AiStrike Solution Brief: Enterprise Behavior Analytics

Nov 12, 2026 · @Nitin

One platform. Every actor. Human and AI.

At a glance

Enterprise Behavior Analytics is one behavioral analytics platform across human and AI actors. AiStrike unifies UEBA and AIDR to detect, investigate and respond to threats involving employees, privileged users, contractors and autonomous AI agents.

- **The insider is no longer only human.** AI agents hold credentials, query systems and take actions, often without the review a human account gets.
- **Threats cross between actors.** A threat that moves from a person to an agent looks like two unrelated, low-risk events to tools that each watch only one of them.
- **AiStrike follows it across.** Behavior from people and agents is analyzed on raw telemetry, classified against shared frameworks, and correlated into one investigation.

The insider is no longer only human

For a decade, insider threat meant people. There is now a second population of insiders, and it is growing faster than the first. Both hold credentials, query systems and take actions.

	People	AI agents
Who	Employees, privileged users, contractors	Copilots, coding agents, SOC agents, business agents
Seen through	Identity, endpoint, cloud, physical access and DLP data	Prompts, retrievals, tool calls, API calls and data access
Why they are hard to catch	Actions look legitimate one at a time	The reasoning is visible, but the actions often are not

With people, the activity was logged and the hard part was the analytics. Agents make both harder:

- **Intent is hard to trace.** An agent calls sub-agents, and those spin up their own activity.
- **Telemetry is patchy.** Enterprise AI tools expose some events. Shadow AI exposes almost none without something on the host.
- **Baselines don't fit.** Most tools baseline users, hosts and IPs. An agent is a combination of all three.

Security tools see individual actors

UEBA watches people and AI agent security watches agents, so neither holds the behavioral context of the other. Each does its job for its own actor.

	UEBA	AI agent security
Sees	Users and entities	AI agents, prompts and tool use
Strong at	Baselining human behavior and scoring risk	Governing agent identity and what reaches the model
Lacks	What the user's AI agents did on their behalf	What the human behind the agent was doing

The gap is fragmented behavioral context. An agent's behavior only means something when you can tie it to the user who launched it and the host it ran on. UEBA and AIDR are two halves of the same question.

What Enterprise Behavior Analytics does

AiStrike runs analytics on telemetry, not just alerts, from both kinds of actor.

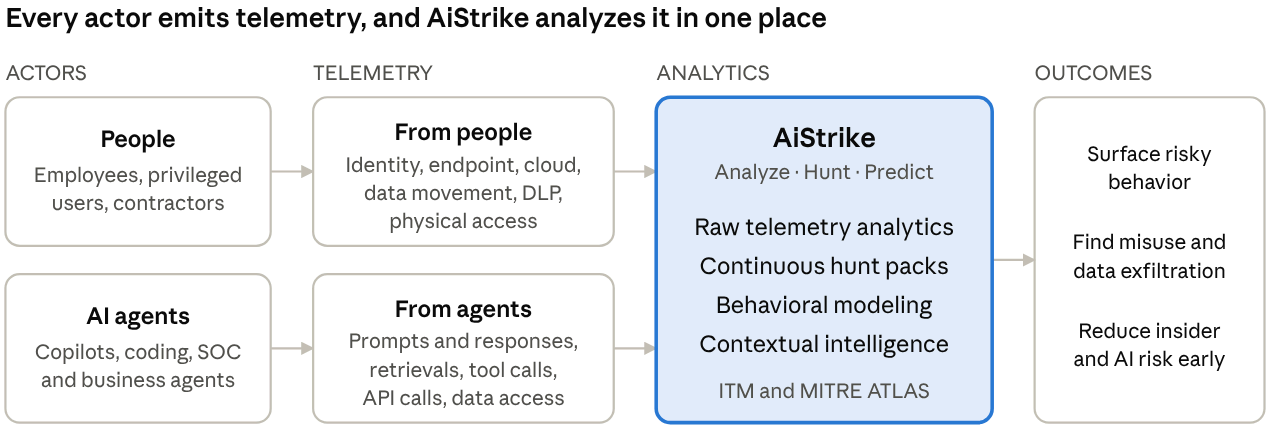
Capability	What it does
Raw telemetry analytics	Analyzes raw activity from people and agents, not only alerts, to find patterns no single event reveals.

