All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

What's new at the RSA? Nothing (almost).

I spent the day walking around the RSA and meeting with folks at untold hundreds of booths. I spent the early evening visiting every one of the "startup" companies. The first most important thing to note is that there was nothing really new. That is not to say that there was nothing interesting...

Standouts

We don't name cyber-security companies, but we do notice interesting trends and exceptions to them, and don't mind naming some folks here and there.

- Most of the recently funded startups ($10M from Bain Capital or similar in the last month or three) seem to be focused on applying the same things already done in networks and endpoints to networks and endpoints in the popular cloud environments.
  - This looks like a strategic play from Bain (and/or others) with the basic concept that these companies will get enough of a following and adequate integration to be acquired as value-add service providers by Amazon, Google, and other cloud providers as the security add-ons, or by existing providers in this arena to capture the market they have not directly addressed yet.
  - Like the pharmaceutical business, these major providers are not doing their own apparent R&D in these areas, so startups will build this out, get enough traction or whatever so the big companies can make an offering, and sell out to big players.
  - Most of the cloud-oriented plays are building to Docker or other platforms that span multiple cloud service providers so the same core can run everywhere.
  - In other words, the same old same old.
- A few interesting areas where players are seeking to emerge include:
  - Measuring authenticity and truthfulness is an interesting one. Using structured questions like counter-intelligence polygraph examiners do, questions over the phone or via other means are put to individuals to detect deception and this is used as a metric for reliability / suitability / authenticity. This is helpful particularly in original identification and high surety periodic or high valued transaction checks. Similarly reduced sign-on spread to all other access mechanism (car / door / etc.) is gaining traction, and there are many small players in this space. The onces getting funded to the tune of $10M are likely to prevail, but some of the smaller players have a chance if they can get good strategies in place and assistance in the channels.
  - Improving the quality and effectiveness of process is a very interesting and important area as well. For the most part, new technology is not necessary to be successful at defending, but having systematic processes that work reliably is, whether with new or existing technologies. Companies seeking to do this through

nearly complete automation and integration with work flows adding human intervention where appropriate are a very important long-term area that is getting too little attention today.

- Deception is rising as there are 8-10 participants, several of whom have gotten $5-$50M in funding, but only a few of which are performing well. Some have contracts with major players, but traction is slow, potentially because their approach to selling to end users is flawed. But it is also an area where the technology works well, and adoption over time is likely, with consolidation coming several years out as the market matures.
- Intelligence and counter-intelligence in the social sphere is finally being recognized as important enough to be able to sell and buy some of it. Closely related is the psychometrics space and related detection methods, which even with their currently low reliability bring some substantial value in niche areas. Note that these issues were screamed from the hilltops to largely deaf ears by Donn Parker, certainly in the 1970s and perhaps earlier. This has some time to go before it really starts to take hold, but as if does, it will become a major component of influence operations and perhaps in a few (5-10) years fuse with the deception space and reduction of security load arena to form a major component of every major program.

So when I say there is nothing new, I really mean to say that progress is incremental and perhaps appropriately focused on better execution, better covering areas previously ignored, and a business focus rather than a technical breakthrough focus.

An buyer/seller approach to adopting these solutions

As many of my readers know by now, in addition to being an industry analyst (this article series has now run for about 24 years), I am also increasingly involved in the investment and advisory space for early stage and emerging companies and the exit arena for market leaders. My views above are focused on a market analysis, but I think this can also be helpful to buyers in buying and providers in selling in these arenas.

- **For large enterprise buyers**, each of these emerging areas are well worth doing limited tests, perhaps with several vendors. Pricing issues tend to be negotiable, and it will be important to start to understand how these technologies and approaches work regardless of the level of likely adoption in the short term. It seems very likely that each will be important over time, and being late to test them will likely mean a significant disadvantage in later deployments, among other reasons, because you will have less influence over getting what you want if you wait.

  It may help to work with your advisors and consultants who are in these arenas already to work with the providers to develop these approaches rather than laying it on your existing staff, who are likely overwhelmed with day-to-day operations.

  An alternative that would work would be to hold collaborative bake-offs similar to the Catalyst conference Burton Group events where many potential buyers saw many providers in specific niches in a single room showing not only how the work, but how they integrate both with each other and with different operating environments. I think we might be able to convince at least one such conference to hold such an event as part of their fall conference this year...

- **For mid-sized companies**, you will likely have to wait for channel partner adoption unless you are aggressive in seeking these solutions, because reaching the middle market is hard and slow for emerging technologies and companies.

  We are hoping to help address that issue over time, but I wouldn't hold my breath. In particular, there are some major players doing platform as a service, and there are some major players who are already in the mid-market. The opportunity for mid-market channel partnerships is growing, and I suspect that within 1-3 years many of these companies will be able to reach out to, or at least be readily available to, mid-sized companies wishing to improve their protection.

  Having said this, a key component to success in this arena is automation of the execution of the protection architecture. So-called security orchestration / dev-ops / etc. are the names being used, but regardless of what you call them, without automation, small- and medium- sized companies will have a hard time running the set of protective functions on their own. Thus the emergence of security-as-a-service providing a wide range of protective mechanisms in well-managed bundles, and even better, through cloud service providers, will be the likely best hope for improvement in this area.

- **For early stage providers in these spaces**, current and near-term traction is likely to be limited by your contacts and access to channel partners. It is rarely the best technology or the first to market that wins the day in these spaces. Early players with substantial funding are already educating the market, but some good quality and better managed followers are likely to win out. My view is that you should seek out conferences with bake-offs in the emerging spaces, get in front of more enterprise players, find channel partnerships with mid-market companies who already have a foothold, …

  OK – just kidding. When you are small and trying to emerge, you cannot try everything. Rather, each company will have to find their niche and work toward it. There is no single strategy that will work. I do advise you to be cognizant of the limitations in the market as well as your own limitations, and seek out areas with matches that allow you to gain traction where you can "land and expand". Otherwise, the cost of sales will end up too high, the turn time will take too long, and you will not grow fast enough to win the race, or at least end up in the money.

Moscone

One last mention here. Moscone Center's new configuration is a big improvement, at least for the RSA. It's a bit confusing for old-timers, but the space for many more companies makes the show all the more informative in terms of seeing who's in the space, and the fusion of the North and South areas into one enormous show floor is, in my view, all good. It was less noisy and easier to navigate, with more earlier stage companies present. All of this is good, for me...

Conclusions

"Nothing new" applies to the security market in general as well as the technologies. The same patterns we saw in the late 1990s seem to be present today. Better, faster, cheaper – sure - but easier also continues to dominate the market. Finding the positive value for customers rather than just selling fear is the real winner. And I think there emerging areas can do that.

