

State of Security Vendors

Blackhat 2025

Andy Ellis



Key Takeaways

The 359 observed Blackhat vendors, by and large, did a decent job of making their booths tell you enough of what they did so that you could self-select who to talk to, because there isn't enough time to talk to every vendor. Almost 20% missed the mark: 16 vendors had no useful visible messaging and 55 had unclear messaging.

As expected, AI was everywhere (on 1 in 3 booths), and it was sometimes hard to tell *exactly* what a vendor meant about how they used AI. 118 vendors mentioned AI. 18 vendors appeared to be securing your AI *usage*, from GenAI to in-house agents (although only two mentioned MCP). 20 vendors mentioned agents/agentive, and another 20 used AI as an adjective (AI-led, AI-enhanced, etc), while 60 just mentioned AI.

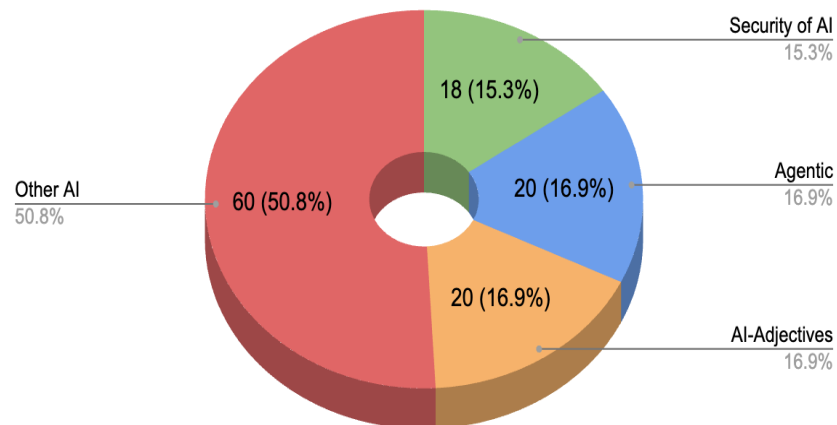
The biggest space? Code security, with 105 vendors (not including the application delivery side of the house).

Surprising absence? Deepfake detection. Maybe all the VCs are excited about it, but only 3 vendors on the show floor advertised it ... and one of them was a reseller of another.

Platforms abound! 32 vendors mentioned being some kind of platform.

Untrusted? Zero trust only appeared on 6 booths.

AI marketing at Blackhat 2025



Methodology

To put it frankly, my methodology was awful. I got this idea at the last minute: I'd walk the show floor and make observations. I started on Tuesday morning (surprise, the show floor wasn't open yet!), making notes on the banners in the halls: The vendor name, and what they said about themselves. I kept notes on a Kindle Scribe, and it took 23 pages by the time I finished on Thursday. Other than my speaking time on Wednesday, I spent all of the time the show floor was open, walking the floor. I didn't use a map, so I missed a lot of folks on Wednesday. Thursday I tried to fill in all of the gaps I missed, aided by a few helpful CROs and CMOs who challenged me to come find their booths.

I hit most of the larger booths on Wednesday, and most of the smaller booths on Thursday. I also posted a teaser on Wednesday of my project, and a *lot* of Blackhat vendors saw it. So booth behaviors that I might have coded as large vs small might instead be correlated to the observer effect. While I tried using AI & OCR to transcribe my notes, it was a disaster: I ended up handcopying my notes into a spreadsheet for analysis.

Category Observations

AI is the new hotness. The AI Security Operations Center appears to be the hot space, with 18 vendors laying claim to the market. Another 7 don't claim AI, but operate in the Security Operations and Automation space. This space is likely to be a bloodbath over the next few years, but I hope it does pan out. Even if that means that at RSAC 2027 we'll see The AI CISO at a booth.

Exposure is the new Risk. Many vendors who *used* to say Risk Management now say Exposure Management. That doesn't mean Risk is dead, though. Veracode and Qualys introduce Application Risk Management and the Risk Operations Center, respectively, and the Human Risk Management and GRC spaces aren't (yet) pivoting to new language.

Is Security Management going to converge? With 13 vendors in CTEM and 6 in some form of Security Success Management (using your existing tools, better), it's possible we're heading into a converging era: do security teams need to focus more on the success of existing tools, rather than deploying more point solutions?

AppSec is ... confusing. 54 vendors operate in Application Security, from Open Source Code Safety through Vulnerability Management through AppSec Posture Management and into Runtime Security. Add in another 29 vendors in Threat Intelligence and Offensive Security, 13 in Continuous Threat and Exposure Management (CTEM), and 9 in some flavor of Cloud Security, and it's clear: we still don't trust our code.



Booth Observations

Vague or oddly specific? Larger vendors were more likely to go extremely vague in their booths and marketing. That's okay if you're a name everyone knows: CrowdStrike can get away with vague "Stop the Breaches" messaging. Other large vendors went oddly specific, not mentioning their core business at all, focusing on a subset of products. It felt like an odd choice, although there was one standout: HP, whose booth simply read "Find, lock and erase a PC, even when it's turned off." This was a well-executed choice: it stood out to folks walking by, giving a little brand boost.

Bold is ... Banal. There were a surprising (34) number of vendors who had some form of superlative in their tagline. More senior buyers tend to discount these, so it can have a mixed effect: some buyers believe you, and others will mistrust you. Everything from "THE such-and-such company" (which honestly made me think a little of "THE Ohio State University"), to "The First," "The Only," "100%," and "The #1." At least one vendor specified the geography that they were the superlative in, which struck me as an ... odd choice.

