MARKET NOTE

When Behavior Speaks Louder Than Content: AI Uniti and the Emergence of Behavioral Threat Intelligence

Sakshi Grover Craig Robinson

EXECUTIVE SNAPSHOT

This IDC Market Note reflects IDC's observations following its discussion with AI Uniti and examines the emergence of behavioral threat intelligence as an evolving area within enterprise cybersecurity.

As GenAI accelerates the creation of synthetic media, coordinated influence campaigns, and AI-enabled deception, organizations are increasingly required to protect not only infrastructure and identities but also digital trust, reputation, and information integrity. During the discussion, AI Uniti outlined its approach to detecting coordinated narrative manipulation through behavioral analytics, cross-platform correlation, deterministic investigations, and integrated deepfake detection. IDC believes these capabilities reflect the broader convergence of cybersecurity, digital risk protection, AI trust, and governance as enterprises seek to strengthen resilience against increasingly sophisticated AI-driven influence operations.

Key takeaways

- AI Uniti is positioning behavioral threat intelligence as a complementary intelligence layer that extends existing security operations center (SOC), threat intelligence, and digital risk workflows rather than replacing them.
- The company is expanding beyond behavioral detection into AI trust and governance through LLM Protect, AI answer monitoring, integrated deepfake detection, and AI-assisted investigations.
- IDC research indicates growing enterprise demand for explainable AI, digital authenticity, and governance as AI-generated misinformation and synthetic identities become increasingly prevalent.
- Behavioral threat intelligence remains an emerging market, creating opportunities for vendors that can integrate behavioral analytics, content authenticity, and AI governance into existing enterprise security operations.

July 2026, IDC #AP54792626

IN THIS MARKET NOTE

This IDC Market Note examines AI Uniti's approach to behavioral threat intelligence and its implications for the evolving cybersecurity market. Rather than focusing on malware, infrastructure compromise, or identity attacks, AI Uniti seeks to identify coordinated narrative manipulation by analyzing behavioral indicators, including temporal synchronization, engagement patterns, network relationships, amplification behavior, and cross-platform coordination, to detect coordinated influence campaigns before they materially affect enterprise operations, reputation, or public trust.

The company's Signal platform combines behavioral analytics with deterministic evidence chains designed to support enterprise investigations, regulatory reporting, and legal proceedings. Unlike conventional narrative intelligence platforms that primarily analyze content using AI or analyst review, AI Uniti positions behavioral coordination as a more resilient indicator of coordinated activity because behavioral patterns are inherently more difficult to manipulate than content alone. During the discussion, AI Uniti also shared supporting documentation describing how its methodology aligns with published academic research on coordinated inauthentic activity.

IDC's discussions with AI Uniti also highlighted the company's expansion beyond behavioral threat detection. Signal now incorporates deepfake detection across image, audio, and video, enabling organizations to assess both who is coordinating an activity and whether the associated media is synthetic within a single investigative workflow. The company has also introduced customer-specific AI agents designed to investigate coordinated campaigns using explainable evidence trails, AI answer-layer monitoring across major foundation models, and LLM Protect, a runtime governance layer intended to secure enterprise AI agents. Collectively, these developments indicate that AI Uniti is expanding beyond narrative intelligence toward a broader platform focused on AI trust, governance, and the detection of both human- and AI-generated influence operations.

IDC'S POINT OF VIEW

Behavioral threat intelligence represents one of the more interesting emerging areas within enterprise cybersecurity because it extends security visibility beyond traditional infrastructure into digital trust, enterprise reputation, financial integrity, and coordinated influence. Historically, security operations have concentrated on detecting malicious code, compromised identities, lateral movement, and network anomalies. However, the rapid adoption of GenAI has fundamentally changed the economics of creating and distributing misinformation. Text, images, audio, and video can now be generated, translated, paraphrased, or manipulated at scale, reducing the effectiveness of content-centric detection approaches that rely primarily on language, sentiment, or media classification. As a result, organizations are increasingly recognizing that behavioral indicators, such as

temporal synchronization, coordinated amplification, network relationships, and cross-platform activity, are significantly more difficult to manipulate than content itself. IDC expects this shift to influence not only narrative intelligence platforms but also broader digital risk protection, cyberthreat intelligence, and AI trust markets.

This market transition is reflected in IDC's *Asia/Pacific Security Study, 2025* (n = 500). While AI-enhanced phishing and impersonation (58.4%), LLM prompt injection and model manipulation (57.6%), AI-powered ransomware (57.0%), and automated malware creation (56.8%) remain the leading AI-driven security concerns, organizations also rank AI-generated disinformation campaigns for reputational or operational disruption (56.2%) among their top threats. This suggests that enterprises are increasingly recognizing AI-enabled influence operations as a cyber resilience challenge alongside more traditional technical attacks, rather than viewing them solely as communications or brand management issues. Concerns around AI-generated disinformation are particularly pronounced among organizations in professional services (67.1%) and healthcare services (60.0%), where trust, reputation, and the integrity of public information directly influence business outcomes.

