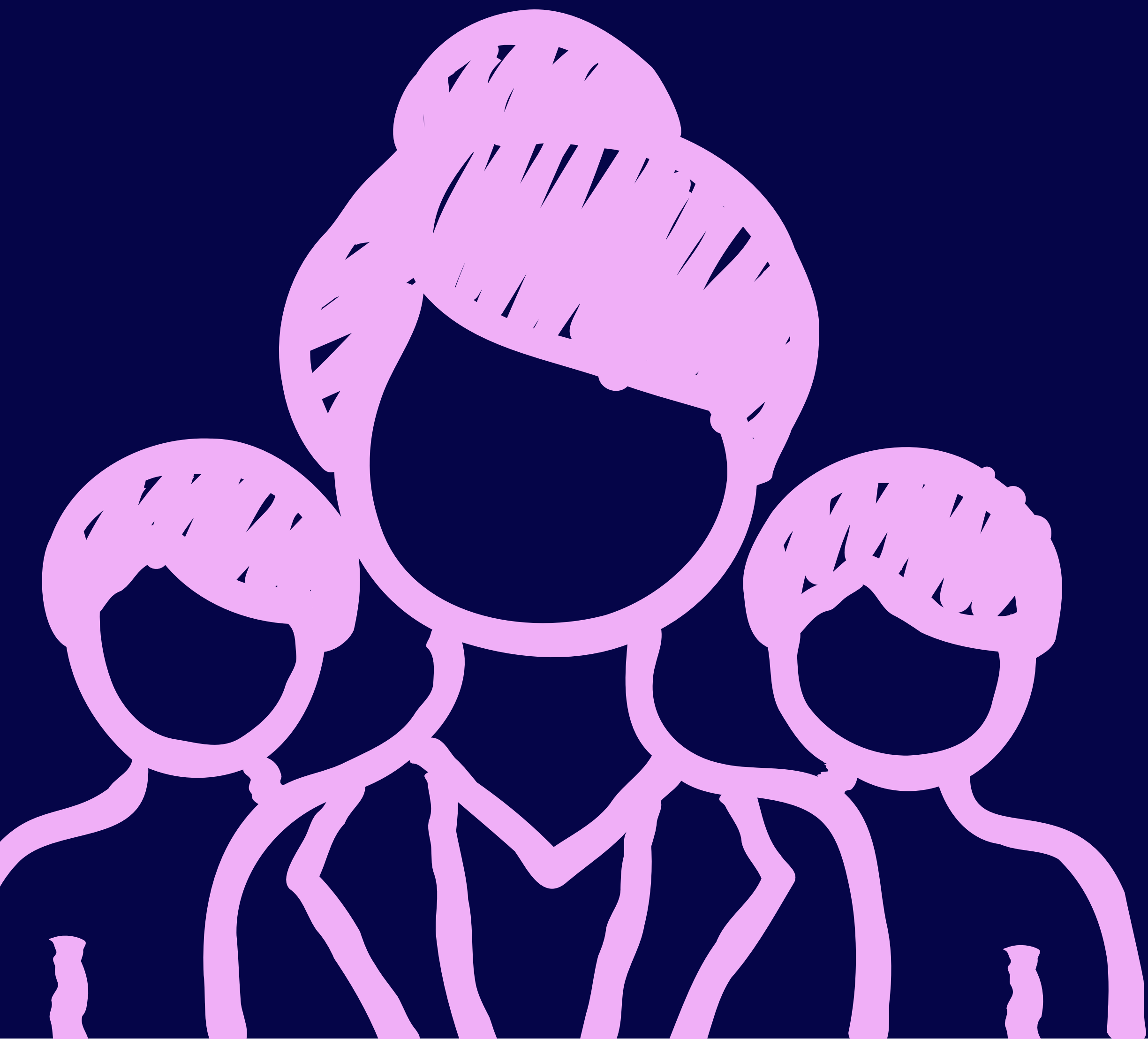


The New Early-Stage Cybersecurity PR Playbook

From Stealth to Category Credibility

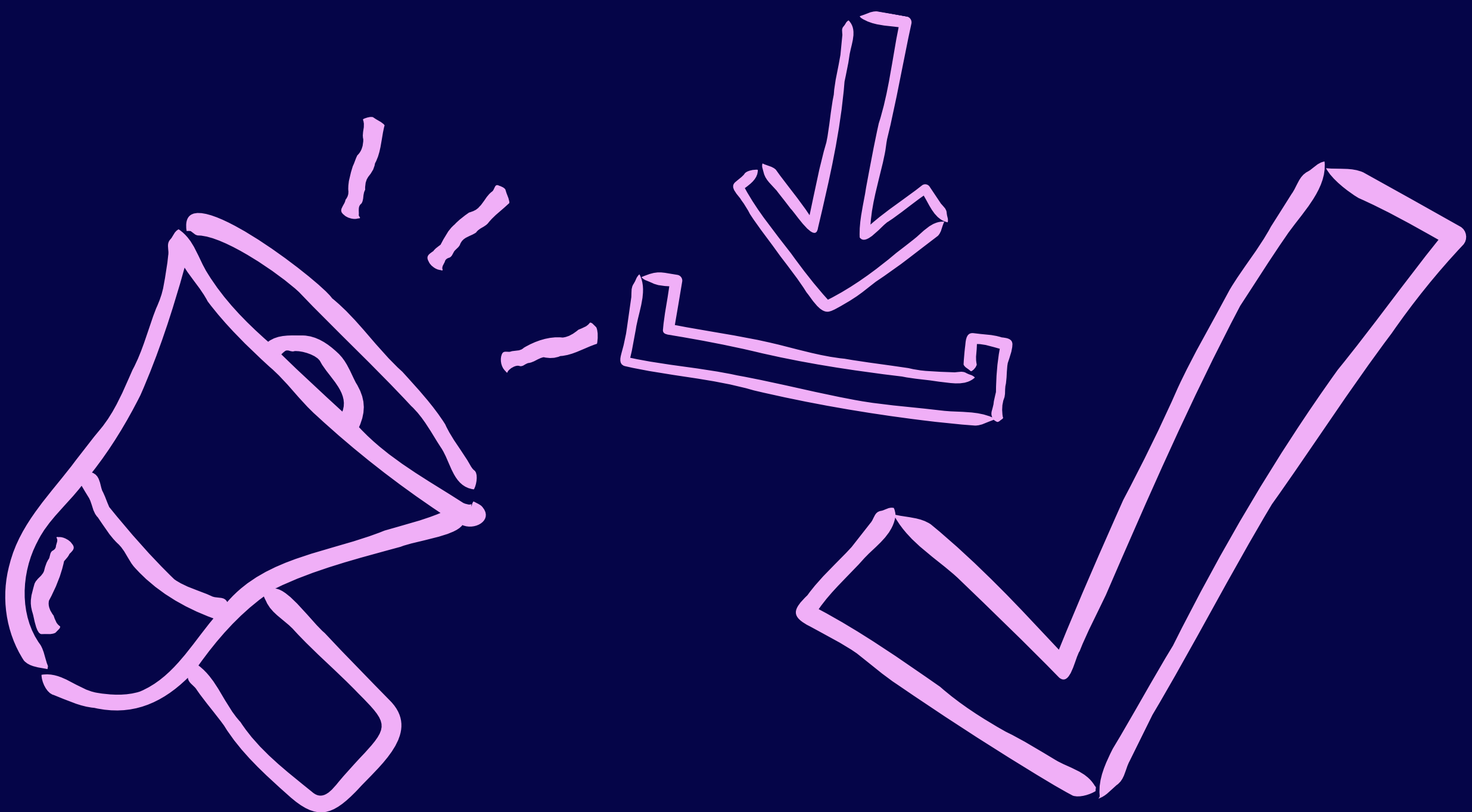


Introduction: The Narrative Gap That's Costing You Deals

In the 2000s through to the 2010s, cybersecurity followed a reliable pattern. A CEO could be confident that a genuinely differentiated product was enough to build a company on. If your detection was faster, your false positive rate lower, your architecture more elegant than what existed, you could build in the knowledge that your technical advantage was your moat against competitors.

