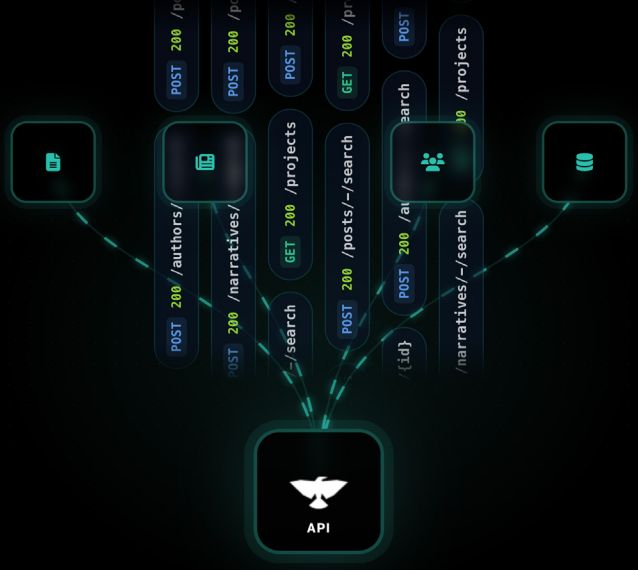
BLACKBIRD.AI

CONSTELLATION API

Embed Narrative Intelligence Directly Into Your Enterprise Systems — Dashboards, Investigations, Reporting Workflows, and Beyond



Modern threat intelligence and corporate risk programs demand more than a standalone interface. Today's security, risk, and communications teams need narrative intelligence data to flow directly and automatically into the tools they already operate — SIEMs, case management platforms, crisis comms, and executive threat monitoring systems. Narrative intelligence has historically been siloed. Analysts must log into a separate platform, manually extract findings, and re-enter them into internal systems. This creates friction, delays, and gaps — especially when threats move at machine speed. Here are just some of the challenges teams face today:

- **Narrative attacks move faster than manual workflows:** AI has collapsed the cost of narrative attack campaigns and influence operations. Threat actors continuously create, test, and amplify harmful narratives faster than any analyst can track them manually.
- **Data lives in too many places:** Security, communications, and risk teams each maintain separate tools. Narrative intelligence needs to seamlessly make it into the systems where critical decisions are made.
- **Integration is expensive and slow:** Building custom data pipelines from scratch requires significant engineering investment and ongoing maintenance.
- **Scale demands automation:** Organizations monitoring dozens of projects, hundreds of narratives, and thousands of posts cannot rely on manual exports and copy-paste workflows.

ANALYTICAL RISK

Teams that cannot programmatically access narrative data are forced into reactive postures. By the time findings are manually extracted and distributed, the window for proactive intervention has often passed. Organizations need narrative intelligence that is queryable, portable, and actionable—not isolated within a single interface.

OPERATIONAL RISK

Without API access, integrating intelligence data into SOC tooling, executive dashboards, or automated alert workflows requires significant manual overhead. This limits the speed and scale at which narrative intelligence can inform decisions across security, risk, and communications functions.

REPORTING RISK

Siloed data sources force analysts to manually compile findings across platforms before they can report up. Every step in that chain introduces delay, inconsistency, and the risk of critical signals being missed.

How Blackbird.AI's Constellation API Can Help

Operational centers want narrative intelligence connected directly to their other data sources for a complete picture of threats across their digital landscape. Constellation API was built for this. It opens up programmatic access to Blackbird.AI's Constellation Narrative Intelligence Platform's full intelligence stack: narrative discovery, risk scoring, bot detection, cohort analysis, coordination evidence, and state actor attribution. The API enables integration with SIEM and SOAR platforms, custom application development, and AI agent consumption via the emerging Model Context Protocol (MCP). With public developer documentation at docs.blackbird.ai, enterprise-grade authentication, and SOC-2 compliance, organizations can begin enriching their security workflows with narrative intelligence data in minutes.

The Constellation API bring Blackbird.AI's narrative intelligence directly into your internal systems, enabling you to aggregate, correlate, and operationalize high-fidelity insight into narrative attacks, authors, and posts targeting your executives and organization at scale. Constellation API make narrative intelligence portable, queryable, and actionable.

