BLACKBIRD.AI

RAV3N RECON

Protect Against Narrative Attacks Associated With Influencers, Affiliates, and Threat Actors That Cause Reputational, Financial, Operational, and Executive Harm

Modern digital engagement comes with modern narrative risk. Today's brand reputation crises often originate with influencers, affiliates, and threat actors, posing risks to your organization. They include: **spokespeople, creators, celebrities, ambassadors, superfans, executives, and threat actors**. Influencers and affiliates leverage their large following, reach, and credibility to endorse brands, promote products and services, and build brand trust. Affiliates are individuals or businesses who partner with brands to promote products through unique links or codes, earning a commission on sales generated. Threat actors create AI-based narrative attack campaigns for financial gain, operational disruption, and physical harm. Here are just some of the opportunities and challenges companies face:

- Influencer and affiliate marketing are exploding: Influencer marketing is a $32 billion global market, and affiliate marketing is a $15 billion industry.
- Brand budgets are growing: Top brands are increasing their influencer and affiliate marketing programs to boost their reach and sales.
- Threat actors AI-based campaigns: Cybercriminals, hyper-agenda-driven individuals, and nation-state communities are creating AI-based narrative attack campaigns to do financial, operational, and even physical harm.
- Manual, expensive due diligence: Brands and Security Operations Centers rely on manual reviews of thousands of influencers, affiliates, and threat actors, resulting in high costs, frequent errors, and slow turnaround.

BRAND REPUTATION AND FINANCIAL RISK

Brands partner with influencers and affiliates to expand their reach, audience, and platforms. Brands don't have a fast way to understand the risks associated with an influencer or affiliate that could ultimately harm the brand. If they are doing any vetting today, it's costly and manual, and it takes a long time to comb through an influencer's or affiliate's profile to gain a clear understanding of current risks. When things go right, brands can accelerate growth. When they go wrong, harmful narratives can damage brand reputation in an instant. A single phrase, post, or comment can quickly scale out of control and blindside a brand, causing significant financial, reputational, operational, and even physical harm. For finance, pharma, alcohol, and gambling brands, "reasonable oversight" of every promoter is required—or face fines, public backlash, or loss of consumer trust. The potential for success is high, but so are the risks.

> "Reputation is not just your brand. It's all your affiliates." — Major U.S. Bank

OPERATIONAL RISK

AI has transformed the economics of narrative attacks driven by disinformation, misinformation, and deepfakes. The cost has collapsed so dramatically that threat actors can now continuously create, test, amplify, and adjust harmful campaigns to target companies alongside cyberattacks. Cybersecurity and Security Operations teams manually track threat actors and use traditional OSINT techniques to understand their intentions, resulting in high costs, frequent errors, and inefficient use of analysts' time.

EXECUTIVE PROTECTION RISK

Security teams are monitoring the physical environment to protect their executives. Threat actors use online narrative attack campaigns to identify targets, inflame tensions, and justify violence. This convergence demands that executive protection programs integrate narrative intelligence with physical security protocols. When an individual or organization is identified as a potential threat to their executives, teams, or physical assets, security teams need to quickly assess an actor's digital footprint and reach out to understand the potential impact better and inform a confident mitigation strategy.

How Blackbird.AI's RAV3N Recon Can Help

Blackbird.AI's RAV3N Recon narrative intelligence analyzes harmful narratives affecting your executives and organization, including Influencer and Affiliate risk (spokespeople, creators, celebrities, and executives) and Threat Actor narrative and physical attacks, across **text, images, videos, and audio**, scanning up to 2 years of content in minutes.

RAV3N Recon Narrative Intelligence Features include:

1. INFLUENCER RISK ASSESSMENT

Determine whether a social creator is safe to partner with based on their narratives: high volume, real-time media, and major brand exposure.

- *Example Inputs*: Top influencers' names and affiliates
- *Primary Users*: Brands, PR agencies, Ad firms, Regulatory compliance teams

2. CELEBRITY RISK ASSESSMENT

Only need a name and one social handle (Report accuracy improves with additional query inputs).

- Risk report runs in 5-10 minutes
- Risks are prioritized by heat-score on reputational exposure
- Risks are organized into 26 unique categories
- Drill down into the narratives present in the posts being discussed/engaged in
- Access the posts of concern to understand the risk directly on the platform
- Narrative Threat Matrix with key themes and channels
- PDF summary briefing for each target
- Interactive dashboard highlighting what matters most

- Multimodal and Cross-platform analysis across top social media platforms
- Export reports to include in other reporting, etc

Ensure celebrities and public figures under management are not carrying unseen narrative risk.

- *Example Inputs*: Sports stars, musicians, movie actors
- *Primary Users*: Talent agencies, Sports leagues, Teams, Streaming platforms

3. THREAT ACTOR RISK ASSESSMENT

Protect entities for reputation/narrative risk before, during, and after narrative and cyber attacks.

- *Example Inputs*: cyber criminals, fraudsters, nation-state actors
- *Primary Users*: Threat intel analysts, Security Operations Center, CISO

4. EXECUTIVE RISK ASSESSMENT

Complement Executive Protection with narrative monitoring for C-suite and key personnel.

