Resonance

PLAYBOOK · 2026

The new early-stage cybersecurity PR playbook.

From stealth to category credibility.

A playbook by Resonance and Agentcy
For cybersecurity founders and CMOs

resonancecrowd.com

What this playbook covers.

Four areas that matter most for early-stage cybersecurity companies. Each is meant to be used: taken into a team meeting, tested against your current plan and used to make better decisions.

—	**Introduction** The narrative gap that's costing you deals.	3
01	**Coming out of stealth** When to go public, and how to time it for narrative impact as well as product readiness.	5
02	**Funding announcements** Framing, sequencing and the follow-on content that turns one day of news into lasting credibility.	8
03	**Analyst relations** Why to start before you feel ready, and what waiting costs in deals you never knew you lost.	12
04	**Technical messaging** Why the language that wins the demo room fails in mainstream press, and how to fix it.	15
—	**Conclusion** Category credibility is built quarter by quarter.	18

IN BRIEF

- **Exit stealth on narrative readiness.** Go public when you can state your category in a sentence, name a referenceable customer and tell one founding story.
- **Make the funding announcement work harder.** Lead with the market problem, brief one tier-one journalist under embargo and plan eight weeks of follow-on content.
- **Start analyst relations early.** Analysts shape shortlists long before a formal evaluation.
- **Translate the technical message.** Consequence first, then mechanism, then what makes you different.
- **Build credibility every quarter.** Every briefing and proof point adds to the record.

The narrative gap that's costing you deals.

From the 2000s well into the 2010s, cybersecurity followed a reliable pattern. A genuinely differentiated product was enough to build a company on.

If your detection was faster, your false-positive rate lower or your architecture more elegant than anything else available, you could build in the knowledge that your technical advantage was your moat.

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.

That world is gone.

The world has changed. Has your strategy?

AI has compressed the product development cycle. Technical differentiation is now 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. Your competitors are building faster, and their investors are better resourced.

The buyer problem

Buyers increasingly use AI assistants, alongside analyst reports and peer referrals, to draw up their first shortlist of cybersecurity suppliers. The shortlist exists before your sales team 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 product, that gap is a commercial problem.

Deals stall. Evaluations leave you out. Talent chooses the company whose name it already knows. The investor who would have led your next round passes for want of third-party validation.

> The narrative gap can be closed. It takes one shift in thinking: communications is part of the go-to-market, running alongside the product from the earliest stages. Bolted on once the product is ready, it arrives too late.

01

Coming out of stealth: timing is strategy.

The move from stealth to public is one of the most consequential communications decisions an early-stage company makes. Most get it wrong in one of two ways.

Too late

They stay in stealth too long and miss 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 land with the audiences who matter.

Both are strategy failures a fast-growing start-up can ill afford. A closed round is only part of the trigger for going public. The rest is narrative readiness.

Three questions before you go public.

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

01

Can you describe your category in one sentence?

Describe the shift in the world that makes your product necessary now. What the product does comes second.

"We make endpoint detection faster" is a product description. "Attackers now move laterally in under four minutes, and detection tools built for an older threat landscape can't keep up" is a category narrative. The first gets a polite nod. The second makes a journalist stop scrolling and a CISO forward it to their team. Don't go public until you can produce the second kind reliably.

02

Do you have a customer you can reference, even obliquely?

"A Fortune 500 financial services firm cut mean time to detect by 60% in 90 days" carries far more weight than "we are working with leading enterprises". Specificity signals credibility.

You need a sector, a metric and a timeframe: evidence that a real security team has stress-tested the technology in a real environment. Journalists and influencers are always looking for the next big thing, and that extra layer of evidence is what makes them sit up.

03

Is the founding team's story coherent and on the record?

In cybersecurity the team is the first proof point. Before the product has public validation, reporters and analysts are betting on whether the people behind it can solve the problem they describe.

Get the origin story straight before you go near a journalist: what you saw in the market, why existing solutions failed and why this team is the one to fix it. Then make sure every founder tells it the same way.