Punctuation is Painful. A lot of booths had taglines that looked like they were just copy/pasted out of a marketing brand text file. The Chicago Manual of Style doesn't really apply to words on a booth, and punctuation is (mostly) unnecessary. I know that the Oxford comma is currently out of fashion, so ... don't punctuate your lists with commas. Extra points for marketers who used clever spacing to create lists

(e.g., Cloudflare, Trufflehog). If your punctuation is important for how the customer should hear it (e.g., Mimecast's "Human Risk, Managed"), then keep it in. Otherwise, try to eliminate all commas and apostrophes to reduce reader friction.

Borrowing Credibility. The smaller the customers in the vendor's ICP, the more likely the booth was to have references on it, from number of customers to analyst recognitions. This seemed especially true in the all-in-one platforms (MDR, SIEM, SOAR, etc) aimed at the mid-market.

The Enemy's Gate is NOT Down. You never know what direction someone is going to come from when they reach your booth, and you need to consider what they will see first. A few vendors had a set of taglines that worked well as a cluster, but then each approach to the booth had only one tagline visible. People wander the show floor in lots of directions, and unless you have one of the smaller booths, you don't have a "front" to aim towards the enemy, er, prospect.

The Circus Has Not Left Town. A handful (11) of vendors focused more on the theme of their booth than on their messaging. I think it mostly isn't helpful, even if it gets a lot of badge scans. These booths end up feeling overcrowded and unapproachable to serious browsers, so may be overlooked.

Ignoring the Adversary. Only 6 vendors explicitly claimed to be able to beat specific adversaries (e.g., "hacker-proof"). Historically, this is a great way to get shamed by the security community, so it's nice to see that we can learn from past marketing mistakes.



Behavioral Observations

Big or hungry? The bigger the booth, the more likely I was to be ignored. For every booth, I stood ten to twenty feet away—often across the aisle—and took notes. On day one, when I observed larger booths, only 6 companies approached me and asked what I was doing. Most of those were shallow booths with only one “front”. Walking by smaller booths, I was engaged by closer to a third of all booths.

Canned pitches. For the booths I talked to, a good chunk of staff really only had one goal, whether it was “give a demo” (smaller, founder-led booths) or “offer swag” (larger booths). Those missed an opportunity. Closer to hitting the mark were the buyer checks (“are you interested in X?”). Very few booths did early and engaging qualification (e.g., “Is your organization embracing GenAI?” vs “Are you interested in GenAI security?”).

“Hi.” Many booths, especially in the mid-size section, had staff who would just try out a “Hi” as you walked past. I know this strategy often works out on the street, but does it work to stop security buyers?

Summary Data

Category

- Application Security & AppSec Testing: 54 vendors
- Threat Intelligence & Offensive Security: 29 vendors
- Identity & Access Management: 29 vendors
- Specialized Tools: 25 vendors
- Security Operations and Automation: 25 vendors
- AI Security (AI): 18 vendors
- Endpoint Security (EDR): 18 vendors
- Network Security & Zero Trust: 17 vendors
- Human Risk Management (HRM): 17 vendors
- Website Application Security & Fraud Prevention: 14 vendors
- Security Incident & Event Management (SIEM): 14 vendors
- Continuous Threat Exposure Management (CTEM): 13 vendors
- Data Security / Data Loss Prevention (DSPM): 11 vendors
- Governance, Risk, and Compliance (GRC): 10 vendors
- Managed Detection & Response (MDR): 10 vendors
- Cloud Security Posture Management (CSPM): 9 vendors
- SaaS Security: 6 vendors
- Security Success Management: 6 vendors
- OT/ICS Security: 4 vendors
- Global Systems Integrators (GSI): 3 vendors
- Third Party Risk Management: 3 vendors



Buzzwords

- AI: 85 vendors
- Agent: 25 vendors
- Deepfake: 3 vendors
- Enterprise: 11 vendors
- Exposure: 10 vendors
- Human: 13 vendors
- Modern: 6 vendors
- Platform: 32 vendors
- SOC: 14 vendors
- Zero Trust: 6 vendors

Want to learn more on how to
Cultivate CISOs? Join this
introductory workshop for field
marketers and SDRs:
<https://lu.ma/g59xbxhs>

About Us

Duha is a boutique consultancy that provides a spark of genius at the intersection of security, leadership, product, and messaging, led by legendary CISO Andy Ellis. Duha advises CISOs on career development, executive engagement, and board communications. Duha also supports security vendors on go-to-market and product strategy. Interested in engaging Andy for a workshop on Cultivating CISOs for your SDRs and field marketers, a conversation about your messaging, or with a leadership keynote for your next event? Contact andy@duha.co.

Andy Ellis is a Hall of Fame CSO, former VC Partner, and the author of 1% Leadership. He is the editor of howtociso.com, a co-host of The CISO Series podcast, and is an experienced board member and advisor to numerous companies. A former Air Force officer and MIT graduate, Andy brings a renaissance approach to every engagement, with accolades including an Air Force Commendation Medal, The Wine Spectator Award of Excellence, The Spirit of Disneyland Award, the CSO Compass Award, and the SANS/DMA Podcast of the Year.

