GRACKERAI RESEARCH REPORT

How B2B Cybersecurity Buyers Use AI Assistants

Prompt Patterns & Purchase Behavior

Published February 2026 · 250 Buyer Prompts Analyzed · 6 AI Platforms · CISO, Security Analyst, IT Manager Personas

Executive Summary

AI assistants are reshaping how cybersecurity professionals discover, evaluate, and shortlist vendors. This report examines the specific prompt patterns, platform preferences, and purchase behaviors of cybersecurity buyers using AI assistants — revealing the AI-informed CISO who builds vendor shortlists before ever visiting a company website.

90%

of B2B buyers used generative AI during their purchase journey in 2025 (Forrester)

73%

of B2B tech buying journeys now complete in 12 weeks or less (Google/NRG, Dec 2025)

58%

of B2B buyers switched vendors in the past 6 months — AI is disrupting incumbency

34%

of qualified B2B leads now originate from AI search — the #2 lead source (10Fold, 2025)

1. The AI-Informed Cybersecurity Buyer

1.1 Who Is Using AI for Purchase Research?

Senior decision-makers — CISOs, VPs of Security, and Security Architects — are among the most active AI search users for vendor evaluation. These buyers face complex, multi-vendor decisions with high stakes and limited time for manual research.

Buyer Persona	Primary AI Use Case	Preferred Platform	Prompt Complexity
CISO / VP Security	Vendor shortlisting, architecture validation	ChatGPT, Perplexity	High — multi-variable
Security Architect	Technical comparison, integration research	Perplexity, Claude	Very High — protocol-level
SOC Manager	Tool comparison, workflow optimization	ChatGPT, Gemini	Medium — operational focus
IT Director	Budget analysis, feature comparison	ChatGPT, Google AIO	Medium — ROI focused

1.2 When in the Buying Journey?

- **Phase 1 — Problem Framing (30% of prompts):** "What's the difference between XDR and SIEM?"
- **Phase 2 — Vendor Shortlisting (45% of prompts):** "Best endpoint security for mid-market financial services?" — highest pipeline impact.
- **Phase 3 — Deep Evaluation (25% of prompts):** "Does [Vendor X] support MITRE ATT&CK; mapping natively?"

2. Prompt Pattern Taxonomy

The Seven Prompt Archetypes

Archetype	Pattern	Example	Frequency
Category Explorer	"What is / What are..."	"What are the leading ZTNA solutions?"	18%
Best-In-Class Seeker	"Best / Top / Leading..."	"Best SIEM tools for SOC teams under 20"	24%
Head-to-Head Comparer	"[A] vs [B]"	"CrowdStrike vs Defender for healthcare"	19%
Constraint-Based	"Best X for [constraint]"	"Best EDR for 500-person fintech with SOC 2"	15%

Archetype	Pattern	Example	Frequency
Alternative Seeker	"Alternatives to [Vendor]"	"Alternatives to Palo Alto for mid-market"	9%
Technical Validator	"Does [Vendor] support..."	"Does Wiz integrate with Terraform?"	8%
Risk Assessor	"Problems with..."	"Common complaints about Splunk pricing"	7%

The "Stack Query" Phenomenon

A unique cybersecurity behavior: buyers ask AI to recommend entire security stacks rather than individual tools. "Design a complete security stack for a 500-person SaaS company with $500K annual budget." These queries recommend 5–8 vendors simultaneously — massive pipeline opportunities for vendors with content explaining where their product fits in the broader security architecture.

3. Platform-Specific Buyer Behavior

- **ChatGPT (400M+ weekly users):** Most common starting point. Multi-turn conversations (3–5 turns). Heavy Wikipedia citation bias (48%). Buyers treat as starting point, not final authority.
- **Perplexity:** Preferred by technical buyers wanting sourced, real-time info. Cites vendor websites most frequently (19%). Visible citations build brand trust.
- **Google AI Overviews:** Ambient influence — appears during regular searches (16%+ of results). CTR drops 34.5% when AIO appears. Draws exclusively from Google's index.
- **Claude:** Favored by technical architects for deep-dive analysis. Emphasis on accuracy makes it a trust-building citation source.
- **Gemini:** Usage correlates with Google Workspace adoption. Leverages Google Knowledge Graph extensively.

4. What Makes Buyers Trust AI Recommendations

Trust Level	Source Type	Buyer Behavior
Highest	AI cites recognized analyst firm (Gartner, Forrester)	Accepts with minimal verification
High	AI cites multiple independent sources agreeing	Proceeds to vendor website
Moderate	AI cites vendor's own documentation	Cross-references with review sites
Low	AI provides recommendation without visible sources	Searches independently to validate

The Verification Loop

67% of cybersecurity buyers take additional steps after an AI recommendation: cross-platform check (42%), source investigation (38%), peer validation (29%), review site confirmation (25%).

> ***Implication:*** *Being cited by AI is necessary but not sufficient. Your website, review profiles, and third-party coverage must all reinforce the AI recommendation when buyers verify.*

5. The Prompt-to-Purchase Pipeline

Pipeline Stage	Prompt Pattern	Content Needed	Conversion Impact
Awareness	"What is zero trust?"	Educational content, glossaries	Low direct, high brand impression
Consideration	"Best EDR tools for healthcare"	Listicles, comparison pages	Medium — enters consideration set
Evaluation	"[Vendor A] vs [Vendor B]"	Comparison matrices, alt pages	High — influences shortlist
Validation	"Does [Vendor] support [feature]?"	Technical docs, integration guides	Very High — confirms/eliminates
Decision	"[Vendor] pricing"	Transparent pricing, ROI calculators	Highest — triggers purchase

The typical purchase-related AI journey involves 8–15 distinct prompts spread across 2–4 sessions over 1–3 weeks. Vendors cited consistently across all stages have the highest shortlist probability.

6. Recommendations for Cybersecurity Vendors

- **Map your prompt coverage.** Identify the 50 most common buyer prompts in your category. Most vendors cover fewer than 20%.
- **Create constraint-ready content.** Address specific buyer constraints (company size, industry, compliance, budget, tech stack).
- **Invest in integration documentation.** Every integration needs a dedicated, technically detailed page.
- **Build honest comparison content.** Balanced comparisons that acknowledge competitor strengths earn more citations.
- **Prioritize Perplexity and Google AI Overviews.** Highest-quality cybersecurity buyer traffic.
- **Support the verification loop.** Ensure website, review profiles, and third-party coverage reinforce AI recommendations.
- **Update content monthly.** Content older than 90 days loses citation eligibility rapidly.
- **Track multi-prompt journeys, not single citations.** Measure visibility across the full buyer journey.

About This Research

Based on analysis of 250 cybersecurity buyer prompts tested across six AI platforms (Sep 2025 – Jan 2026). Supplemented by published research from Forrester, Gartner, Google/NRG, and 10Fold Communications. GrackerAI is the pioneering AI-powered AEO and GEO platform for B2B SaaS companies.

Get Your Free AI Visibility Audit

See how your brand performs across AI platforms — benchmarked against competitors. Visit **portal.gracker.ai** to start your free analysis or **gracker.ai/demo** to book a demo.