If you can answer all three, you are ready. If you can't, the extra time will sharpen your messaging and positioning, and that pays off long after launch.

The competitive clock.

Stealth offers no protection from competitors. In a hot category, and in 2026 most of cybersecurity qualifies, your rivals are building their story while you build your product. Three things make the first story hard to dislodge.

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. 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 it. Early inclusion shapes how the whole market thinks about the space.

AI answers favour the established

A company with a long-term generative engine optimisation (GEO) strategy, publishing trusted, high-quality content, will lead the answers on the main AI assistants, and is hard to dislodge once it does.

A premature announcement is recoverable. You can refine the message, add proof points and refocus. A rival owning your category narrative before you have spoken publicly is much harder to reverse.

THE GOLDEN RULE

You can't reclaim a category story that someone else has already filed. When in doubt, favour narrative readiness over perfect product readiness.

02

Funding announcements: make them work harder.

A funding announcement is the most reliable news a start-up will ever have. The round has closed, the numbers are real and the investors carry brand weight you can borrow.

Used well, it

- establishes your category positioning
- introduces your founding story to a new audience
- starts a pipeline of follow-on coverage
- gives sales the social proof that shortens enterprise evaluations

Used badly, it

- generates one day of news
- earns a few trade press pickups
- disappears without trace inside a week
- leaves the business no lasting narrative asset

The difference comes down to preparation and framing. The size of the round matters far less.

Lead with the problem. The cheque is the evidence.

A PRESS RELEASE OPENING

"We raised £12 million."

A STORY

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

The strongest cybersecurity funding announcements place the raise inside a larger story about the market, the threat landscape and why this team is the right one to respond. Journalists write about conflict, consequence and change. Give them those three and the funding becomes the proof point in the story.

Embargo and sequence deliberately.

If your round is significant, you have options. Use them. A well-run embargo can deliver a tier-one exclusive to the journalist most likely to write a feature, with the release going to the trade press the moment the embargo lifts.

2–3 WEEKS BEFORE

Tier-one briefing

An exclusive under embargo, with a prepared brief, a customer reference and an investor quote.

ANNOUNCEMENT DAY

Embargo lifts

The feature runs and the release goes to the trade press at the same moment.

WEEKS 3–8

Follow-on cadence

Bylines, a research story and analyst notes keep the story moving.

One feature outweighs a hundred pickups.

A 1,200-word feature in TechCrunch or the Financial Times that tells your founding story, market thesis and customer evidence does more commercial work than dozens of thin, often automated trade pickups of the wire release.

Brief your tier-one target two to three weeks before the announcement, under embargo, with a prepared brief, a customer reference and an investor quote. That gives them time to report the story in depth.

CHECK WHAT AI ASSISTANTS CITE

The publications AI answer engines rank highest may surprise you. Top trade titles often sit alongside the nationals, so coverage in technical publications gives you breadth and depth.

Use your investors' voices.

Your lead investor has probably backed a dozen cybersecurity companies and spent years thinking about where the market is going. Their views on the threat landscape, on the shifts driving investment and on why they backed you are a content asset most founders never use.

A quote from a respected partner at a tier-one VC, placed well in a feature, is a real reputational milestone. It is validation from someone with money riding on reading the market correctly.

Plan what happens after the announcement.

The announcement opens the story. Plan the follow-on content before the release goes out.

Week 3	**A byline on the threat**	Your CISO-in-residence writes on the threat landscape your product addresses.
Week 6	**A data-led research story**	Pitched to the technology trade title that AI assistants cite most in your category.
End of quarter	**An analyst note**	Inclusion in an analyst note, so you are a known quantity before the formal evaluation cycle begins.

The companies that win the post-announcement period treat the round as a beginning. The press release opens a door. The programme keeps it open.

03

Analyst relations: start before you feel ready.

Almost every early-stage cybersecurity company makes the same mistake with analysts: it waits until it is “big enough”. That decision usually rests on one of two myths.

MYTH ONE

Analysts aren’t worth engaging until you have a place in a Magic Quadrant, a Hype Cycle or a Forrester Wave.