Export-Driven Use Cases

- **Unified Reporting:** Feed narrative attacks, author information, and posts into internal dashboards for consolidated threat reporting across security, risk, and communications teams.
- **Additional Signals:** Map Blackbird.AI narrative intelligence to non-Constellation data sources, including your threat and risk intelligence, to enrich existing risk workflows and SIEM tooling.
- **Custom Visualizations:** Render Constellation narrative intelligence in internal visualization systems, surfacing risk patterns and actor networks in formats tailored to your team.
- **Investigation Linking:** Connect Constellation narrative intelligence to case management platforms, ticketing systems, or monitoring tools for end-to-end investigative workflows.
- **Automated Intelligence Flows:** Route Constellation narrative findings automatically across security, risk, communications, and executive teams without manual extraction or re-entry.

What Data Is Available by Endpoint

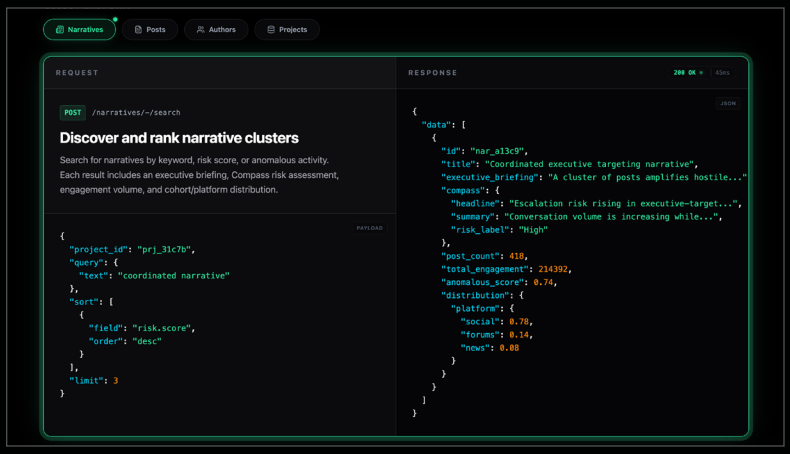
The Constellation API expose three intelligence endpoints — Posts, Narratives, and Authors — each delivering a distinct layer of structured, AI-enriched data. The Projects endpoint supports the workflow by allowing you to enumerate your available Constellation narrative intelligence projects before querying the intelligence endpoints.

ENDPOINT	PURPOSE	KEY DATA AVAILABLE
Projects	Identify the datasets you have in Constellation	Project name, ID, post count, data availability status
Narratives	Return clusters of related content representing coherent narratives	Narrative title, executive briefing, Compass headline and summary, Compass risk label, post count, total engagement, anomalous score, cohort and platform distribution
Posts	Retrieve enriched social posts from a Constellation project	Post text, platform, timestamp, narrative identifier, author username, detected language
Authors	Provide actor-level intelligence for accounts in a project	Username, bio, cohort membership, bot-like classifier, follower and following network statistics

Constellation API Workflow

The Constellation API follows a straightforward four-step workflow:

1. **Authenticate:** Include your API key in the Authorization header of every request.
2. **List Projects:** Query the Projects endpoint to retrieve your available Constellation projects and identify the project ID needed for subsequent queries.
3. **Query Intelligence Endpoints:** Use the project ID to search Posts, Narratives, or Authors — filtering, sorting, and paginating results as needed.
4. **Retrieve Enriched Results:** Parse the structured response to extract narrative discovery, risk scoring, bot detection, cohort analysis, coordination evidence, state actor attribution, author intelligence, and post-level data for use in your systems.



Getting Started

Getting started with the Constellation API requires a Blackbird.AI API key, available to participants in the Early Adopter Program. Full API documentation, endpoint references, and sample responses are available at docs.blackbird.ai/constellation.

OPTION	DESCRIPTION
Early Adopter Program	Get production access, discounted pricing, and direct influence on the API roadmap
Schedule a Demo	See the Constellation API in action with your own Constellation project
Get Pricing	Discuss enterprise pricing and integration support

About BLACKBIRD.AI

BLACKBIRD.AI protects organizations and executives from narrative attacks that cause financial, operational and reputational harm. Our AI-driven Narrative Intelligence Platform identifies key narratives that impact your organization/industry, the influence behind them, the networks they touch, the anomalous behavior that scales them, and the cohorts and communities that connect them. This information enables organizations to proactively understand narrative threats as they scale and become harmful for better strategic decision-making. A diverse team of AI experts, threat intelligence analysts, and national security professionals founded Blackbird.AI to defend information integrity and fight a new class of narrative threats. Learn more at Blackbird.AI.