Sales Pulse Research Update **May 15, 2024**

SPR Update - Security - Takeaways from RSA (PANW, CRWD, S, OKTA, ZS, Select Private Companies)

We attended RSA and picked up a variety of observations. Most were consistent with the views we presented in our pre-RSA note for vendors with April 31 fiscal quarter ends.

RSA was well attended. We heard ~50,000+ attendees but there were ~35 fewer exhibitors than last year. Hot topics: AI, Identity, CNAPP, SASE, Next Gen SIEM, DSPM.

Key Takeaways:

- Slightly elevated discounting persists to help move deals in this challenges spending environment. Budget is there but spending is challenged.
- Vendor consolidation trend continues.
- 2H pipeline/forecasts appear more based on expectations & hope verses actual forecasted deals and projects.
- US Fed feedback is that the last 4 months where “steady” and good but not the blow out quarters companies experienced last year. It’s also possible there could be some large deals that we don’t know about for companies like PANW, ZS. The expectation is that USFed spending from now, until end of Sept, will be about 15% higher than last year.
- Next Gen Siem (CRWD, PANW, S) is seeing solid traction, large deals, often 7 figure. Many claims of moving off Splunk/Logrythm/IBM Qradar and saving up to 80%.
- SASE still solid but also characterized by rapid increased competition, NetSkope and Cato coming on strong. Cato booth was very busy, and winning with solid technology and better pricing compared to PANW/ZS so they are seeing some takes outs.
- Still picking up concerns about FortiSASE - multiple products, cloud architecture a combo of their own 4 POPS and Google on ramps, poor internal support, etc. Often requires on site FW to perform some functions referred to “on prem SASE”.
- Identity related solutions all VERY STRONG. Pertains to OKTA, CYBR, MSFT and ITDR (crwd and S) and also cloud CNAPP.

Vendors

CRWD

At this point channel feedback on Crowdstrike is the strongest of the April 31 qtr end companies. This includes some indications they may have stopped or slowed shipping with distribution before Qtr end. Crowdstrike announced Falcon for Defender at RSA. This product targets all the MSFT Defender shops that realize Defender is deficient and they can put Falcon for Defender next to it, and CRWD sees and stops what Defender misses…..nice move.

CRWD also announced Falcon next-generation SIEM for AI-native SOCs. As part of the enhancements, the vendor expanded the use cases of its genAI security analyst tool Charlotte AI. "Charlotte AI now is available for all data in the vendor's next-gen SIEM, which allows analysts to ask any question of Falcon data in the Falcon platform in plain language, including product documentation or Knowledge Bases."

PANW

Palo Alto did not exhibit at RSA…a bold move. Palo announced, during RSA, its proprietary AI system that combines genAI, machine learning (ML) and deep learning (DL) capabilities. It is built on the vendor's security dataset and proven playbooks and designed for guided automation and actionable insights.

We did pick up more positive feedback around EU Distribution which piggybacks off of our previous US Disty "in-line" sentiment. EU looks a bit stronger than US, at this point. Note that PANW now does a significant business through the Marketplaces, and also direct between the VAR/Reseller and Palo. IE the ~140M UHC deal was between Optiv and Palo…..it did not go through Two Tier Distribution. It is becoming more common for the larger deals to be direct between the VAR and Palo.

We consider it positive that Two-Tier Distribution is "holding its own" while these other "competitive" purchasing channels increase in business.

S

We picked up a lot of legitimate excitement and momentum around SentinelOne. Both CRWD and S are seeing more "boomerang" opportunities when MSFT shops come back to revisit their Defender decision. S DataSet next gen SIEM has solid traction that includes functionality including better ingestion/storage capabilities (CRWD partners with CRBL for this). Purple AI is off to a good start, unlimited/very flexible # of AI queries.

And they announced "CNAPP with unique Offensive Security Engine™ that thinks like a hacker to move beyond the theoretical and deliver Verified Exploit Paths™" . A revolutionary solution built on SentinelOne's acquisition of PingSafe in February 2024. The agentless Cloud Native Application Protection Platform (CNAPP) is uniquely designed to assess environments like a hacker would, simulating attack methods to provide a prioritized, evidence-based list of exploit pathways that security teams can use to prioritize their time and prevent attacks before they happen.
As we discussed in our May 6th note, S has a serious focus on CNAPP and is optimistic they can be successful.

OKTA

Per the May 6th note it does appear Okta is back to BAU (Biz As Usual) plus a more stable sales team. We also heard that IGA and PAM are contributing additional revenue.

While in a meeting with CYBR, they shared that they are encountering OKTA PAM more in the lower end of the market.

ZS

While ZS is an impressive company, we are not picking up the same levels of enthusiasm as in past. There could be some large USFed deals not on our radar. Perhaps the competitive environment is complicating and slowing deals. Perhaps the folks leaving ZS heading to Wiz/Dali, while at the same time NOW folks following Mike Rich to ZS, is possibly causing some short term disruption.

