CISOs see Permanent Shifts in Cyber Strategies due to COVID & Remote Work

As we’ve reported extensively, the pandemic has affected cyber security markets perhaps more than any other. Remote work has caused CISOs to shift spending priorities toward identity access management, endpoint and cloud security. COVID has been a benefactor for nextgen security companies [...]
CISOs see Permanent Shifts in Cyber Strategies due to COVID & Remote Work

As we've reported extensively, the pandemic has affected cyber security markets perhaps more than any other. Remote work has caused CISOs to shift spending priorities toward identity access management, endpoint and cloud security. COVID has been a benefactor for nextgen security companies that participate in these sectors. Notably, we believe tactical responses to the coronavirus have resulted in productivity improvements that will create permanent change in the way organizations defend themselves against cyber threats.

In this week’s Breaking Analysis, we’ll provide you with our quarterly update of the cyber security space and share fresh ETR data on the market. We also have the results from Erik Bradley’s most recent VENN roundtable, conducted with three senior chief information security officers.

No Single Pane of Glass Answer in Cyber

Despite the aspiration, there is no silver bullet to protect organizations from cyber attacks. The complexities of security are quite enormous and require a layered defense approach. They range from securing internal networks to endpoints, DMZ subnets, external traffic security, data in motion, data at rest, protecting from ransomware, dealing with Web traffic and emails/phishing threats. Not to mention threats from internal employees and contractors.

Cyber security snapshot

- No (single pane of glass) silver bullet in sight
- Need for a layered defense continues to fragment the market
- Identity mgt, endpoint & cloud security remain momentum plays
- Hardware-based firewalls continue to be under pressure
- Skills shortage heightens the automation mandate
- Elastic, Netskope, Cloudflare & Carbon Black hit our radar this quarter
- Microsoft, Palo Alto Networks, Okta, Crowdstrike, Cisco, CyberArk, Sailpoint, Zscaler, Proofpoint remain focus vendors
- Even skeptical CISOs believe permanent changes are taking shape

As we mentioned at the open and shown above, there are three areas of security offerings in particular that have seen significantly elevated spending momentum and that has translated to the valuations of several companies including Crowdstrike, Okta, Zscaler and others. Zero trust security has gone from buzzword to reality. Spending shifts to these technologies has siphoned off demand for traditional hardware-based firewalls. Although CISOs seem to be hedging their bets as at some point they realize people are going to come back to the office.

Lack of talent remains the CISOs biggest challenge to securing applications and data and automation, while sometimes viewed as risky, is becoming increasingly important.
Vendor Spotlight

Several companies have hit our radar this quarter and were highlighted in the CISO panel including Elastic, which has seen momentum as an open source alternative to Splunk. Notably, multiple CISOs on the panel cited concerns related to Splunk’s pricing and sales tactics, comparing them to those of EMC of the past.

Cloudflare broke into the top 10 in the ETR survey based on Net Score or spending momentum for those companies with more than 50 mentions in the survey. Cloudflare offers CDN capabilities and provides security for Websites.

As well, Netskope, a cloud security specialist, cracked the top ten in terms of Net Score and received high marks from the CISO panel, particularly with respect to its vision and roadmap.

Microsoft, Palo Alto Networks, Okta, Crowdstrike, Cisco, CyberArk, Sailpoint, Zscaler and Proofpoint remain focus vendors in the ETR survey as measured by spending momentum and presence in the data set. We’ll discuss more about these companies later.

Finally, even CISOs that were skeptical about the permanence of the effects of COVID are seeing business benefits that suggest many of these shifts are secular and not cyclical. Indeed, prior to the pandemic, ETR survey data shows that about 16% of organizations’ workers were primarily remote. CIOs expect that number to more than double post pandemic at 34%.

Plotting the Cyber Security Vendors

The chart below shows one of our favorite views in a two-dimensional graph. On the Y axis we show Net Score, which measures spending velocity by looking at the net percentage of customers spending more versus less money in the ETR survey. The X axis measures Market Share or pervasiveness in the survey. We’ve included a select list of companies for this view and only include those with more than 50 responses in the data. In the upper right you see a table that shows the data sorted by Net Score for each vendor.

Note: We left Microsoft out of this view because they are so dominant in the data set it makes it hard to compare the others. We’ll talk about Microsoft later in this post.
As we indicated, Elastic has taken the top spot just barely edging out Okta who took over from Crowdstrike in the last survey. You can see the significant market presence of Palo Alto, Splunk and the most pervasive vendor, Cisco. Note that Cisco also owns Umbrella and Duo which both have meaningful N’s in the survey. If we were to combine these into one view of Cisco it would pull the company even further up and to the right. Security is one of the bright spots in Cisco’s portfolio and shows consistent year on year growth each quarter.

