
AEO for Cybersecurity: What Gets a Security Vendor Cited

51% of B2B buyers now open an AI chatbot first. Why gated security content can't be cited, the three buyers in every cyber deal, and a ninety-day fix for a team of four.

Kapil Raina

Principal, Cyber GTM, LLC
[linkedin.com/in/kapilraina](https://www.linkedin.com/in/kapilraina)

October 2026

An easy way to generate inbound leads? Get your prospect to raise their hand and reach out to you directly through the content you have already created.

Plenty of agencies claim they can do this quickly. I have been getting three answer-engine pitches a week, most of them recycled SEO decks with the nouns swapped. That is why I went and looked at the research myself rather than taking anyone's deck at face value, and what I found doesn't match what's being sold.

(At the end I share the tl;dr — and how you can see where your company stands and what to do about it.)

The agency or tool pitch is usually about restructuring your website. The evidence says on-page work is the weakest lever available, and done carelessly it makes things worse. Almost everything that matters happens on property you don't own.

Start with the size of the shift. G2 surveyed 1,076 B2B buyers and decision-makers in March 2026:

- **51%** now start product research with an AI chatbot rather than Google, up from 29% a year earlier
- **69%** ended up choosing a vendor other than the one they walked in planning to choose
- **33%** bought from a company they had never heard of before that conversation started

That last number is the one worth sitting with if you're marketing a Seed-to-Series-B security product. A third of purchases now go to a vendor who wasn't on the list at the start. That is the most open discovery channel this category has had since it consolidated.

How the answer actually gets built

Before the implication, let's look at the mechanism.

An arXiv study ran 1,000 ranking prompts across ten product categories on Perplexity, Claude, Gemini and GPT-4o, then classified every cited domain as brand-owned, earned, or social. In one consumer category, GPT's citations ran 92% earned sources. Google, on the same queries, pulled 33% from brand-owned pages.

The engine retrieves a small set of third-party sources and writes the answer from those. Two to seven domains, typically, against Google's ten blue links.

Which separates two things we've treated as one thing for twenty years: getting traffic and getting cited. Your site can rank perfectly well, pull respectable organic, and never once enter the answer a buyer is reading.

You can't gate your way into an answer

Now count your own library. Say you have eight substantive assets from the last two years. The threat research. A reference architecture. A detection engineering guide. The Magic Quadrant or Wave reprint you licensed. How

many sit behind a form?

I get it, forms generate leads which you can directly attribute to marketing. Can you generate enough in today's hyper-competitive world that way? (There are other ways to compensate — I am happy to share strategies there if you are interested.)

A form is a wall to a crawler. The most citable work our category produces sits in the one place it cannot be cited, and we've been measuring that decision in MQLs.

Nobody made a bad call here, and I want to be clear about that, because the reflex in posts like this one is to imply marketing teams weren't paying attention. Gating was correct for fifteen years of search-indexed discovery. It paid for pipeline, it fed sales, and every one of us defended it in a QBR. The layer underneath moved.

The analyst reprint is the version that still gets me. Six figures for third-party validation, and it lands on a campaign subdomain behind a form where no crawler will ever reach it. You bought a sales asset and told yourself you bought authority. Worse still, a competitor licenses the same report, builds an ungated page around it, and captures that authority instead.

There's a fix that costs nothing: split the asset. The analysis, the definitions, the charts and the argument go ungated as HTML on a domain you control. The dataset, the assessment template, the calculator, the full PDF stay behind the form. You keep the capture mechanism and stop hiding the citable layer.

Cloudflare has run the extreme version of this for years. The Cloudflare Learning Center is sixteen topic hubs across DDoS, DNS, SSL/TLS, SASE, bots, email security and AI, one concept per URL, no form anywhere: cloudflare.com/learning. And if someone on your team argues that ungated means lightweight, send them Snyk's Snyk Learn. The lessons are fully readable without a login, including interactive attack simulators and vulnerable-versus-secure code in nine languages — only the quizzes and progress tracking need an account: learn.snyk.io. The signup sits on the page, not in front of it.

Then run the number almost nobody in cyber has run. Of the MQLs that gate produced last quarter, how many became qualified pipeline? At most companies the honest answer makes this a short conversation.

Security doesn't have a buyer. It has three.

This is where playbooks imported from general SaaS fall apart, and it's the part most AEO advice gets wrong about our category specifically.

One is the economic buyer. Your CISO, joined by the CIO or CFO once consolidation is on the table. The questions come framed as decisions rather than products: what controls do we need before a SOC 2 Type II, how do we get from twelve tools to six, what does the board need to see about our SEC 8-K materiality process. They work in National Institute of Standards and Technology (NIST) CSF 2.0 functions, Cloud Security Alliance

guidance, ISO 27001 Annex A controls, FAIR, cyber insurance underwriting language. They verify with other CISOs, in a private Slack or at an Evanta, a Gartner Company dinner.