Buyers could feel it in a proof of concept. Analysts could validate it in a briefing. Word spread through practitioner networks, and the product sold itself to the people who mattered.

The product sold itself to the people who mattered. That world is gone.



The World Has Changed — Has Your Strategy?

Early-stage companies now face a future where AI has compressed the product development cycle to the point where technical differentiation is harder to sustain, harder to demonstrate, and harder to communicate than it has ever been.

The Speed Problem

The gap between a novel architecture and a commoditised one is measured in months, not years. Your competitors are building faster. Their investors are better resourced.

The Buyer Problem

Your buyers are increasingly using AI systems — not just analyst reports or peer referrals — to form their initial shortlist of cybersecurity partners before your sales team ever gets a call.

The Narrative Gap

The distance between the quality of your technology and the credibility of your public story. In cybersecurity, where trust is the actual product, that gap is a commercial problem.

Deals stall. Evaluations exclude you. Talent chooses the company whose name they've already heard. The investor who would have led your next round passes because they don't have enough third-party validation. The good news: the narrative gap is entirely closeable — but it requires understanding that communications is not something you layer on top of your go-to-market after the product is ready. It is part of the go-to-market, running in parallel from the earliest stages.

What This Playbook Covers

This playbook breaks it down across four areas that matter most for early-stage cybersecurity companies. Each section is designed to be actionable — something you can take into a team meeting, test against your current plan, and use to make better decisions.

1

Coming Out of Stealth

When to make the transition — and how to time it for maximum narrative impact rather than product readiness alone.

2

Funding Announcements

How to make funding announcements work harder — framing, sequencing, and follow-on content that builds lasting credibility.

3

Analyst Relations

How to approach analyst relations before you think you're ready — and why waiting is costing you deals you never knew you were losing.

4

Technical Messaging

Why the technical messaging that serves you in a demo room will actively hurt you in mainstream press — and how to fix it.

Part One: Coming Out of Stealth — Timing Is Strategy

The stealth-to-public transition is one of the most consequential communications decisions an early-stage startup makes, and most get it wrong in one of two ways.

Too Late

They stay in stealth too long, missing the window to shape the market narrative before a better-resourced competitor does.

Too Early

They announce before they have the proof points, the customers, or the clarity of message to make the announcement land with the audiences who matter.

⚠️ Both outcomes are strategy failures that fast-growing startups can ill afford. The trigger for going public isn't just funding — it's **narrative readiness**.



Three Diagnostic Questions Before You Go Public

Ask yourself these three questions before you pull the trigger on any public announcement. If you can't answer all three cleanly, more runway in stealth is time well spent on narrative development.

1 Can you articulate your category in one sentence?

Not what your product does — what shift in the world makes your product necessary right now. *"We make endpoint detection faster"* is a product description. *"Attackers now move laterally in under four minutes — detection tools built for the 2026 threat landscape can't keep up"* is a category narrative. One gets a journalist to stop scrolling. One gets a CISO to forward it to their team. Don't go public until you can reliably produce the second kind.

2 Do you have a customer you can reference — even obliquely?

"A Fortune 500 financial services firm reduced mean time to detect by 60% in 90 days" is not the same as *"we are working with leading enterprises."* Specificity signals credibility. You need a vertical, a metric, a timeframe — something that tells the reader this technology has been stress-tested by a real security team in a real environment. Influencers in the press and social media are always looking for the next gamechanger; this extra layer of evidence ensures people will sit up when they read your news.

3 Is your founding team's story coherent and on-record?

In cybersecurity, the team is the first proof point. Before your product has public validation, reporters and analysts are making an early-stage bet on whether the people behind it have the pattern recognition to solve the problem they're claiming to solve. Get your origin story straight, consistent, and compelling before you go anywhere near a journalist. What you saw in the market, why existing solutions failed, why this team is the one to fix it — and make sure every founder tells that story the same way.

✔ **If you can answer all three cleanly, you are ready.** If you can't, more runway in stealth is time well spent — and will give you invaluable clarity on your messaging and positioning that will bear dividends further down the line.

The Competitive Clock Argument

Stealth is not a competitive moat. If you're building in a hot category — and in 2026, most of cybersecurity qualifies — your competitors are building their story while you're head down just building your product.