Having said that, some CISOs complain that Cisco’s propensity to rely on acquisitions to fill gaps has caused them integration challenges in the past.

Let’s come back to Palo Alto for a moment. We’ll make some comments later regarding their position relative to Fortinet but we want to call them out here. CISOs really like working with Palo Alto Networks. They consider Palo Alto a trusted leader with a strong portfolio and vision.

Let’s turn our attention to the pack. As we mentioned, Okta’s momentum is notably elevated and meaningfully higher than the others. Its presence continues to increase to the right as does Crowdstrike’s. However Crowstrike has come off its Net Score highs. We’re not so concerned because they’re dramatically increasing their presence on the X axis each survey…but so it Okta so that’s something to watch.

We’ve included Carbon Black for the first time because they’re a VMware acquisition and have a decent presence in the data set. VMware CEO Pat Gelsigner is on a mission to “fix security” and the company has made a number of moves in cyber. VMware has a very good track record of execution and while fixing security is a highly aspirational move, with its installed base and history of success we wanted to include them here. As well, they are getting the attention of the CISOs in the ETR panel so we’re keeping an eye on VMware and Carbon Black.

How Security Positions Have Changed During COVID

We’re going to show you four tables here, comparing the Net Scores and Market Shares of the cyber companies for the January, April, July and October surveys. So pre-COVID and through the year.
Pre-COVID Positions

The leftmost chart below is sorted by Net Score and the right by Shared N which is the number of mentions in the survey.

![ETR Security Sector Sorted by Net Score and Shared N](chart.png)

When you go back to the January survey, you see Crowdstrike was already doing very well with an elevated Net Score of 68.3% and 123 mentions. Please ignore those companies with less than 50 N as we didn’t filter the data back then. We’re still learning how to best apply the ETR platform. Okta was also elevated and you can see the others on the list.

The rightmost chart is sorted on Shared N, which measures the number of mentions for the vendor in the security sector of the ETR data set.

Last year we came up with a method to assign stars to those companies that had both top Net Scores and large Shared N’s in the survey and you can see Microsoft, Splunk, Palo Alto, Proofpoint, Crowdstrike, Zscaler and CyberArk made the cut and received four stars. And we gave two stars to Cisco and Fortinet because they had strong Net Scores and very high presence in the survey.

April…The Lockdown’s in Full Swing

Ok so we tightened things up a bit in April and only included those companies with more than 50 N. And in the chart below we cut the top 10 – that’s the red line and including Dell EMC (RSA) and IBM for context. And you see Crowdstrike shot to the top and held 66% and increased its Shared N. And you can see the stars on the right.
July...The Dog Days of Summer Bring Hope for an End.

By this point we were well into the pandemic here. CISOs have had time to respond and here was the picture this summer. You can see in the leftmost chart below, Okta jumped way up on the left in spending momentum and Crowstrike moderated - although remained elevated. They are not direct competitors but it’s instructive to compare these firms. And you see the green arrows show the direction of the momentum of the Net Score. Crowstrike was a concern because its Net Score dropped and its presence in the data set moderated. But the company continued to report strong revenue growth and the stock remained a darling. So some mixed signals in the data.
Okta, Microsoft, Cisco, Palo Alto, Splunk, etc. remained very strong

**October...The Pandemic is Back, Investors are Confused**

In the chart below we continue to fine tune our analysis. You can see two red lines. The top one is the top ten cutoff and the second line is the top twenty. As we said, Elastic hit the radar for Net Score but still not pervasive enough to hit the right hand top players with only 61 Shared Ns. So Okta in our view continues to hold the top spot for momentum and made the top ten cut for Shared N. Its Shared N jumped from 139 to 185...so more and more mentions. People are increasingly relying on Okta for identity access management.
Breaking Analysis: Sparked by COVID, CISOs see Permanent Shift in Cyber Strategies

Net Score & Market Penetration for top 20 cyber co’s

For the green arrow – the momentum lines – we’ve tried to take Shared N into account this time, so even though for example Crowstrike’s Net Score dropped from 50% down to 43%, its Shared N (or mentions) jumped from 119 to 162, a 36% jump. You might be thinking why is that significant? Well, CIOs and IT buyers in the ETR survey are asked to choose the areas with which they are most familiar, and then answer which vendors they use. So the fact that companies like Okta, Palo Alto, Crowdstrike and several others we’ve highlighted increase, is a very strong signal in our view.

