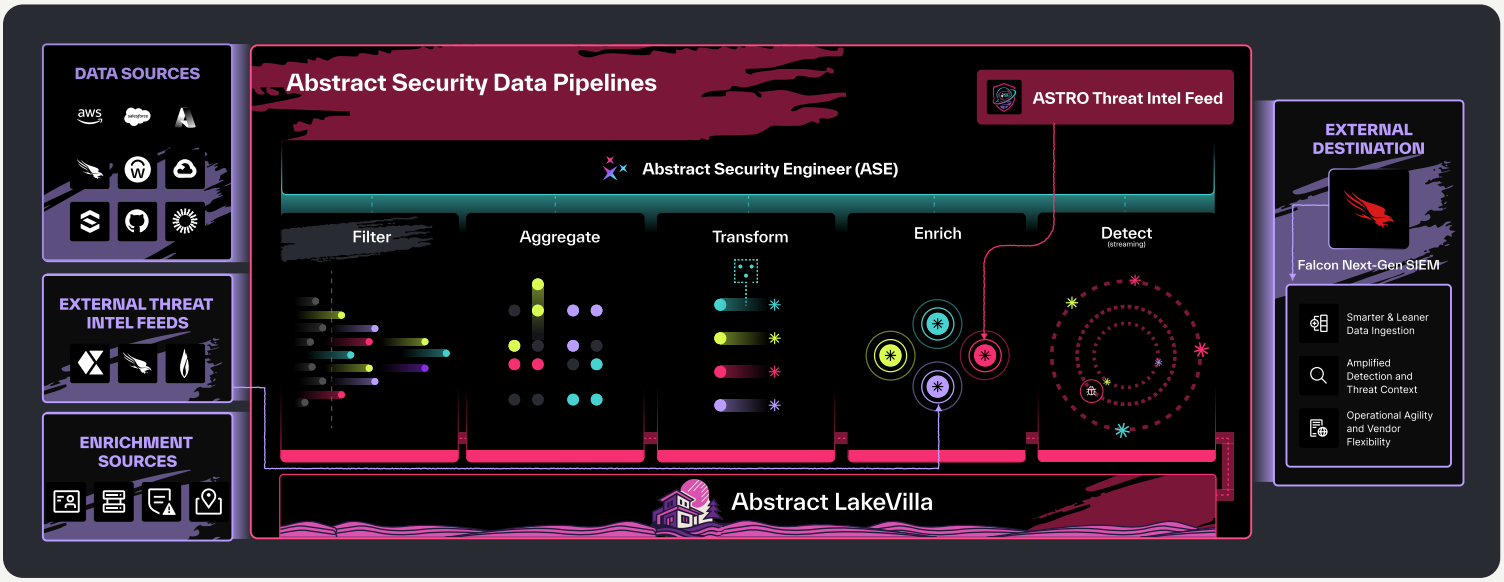
abstract security

# Abstract + CrowdStrike Falcon Next-Gen SIEM: Better Together

CrowdStrike Falcon NGSIEM delivers industry-leading, AI-driven detection and response. Abstract enhances this power by acting as a precision data layer—streamlining ingestion, enriching telemetry, and reducing noise so Falcon NGSIEM works on the highest-quality data possible.
**The result: faster detection, lower costs, and more accurate investigations.**




## Top 3 Reasons to Use Abstract with CrowdStrike Falcon Next-Gen SIEM

### 01. Simplify Data Ingestion at Scale

- **CrowdStrike Falcon NGSIEM** ingests data through APIs, agents, and connectors, giving organizations strong coverage across endpoints, identities, and workloads.
- **Abstract** adds hundreds of SaaS-native integrations and drag-and-drop pipelines that automatically scale with no maintenance.
- **Together:** Teams onboard diverse data sources faster and maintain centralized, high-quality telemetry with less effort.

## 02. Improve Efficiency With Intelligent Data Reduction

- **Falcon NGSIEM's** AI-driven detections and analytics deliver the most value when operating on high-signal data.
- **Abstract** filters noise, deduplicates events, and enriches telemetry in real time before forwarding to Falcon NGSIEM.
- **Together:** Organizations cut data costs, reduce noise, and provide Falcon NGSIEM with cleaner inputs for sharper analytics.

