The pandemic not only accelerated a shift to digital, it highlighted a rush of cyber criminal sophistication, collaboration and chaotic responses from virtually every major company on the planet. The SolarWinds hack exposed digital supply chain weaknesses and appears to have accelerated so-called island hopping techniques that are exceedingly difficult to detect. Moreover, the will [...]

© 2021 Wikibon Research | Page 1
The pandemic not only accelerated a shift to digital, it highlighted a rush of cyber criminal sophistication, collaboration and chaotic responses from virtually every major company on the planet. The SolarWinds hack exposed digital supply chain weaknesses and appears to have accelerated so-called island hopping techniques that are exceedingly difficult to detect. Moreover, the will and aggressiveness of well-organized cyber criminals has elevated to the point where incident responses are met with counter attacks designed to both punish and extract money from victims via ransomware and other criminal activities involving a double extortion maneuver. One upshot is the cybersecurity market remains one of the most enduring and attractive investment sectors for those that can figure out where the market is headed and which firms are best positioned to capitalize.

In this Breaking Analysis we’ll provide our quarterly update on the security industry and share new survey data from ETR and theCUBE community that will help you navigate through the maze of corporate cyber warfare. We’ll also provide our thoughts on the game of 3D chess that Okta CEO Todd McKinnon is playing against the market.

**Cybersecurity: Complicated, Fragmented Fast-moving**

And this chart below says it all.

It’s an interactive graphic from Optiv, a Denver, CO-based SI focused on cyber. They’ve done some excellent research and put together an awesome taxonomy. And mapped vendor names within the framework to help users navigate the complex security landscape. There are over a dozen major sectors within the security market and nearly 60 sub-sectors. From monitoring, vulnerability assessment, identity, asset management, firewalls, automation, cloud, data center, SIEM, threat detection and intelligence, endpoint, network and on and on. It’s a terrific resource and can help you understand where players fit and connect the dots in the space.

**Market Dynamics in Cyber are Consistently Frustrating & Lucrative**

Since the beginning of cyber time we’ve talked about the increasing sophistication of the adversary and the
back and forth escalation between good and evil. And unfortunately this trend is unlikely to stop. An increasing concern is that criminals continue to escalate their collaboration, now offering ransomware-as-a-service.

An increasing concern is that criminals continue to escalate their collaboration, now offering ransomware-as-a-service (RaaS) on the dark Web. With RaaS, criminal organizations with insider access to corporations can outsource the technical aspects of the hack. These services are highly organized with help desks and support teams that will collaborate with other criminals to steal valuable information, negotiate ransoms and extort victims.

### Market Dynamics in Cybersecurity

- Continued sophistication of adversaries*
  - Destructive attacks up 118% from 2020
  - More than 50% of attacks targeted non-public market information
  - 57% of surveyed banks saw an increase in wire fraud
  - 38% of banks reported an increase in “island hopping” activity
  - 63% of the time, adversaries counter attack when discovered
  - 75% of CISOs surveyed report to the CIO
- Cloud, endpoint & identity remain key themes
- Migration to cloud triggers a change in IAM (ESG Stat)
- Market remains highly fragmented
- M&A is accelerating - Transaction volume up 40% past 5 months

*Key findings from VMware’s Modern Bank Heists 4.0 report

The first bullet and sub bullets contain findings from Carbon Black’s annual Modern Bank Heists report – this is the fourth and of course is now under VMware’s brand as the Carbon Black acquisition catalyzed the creation of VMware’s cloud security division.

Destructive malware attacks according to the recent study are up 118% from last year. One major takeaway from the report is that hackers aren’t just conducting wire fraud – they are – 57% of banks surveyed saw an increase in wire fraud activity – but the cyber criminals are also targeting non-public information such as future trading strategies. This allows the bad guys to front run large block trades, which has become a very lucrative practice.