Media Framing Is Sticky

A journalist who writes the defining story about a new category tends to call the same company the next time the topic is live. The companies that own the category narrative in year one rarely lose it.

Analyst Vocabulary Compounds

A Gartner analyst who includes a vendor in an early Innovation Trigger note keeps tracking them. Early inclusion shapes how the entire market thinks about your space.

GEO Strategy Dominates AI

The company with a long-term Generative Engine Optimisation (GEO) strategy driving out high-quality, trusted content will top the responses on all the key LLMs — and be difficult to dislodge.

The cost of a premature announcement is manageable — you can iterate the message, add proof points, refocus the narrative. The cost of a rival owning your category narrative before you've spoken publicly is structurally harder to reverse.

⊗ **The Golden Rule:** You can't reclaim a category story that someone else has already filed. When in doubt, lean towards narrative readiness over perfect product readiness.

Part Two: Funding Announcements — How to Make Them Work Harder

A funding announcement is the single most reliable piece of news a startup will ever have. The round closed, the numbers are real, and the investors carry brand weight you can borrow.

Used Well

- Establishes category positioning
- Introduces your founding story to a new audience
- Creates a pipeline of follow-on coverage
- Gives your sales team social proof that shortens enterprise evaluation cycles

Used Badly

- Generates one day of news
- A few trade press pickups
- Disappears without trace inside a week
- Leaves no lasting narrative asset for the business

❏ The difference between the two outcomes is almost entirely in the **preparation and framing** — not the size of the round.



Lead With the Problem, Not the Cheque

✗ Press Release Opening

"We raised £12 million."

✓ A Story

"The attack surface for critical national infrastructure has tripled since 2022 — we just raised £12 million to close the gap."

The best cybersecurity funding announcements embed the capital raise inside a larger narrative about the market, the threat landscape, and why this team is the right one to respond. Journalists do not write about money. They write about conflict, consequence, and change. Give them those three things and the funding becomes the evidence, not the sole subject.

