

State of Security Vendors

AtISecCon 2026

Andy Ellis



About AtlSecCon

Atlantic Security Conference is a large regional security conference in Halifax, Nova Scotia. With somewhere in the neighborhood of two thousand attendees, it draws attendees from all over the northeastern parts of the US and Canada (and it lives in the Atlantic Time Zone, the best time zone). Its conference floor is much less of a carnival than the national conferences, with most booths being smaller, decorated with either a single rollup, or with an 8'x8' standing screen. A few had monitors as well, with cycling content.

AtlSecCon also had *experiential suites*, breakout rooms just off the show floor, with one or two exhibitors using those in various ways.

Key Takeaways

The 71 exhibitors at AtlSecCon were an interesting slice of the vendor demographic, with entire major categories going wholly unrepresented. Most notably, no pure-play GRC, TPRM, OT, Threat Intelligence, or SaaS Security vendors were here, ceding this market almost entirely to the all-in-one companies. There were very few Application security companies. Instead, the focus from an exhibitor perspective seemed to be Data, Network Security/Zero Trust, All-in-one, and Enablement focused solutions. This *probably* reflects a belief that local practitioners work for smaller enterprises, which may have been accurate pre-Covid, but feels less so in the distributed work environment of today.

While only 2 exhibitors had zero visible messaging in their booth, another 13 had such vague or unclear messaging that you'd be misled into another direction. The backup & recovery space of data security was the biggest offender, with virtually every exhibitor focusing on the vague term "resilience."

Notable and Niche Keywords

- AI (25 exhibitors)
- Resilience (6 exhibitors)
- Zero Trust (4 exhibitors)

Booth Challenges

The constrained layout left marketing teams without the ability to emulate the Halloween feel of RSAC or Blackhat, instead relying on messages that would fit onto their rollups. Even so, many of the designs needed review *on a show floor*: all the key messaging was in the middle third of the display, where it was often blocked by the humans in the booth. Meanwhile, the top 1-2 feet of the displays was often left empty, or containing only a logo.

Methodology

This report is built based on observations made, in person, looking at each of 71 exhibitor booths on the AtlSecCon 2026 show floor. Taking about two hours, 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 three very specific questions:

- Was the booth strongly themed?
- Did I understand what the company did, based on the booth alone?
- How did the company handle the Oxford comma?

I then tried to determine whether my impression of what the company did matched what I already knew, or quickly checked their website, to assess what broad market space they were in. Sometimes, I ended up more confused: the booth designer clearly thought the company was in a different space than whoever wrote their copy.

What I didn't collect? Personalized pitches, shwag giveaways, or anything beyond what was directly observable.

Consuming this Analysis

This report is *not* just a product or CISO view of the security market. Rather, it's a *marketing* perspective: how do event marketers see the cybersecurity landscape, and their role in it? What do *they* think that security buyers are looking for and buying? That is then filtered through a CISO/VC perspective.

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 cold outreach to those leads. As a result, larger exhibition floors often have a Halloween feel to them, with attendees trading their contact information in exchange for some piece of marketing shwag. Smaller exhibition floors still have some of that feel, but smaller booths with open sides makes them more approachable.

Booth Overview

The Continued Dominance of AI and Agents

Much like RSAC, 35% of the exhibitors mentioned AI or agents in their marketing. Rarely did it feel like specifically AI-focused solutions.

The Oxford Comma

The AP Style Guide eliminates the Oxford comma, but they're still *wrong*. Even if you don't agree with me, failing to use it in your marketing is picking a fight with your potential buyers that you don't need. I spotted three that used it correctly. The only vendor that didn't, had two rollups, side-by-side. One did not have an Oxford comma ... but the other did. That feels like a challenging inconsistency.

