GrackerAI Launches Industry's First Generative Engine Optimization Platform for Cybersecurity SaaS Companies

Platform helps cybersecurity GTM teams capture AI-driven buyer demand as 40% of security decision-makers shift from Google to AI assistants for vendor research

SAN FRANCISCO, CA, UNITED STATES, January 20, 2026 /EINPresswire.com/ -- GrackerAI today announced the launch of cybersecurity industry's first Generative Engine Optimization (GEO) platform, designed to help cybersecurity SaaS companies measure and systematically improve their brand visibility across AI-powered search engines including ChatGPT, Claude, Gemini, Perplexity, and Google AI Overviews.

The launch addresses a critical challenge reshaping cybersecurity go-to-market strategies: while companies invest heavily in traditional search engine optimization, security buyers increasingly use AI assistants to research solutions—creating a new visibility gap that conventional SEO strategies fail to address. Industry data indicates that 40% of B2B buyers now rely on AI assistants for software research, with CISOs and security architects showing particularly high adoption rates when evaluating threat detection, cloud security, and identity management solutions.

> **"**Buyers now ask AI for IAM solutions, SIEM alternatives, & zero-trust platforms rather than relying on Google. If your brand isn't in that AI response, you're not in the buying conversation."
>
> *Deepak Gupta, CEO and Co-founder of GrackerAI*

"Cybersecurity buyers now ask AI for recommendations on IAM solutions, SIEM alternatives, and zero-trust platforms rather than relying on Google. If your brand isn't in that AI response, you're not in the buying conversation. It's that simple," said Deepak Gupta, CEO and Co-founder of GrackerAI. "We've observed cybersecurity companies ranking #1 on Google for their core solutions remain

completely invisible when prospects ask ChatGPT or Claude for vendor recommendations. That disconnect is costing companies millions in lost pipeline."

The Market Shift: From Search Rankings to AI Citations

The traditional cybersecurity marketing playbook—built on Google rankings, paid search, and content marketing—is becoming less effective as buyer behavior fundamentally shifts. According to recent industry analysis, AI-powered search now influences approximately 40% of initial vendor discovery in the cybersecurity sector, yet most security companies have zero visibility in AI-generated recommendations.

This creates a critical challenge for GTM teams: prospects are forming vendor shortlists through AI conversations before ever visiting company websites or engaging with traditional marketing channels. Companies invisible in AI responses are excluded from consideration before sales teams have any opportunity to engage.

"The gap between SEO rankings and AI citations is massive in the cybersecurity space," said Govind Kumar, CTO and Co-founder of GrackerAI. "Security teams searching for vulnerability management, compliance automation, or threat intelligence get AI recommendations that often exclude companies who dominate traditional search rankings. This isn't a marginal optimization—it's a fundamental shift in how buyers discover and evaluate security vendors."

Platform Combines Real-Time Visibility Tracking with Automated Content Optimization

The GrackerAI platform addresses both measurement and improvement of AI search visibility through an integrated approach designed specifically for cybersecurity GTM teams.

Visibility Monitoring:
The system provides real-time tracking of brand mentions across all major AI platforms,

competitive citation analysis showing where competitors appear and you don't, topic identification revealing which security queries trigger brand mentions, and page-level attribution showing which technical content AI engines cite as authoritative sources.

Automated Content Generation:
The platform generates cybersecurity-specific content optimized for AI citation including threat intelligence articles, CVE vulnerability databases, security compliance centers, technical comparison pages, breach analysis reports, and security framework documentation. All content is automatically structured to match the patterns AI engines favor when selecting sources for security-related queries.

Technical Accuracy at Scale:
GrackerAI integrates with over 200 authoritative cybersecurity data sources including the National Vulnerability Database (NVD), MITRE CVE Database, CISA Known Exploited Vulnerabilities, and ExploitDB. This ensures auto-generated security content maintains the technical accuracy required for cybersecurity audiences while optimizing for AI citation patterns—a critical balance for building trust with security professionals.

Early Results Demonstrate Substantial GTM Impact

According to company data, early adopters in the cybersecurity sector have achieved measurable improvements within 60-90 days of implementation. Aggregate results across cybersecurity clients show:

- Average 40% increase in AI visibility scores within 90 days
- 40-80% growth in AI-referred signups for security platforms
- 100-200% increases in organic traffic from quality and optimized content
- 3-5x higher conversion rates from AI-referred visitors compared to traditional search
- 20-35% improvement in qualified security lead volume

Platform data indicates that security companies implementing GEO strategies see particularly strong results in competitive categories where traditional differentiation is difficult—such as CNAPP, SIEM, CSPM, and identity management—where AI recommendations heavily influence shortlist formation.

GTM Implications for Cybersecurity Companies

For cybersecurity GTM leaders, the shift to AI-driven buyer research creates both risk and opportunity. Companies failing to establish AI visibility face systematic exclusion from buying conversations, while early movers can capture disproportionate demand in their categories.

The platform enables several strategic GTM advantages:
1. Category Leadership Positioning: Establish brand as the cited authority when prospects ask AI

about specific security categories or use cases.

2. Competitive Displacement: Appear in AI responses where competitors currently dominate recommendations, capturing demand before prospects reach competitor websites.

3. Technical Credibility: Demonstrate expertise through cited content that answers complex security questions with technical accuracy.

4. Pipeline Acceleration: Attract higher-intent prospects who arrive with AI-validated understanding of your solution category and use cases.

Platform Availability and Cybersecurity Focus

GrackerAI offers a free Seed plan allowing cybersecurity companies to test the platform with up to 50 optimized security-focused pages. Paid growth plans provide expanded capabilities including multiple programmatic SEO (pSEO) portals for CVEs and compliance frameworks, automated security content generation, cybersecurity-specific AI models trained on threat intelligence and industry terminology, and real-time data integration from authoritative security sources.

The platform is available immediately at portal.gracker.ai. GrackerAI is backed by NVIDIA Startups Program, Cloudflare Launchpad, Microsoft for Startups, and maintains strategic partnerships with OpenAI and Anthropic (Claude).

About GrackerAI

GrackerAI is a San Francisco-based B2B SaaS company specializing in AI search optimization for cybersecurity and enterprise software companies. The company pioneered the Generative Engine Optimization (GEO) category to address the fundamental shift from traditional search to AI-assisted vendor research. GrackerAI helps cybersecurity GTM teams measure their standing in AI search results, identify visibility gaps versus competitors, and create technically accurate content that gets cited by AI engines.

For more information, visit https://gracker.ai

Media Team
GrackerAI
+1 855-513-4769
media@gracker.ai
Visit us on social media:
LinkedIn
Bluesky
X

Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.