The prevalence of so-called island hopping is up 38% from an already elevated level. This is where a virus enters a company’s supply chain via a partner and then often connects with other stealthy malware. Techniques are increasingly common where the malware will self-form with other infected parts of the digital supply chain and create actions with different signatures, designed to confuse defenses and target valuable information for exfiltration.

Of major concern is that 63% of banking respondents in the study reported that responses to incidents were met with retaliation designed to intimidate or initiate a ransomware attack to extract a final pound of flesh from the victim. Often with a double extortion gun pointed at the victim’s head that threatens the release of sensitive information that could damage the victim further.
Notably, the study found that 75% of CISO respondents reported to the CIO, which many feel is not the right regime. The study called for a rethinking of the cyber organization, where the CISO has increased responsibility and a direct reporting line to the CEO or COO, with greater exposure to boards of directors.

Many thanks to VMware and Tom Kellermann specifically for sharing this information with us this past week. Great work by the team.

**Recurring Themes in Cyber**

The next set of bullets in the above chart have been derived from previous episodes of Breaking Analysis and continue to evolve.

Cloud of course is the big driver thanks to work from home and the pandemic. And the interesting corollary we see is a rapid re-thinking of endpoint and identity access management and the concept of zero trust. In a recent ESG survey, two thirds (66%) of respondents said that their use of cloud computing necessitated a change in how they approach identity access management (IAM).

As shown in the first graphic from Optiv, the market remains highly fragmented and M&A is way up. Based on our research, it looks like transaction volume has increased more than 40% in the past five months.

**Digging into M&A Activity**

We took a five-month snapshot and were able to count about 80 deals completed in that timeframe.

**Hot Cyber Market - M&A Activity Since December 2020**

- ~80 deals completed in the past 5 months
- More than $20B in transaction value
  - Proofpoint ($12.3B), Auth0 ($6.5B), Armis ($1.1B), IMImobile ($0.73B)
- Themes:
  - SI’s going local - Accenture, Atos, Wipro
  - Israel remains a hotbed of innovation - 5 acq. in the last 5 mos
  - Financial services co’s getting involved - Mastercard, Goldman
  - TAM Expansion - Okta, Crowdstrike, Cisco, Rapid7, Tenable, Fortinet, Sailpoint, PANW, Zscaler, VMware

Those transactions represented more than $20B in value. Some of the larger ones are highlighted above. The biggest of course being Thoma Bravo taking Proofpoint private for a $12.3B price tag. The stock went from the low 130s and is now trading in the low $170s based on the $176 per share offer- a very nice premium paid by the private equity firm.

Perhaps the more interesting acquisition was Auth0 by Okta for $6.5B, which we’ll talk more about in a moment. More private equity action was seen as Insight bought Armis, an IoT security play and Cisco shelled out $730M for IMImobile, which is more of an adjacency to cyber but it will go under Cisco’s security
and applications business run by Jeetu Patel.

But these are just the tip of the iceberg. Some of the themes we see connecting the dots of these acquisitions are:

1. **SI’s go Local.** SI’s like Accenture, Atos and Wipro are making moves in cyber to go local...buying secops expertise locally in France, Germany, Netherlands, Canada and Australia;
2. **Israel Remains a Hub of Innovation.** Israeli-based startups chalked up five acquired startups in the space over the last five months;
3. **Financial Services in the Act.** FS firms are getting into the act with Goldman and Mastercard making moves to own parts of the stack themselves to combat fraud and identity theft; and
4. **TAM Expansion.** Numerous moves to expand markets and fill holes. Okta with Auth0, Crowdstrike buying a log management company, Palo Alto Networks picking up DevOps expertise, Rapid7 shoring up its Kubernetes chops, Tenable expanding beyond insights and going after identity, Fortinet filling gaps in multi-cloud, Sailpoint extending GRC, Zscaler picking up an Israeli firm to fill gaps in access control, and VMware buying Mesh7 to secure modern app development and distribution services.

Tons of activity in the space and it appears to be accelerating.