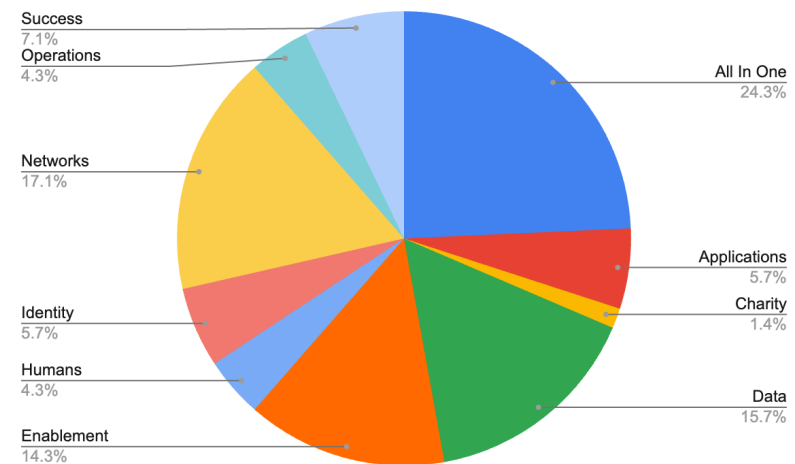
Booth Behaviors

I started walking the exhibitor space during a talks sessions, so I garnered far more attention than I normally do. The layout of the exhibitor space also made it more difficult to assess a booth from afar. I didn't record data (next time!), but I noticed that about a third of the exhibitors had someone who noticed me, made their own assessment of whether they should engage or not, and about a third of those then would wander over to chat with me. About half of the staff who learned what I was doing then asked for an impromptu assessment of their booth.

Design Spectacles

Almost none of the booths held a strong design theme, other than the coffee and candy bars, but do those count?

Category Breakdown



You might look at that chart above and find some surprising things. *There isn't an AI category*, for instance. Other names might be confusing. The guiding principle for this categorization is based on the *environment* that the solution targets.

All In One (17)

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. 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 (4)

Usually the largest category, Applications covers not only traditional AppSec, but also AI Safety tools. AppSec itself is already a fairly wide category, including software supply chain, application testing, runtime security, and some web delivery/browser layer security vendors. Instead, here it's one of the smallest categories.

Data (11)

From DSPM to DLP, with sides of encryption, backup, and 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 or Success focused vendors. Tools focusing on protecting data from AI get included here.

Enablement (10)

Scattered across show floors you'll find Hardware, Internet, Software, and Workforce Development vendors to incorporate into your own products.

Governance (0)

The Compliance Management & Third Party Risk Management spaces come together into the Governance tools category, which sits very adjacent to the Success management category. *Not a single exhibitor at AtlSecCon was in this space.*

Humans (3)

Core to any environment are the endpoints, whose EDRs are so ineffective that we have an entire Human Risk Management space. HRM includes both technical controls like email filtering as well as security awareness training. Several EDR vendors have now branched out sufficiently to be recategorized into the All-in-one space.

Identity (4)

Spanning IAM, IGA, MFA, ITDR, as well as non-human identities, this is a space that is exploding thanks to the rise of agents, since the "I" in "AI" certainly doesn't stand for Identity. This is another space that felt like it had a rather lackluster presence despite the problem space's size.

Networks (12)

A triple space, Networks includes traditional NDR capabilities, as well as SASE, ZTNA, and DDoS Defense. The CDNs generally ended up here (although there is an argument that they should be in Applications, most of their messaging all ends up here).

OT (0)

There are generally a small handful of exhibitors focused directly on the OT, ICS, and IoT worlds. Here, while there were three exhibitors who do work in the OT security space, their messaging at AtlSecCon minimized that as part of larger messaging.

SaaS (0)

While SaaS Security messaging has dropped off in favor of AI messaging, the zero above isn't an indication of a pivot. No SaaS Security vendors were present.

Operations (3)

Whether you're providing a data pipeline, a SIEM, Security Operations/Automation, or Detection Engineering And Threat Hunting, Operations usually comes in at a much larger proportion than this.

Success (5)

In addition to the long-running CTEM and CSPM spaces, there are a growing number of vendors directly focused on helping security teams just configure the controls that *they've already paid for* to achieve Security Success.

Intelligence (0)

All of the offensive security vendors were clearly marketing themselves either as CTEM (part of the Success category) or as Application security vendors, and there were no pureplay Threat Intelligence companies.

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.

