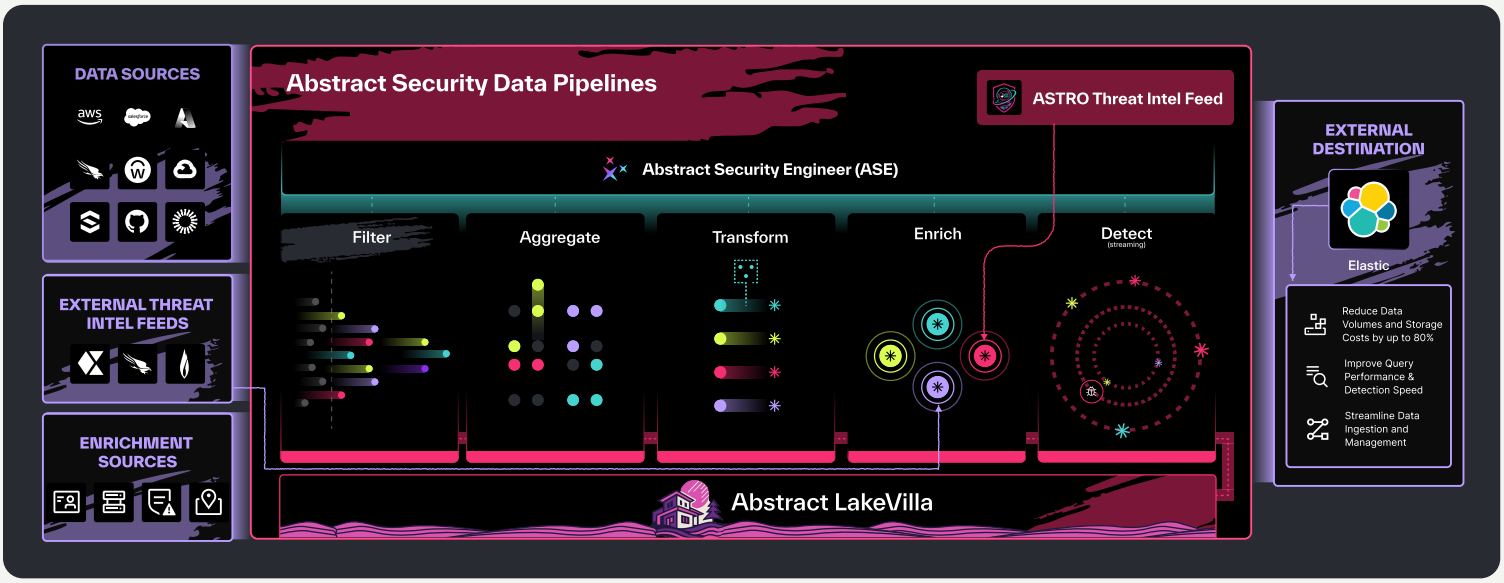
abstract security

Abstract + Elastic Security: Better Together

Elastic Security delivers powerful, AI-driven threat detection and investigation on top of Elasticsearch, giving organizations the ability to analyze security data at scale. Abstract Security complements this by simplifying ingestion with SaaS-native connectors, reducing data volumes before indexing, enriching events in real time, and applying streaming detections in motion. **Together, Elastic and Abstract give security teams broader visibility, faster response, and lower operational costs—without adding complexity to their existing environment.**



Top 3 Reasons To Use Abstract With Elastic Security

01. Simplify Data Ingestion and Broaden Visibility

- **Elastic** provides data collection through Elastic Agents, Logstash pipelines, and agentless integrations for a wide range of sources.
- **Abstract** adds SaaS-native, zero-maintenance API connectors that instantly support hundreds of SaaS and identity sources.
- **Together:** Teams onboard new data sources faster and extend Elastic's visibility into cloud and SaaS environments with less overhead.

02. Reduce Noise and Optimize Data Costs

- **Elastic** pipelines support filtering and enrichment, but often require custom tuning to balance performance and cost.
- **Abstract** reduces data volumes by up to 80% before ingestion with built-in filtering, summarization, and checkpointing.
- **Together:** Organizations lower indexing and storage costs while feeding Elastic with cleaner, high-value data.

03. Expand and Accelerate Detection Coverage

- **Elastic** delivers powerful correlation and detection with a large library of built-in rules and Indicator Match capabilities.
- **Abstract** augments this with thousands of out-of-the-box detections and moves IOC matching into the pipeline for sub-second alerts.
- **Together:** Security teams detect threats earlier and at greater scale, reducing mean time to detect from hours to seconds.

Building on Elastic Security with Abstract

Capability	Elastic Security	Abstract Security
Data Ingestion Setup	Supports Elastic Agents, Logstash pipelines, and agentless integrations to bring in diverse data sources.	Adds SaaS-native, zero-maintenance API connectors that simplify onboarding and extend coverage to SaaS and identity sources.
Data Sources	Collects logs, endpoint, cloud, network, and container data with flexible agent-based and agentless options.	Expands visibility with hundreds of out-of-the-box SaaS and identity integrations, reducing setup effort.
Data Reduction & Pipeline Filtering	Provides ingest pipelines and custom filters to tune data volume and enrich events.	Reduces data by up to 80% before ingestion with built-in filtering, summarization, and checkpointing.
Detection Rule Scalability	Includes over 1,400 built-in detection rules with support for custom logic.	Augments Elastic's library with thousands of additional streaming detections across SaaS, identity, and multi-cloud telemetry.
Expand Detection Coverage	Indicator Match Rules enable correlation of threat intel with ingested data.	Shifts IOC matching into the pipeline for real-time detection at scale, reducing MTTD from hours to seconds.

Ideal Use Case:

Elastic Security provides powerful analytics and detection across large, complex data environments. Abstract Security complements this by streamlining SaaS and identity ingestion, reducing volumes before indexing, and adding real-time detections in motion. Together, they give teams broader visibility, faster response, and lower costs — maximizing the value of Elastic at scale.

01. Simplify Data Ingestion and Broaden Visibility

- Elastic brings in data through Agents, pipelines, and agentless integrations, giving broad coverage across infrastructure and cloud. Abstract complements this with SaaS-native API connectors that add hundreds of SaaS and identity sources with zero maintenance. The result is broader visibility with less complexity in onboarding.

02. Reduce Noise and Optimize Data Costs

- Elastic's ingest pipelines provide flexible filtering and enrichment once data is collected. Abstract lightens the load earlier by filtering and summarizing at the source, reducing volumes by up to 80% before data reaches Elastic. This combination lowers storage and compute costs while ensuring the data Elastic processes is already high-value and context-rich.

03. Match Against Millions of IOCs with Zero Latency

- Elastic Indicator Match Rules correlate threat intelligence with ingested data for precise detections. Abstract moves IOC matching into the pipeline, enabling sub-second detection at massive scale without extra compute strain. Security teams gain faster insights while still benefiting from Elastic's powerful investigation capabilities.

04. Scale Detection Rules to Meet Growing Needs

- Elastic provides more than a thousand built-in rules and supports custom detection logic. Abstract extends coverage with thousands of additional streaming rules across SaaS, identity, and cloud telemetry. This creates a stronger detection layer that scales seamlessly as environments evolve.

05. Accelerate Detection Speed and Improve Response

- Elastic powers advanced analytics once data is indexed in Elasticsearch. Abstract adds streaming detections that surface alerts in seconds before data is stored. Analysts get immediate signal from streaming detections while still retaining Elastic's depth for long-term analysis and compliance.