However, recognizing these threats is only part of the challenge. IDC's research also found that 40.6% of organizations in Asia/Pacific cited explainability, transparency, compliance risks, hallucinations, and false positives as significant barriers to adopting AI-based security technologies, reinforcing enterprise demand for deterministic, evidence-based AI capabilities rather than opaque machine learning models. These findings closely align with AI Uniti's emphasis on explainable behavioral analysis, traceable evidence, and evidence-backed investigations.

IDC believes AI Uniti's architectural approach reflects this broader market evolution. Rather than positioning Signal as another security analytics platform, the company integrates behavioral intelligence into security information and event management (SIEM); security orchestration, automation, and response (SOAR); and cyberthreat intelligence platforms, enriching existing enterprise security workflows rather than replacing existing security controls. IDC believes this integration strategy lowers adoption barriers because enterprises can extend current security investments while improving visibility into coordinated narrative attacks that conventional technical telemetry is not designed to detect.

IDC also notes a subtle but important shift in how organizations approach narrative-based threats. Traditional social listening, sentiment analysis, and many narrative intelligence platforms primarily focus on *what* is being communicated. Behavioral threat intelligence instead seeks to understand *who* is coordinating activity by analyzing relationships between actors, behavioral synchronization, amplification patterns, and cross-platform interactions. IDC believes these approaches are complementary rather than mutually exclusive, with behavioral intelligence providing an additional layer of context that is increasingly valuable

as AI-generated content becomes easier to produce and more difficult to distinguish from authentic communications.

Beyond security operations, the discussion with AI Uniti highlighted a diverse range of enterprise use cases spanning financial market manipulation, geopolitical influence campaigns, brand protection, regulatory investigations, competitive intelligence, and mergers and acquisitions (M&A) due diligence. These examples demonstrate that behavioral intelligence is expanding beyond traditional cybersecurity use cases into broader enterprise risk management, where digital narratives increasingly influence market value, executive credibility, regulatory outcomes, and customer trust. As organizations seek to better understand whether negative narratives are organic or artificially coordinated, behavioral intelligence is emerging as an additional source of enterprise risk intelligence rather than simply another monitoring capability.

A notable differentiator presented during the discussion was AI Uniti's emphasis on deterministic evidence chains rather than probabilistic AI scoring. Unlike many AI-enabled security products that provide confidence scores with limited visibility into how conclusions are reached, AI Uniti's platform seeks to provide explainable behavioral evidence that can support enterprise investigations, legal proceedings, regulatory reporting, and executive decision-making. As AI adoption accelerates across security operations, IDC expects explainability and auditability to become increasingly important design principles, particularly for organizations operating in highly regulated industries.

AI Uniti has also expanded Signal beyond behavioral coordination detection by integrating deepfake detection across image, audio, and video into the same investigative workflow. This enables organizations to assess both who is coordinating a campaign and whether the associated content is synthetic through a unified investigation process. The company has further introduced AI answer-layer monitoring across leading foundation models, customer-scoped investigative AI agents, and LLM Protect, a runtime governance capability designed to secure enterprise AI agents. AI Uniti has also extended these capabilities through Model Context Protocol (MCP) integrations, enabling behavioral investigations to be initiated directly from enterprise AI assistants and embedded within agentic AI workflows. Collectively, these developments indicate that AI Uniti is extending its portfolio beyond behavioral threat detection toward AI trust and governance capabilities that address both human- and AI-generated influence operations.

IDC believes this expansion aligns with broader market trends. *IDC FutureScape: Worldwide Security and Trust 2026 Predictions — Asia/Pacific (Excluding Japan) Implications* predicts that by 2028, 50% of enterprises deploying agentic AI across APEJ will require an AI bill of materials (AI BOM) to support continuous security assurance, governance, and compliance. IDC also predicts that by 2028, 10% of enterprise PC users across APEJ will have deepfake detection capabilities running locally, reflecting the growing

importance of verifying digital authenticity alongside traditional cybersecurity controls. Furthermore, IDC predicts that by 2028, 85% of organizations across APEJ will experience phishing attacks leveraging synthetic identities that combine authentic and AI-generated information. Collectively, these predictions highlight a broader shift toward securing not only AI models but also AI-generated content, synthetic identities, AI agents, and the trustworthiness of digital interactions. As organizations face increasingly sophisticated influence operations and AI-enabled deception, technologies capable of correlating behavioral signals with content authenticity are likely to become an increasingly important component of enterprise cyber resilience. AI Uniti's recent expansion into LLM Protect, AI answer-layer monitoring, integrated deepfake detection, and behavioral investigations reflects this broader evolution from AI security toward AI trust and governance.

From a market perspective, IDC views AI Uniti as operating across several adjacent technology domains, including digital risk protection, cyberthreat intelligence, narrative intelligence, AI trust and governance, and brand risk intelligence. Rather than competing directly within any one of these established categories, the company is positioning behavioral threat intelligence as a complementary intelligence layer focused on coordinated influence operations. This positioning creates opportunities for differentiation while reflecting the characteristics of an emerging market, where dedicated budgets, procurement models, evaluation criteria, and organizational ownership are still evolving.

