State of Security Vendors

Blackhat USA 2026

Andy Ellis

Key Takeaways

We have entered into an AI world. While nearly half of booths *didn't* directly mention AI or agents in their taglines, the effects of AI are everywhere. Multiple spaces (Identity, SaaS, AppSec, Data) have almost every vendor leading with AI; existing unsolved problem areas just got worse.

At the same time, there's a clear trichotomy in the market: tools that tell you how bad things are; tools that stop adversaries, and tools that prevent problems from occurring. While you'd suspect that the tools that fix things would dominate, the tools that merely tell you how bad things are seem to be frustratingly plentiful.

Notable and Niche Keywords

- AI (199 booths)
- Agent/agentic (104)
- Autonomous (20)
- Enterprise (19)
- Exposure (20)
- Frontier (8)
- Human (20)
- Platform (50)
- Resilience (12)
- Risk (32)
- SOC (36)

Entirely lost

57 booths didn't have enough messaging for me to figure out what they did.

Methodology

This report is built based on observations made, in person, looking at each of the 450 exhibitor booths on the BHUSA 2026 show floor. Taking about 12 hours across three days, each booth was observed, with major visible taglines, branding, and important keywords recorded via dictation on an iPhone directly into a spreadsheet. That spreadsheet had been prepopulated with the exhibitor list.

Each booth was quickly assessed in real-time to answer very specific questions:

- Did I understand what the company did, based on the booth alone?
- Was the booth strongly themed?
- Was the company messaging overly bold ("we're the first!") or overly aggressive ("CISOs don't know anything!")? 13 were bold, and 3 aggressive.
- How did the company handle the Oxford comma?

The taglines were checked against my existing dataset from previous conferences, the vendors websites, or conversations with the booth staff, so that I could categorize *what* the vendor actually did (not just "AI").

What I didn't collect? The taglines from all the *non*-exhibitors, whether they had another space, were advertising somewhere, or were just walking billboards. There weren't as many alternate venues for vendors as you see at RSAC (half of the Blackhat exhibitors were not RSAC exhibitors, and that isn't just startups.

Consuming Booths

Conference booths serve very different purposes, with vastly different observers, and these purposes are sometimes in conflict. In vaguely priority order (from the buyer perspective) these are:

1. Provide an educational experience for a practitioner to learn more about a security problem, a vendor's approach to it, and gain familiarity with the product.
2. Enhance or establish brand awareness to security decision makers.
3. Demonstrate to VCs the viability and velocity of a company in anticipation of its next round.
4. Collect badge scans, as a (poor) proxy for leads.

But this report is *not* a product or CISO view of the security market. Rather, it's a *marketing* perspective: how do event marketers implicitly see the cybersecurity landscape, and their role in it? What do *they* think that security buyers are looking for and buying?

There's a further nuance to this view. Event marketers often have a very perverse incentive. Common marketing practices drive to maximize the number of *touches* that a company has with security practitioners, *whether or not a practitioner is in market now, or will ever be*. This drive is motivated partly by the battle over revenue attribution, and partly over the lead generation model of maximizing leads of any quality, and filtering via fairly cold outreach to those leads. As a result, exhibition floors often have a Halloween feel to them, with attendees trading their contact information in exchange for some piece of marketing shwag.

As a result, so many booths seem to be nothing more than beautiful bait, luring in the unsuspecting attendee until they can be hooked into coughing up their personal details. At the other end of the spectrum, some booths are simply a product sheet, listing every feature in a company's product. Any demographic analysis covering both ends of that spectrum will have some infelicities.

Finding Booths

Compared to last year, there were about a hundred more booths. Some of that was the AI zone, and a handful of very large companies *also* had standup kiosks among the startups, but it was challenging to randomly find booths. The pillars in the Mandalay Bay meant there was a "right" way and a "wrong" way to traverse the hall (guess which one I'd pre-planned?), and this constraint affected idle wanderers.

Several booths were adjusted in near real-time, as locations that looked reasonable on a floorplan ended up being less than palatable in person. There were 15 empty booth locations (although 4 of those ended up being in a row that completely disappeared).

Booth Overview

The Continued Rise of AI and Agents

If you felt like every company was an AI company, you were close to being correct. 235 booths mentioned AI, agents, or agentic, with a handful more including nearby terms like autonomous or automated. It was harder to find companies that *didn't* mention AI.

More vendors were marketing fleets of agents, rather than a single agent; the rise of true agentic organizations may be on the horizon. Other vendors were aiming at governing agents built by third parties (almost every former SSPM vendor has moved to this space), while yet more were aimed at managing your marquee agents (I'd call this the Agentic Security Posture Management space, but ASPM is already taken).

Design Spectacles

Many booths have a mild theme running through the booth. Some were strongly themed, and yet more were entirely a theme (I'd call them circuses, but there was literally a booth whose design was a circus tent). 7 of the 39 strongly themed booths had little or no visible messaging. That's a slightly higher rate than the baseline.

