Above × CrowdStrike

BETTER TOGETHER

Falcon sees everything. Above understands it.

Above turns CrowdStrike Falcon's endpoint ground truth into finished Insider Risk investigations, fused with browser, SaaS, email, and identity activity into one behavioral timeline per identity, human or AI. Falcon keeps detecting and preventing at the endpoint; Above reasons over sequence and intent across the human. Nothing is replaced.



Two layers, one loop.

Modern endpoints emit a firehose: process executions, file operations, network connections, logons, device events. Falcon captures it richly: the ground truth of activity. But raw telemetry is high-volume, low-context, and endpoint-scoped, and the riskiest insider stories unfold across surfaces no single sensor sees end to end. Above ingests Falcon telemetry read-only, correlates it with everything the browser, SaaS, email, and identity layers see, and returns the finished case: the story, the sequence, the evidence, and a verdict. Risk context then flows back to the endpoint, closing the loop where Falcon acts.

What Above ingests from Falcon

Read-only, through the Falcon integration.

CONTINUOUS SYNC · STORED

Host inventory · Logins · IP / MAC history · EDR detections

ON-DEMAND DEEP QUERY · LIVE, SCOPED

Process · File · Network · Logon · Registry · USB

Deep telemetry is live-queried during an investigation, scoped to the identity under review, not stored.

What Above hands back

- One behavioral timeline per identity: endpoint fragments fused with browser, SaaS, email, and identity activity
- Verdicts with evidence: what happened, in what sequence, and whether it reads as negligence, curiosity, or intent
- Risk context for response, up to endpoint containment through the Falcon integration
- Coverage for the cases EDR was never built to close: departure-with-data, shadow AI, fraud, agentic identities

Falcon: detection & prevention at the endpoint. **Above:** intent & investigation across the human. No rip-and-replace.

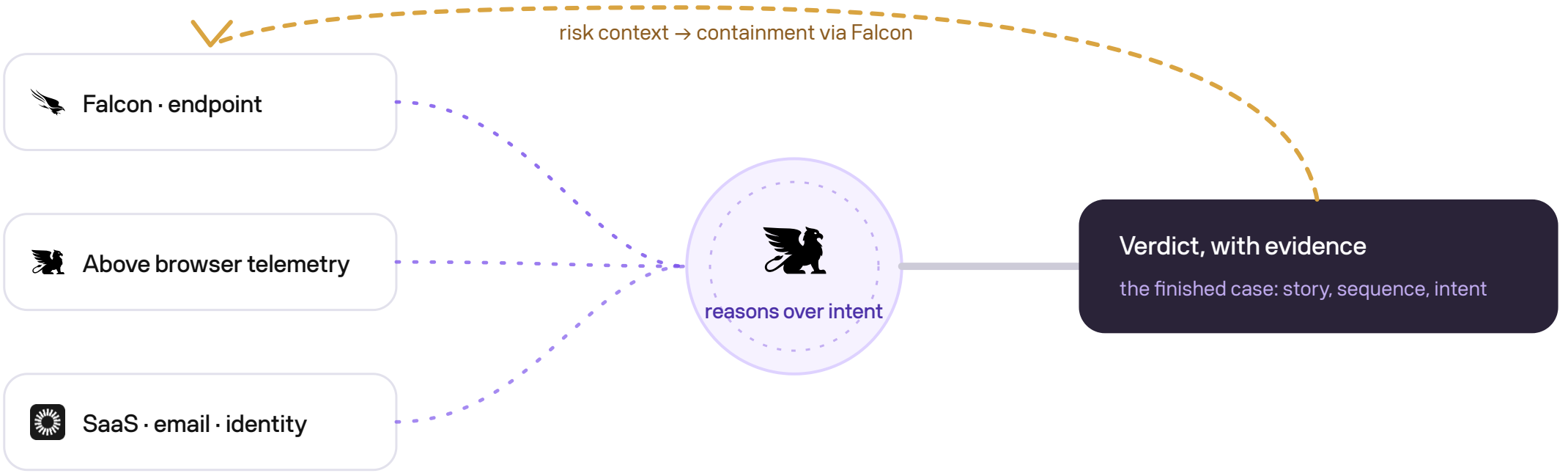
A 2 a.m. login is noise. A 2 a.m. login + a repo clone + a personal-email draft is an investigation.

02:04	Login from a new device	FALCON
02:11	Source repository cloned	FALCON · DEEP QUERY
02:26	Files staged to a personal drive	BROWSER
02:31	Offer letter opened in personal email	BROWSER

VERDICT Departure with data: every claim cited to its evidence. A human confirms before anything happens to a person.

Illustrative investigation. Each fragment was visible to one sensor in isolation; the story only exists when they are read together.

The loop, end to end



Correlated alongside Falcon

Representative sources Above fuses with Falcon telemetry to build one investigation-ready timeline.

- Above browser telemetry
- Google Workspace
- Okta
- Slack
- Workday
- Personal transfer channels

- Read-only access to Falcon telemetry
- Scoped to the identity under investigation
- Deep telemetry live-queried during an investigation, not stored
- SOC 2 Type II and ISO/IEC 42001

© 2026 Above Security, Inc.
CrowdStrike and Falcon are trademarks of CrowdStrike, Inc.

BETTER TOGETHER

See the loop with your own Falcon data.

Read-only to connect. Reach us at contact@above.security.