Capability	What it does
Continuous hunt packs	Prepackaged hunts search continuously for multi-stage, low-and-slow behavior that stays under every threshold.
Behavioral modeling	Learns what is normal per user, agent and peer group, and combines intent signals, such as leavers, with activity.
Contextual intelligence	Classifies signals with the Insider Threat Matrix™ and MITRE ATLAS, and correlates them with identity and data context.

An anomaly is where the investigation starts. Legacy UEBA ends in a queue: telemetry, a behavioral anomaly, a risk score, then a person investigates. AiStrike carries each anomaly through investigation and evidence to a risk determination and a governed response. The measure is anomalies investigated to a conclusion, not anomalies produced.

How it works

Every actor emits telemetry, not just alerts, and AiStrike analyzes both streams in one place.



How Enterprise Behavior Analytics works · actors, telemetry, analytics, outcomes

The threat model then works in three steps:

1. **Monitor.** Behavior anomalies are collected across people and AI agents.

2. **Classify.** Anomalies are classified with the Forscie Insider Threat Matrix™ (ITM) for people and MITRE ATLAS for AI agents.
3. **Correlate.** Classified signals are stitched into toxic combinations in one threat model, revealing what no single anomaly shows.

Intent is added wherever possible. Insider threat is either intentional, such as exfiltration or sabotage, or accidental, such as emailing files to yourself or uploading sensitive files to ChatGPT. Intent signals, such as a departing employee, are combined with activity, so the same action is weighed differently for a leaver than for someone on a new project.

What it detects

The same patterns appear whether the actor is a person or an agent. Each event is routine on its own. The pattern only shows against a baseline for that actor, over time.

Pattern	In people	In AI agents
Unusual sequence	After-hours badge access, restricted share, bulk file deletion	retrieve_doc, then send_email, then an external API
Abnormal data access	A user opens restricted data outside role and peer group	An agent accesses sensitive data it has never touched
Low-and-slow	Access day 1, discovery day 4, staging day 9, transfer day 16	Subtle, multi-step activity that never triggers an alert
Abuse, no exploit	Legitimate access used for an unsanctioned purpose	Legitimate access used at unsanctioned volume

The cross-boundary case: a person uses an AI agent to exfiltrate data.

1. An employee accesses sensitive files outside their normal behavior.
2. An AI agent acting for them retrieves documents and invokes external tools.
3. AiStrike correlates both actors into one investigation.

Neither the employee's activity nor the agent's individual actions necessarily trigger an alert. The combined sequence reveals the risk. This is what makes Enterprise Behavior Analytics more than UEBA plus AIDR.

Why AiStrike

AiStrike is built to reach a conclusion about behavior, not to add another queue.

- **Human-agent correlation.** Correlates behavior across human identities, AI agents, applications, tools and data into one investigation.
- **Works with the data you have.** Uses telemetry from existing SIEMs, data lakes and security platforms. Agent telemetry arrives through direct API and AI security tool integrations.
- **Framework-based threat model.** Signals are classified with the Insider Threat Matrix™ and MITRE ATLAS, then stitched into toxic combinations.
- **Analytics plus AI investigation.** Combines deterministic and statistical behavioral analytics with AI-driven investigation and contextual prioritization.

Next step

To see how this applies to your environment, ask AiStrike for:

- The Enterprise Behavior Analytics data sheet.
- A walkthrough of the cross-boundary scenario, using the telemetry sources you already have.

Further reading: A Parallel Universe of Insiders. Learn more at aistrike.com.