS, identity, and multi-cloud sources. This unifies the data strategy, reduces complexity, and gives teams flexible, no-code deployment options designed to scale as threats evolve.