MYTH TWO

Analyst relations is pay-to-play, so without a research contract there’s no point picking up the phone.

Both are wrong, and both cost deals the company never knew it was losing. Analysts shape buying decisions before your sales team is in the room. When a CISO at a mid-market enterprise starts evaluating your category, an early step is often a Gartner inquiry or a Forrester briefing. Analyst reports and news coverage also dominate what AI assistants cite.

If you are missing from an analyst’s mental model, and from the shortlist they keep for inquiry calls, you are out of the running.

What early analyst relations is for.

Enter their vocabulary

Get your company into the analyst's vocabulary, so they mention you on inquiry calls with enterprise buyers.

Course-correct your messaging

Learn how they frame your category, and adjust your messaging and roadmap to match.

Build relationships early

Know the analysts who will one day evaluate your space formally, so you arrive as a known quantity.

Gather market intelligence

Find out which proof points most impress someone who sees the whole market, and feed that back to your teams.

How to run your first analyst briefing.

Prepare a tight 20-minute narrative and leave the other 20 minutes for questions.

20 minutes	20 minutes
Your narrative	Their questions

The market problem
with data

Your approach
with the difference stated

Customer traction
early or anonymised is fine

Your roadmap
where you are heading

Watch what they push back on

Pushback shows exactly where your market story has gaps.

Watch where they lean in

Where an analyst leans in shows what is genuinely different. Both signals are worth more than most market research you could commission.

Follow up within 48 hours

Reference something specific the analyst said. It shows you were listening and builds goodwill over time.

What to send ahead.

Skip the marketing collateral. Send a one-page problem statement, and an NDA if you plan to share sensitive technical detail.

Analysts respect concision. They have been sent every flavour of over-produced deck by every vendor in your space. A clean, opinionated one-pager shows you know your subject and respect their time.

Track what analysts say, and shape the category vocabulary.

If an analyst you briefed starts using language or framing in reports or keynotes that they hadn't used before, that is a signal: you are shaping the category vocabulary. It 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 the monitoring

Tracking this takes constant monitoring of analyst output. The best approach brings it into one dashboard, with live updates on what analysts are saying and when your keywords appear.

Unify your intelligence

One view of how your brand shows up across media, social and AI answer engines lets you understand, influence and measure the programme as it scales.

The companies that lead their category taught the market how to think about the problem they solve.

04

Why technical messaging fails in mainstream press.

Founders find this the hardest part to hear. The architecture is elegant, the approach is novel and the benchmarks are real. None of it matters to a journalist at the Financial Times, Sky News, Wired or MIT Technology Review.

Mainstream journalists write for their readers. To be part of their story, show how your company connects to a change in the world those readers care about.

The failure pattern.

It leads with architecture

“Our proprietary graph-based correlation engine processes telemetry from across the kill chain in real time...” The product is defined before the problem it solves.

It uses untranslated jargon

“SOAR integration”, “zero-trust enforcement”, “AI-native detection”: category language with no translation for a general reader.

It measures in unrelatable metrics

“Sub-millisecond query latency”, “99.97% detection accuracy across 14 attack frameworks”: numbers a non-practitioner can’t evaluate.

It buries the human consequence

The business or human impact turns up three paragraphs down, if at all, and the result reads like a vendor brief.

What lands instead.

Mainstream coverage of cybersecurity reliably features operational consequences, human stakes, and the policy or business fallout of a security failure.

A hospital cyberattack makes the national news because patients were diverted, operations were cancelled and lives were at risk. Its technical profile barely features. That is the level of translation mainstream coverage needs, and it is a discipline you have to build deliberately.

The message hierarchy fix.

Keep the technical substance: it matters to analysts, trade press and sophisticated buyers. Sequence the message for each audience instead. Knowing how national journalists work, what they write and how they like to be pitched is what separates winning from losing here.

LAYER 1	**The consequence** A plain headline of the attack's real-world impact that anyone could understand.
LAYER 2	**The mechanism** A plain-English account of the technical steps the attack takes.
LAYER 3	**The differentiation** Your solution, data advantage or technical approach that stops that specific attack.