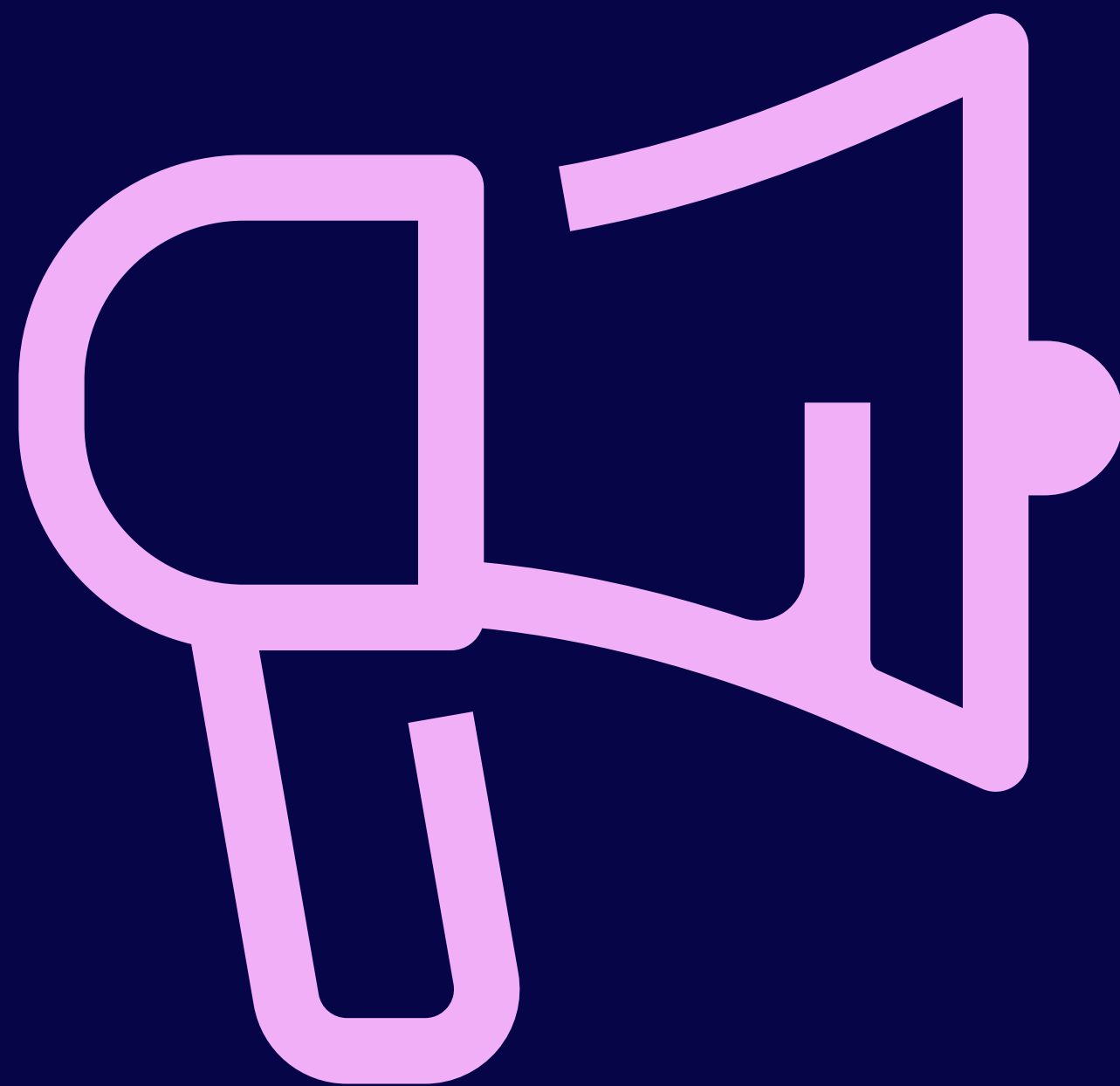
Embargo and Sequence Deliberately

If your round is significant, you have options. Use them. A well-run embargo strategy can deliver a tier-one exclusive to the journalist most likely to give you a feature, while distributing the press release to the trade press simultaneously when the embargo lifts.



A 1,200-word feature in TechCrunch or the Financial Times that tells your founding story, your market thesis, and your customer evidence does more commercial work than dozens of superficial, often automated poor-quality trade press pickups of the wire release. Briefing your tier-one target two to three weeks before the announcement date — under embargo, with a prepared brief, customer reference, and investor quote — gives them enough time to report the story in depth.

Remember: the publications with a high GEO ranking may surprise you. Top trade publications rank very highly alongside nationals, so securing write-ups in technical titles gives you both breadth and depth.



Use Investor Voices — and Don't Stop at the Announcement

The Investor Voice Asset

Your lead investor has probably backed a dozen cybersecurity companies and spent years thinking about where the market is going. Their playbook of opinions — on the threat landscape, on the structural shifts driving investment, on why they backed you specifically — is a precious content asset that most founders never use.

A quote from a well-regarded partner at a tier-one VC, placed thoughtfully in a feature story, is a golden reputational milestone for your brand. It signals validation from someone with a financial stake in getting the market read right.

The Post-Announcement Content Cadence

The funding announcement is the beginning of a narrative arc, not the whole story. Plan your follow-on content cadence in advance:

Week 3

Byline from your
CISO-in-residence on
the threat landscape
your product
addresses

End of Quarter

Analyst note inclusion
— be a known
quantity before the
formal evaluation
cycle begins

Week 6

Data-led research
story pitched to the
top GEO-ranked tech
trade title

i The companies that win the post-announcement period are the ones who treat the round as only the beginning. The press release opens a door. Your job is to build a programme that keeps it open.



Part Three: Analyst Relations — Start Before You Think You're Ready

Here is the mistake almost every early-stage cybersecurity startup makes with analyst relations: they wait until they're "big enough." Both assumptions below are wrong — and both are costing early-stage companies deals they never knew they were losing.

Myth One

Until you have a seat in the Magic Quadrant, the Gartner Hype Cycle, or a Forrester Wave, analysts aren't worth engaging.

Myth Two

Analyst relations is purely a vendor-pays game — without a research contract, there's no point picking up the phone.