The Oxford Comma

Booths did a much better job at copyediting, and using the Oxford comma correctly, than in past conferences. 30 out of 36 vendors who had a list in a sentence correctly used the Oxford comma. *[Note: if you want to respond with the AP Style Guide, note that it specifies skipping the comma where space is limited and it there would be no opportunity for confusion.]*

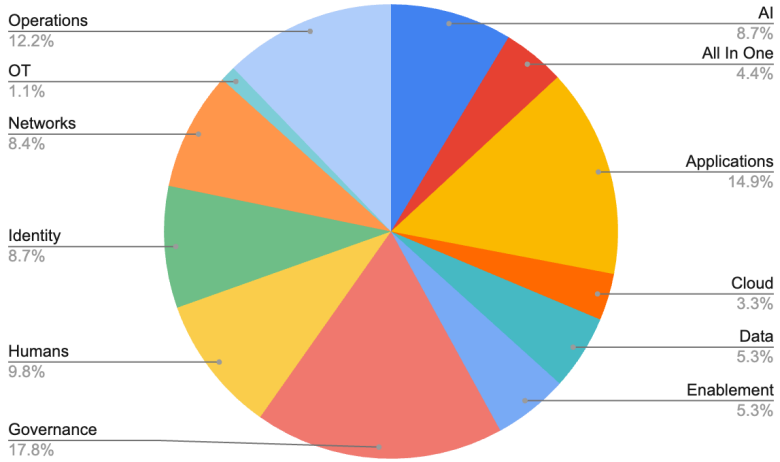
Booth Behaviors

Loud and proud. This may be an observer artifact–I now wear two hearing aids instead of one–but it felt like the booths with microphone-enabled staff were louder than usual. Speakers were on the edge of blowing out, and it created a steady background beat that interfered with thinking, conversations, and voice dictation. One booth's performer was cupping the microphone, and yelling loudly enough into it to be physically uncomfortable as I walked by.

More assertive staff. Booth staff at midsize and small booths seemed even more assertive than last year or at RSAC. This again may be an observer effect (at Blackhat 2025 I took notes on a tablet; at RSAC I was dictating into my phone; this year I was dictating at my hearing aids) which left me looking more approachable.

Less Aggressive badge scanning. No one tried to scan my badge without permission, and only a small handful even asked. This year I had a *media* badge, which may have affected this.

Category Breakdown



You might look at that chart above and notice that it doesn't seem to match up to normal industry breakdowns. The guiding principle for this categorization is based on the *environment* that the solution targets.

AI (39)

This is the first report where I'm breaking out AI as its own category. This is predominantly for AI *governance and observability* solutions, with a healthy dose of AI safety companies. If a vendor is using AI to do anything that isn't "govern other AI use," they'll appear in a different (and relevant) category. This category includes the former SaaS security vendors, who have generally pivoted to be AI security.

All In One (21)

The All-in-One category is for vendors that are basically "outsource a big chunk of your security to us", either as a managed service, as a comprehensive platform, or by providing consulting services (10). While arguably, consulting could be attached to the Enablement category instead, it lives here because this is more about delivering your own *security* rather than your own *product*.

Applications (67)

No longer the largest category, Applications now covers only traditional AppSec (87) services. AppSec itself is already a fairly wide category, including software supply chain, application testing, and runtime security.

Cloud (15)

Traditional CSPM/CNAPP vendors fall into this category, as well as cloud configuration and management tools. Cloud security seems to be fairly robust against AI marketing (they're all using AI, and discussing AI, but generally still are clearly targeting "secure the cloud."

Data (24)

From DSPM to DLP, with sides of encryption and backup/recovery, data security solutions are often found across varied environments, but with a clear focus on data as it lives in or passes through those environments. Data security vendors often have a hard challenge differentiating themselves from Application Security focused vendors. Tools focusing on protecting data from AI get included here.

Enablement (23)

Scattered across the show floor you'll find Hardware and Software vendors to incorporate into your own products. You'll also find a handful of Workforce Development vendors, either helping you find staff, or training your existing staff.

Governance (80)

Now the largest category, Governance includes not only the traditional Compliance Management and Third Party Risk Management spaces, but has also been expanded to include Continuous Threat & Exposure Management (CTEM), Unified Threat Intelligence, and Offensive Security as well. All of these are *knowledge* disciplines, enabling a buyer to understand their risk profile. Threat Intelligence companies that pivoted into Detection Engineering or Threat Hunting are instead included in Operations.

Humans (44)

Core to any environment are the endpoints, but EDRs alone are ineffective enough that we have an entire Human Risk Management space. HRM includes both technical controls like email filtering as well as security awareness training.

Identity (39)

The long-running challenges of Identity have exploded with the rise of agents using humans' identities. Spanning IAM, IGA, MFA, ITDR, as well as non-human identities, this space continues to grow, since the "I" in "AI" certainly doesn't stand for Identity.

Networks (38)

A triple space, Networks includes traditional NDR, as well as SASE, ZTNA, and Web Security. Web application firewalls, bot management, and fraud management tend to end up here as part of the Web Security space.

OT (5)

There are a small handful of exhibitors focused directly on the OT, ICS (or CPS), and IoT worlds.

Operations (55)

Whether you're providing a data pipeline, a SIEM, Security Operations/Automation, or Detection Engineering And Threat Hunting, Operations comes in third with the most exhibitors. The AI SOC is probably the hottest "let AI take over a security job" space.

About Us

Duha is a boutique consultancy that provides a spark of genius at the intersection of cybersecurity, leadership, product, and messaging, led by legendary CISO Andy Ellis. Duha advises CISOs, CMOs, CROs, and other executives on improving themselves and their teams. 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.