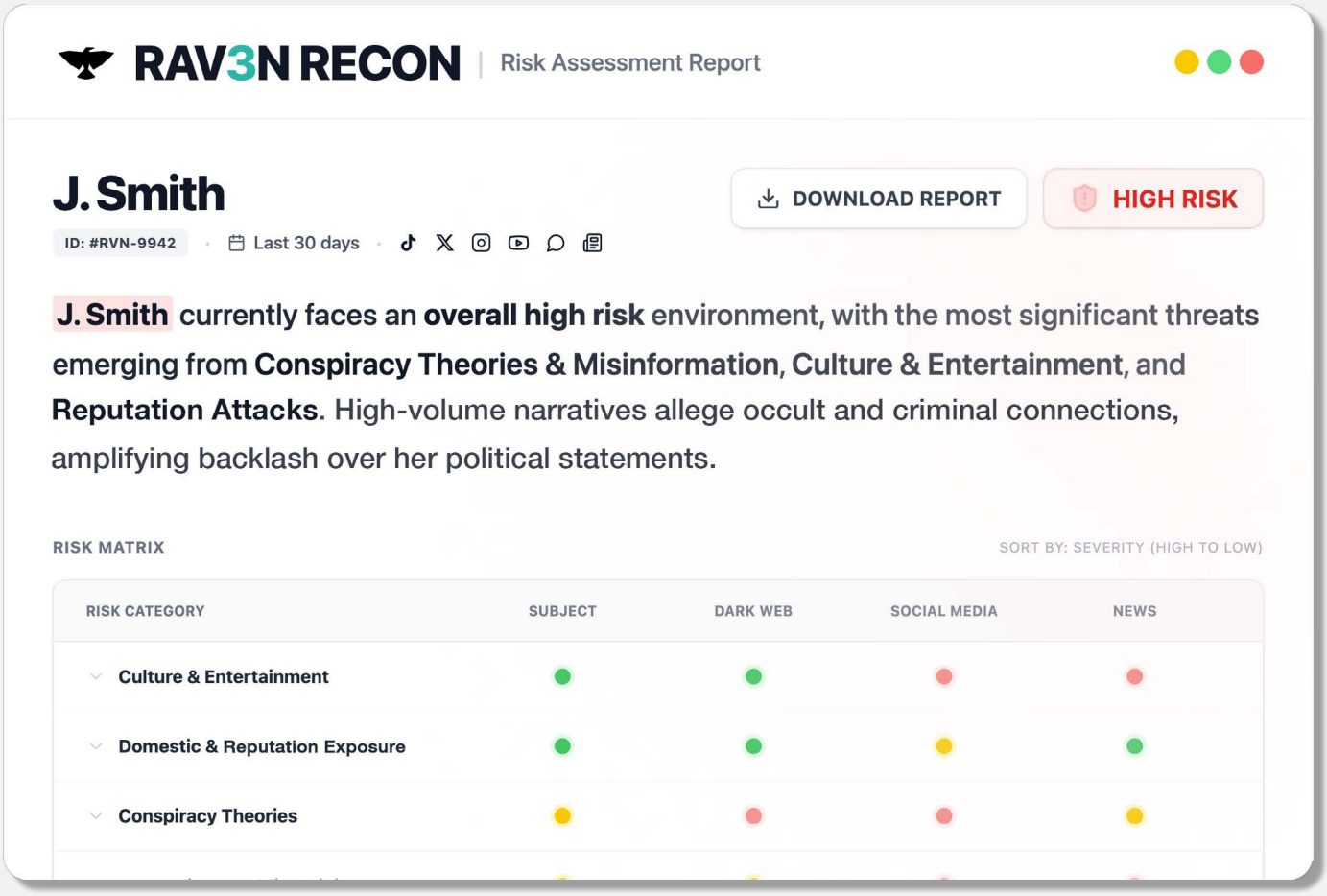
- *Example Inputs*: Corporate executives, government leaders
- *Primary Users*: Enterprise security, CorpComms, Risk teams

RAV3N Recon Risk Lenses We Monitor

LENS	DESCRIPTION
Advocacy	Personal stances, religious messaging, activist causes, and controversial endorsements
Lifestyle	Substance use, toxic content, risky behavior
Tone	Hostile language, profanity, bullying, harassment patterns
Physical Threats	Violence, doxxing, stalking behavior, incitement, weapon mentions
Risky Promotion	Financial schemes, misleading health claims, and FTC violations
Sensitive Material	Explicit material, hate speech, discriminatory content
Corporate & Legal	Criminal issues, legal exposure, regulatory risk
Operational	Cybersecurity, supply chain, technology risks
Crisis & Reputation	Crisis response, reputation attacks, mobilization
Misinformation	Conspiracy theories, deepfakes, and manipulation