Interesting private companies…a few stand outs in our opinion

Cato Networks – appears to be getting more traction and breaking out from SMB into Large Enterprise. They apparently won a 7 figure deal w Ulta Beauty. Cato built a solid global network (like NetSkope), supported by an impressive data lake, and even XDR. They also have managed services offerings. Cato has solid technology, reduces complexity (converged SASE and SDWAN) , and is less expensive than PANW and ZS. Cato's product is all built in-house. They have 2,300 customers and over 80 POPS globally. They also combine both network and security and treats all traffic the same if it's from the cloud or on prem.
Cato has taken out both PANW and ZS based on better price and functionality. Cato, like NetSkope, shares that if they are in the POC, they win 70% of the time. Cato also has a solid play around their ability to rapidly deploy, compared to some competitors.

Cyera - relatively new in the DSPM space. Palo bought Dig, Crowdstrike bought Flow, and there is stand alone vendor VRNS. We found Cyera (agentless) impressive based on a new platform (compared to VRNS having been around for years) that "continually discovers, classify, protect, and monitor in any cloud data store." "Automatically uncover the data an organization has, how it's managed, and how to remediate the security and compliance risks that are uncovered." This continual discovery and protection of data is becoming a big deal. Cyera starts discovering in hours, and with APIs (that VRNS might not have) ties into cloud providers, and in a comparatively short time (day/days verses weeks) discovers and classified all data. Cyera should be watched to monitor the potential impact on VRNS.

NetSkope – We are still seeing NetSkope having positive traction, and establishing a solid VAR channel that has been increasingly impressed with both the product and company. They now have ~3,500 customers (typically larger companies compared to Cato's 2,300 customers mostly SMB). NetSkope has also built a fast, low latency, global network on top of their CASB/DLP DNA which offers a solid Zero Trust approach. At RSA they shared the new AI functionality that only blocks certain aspects of sites like ChatGPT scanning for, and stopping, sensitive information. NetSkope also has FedRAMP HI status which should do well.

Ordr – Armis is main competitor and has been around many years, and doing well, we hear Armis may be sniffing around to IPO. Ordr pops on the scene and states much better at asset discovery in IoT, OT, and IoMT (medical). As example medical devices

are unplugged, rolled around, etc and can be counted 2x+ so not accurate. Bottom line is no one know all assets so it's crucial the assets are discovered in detailed, and accurate. They have a relationship with CRWD for asset discovery. "Automatically ID devices with risks and vulnerabilities, simplifying the generations of zero trust segmentation policies. It also proactively segments vulnerable and mission-critical devices, reducing the attack surface PRE-attack……preventing thousands of lateral movement attempts." We found Ordr impressive, mature demo, and possibly disruptive to Armis.

Torq- focused SecOps and "hyperautomation" of security teams removing security teams manually managing threat detection and remediation at scale, and ensuring their systems are talking to each other , and working together in concert. Torq is AI-powered enabling a fast learning curve. Competition is PANW/Demisto, Swimlane, SPLK, and IBM.

As always, we are happy to discuss in more detail,

Important Disclosures:

Facts and the other information contained in this report have been obtained from public sources considered reliable but are not guaranteed in any way. No independent confirmation of the truth, correctness or accuracy of the information presented has been

made by Sales Pulse Research, LLC.

This report is published solely for information purposes and is not an offer to buy or sell or a solicitation of an offer to buy or sell any security or derivative. Sales Pulse Research, LLC accepts no responsibility for any loss or damage suffered by any person or entity as a result of any such person's or entity's reliance on the information presented in this report. Opinions and estimates expressed herein constitute judgments as of the date appearing on the report and are subject to change without notice.

Employees of Sales Pulse Research, LLC may from time to time acquire, hold or sell a position in the securities mentioned herein in this report.

All of the recommendations and views about the securities and companies in this report accurately reflect the personal views of the analyst(s) of Sales Pulse Research, LLC. No part of analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the research analyst.

Contact:

Tom Morphis
Sales Pulse Research, LLC ®
(404) 217-7626
www.salespulse.net
tom@salespulse.net

Sarah Crane
Director of Channel Relationships and Business Development
Sales Pulse Research, LLC
(704) 989-2930
sarah@salespulse.net
www.salespulse.net

Steve Thompson
BI and Analytics, Observability
Sales Pulse Research, LLC®
704-467-6749
steve@salespulse.net

Michael Millar

Sales Pulse Research, LLC
mike@salespulse.net
941-209-8788
www.salespulse.net

Mike Rothman
Cyber Security Contributing Analyst
Securosis, LLC
www.salespulse.net

Greg Flick
UCaaS Contributing Analyst
Sales Pulse Research, LLC
www.salespulse.net