**Comparing Cyber Spend Relative to Other Tech Sectors**

ETR uses the concept of market share which is a measure of pervasiveness in the survey. So for each sector it calculates the number of responses divided by the total to get a sense for how prominent the sector is within the CIO and IT buyer communities.

The chart above shows the full ETR tech sector taxonomy with security highlighted across three survey periods, April last year and January and April of 2021. You shouldn’t expect big moves in market share over time – so relatively stable by sector. The big takeaway comes from observing which sectors are most prominent. That red dotted line is imposed at 60% and you can see there are only six sectors above that line and cyber security is one of them.
We know security is important and a large market but this puts it in context of other sectors.

**Cyber is not an Open Checkbook for CISOs**

We know from previous Breaking Analysis episodes that despite the importance of cyber and the urgency catalyzed by the pandemic, budgets are not unlimited and spending is actually bounded— it’s not an open checkbook for CISOs as shown in this chart below.

![Graph showing market share and net score](chart.png)

The above graphic is a two dimensional chart showing Market Share on the horizontal axis and Net Score on the vertical axis. Net Score is ETR’s measurement of spending velocity. And we’ve superimposed a red line at 40% because anything over that we consider extremely elevated. We’ve limited the number of sectors to simplify the graphic. And you can see only the big four, containers, AI, RPA and cloud, exceed that magic water line.

Information security is highlighted in red and is respectable, but it competes for budget with other important budget items.

This of course creates challenges for organizations because not only are they strapped for talent as we’ve reported. In addition, like everyone else in IT, they face ongoing budget pressures. Research firm, Cybersecurity Ventures estimates that in 2021, $6 trillion worldwide will be lost on cyber crime. Conversely, research firm Canalys pegs security spending somewhere around $60B annually. IDC has it much higher at around $100B. So either way, we’re talking about spending between 1% to 1.6% annually as a percentage of what’s stolen. This is tiny when you consider the consequences.

**Double Clicking into the Cyber Company Landscape**

Below is the same XY graphic with the cyber companies respondents report using in the ETR survey. The usefulness of the red lines is to the right of 20% on the horizontal axis indicates the largest presence in the survey. And the magic 40% line shows those firms with the most elevated momentum on the vertical axis.
Only Microsoft and Palo Alto exceed both high water marks. But Splunk and Cisco are prominent horizontally. And there are numerous companies to the left of the 20% line and many above the 40% mark on the vertical axis.

The bottom left quadrant includes many legacy names that have been around for a long time and there are dozens of companies scoring higher that show spending momentum on their platforms - i.e. above single digits.

So that picture is like the first one we showed you...a very crowded space.

**Zoom in on Some of the Leaders**

Below we present the same graphic dimensions and we’ve superimposed the data that determine the plot positions on the lower right. Net Score and Shared N including only companies with more than 100 N.
What does this data tell us about the market? Microsoft is dominant as always — it seems in all dimensions. But let’s focus on that red line for a moment. Some of the names we’ve highlighted over the past two years show well.

First Palo Alto Networks. Pre-COVID lockdown, as you may recall, we highlighted the valuation divergence between Palo Alto and Fortinet. We said Fortinet was executing better on its cloud strategy and Palo Alto was, at the time, struggling with the transition, especially with go to market. But we told you that we were bullish on the company because of its track record and the fact that CISOs consistently tell us they see Palo Alto as a thought leader in the space and they want to work with the best...especially the larger company CISOs. Palo Alto has recovered very nicely and is rapidly moving customers to its next generation platforms. We remain impressed by the company’s execution and ability to compete.

Some other names that hit our radar in the ETR data a couple of years ago continue to perform well, specifically Crowdstrike, Zscaler, Sailpoint and Cloudflare. Cloudflare just reported and beat earnings but was recently off on tech headwinds as it got caught in the rotation. But the company is doing well, growing nicely and has momentum as you can see from the ETR data.

We put the double star around Proofpoint to highlight that it was worthy of fetching $12.3B from private equity - so nice exit there- supporting the continued consolidation trend.