Analysts shape buying decisions before your sales team ever gets in the room. When a CISO at a mid-market enterprise starts evaluating your category, the first thing their team does is a Gartner query or a Forrester briefing. Analyst reports and news items dominate the top rank of mentions on LLMs. If you are not in that analyst's mental model — if they haven't heard of you, haven't noted your approach, don't have you on a shortlist they keep for inquiry calls — then you are not in the running.

The Real Goals of Early Analyst Relations



Enter Their Vocabulary

Establish your company in the analyst's vocabulary so they mention you in inquiry calls with enterprise buyers.



Course-Correct Messaging

Understand how they're framing your category, and adjust your messaging and product roadmap accordingly.



Build Relationships Early

Build relationships with analysts who will eventually evaluate your space formally, so you are a known quantity rather than a cold submission.



Gather Market Intelligence

Get early intelligence on which proof points are most compelling to a market-level observer — and feed that back to your teams to adjust accordingly.

How to Run Your First Analyst Briefing

Prepare a tight 20-minute narrative that covers the market problem (with data), your approach (with differentiation clearly stated), your customer traction (even early-stage, even anonymised), and your roadmap. Leave 20 minutes for questions.

→ **Watch What They Push Back On**

Pushback tells you exactly where your market story has gaps. This is more valuable than most market research you'll commission.

→ **Watch Where They Lean In**

Where an analyst leans in tells you what's genuinely differentiated. Both signals are worth more than most market research you'll commission.

→ **Follow Up Within 48 Hours**

Reference something specific the analyst said that was useful. This signals you were genuinely listening and builds disproportionate goodwill over time.

What to Send Ahead

Do **not** send marketing collateral ahead of the briefing.

Send a **one-page problem statement** and an NDA if you have sensitive technical details to share.

Analysts respect concision and directness. They have been sent every flavour of over-produced deck by every vendor in your space. A clean, opinionated one-pager signals that you know what you're talking about and respect their time.

Track What Analysts Say — and Shape the Category Vocabulary

If an analyst who attended your briefing starts referencing language or framing in their reports or conference keynotes that they hadn't used before you spoke with them, that is a signal. You are shaping the category vocabulary. That is category building in its most durable form, and it compounds with every briefing, every follow-up, and every piece of evidence you add to the record.



Operationalise Your Monitoring

Tracking this requires constant monitoring of analyst output. The best approaches focus on operationalising this data in one dashboard, with live updates on what the analyst is saying — and crucially, when these keywords are mentioned.