Most early-stage cybersecurity companies publish layer three everywhere, then wonder why mainstream journalists don't respond. Good programmes find the layer that works for each journalist, build the relationship and earn far more meaningful coverage.

The dual-audience test.

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

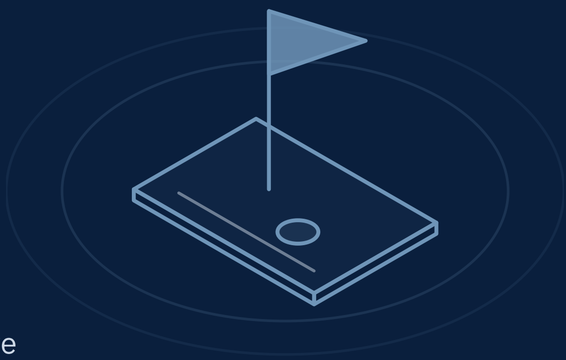
Invest in spokespeople early

The best cybersecurity communicators are founders and senior practitioners who move fluently across all three layers. They can turn a zero-day into a governance conversation in one breath, and explain what a supply chain compromise means for a pension fund trustee without losing the technical credibility that makes them worth quoting.

Treat media training as revenue

Seen this way, media training for technical founders is a revenue-generating investment. It compounds from the first interview onward.

Category credibility is built quarter by quarter.



The companies that win early-stage cybersecurity communications rarely have the biggest PR budgets. They have the clearest narrative, the most disciplined timing and the most deliberate sequence of stakeholders.

01

Every stealth exit is a first impression.

Make it count with narrative readiness as well as product readiness.

02

Every funding announcement is a narrative investment.

Frame it around conflict, consequence and change.

03

Every analyst briefing is a market education moment.

Start before you feel ready, and shape the vocabulary of your category.

04

Every mainstream story is a trust signal.

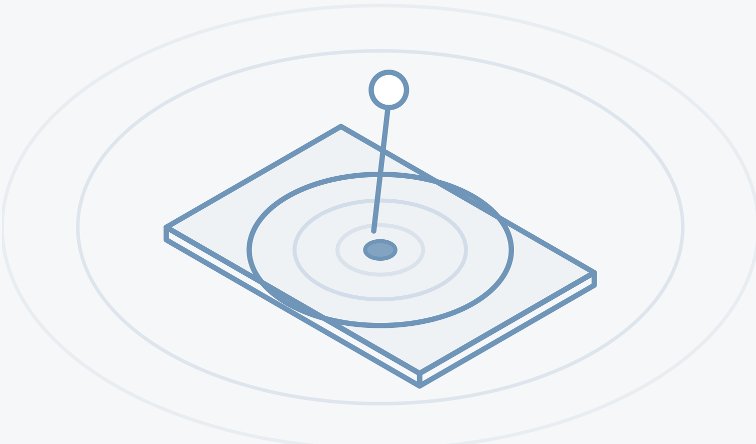
It reaches buyers who won’t call you until they have already drawn up a shortlist.

Start now.

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.

Run it as an operation. Bring together what your targets are saying, the gaps your competitors are leaving and the effect your coverage is having. Measure more than coverage volume: watch whether the analysts, journalists, CISOs and board members who matter are changing how they talk about the category you want to own.

> That is how you move from stealth to credibility: a sustained, disciplined programme that builds every quarter and compounds with every proof point you add to the record. The competitive clock is already running.



Resonance

ABOUT THIS PLAYBOOK

Close the narrative gap before a competitor does.

Resonance is a strategic communications consultancy that began in B2B technology PR. We work with cybersecurity companies from stealth to scale on positioning, media and analyst relations, spokesperson training and measurement.

Agentcy, the PR operations platform Resonance built, supplies the media, analyst and AI visibility intelligence behind the programme.

---

hello@resonancecrowd.com
resonancecrowd.com/sectors/cybersecurity
agentcy.com.pr

London · Manchester

Resonance