The other is the technical evaluator. Security architect, cloud security lead, IAM architect, platform engineer, and others. Their whole question is fit. For example, where does this sit, what identity does it need, how tightly can that role be scoped, what's the blast radius when it fails at 2am. NIST SP 800-207, OCSF, SCIM and SAML and OIDC, eBPF versus kernel module, data residency. This person reads your documentation before your website and judges you on whether the docs are honest about limitations.

And then finally the operator, including the SOC analyst at any tier, detection engineer, threat hunter, IR lead, AppSec engineer, red teamer, and others. What they want to know is whether it survives reality in production: tuning burden, false-positive rate, what the queue looks like on day 30. MITRE ATT&CK technique IDs, Sigma and YARA, detection-as-code, MTTD and MTTR, Atomic Red Team. They verify on r/netsec and r/blueteam, in DFIR Discord servers, in your GitHub issues, and in whatever Clint Gibler's tl;dr sec or Zack Allen's Detection Engineering Weekly said about your space last Tuesday.

Economic buyer, technical evaluator, operator. Three question shapes, three vocabularies, three verification surfaces, and content written for "the security buyer" retrieves cleanly for none of them.

One thing to settle before you write anything: which of the three is your entry point. It varies by category and getting it wrong is expensive. GRC and compliance tooling enters through the economic buyer. Detection, response and AppSec enter through the operator. Identity, cloud infrastructure security and most platform plays enter through the architect. Write board briefs for a category whose real entry point is a detection engineer and you'll produce a year of content nobody retrieves.

Worth noting that in security the operator both starts the evaluation, because someone has to say "we should look at this," and can end it. The surface most vendors deliberately avoid is the one holding veto power.

For what an architect-facing asset looks like when it's built to be retrieved, Wiz (now part of Google) has a page defining agentless versus agent-based scanning that treats both approaches fairly, including the one Wiz doesn't sell, before it positions anything. Boundary content answers the comparison question directly, which is the shape engines resolve first, and almost nobody in security produces it.

Why "better ASPM" can't be retrieved

Four companies currently call themselves the AI SOC analyst. Ask an engine about AI SOC analysts and it returns closer to a hundred names, which is the same as returning none of them. One has already moved to "the Agentic SOC" to get out of the crowd.

Two different problems get mashed into one word here. Optimization is placing well inside a set of candidates. Entry is getting into the set at all.

Olivier Martinez’s critical survey of 45 GEO studies found that measured optimization gains are “conditional on a source already being present in a fixed context,” and that no reviewed technique shows a durable cross-platform effect on organic discoverability. Across 171,003 documents, body-only rewrites actually cut top-10 presence after reranking by roughly 16%.

So how efficient can you really be with a “rewrite the page and hope” approach if you’re not in the candidate set to begin with?

For an early-stage company, entry is the whole problem, and entry is dramatically cheaper on a narrow question with a name attached. “Better ASPM” has maybe four hundred pages already saying it. The engine picks a few and you’re not among them. “Why agent-based tooling fails in OT environments where you can’t patch the endpoint” has almost nothing written about it. Same writing effort, completely different odds.

From my Preempt Security days (which was acquired by CrowdStrike): we were a sub-\$10M company inside a category the incumbents already owned, and nothing we said about the category itself moved anything. The narrow arguments did — in our case focusing on Zero Trust as we joined CrowdStrike. The Zero Trust page I developed on CrowdStrike.com became one of the ten most visited pages on the site, precisely because of the structure, the citations, the narrow POV (and their amazing SEO/AEO team).

Chainguard is running the disciplined version of this right now. “Zero known CVEs,” plus published per-image vulnerability comparisons inviting you to check the claim yourself — here’s the Python one: edu.chainguard.dev/chainguard/chainguard-images/vuln-comparison/python. Node, Bash, Maven, PHP, Git, etcd and MinIO each have their own.

Note the word “known.” The hedge is what makes the claim survivable under scrutiny, and a claim you can defend beats a claim that sounds bigger.

Three tests before you commit to a point of view. Can someone outside your company restate it in one sentence after one read? Does it make an enemy — and if nobody would argue with it, is it a position or just a description? Is it falsifiable?

Analyst relations moved line items

Gartner and Forrester still matter for the enterprise deal. I’ve bought Tier 1 coverage more than once and I’d buy it again. What changed is what it’s for: analyst relations is a distribution channel now, and most of us are still budgeting it as credibility. Different purchases. Credibility gets cited in a sales deck. Distribution gets cited by an engine. Only one of them has to be crawlable.