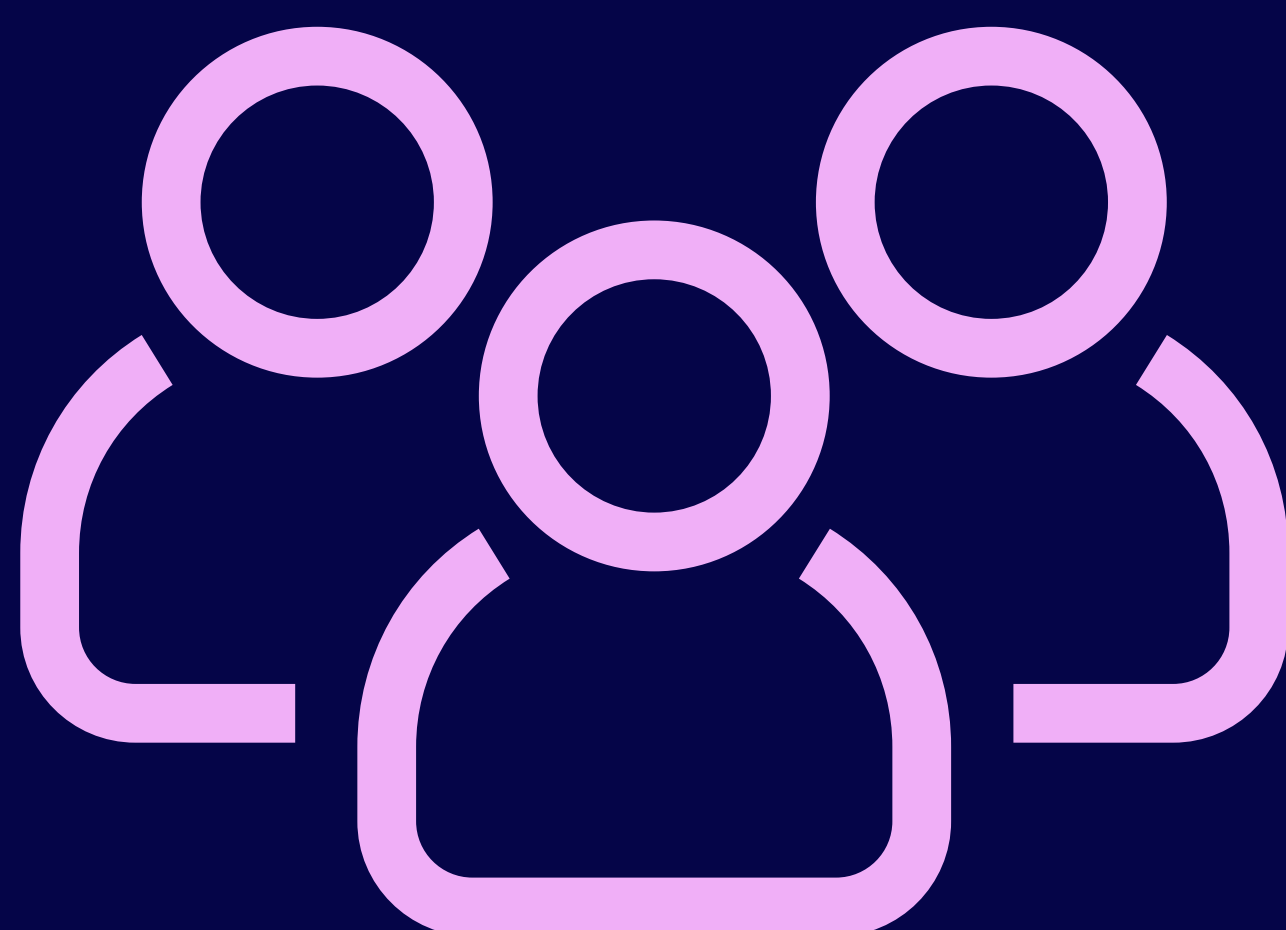
Unify Your Intelligence

A unified approach will help you scale your comms programme: focusing on understanding, influencing, and measuring how your brand shows up across media, social, and AI answer engines simultaneously.

The Long-Term Dividend


The companies that become category leaders in B2B cybersecurity don't just win on product; they win because they taught the market how to think about the problem they solve. This category creation bears dividends in the long run.

The companies that become category leaders in B2B cybersecurity don't just win on product; they win because they taught the market how to think about the problem they solve.



Part Four: Why Technical Messaging Fails in Mainstream Press

This is the section founders find hardest to hear because the technical messaging usually reflects something they're genuinely proud of. The architecture is elegant. The approach is novel. The benchmark results are real and impressive. And none of that matters to a journalist at the Financial Times, Sky News, or even a broadly-read tech title like Wired or MIT Technology Review.

 Mainstream journalists are not writing for your buyers. They are writing for their readers. Your job, if you want to be part of their story, is to show them how your company connects to a shift in the world that their readers care about.

The Technical Messaging Failure Pattern

01

Leads With Architecture

"Our proprietary graph-based correlation engine processes telemetry from across the kill chain in real time..." — defining the product before establishing the problem it solves.

03

Measures in Unrelatable Metrics

"Sub-millisecond query latency," "99.97% detection accuracy across 14 attack frameworks" — technical metrics that non-practitioners cannot evaluate.

02

Uses Untranslated Jargon

"SOAR integration," "zero-trust enforcement," "AI-native detection," "lateral movement correlation" — category language without translation for a general audience.

04

Buries the Human Consequence

The business or human impact appears three paragraphs down — if it appears at all. The result reads like a vendor brief, not a news story.