The Okta Chess Match

Let’s turn our attention to Okta and Auth0. This is a very interesting play for Okta and we want to drill into it a bit.

Okta is acquiring Auth0 for big money. Why? Well we think Todd McKinnon wants to run the table on Identity and then continue to expand his TAM, which he must do to justify a $30B+ valuation. Okta’s ascendency around identity and single sign-on is notable. The fragmented pictures we showed earlier scream for simplification and trust and that’s what Okta brings. But it competes with some major players, most notably Microsoft with Active Directory. So of course Microsoft is going to dominate in its massive customer base but the rest of the market was wide open and McKinnon saw the opportunity to dominate.
Okta comes at this from an enterprise perspective, bringing top/down trust to the equation and throwing a big blanket over all the discreet SaaS platforms and unifying employee access. Okta’s timing was perfect as it was founded in 2009, just as the massive SaaS-ification trend was happening around CRM, HR, service management and cloud.

But the one thing that Okta didn’t have that Auth0 does is developer chops. While Okta was crushing it with its enterprise sales strategy, Auth0 was laser focused on developers and building a bottoms up approach to identity. By acquiring Auth0, Okta can dominate both sides of the barbell and capture the fat middle.

So yes it’s a pricey acquisition but in our view it’s a great move by McKinnon.

We haven’t interviewed McKinnon but last week we spoke to Arun Shrestha, the CEO of security specialist BeyondID, a platinum services partner of Okta and zero trust expert. He worked at Okta for a number of years and shared with us a bit about McKinnon’s style and think big approach.

Shrestha said something that caught our attention. He said “firewalls used to be the perimeter, no people are...” And while that’s self-serving to Okta and probably BeyondID – it’s true. People, apps and data are the new perimeter and they’re not in one location. That’s the point.

Now we had lined up an interview with Diya Jolly who is the Chief Product Officer at Okta for this past week, knowing we were running this episode but she unfortunately fell ill the day of our interview and had to cancel. But we want to follow up with her and understand how she’s thinking about connecting the dots with Auth0, devs and enterprises.

Looking Deeper into Identity Shows Okta’s Hand

The chart below depicts several of the major identity players with a a breakdown of ETR’s Net Score for each.

---

Net Score comprises five elements. The lime green is adding the platform new. The forest green is spending 6% or more, the gray is flat spend, the pinkish is spending less and the bright red is leaving the platform. Subtract the red from the green and you get Net Score, which you can see superimposed on the
right hand chart at the bottom...the first column. The second column is Shared N which indicates the number of responses and is a proxy for presence in the market.

Look at the top two players in terms of spending momentum. SailPoint is right there too but Auth0 combined with Okta’s distribution channel will extend Okta’s lead in our view.

And then there’s Microsoft with a big presence and momentum. One caveat is this includes all of Microsoft’s security offerings, not just identity - but it’s there for context. And CyberArk as well includes its acquisition of Idaptive but also other parts of the CyberArk portfolio. And you can see some of the other names, many which you’d find in the Gartner Magic Quadrant for identity.

As we said...we really like this move by Okta. It combines positive market forces with lead offerings from well run companies...that have winning DNA will passionate people.

Okta’s Presence in CyberArk & SailPoint Accounts Looms Large

To further emphasize what we see happening in identify, take a look at the data below. The chart shows ETR data for Okta within SailPoint and CyberArk accounts. Out of the 230 CyberArk and SailPoint customers in the data set, there are 81 Okta accounts – that’s a 35% overlap.

And the good news for Okta is that within that base of SailPoint and CyberArk accounts, Okta, as shown by the Net Score line, highlighted in green, has very elevated spending momentum. And the kicker is if you read the fine print in the column, ETR correctly points out that while SailPoint and CyberArk have long been partners with Okta...at the recent Oktane21 event, Okta announced that it was expanding into privileged access management (PAM) and identity governance. Hello to co-opetition in the 2020s.