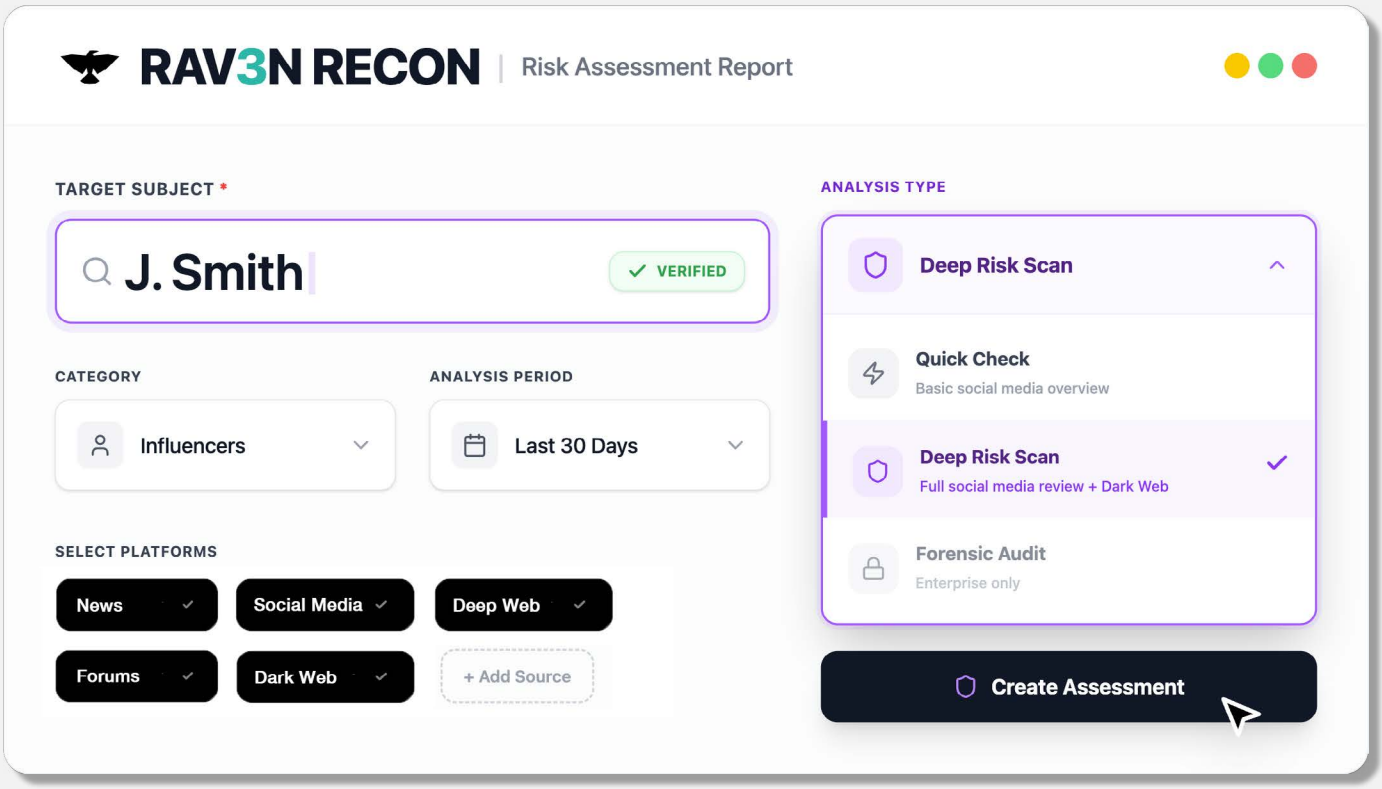
RAV3N Recon Dashboard and Narrative Risk Assessments

Every completed narrative risk assessment can be logged with subject, status, and date. Risks are prioritized by heat score for reputational exposure (e.g., Negligible, Low, Medium, High). The search and filters let teams quickly find historical assessments for follow-up action.



Create New Narrative Risk Assessments in a Fraction of the Time

Analysts can spin up back-to-back narrative risk assessments by posting a subject's social handles, selecting a look-back window for posts and public mentions, and adding email recipients. Hitting Submit queues the job and completes the assessment.



Blackbird.AI's RAV3N Recon narrative intelligence helps protect against harmful narratives associated with influencers, affiliates, and threat actors that cause reputational, operational, and executive harm. What's changed over the past year isn't simply volume or virality. It's speed, coordination, and automation. AI has collapsed the cost of influence. Narrative attacks are no longer isolated incidents. They run continuously, adaptively, and at machine speed, accelerated by an agentic AI world that evolves daily.

The implications are profound. Narrative risk from influencers, affiliates, and threat actors now impacts brand reputation, destabilizes leadership teams, amplifies cyber incidents, and escalates into physical risk. This is why organizations are beginning to treat narrative intelligence as core infrastructure rather than an optional capability and why business leaders are now treating narrative risk as something to prepare for rather than react to. Blackbird.AI's RAV3N Recon narrative intelligence is the product that can help.

To learn more about how Blackbird.AI's RAV3N Recon can help, book a demo.

About BLACKBIRD.AI

BLACKBIRD.AI protects organizations from narrative attacks that cause financial, reputational, and physical harm. Our AI-driven Narrative Intelligence Platform identifies key narratives that impact your executives/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.