Tier 1, meaning Gartner and Forrester and IDC, is expensive, slow and mostly paywalled. In the answer layer the crawlable artifact is the press release announcing your placement, not the report. And now some of the reports

come with user-adjustable weights, so they don't always guarantee the exact positioning you would like to see for each user.

Tier 2 is GigaOm, Omdia (part of Informa TechTarget), IDC, KuppingerCole Analysts (the serious one in identity), Enterprise Strategy Group, Constellation, RedMonk, EMA. Cheaper, faster, far likelier to appear in crawlable form. A Series A security company has a realistic path into a GigaOm Radar this year and none at all into a Magic Quadrant.

Tier 3 is where cybersecurity is genuinely unlike any other B2B category. We have a real independent analyst layer (albeit some are direct pay to play), ungated by default and increasingly cited by name: James Berthoty at Latio, Francis Odum at Software Analyst Cyber Research, Clint Gibler at tl;dr sec, Chris Hughes at Resilient Cyber, Zack Allen at Detection Engineering Weekly, Ross Haleliuk at Venture in Security, Mike Privette at Return on Security.

The proof this tier carries commercial weight: Dynatrace issued a press post about being named a Cloud Security Innovator in Berthoty's 2025 Cloud Security Market Report, and Sweet Security built a landing page around coverage from the same one-person firm. Berthoty publishes at pulse.latio.tech.

Paywalled Tier 1, crawlable Tier 2, and an independent Tier 3 that costs a calendar hour. Most security companies are funding the first and ignoring the third (and if you need a strategy for influencers, message me — happy to help).

What ninety days looks like

Most teams reading this have two to five marketing people and no agency worth the retainer, so running everything at once isn't the assignment.

First month: write the POV as one sentence, build a fixed set of 30 to 50 buyer prompts and run a baseline across ChatGPT, Perplexity, Claude and Google AI Overviews, and claim your Gartner Peer Insights and G2 profiles.

Second month: ship one canonical ungated page for your POV term, definition in the first fifty words, headings written as the questions buyers actually type. Start review generation with your ten happiest customers. Book three Tier 3 briefings, which cost nothing but calendar time.

Third month: publish the operator-facing asset, the honest one, including where your product doesn't fit. Start original research, because data collection is the long pole.

On that last one, the ceiling is higher than most early-stage teams assume. Wiz was about eighteen months old when it disclosed ChaosDB, the Azure Cosmos DB cross-tenant vulnerability, and gave it a standalone ungated microsite with an attack diagram, a disclosure timeline and named researchers: chaosdb.wiz.io. The Register and SecurityWeek covered it, which is exactly the non-routine independent coverage that both Wikipedia notability and AI retrieval reward — and that no volume of funding-announcement PR produces. No threat intel team? Publish your own telemetry. Coalition, Inc. built an annual franchise out of claims data nobody else holds.

Tell your CEO the timeline before you start. Two to three months before anything moves in a prompt set, six before there's a trend worth reporting. Promise faster and you'll lose the mandate in month three.

And when you run that prompt set, the useful output isn't your own score. It's the list of domains the engine cited instead of you. A review site you're thin on, a publication you've never briefed, a subreddit thread you weren't in, a definitional page somebody else wrote. Ten months of that column assembles your entire third-party strategy for free.

Which reframes what this work actually is. We've been treating answer-engine visibility as a content problem, and it isn't one. It's an analyst relations, community and original research problem that happens to show up in a chatbot.

Sources

- G2, *The Answer Economy*, survey of 1,076 B2B buyers, fielded March 2026 — <https://company.g2.com/news/g2-research-the-answer-economy>
- Chen, Wang, Chen & Koudas, *Generative Engine Optimization*, arXiv:2509.08919, September 2025 — <https://arxiv.org/html/2509.08919v1>
- Martinez, *Optimizing Visibility in Generative Engines: A Critical Survey*, arXiv:2607.14035, July 2026 — <https://arxiv.org/abs/2607.14035>
- Chainguard vulnerability comparison — <https://edu.chainguard.dev/chainguard/chainguard-images/vuln-comparison/>
- Dynatrace on Latio's 2025 Cloud Security Market Report — <https://www.dynatrace.com/news/blog/dynatrace-named-cloud-security-innovator-in-latios-2025-cloud-security-market-report/>

The tl;dr

I put the knowledge shared in this article — and then some — into the **CyberGTM AEO Analysis Kit**: a 40-prompt measurement set with its scoring method, a nine-dimension readiness scorecard, the gated-asset audit including cost per qualified opportunity by asset, a ninety-day plan with owners, the full three-tier analyst target list, and a six-part POV stress test. Every section closes with a live security company doing that part well, linked, so you have something to copy rather than only something to score.

If you are a cybersecurity vendor, message me and I am happy to share a free, full report on where your website sits. It not only gives an assessment, it gives a priority of what to do.