## 03. Expand Detection Agility Across Environments

- **CrowdStrike Falcon NGSIEM** provides industry-leading threat intelligence and AI detections across endpoints and workloads.
- **Abstract** extends this by applying in-stream rules to SaaS, identity, and cloud data, surfacing early indicators before they hit Falcon NGSIEM.
- **Together:** Security teams gain faster visibility across the full stack, improving speed and fidelity of detections.

# Building on CrowdStrike Falcon Next-Gen SIEM with Abstract Security

| Capability | CrowdStrike Falcon NGSIEM | Abstract Security |
|---|---|---|
| **Data Ingestion & Pipeline Setup** | Collects telemetry via APIs, agents, syslog, and connectors for broad endpoint, identity, and workload visibility. | Extends coverage with hundreds of SaaS-native and multi-cloud integrations; drag-and-drop pipelines speed onboarding without custom scripts. |
| **Integration Maintenance** | Ensures data flow through connectors and validation in the Falcon NGSIEM UI. | Minimizes upkeep with out-of-the-box API connectors that keep data streaming cleanly into Falcon NGSIEM. |
| **Data Reduction & Filtering** | Normalizes and enriches data for analytics; filtering supported through connectors. | Filters noise, deduplicates events, and enriches telemetry in-stream before Falcon NGSIEM ingests it, improving fidelity. |
| **Parsing & Tuning Overhead** | Provides onboarding, normalization, enrichment, and real-time log processing. | Centralizes data collection, filtering, and routing in one platform, reducing complexity and ensuring consistent, high-quality data delivery into Falcon NGSIEM. |
| **Performance & Cost Optimization** | Scales log analytics and storage for enterprise environments; efficiency depends on pipeline configuration and tuning. | Reduces volumes by up to 80% with built-in reduction functions, lowering storage/processing spend while preserving critical signals. |
| **Threat Enrichment** | Delivers integrated threat intel and adversary context post-ingestion. | Complements this with real-time enrichment in the pipeline using partner feeds, so Falcon NGSIEM operates on enriched data from the start. |
| **Flexibility** | Deep integration with the CrowdStrike ecosystem. | Expands architectural options with vendor-agnostic routing while keeping Falcon as the core analytics hub. |

# Ideal Use Case:

CrowdStrike Falcon NGSIEM delivers scalable visibility, analytics, and adversary intelligence across endpoints, identities, and workloads. Abstract Security strengthens this by simplifying SaaS and cloud onboarding, filtering and enriching telemetry in-stream, and surfacing early detections. Together, they give security teams cleaner data, lower costs, and faster, more precise detections.

# Optimize Performance and Cut Costs Upfront:

Abstract's reduction-first approach streamlines your data quality from the start, improving overall data quality and lowering storage and processing expenses at Crowdstrike Falcon NGSIEM without extra manual effort.

## 01. Simplified Data Ingestion at Scale

- Falcon NGSIEM ingests data through APIs, agents, and connectors to provide deep visibility across endpoints, identities, and workloads. Abstract extends this reach with hundreds of SaaS-native and multi-cloud integrations that require no custom scripts, streamlining ingestion and accelerating onboarding.

## 02. Automated Pipeline Setup & Scaling

- Falcon NGSIEM's connectors support flexible data routing and processing. Abstract adds drag-and-drop pipelines that scale automatically and eliminate manual configuration or tuning. This makes it easier for teams to keep Falcon NGSIEM supplied with the right data while reducing operational overhead.

## 03. Responding to Fast-Moving Threats

- CrowdStrike research shows adversaries can pivot within an average breakout time of just 48 minutes. Abstract strengthens Falcon NGSIEM's response advantage by detecting anomalies in-stream, surfacing early signals before telemetry lands in Falcon NGSIEM. This reduces mean time to detect from minutes to sub-seconds, giving Falcon NGSIEM cleaner, high-fidelity events to investigate and contain.

## 04. Expanding Cloud and SaaS Visibility

- Falcon NGSIEM provides unified visibility across endpoints, identities, and workloads. Abstract complements this by extending ingestion to SaaS and multi-cloud sources through no-code integrations, ensuring Falcon NGSIEM has a complete view of the modern attack surface without additional engineering burden.

## 05. Expanding Detection Coverage

- Falcon NGSIEM delivers AI-driven detections and adversary intelligence across the environments it monitors. Abstract enhances this by applying thousands of in-stream detection rules for SaaS, cloud, and identity telemetry. This upstream coverage surfaces threats earlier and reduces noise, so Falcon NGSIEM can operate on enriched, high-value data.