

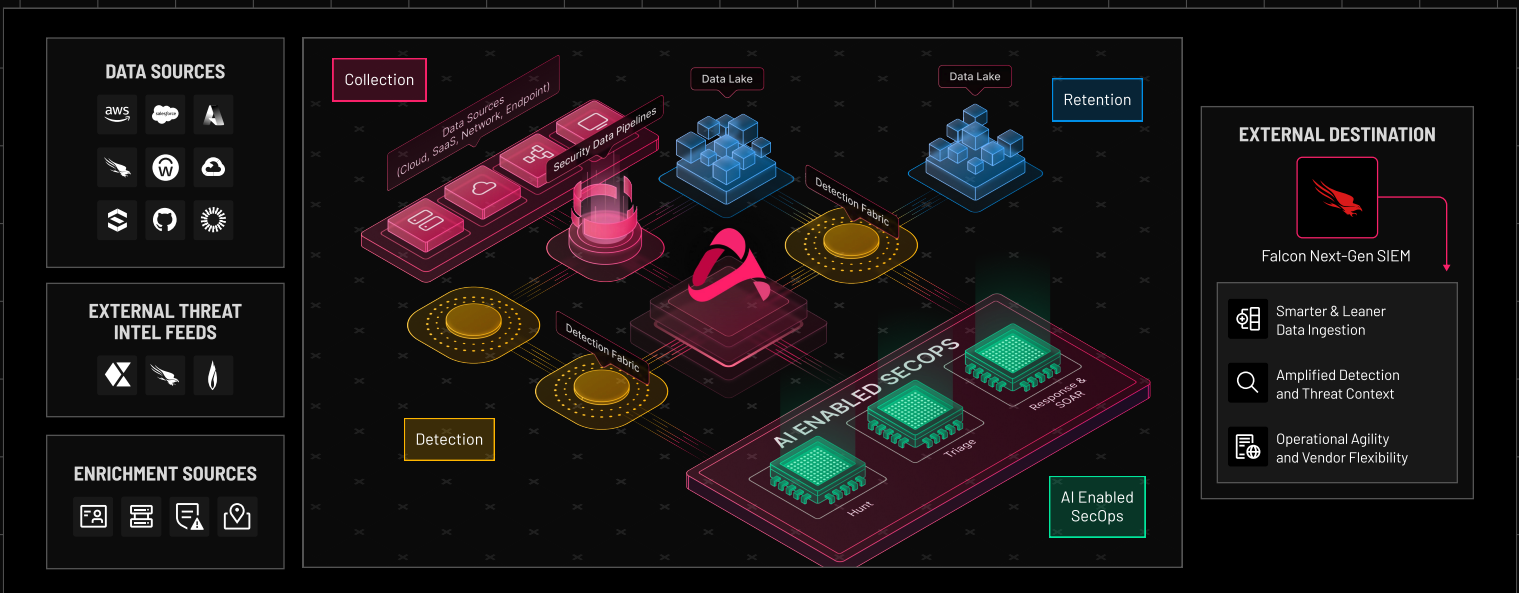


ABSTRACT + CROWDSTRIKE

FALCON NEXT-GEN SIEM BREAK FREE FROM VENDOR LOCK-IN

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 works on the highest-quality data possible.

The result: faster detection, lower costs, and more accurate investigations.



TOP 3 REASONS TO USE **ABSTRACT** AND 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

- **CrowdStrike 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 both speed and fidelity of detections.

BUILDING ON CROWDSTRIKE FALCON NEXT-GEN SIEM WITH **ABSTRACT**

CAPABILITY	CROWDSTRIKE FALCON NGSiEM	ABSTRACT
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 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 without extra manual effort.



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.



AUTOMATED PIPELINE SETUP & SCALING

Falcon'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 supplied with the right data while reducing operational overhead.



RESPONDING TO FAST-MOVING THREATS

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

**SEE IT FOR
YOURSELF.**



Most teams are up and running with real security outcomes on day one. We'll work with your data, your sources, and your environment — no generic demo.

BOOK A DEMO 