Our current thinking is that this bodes well for Okta and CyberArk and SailPoint will have to make some counter moves to fend off an onslaught of Okta in its accounts.
Tracking the Four Star Cybersecurity Firms

We'll wrap up with what has become a tradition on our quarterly security updates. In the charts below, we look at the two prominent dimensions of Net Score and Market Share. Our goal is to observe which companies crack the top 10 for both measures within the ETR data set. Again in this cut we eliminated any firm with less than 100 responses.

Above on the left we have the top 20 sorted by Net Score or spending momentum and on the right we sort on Shared N, which informs the Market Share metric or presence in the data set. The red horizontal lines separate the top ten from the remaining 10 within the top 20.

Our methodology assigns four stars to those companies that crack the top 10 for both metrics. Once again, maintaining that status we see Microsoft, Palo Alto Networks, Okta and Crowdstrike. Those four are joined by Fortinet, which has cracked four star ranks this quarter.

And we give 2 stars to those companies that make it in both categories within the top 20. So Cisco, Splunk, which has been steadily decelerating, and Zscaler, which is just on the cusp. And we kept Carbon Black on the rightmost chart as #21 only because they are just outside looking in on Net Score and with VMware’s presence in the market we think Carbon Black is worth tracking more closely.

Final Thoughts – A New Era of Cyber is Here

Last quarter we did a deeper dive on the SolarWinds hack and we think the ramifications are significant. It has set the stage for a new era of escalation an adversary sophistication.
A major change we see is a heightened awareness that when you find intruders you’d better think carefully about your next moves. When someone breaks into your home, if the dog barks or you come down with a baseball bat or other weapon, you might think the intruder will flee. But if the criminal badly wants what you have in your house, and it’s valuable enough, you might find yourself in a bloody knife fight – or worse.

What’s happening is intruders come to your company via island hopping or insider subterfuge or whatever method. They’ll live off the land, using your own tools against you so they can be stealth. They’ll steal sensitive data – for example, positive COVID test results or other medical data. And when you retaliate, they will double extort you. Meaning, not only will they encrypt your data and hold it for ransom. At the same time they’ll threaten to release the sensitive information, crushing your brand in the process.

So your response must be as stealthy as their intrusion as you marshal your resources and devise a plan.

And you face serious headwinds. Not only is this a complicated situation, but there’s an ongoing and acute talent shortage. As well, many companies are mired in technical debt. Balancing the running of the business, while affecting digital transformations is hard. And risky because the more digital you are, the more exposed you become.

So this idea of zero trust, which people used to call a buzzword, is now a mandate along with automation, because you can’t throw labor at the problem.

Unfortunate or not, this is all good news for investors as cyber remains a market that’s ripe for valuation increases and M&A activity– especially if you know where to look. Hopefully we’ve helped squint through the maze a bit.

**Ways to Connect**

Remember these episodes are all available as podcasts wherever you listen.

Ways to get in touch: Email david.vellante@siliconangle.com | DM @dvellante on Twitter | Comment on our LinkedIn posts.
Check out ETR for the survey data.

Watch the full video analysis:

Photo credit: PR Image Factory

Note: ETR is a separate company from Wikibon/SiliconANGLE. If you would like to cite or republish any of the company's data, or inquire about its services, please contact ETR at legal@etr.ai.
David Vellante is co-CEO of SiliconANGLE Media, as well as co-founder and Chief Analyst at The Wikibon Project, the world’s leading open source technology research community. Dave is a long-time tech industry analyst, entrepreneur, writer and speaker. As co-host of theCUBE - “The ESPN of Tech,” Vellante has interviewed over 5,000 experts since 2010. He is also a co-founder of CrowdChat, an angel funded startup based in Palo Alto using big data techniques to extract business value from social data. Prior to these exploits, Dave founded a CIO consultancy and spent a decade growing and managing IDC’s largest business unit. He lives in Massachusetts with his wife and four children where he is active in town activities including serving as the president of his town’s local "Kiddie Sports" association. Dave holds a B.S. in Applied Mathematics from Union College.

David Vellante
@dvellante
david.vellante@wikibon.org