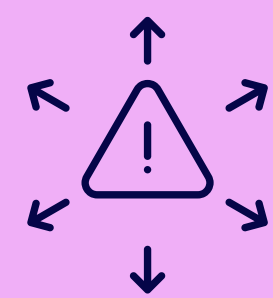
Compare that to what consistently lands in mainstream press coverage of cybersecurity: operational consequences, human stakes, and the policy or business implications of security failure. A hospital cyberattack doesn't make national news because of the technical profile of the attack. It makes national news because patients were diverted, operations were cancelled, and lives were at risk. That is the level of translation required to earn mainstream coverage — and it is a discipline that has to be built deliberately.

The Message Hierarchy Fix

You do not need to strip out the technical substance of your communications. Your technical credibility is an asset: it matters to analysts, to trade press, to sophisticated buyers. What you need to do is sequence your messages appropriately for each audience. Tracking national journalists and building a deep understanding of their ways of working, editorial style, and pitching preferences is the difference between winning and losing here.

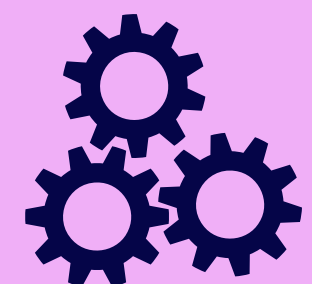
Layer 1: The Consequence Layer

A concise real-world headline of the attack's tangible impact, understandable to a layperson.



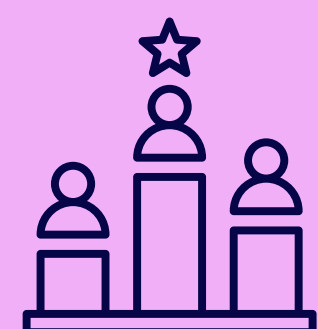
Layer 2: The Mechanism Layer

A plain-English description of the exact technical steps the attack takes.



Layer 3: The differentiation Layer

Your unique solution, data advantage, or technical approach that stops the specific attack.



Most early-stage cybersecurity startups publish layer three everywhere and wonder why mainstream journalists don't respond. Intelligent comms programmes find the layer that works for the journalist, build a relationship, and secure far more meaningful coverage.

✔ **Invest in your spokespeople early and specifically.** The best cybersecurity communicators are founders and senior practitioners who can move fluently across all three layers — who can translate a zero-day into a governance conversation in the same breath, who can explain what a supply chain compromise means for a pension fund trustee without losing the technical credibility that makes them worth quoting.

The Dual-Audience Test

If your CTO can brief a Forrester analyst on your detection methodology at 10am and then explain to a Sky News producer why it matters for NHS resilience at 2pm, that person is worth ten press releases.

Through this lens, **media training for technical founders is a revenue-generating investment that compounds from the first interview onward.**



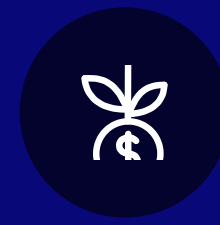
Conclusion: Category Credibility Is Built in Quarters, Not Campaigns

The companies that win in early-stage cybersecurity communications are not the ones with the biggest PR budgets. They are the ones with the clearest narrative, the most disciplined timing, and the most deliberate approach to stakeholder sequencing.



Every Stealth Exit

Is a first impression. Make it count with narrative readiness, not just product readiness.



Every Funding Announcement

Is a narrative investment. Frame it around conflict, consequence, and change — not the cheque.



Every Analyst Briefing

Is a market education moment. Start before you think you're ready and shape the vocabulary of your category.



Every Mainstream Story

Is a trust signal for buyers who will never call you until they have already made a shortlist.

Start with the problem, earn the right to describe your solution, sequence your stakeholders deliberately, and translate relentlessly for every audience you want to reach.

Focus on operationalising your approach — bringing together insights on what your targets are saying, gaps your competitors are leaving, and the impact your coverage is having on the market. Measure success across a range of metrics: from coverage volume to whether the right people — the analysts, the journalists, the CISOs, the board members — are changing how they talk about the category you are trying to own.

- That is how you move from stealth to credibility. Not in a single announcement, not in a burst of activity around a funding round, but in a sustained, disciplined programme of communications that builds with every quarter and compounds with every proof point you add to the record. **Start now. The competitive clock is already running.**