Behavioral threat intelligence is emerging as a cross-functional buying decision precisely because narrative manipulation does not sit neatly within any single risk owner's domain — it touches financial integrity, legal exposure, operational resilience, and executive credibility simultaneously. This creates distinct, complementary use cases across the stakeholder groups most exposed to coordinated influence campaigns:

- **CISOs.** As AI-generated disinformation increasingly converges with traditional cyberthreats, CISOs need behavioral intelligence as an additional layer of SOC visibility, one that enriches existing SIEM, SOAR, and threat intelligence workflows rather than requiring a separate monitoring stack.
- **CFOs/investor relations.** Coordinated narratives designed to manipulate stock price, distort earnings sentiment, or spread false financial claims directly threaten market capitalization and shareholder value; behavioral evidence helps distinguish organic market chatter from deliberate, coordinated manipulation before it materially affects trading activity.
- **General counsel.** Deterministic, evidence-backed investigations (rather than probabilistic AI scoring) provide the traceable, defensible documentation needed to support litigation, regulatory filings, and law enforcement referrals when disinformation or coordinated attacks create legal exposure.

- **Chief risk officers (CROs).** As AI-generated disinformation is increasingly recognized as a cyber resilience issue rather than solely a communications problem, CROs need visibility into coordinated influence operations as a formal category of enterprise risk, alongside more traditional technical and operational threats.
- **CEOs.** Personal or executive-targeted narrative attacks can directly threaten leadership credibility and tenure; CEOs facing reputational threats, whether from activist campaigns, competitors, or coordinated actors, have a direct stake in early detection and evidence-based response.
- **Chief communications officers (CCOs).** CCOs are often the first to feel the operational impact of coordinated narratives across social platforms and need real-time intelligence briefs and remediation guidance to respond quickly and protect brand trust before a narrative escalates.
- **Government affairs.** Coordinated influence campaigns increasingly target policy debates, elections, and regulatory processes; Government affairs teams need behavioral evidence to identify inauthentic activity that could shape public discourse or invite regulatory scrutiny of the organization's own conduct.

Looking forward, IDC expects organizational ownership to become more clearly defined as enterprises increasingly formalize digital trust and AI governance strategies.

Behavioral threat intelligence remains an emerging area within enterprise security rather than a well-defined technology category. As synthetic content, AI-enabled deception, and coordinated influence operations become increasingly sophisticated, IDC expects enterprises to place greater emphasis on understanding how information propagates, who is coordinating campaigns, whether digital content can be trusted, and how AI-driven influence operations can be governed and investigated. Vendors that successfully combine behavioral intelligence, content authenticity, explainable AI, deterministic investigations, and seamless integration into existing security operations will be well positioned to support the next phase of enterprise cyber resilience and digital trust.

Ultimately, behavioral threat intelligence should not be viewed as a replacement for traditional cyberthreat intelligence but as an additional intelligence layer that extends enterprise visibility into digital trust, coordinated influence, and AI-enabled deception. As synthetic content continues to proliferate and influence campaigns become increasingly difficult to distinguish from legitimate digital activity, organizations will require technologies capable of establishing confidence not only in the authenticity of digital content but also in the behavior, coordination, and intent of those distributing it.

LEARN MORE

Synopsis

This IDC Market Note reflects IDC's observations following its discussion with AI Uniti and examines the emergence of behavioral threat intelligence as an evolving area within enterprise cybersecurity.

"Behavioral threat intelligence reflects a broader evolution in enterprise security. The convergence of behavioral analytics, AI governance, and digital authenticity is creating a new operational intelligence layer within enterprise security. As AI-generated content continues to reduce the effectiveness of traditional content-centric detection, organizations must increasingly correlate behavioral telemetry, cross-platform activity, content authenticity, and AI governance to distinguish coordinated influence operations from legitimate digital activity. Rather than viewing narrative manipulation solely as a communications challenge, enterprises are beginning to recognize it as a cyber resilience issue that demands explainable AI, deterministic evidence, and behavioral intelligence to support operational, regulatory, and executive decision-making. The next generation of security platforms will be defined not only by what they detect but by how they establish trust in increasingly AI-mediated environments," says Sakshi Grover, senior research manager, Cybersecurity Products and Services, IDC Asia/Pacific.

"One of the more compelling arguments for behavioral threat intelligence is not just organizational; it is personal. When a company adopts this capability at the enterprise level, its executives get a direct, secondary benefit: their own names, likenesses, and reputations are now being monitored for the same coordinated targeting and deepfake impersonation that threatens the brand. For a CEO or director who has watched a colleague's career damaged by a synthetic video or a coordinated narrative campaign, that is not an abstract capability. It is personal risk reduction, delivered as a byproduct of a broader security investment," adds Craig Robinson, research vice president, Security Services, IDC.

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

IDC India (Delhi)

IDC Centre for Consultancy and Research Pvt.Ltd,
Unit no.221-223, Vipul Plaza, 2nd Floor,
Sector 54, Golf Course Road,
Gurgaon Haryana 122002.
+91 124 476 2300
X: @IDC
blogs.idc.com
www.idc.com