And that’s why for example we give Zscaler two stars. Even though on a relative basis it didn’t make the top ten cut, its Net Score held relatively firm and its Shared N jumped by 39%. So we continue to like names like Zscaler, Okta, Crowdstrike, CyberArk, Proofpoint, Fortinet. And of course Microsoft, which continues to shine brightly.

CISO Sentiment Acknowledge a Permanent Change

Below a comment from a CISO of a global travel and hospitality company. It’s a name you would recognize and obviously this individual’s business was hit hard by the pandemic. So there’s an inherent bias toward a return to the normal but look at the comment.
We agree.

Valuation Changes During COVID

Below is a chart that we’ve been updating since right before the pandemic hit. It compares the performance of the S&P 500 and Nasdaq with specific security players. And we’ve been tracking the revenue multiples on a trailing twelve month revenue basis over time to get a sense of how these companies compare. And while we prefer to use forward looking revenue, we find TTM to be more consistent and frankly easier to access quickly.
Breaking Analysis: Sparked by COVID, CISOs see Permanent Shift in Cyber Strategies

A couple points here are worth noting. First we’ve been talking a lot about the divergence in valuation between Palo Alto and Fortinet. And we’ll show some more data on that in a moment. But we want to share some CISO comments about Fortinet. People sometimes refer to Fortinet as “Forti-Knife” -as in the swiss army knife of cyber. One CISO called them “Forti-everything.” Fortinet is more price attractive, especially for mid-sized companies who don’t have the resources of larger firms that might gravitate toward Palo Alto Networks. The company has been around for a while and has earned the trust of CISOs because of its portfolio and track record.

The other notable item in this data is the rise in value for Okta, Crowdstrike and Zscaler, which have seen values increase 78%, 128% and 124% respectively in the time period we show here. You can see the highly elevated revenue multiples compared to some of the more mature companies. Splunk is an outlier here with negative growth because of its transition toward a subscription model - it messes with the income statement. Splunk is managing through that transition and while it has some extremely loyal customers, some CISOs are getting concerned about the pricing equation.

The bottom line is, generally, there’s a real bifurcation in the market in terms of valuations. And we think that while there’s lots of discussion about these so-called “stay at home stocks” and a shift back when the pandemic subsides - we believe that the productivity benefits of remote work are becoming more clear and these NextGen security companies will continue to thrive.

Palo Alto Networks & Fortinet Valuation Divergence

In February of this year, we noted that there was a widening valuation gap occurring between the two companies. We cited three factors for this gap. First we said that Palo Alto was trying to cloud proof its business and as such it was in transition. And it had some challenges with regard to the pace of that transition, including sales incentives and generally figuring out the model. Second, we said that the shift away from appliance-based firewalls was accelerating and that pressuring Palo Alto’s valuation. And finally
we said that Palo Alto was facing some very tough compares in 2019 relative to 2018 and that was causing investor pause as Palo Alto began shifting to an annual recurring revenue (ARR) model.

We said at the time that CISOs like Palo Alto and we felt that the company would be able to successfully address these issues in 2020 and this gap would close. The chart below shows that PANW has begun to reverse this trend.

The yellow line is Fortinet. The blue is Palo Alto Networks and you can see the growing gap coming into and through 2020, which is finally compressing, thanks to a nice earnings report that beat on EPS and revenue this month. Now we continue to believe that Fortinet has done a good job, a better job, of moving to a cloud model; and Palo Alto has largely relied on acquisitions to accelerate this trend so we’ll see if the company can continue to thrive during the transition to cloud. But there is little doubt that CISOs want to work with Palo Alto and remain committed to having a strategic relationship with the company.

**2020 has Accelerated What we Knew was Coming**

The shift to subscription models is well underway, buoyed by cloud and next generation SaaS-based security players. Splunk is in transition, Cisco and Palo Alto’s transitions underscore the importance of this trend and virtually all historically on-prem players are being forced to respond and develop ARR models.
ETR survey data and anecdotal information from theCUBE community highlight what the ETR VENN CISOs are saying - that the Internet is becoming the new private network and the trends toward cloud based and remote worker support are delivering benefits that CEOs and CFOs will push to operationalize.

CISOs must continue to take a multi-layered approach to defending their data, applications and users and as such, a fragmented market with specialists will continue for quite some time.

Despite these clear trends, CISOs face a pressing challenge. The timing of the return to the semi-normal is uncertain and we still don’t have a clear picture of what the future will look like. As such, incumbent firms with hardened networks will have to remain in a hybrid holding pattern to accommodate whatever happens. This means budgets will be stretched. While security remains a top priority, don’t expect an open checkbook going to the SecOps team. Throwing money at the problem wouldn’t solve it anyway. Rather a balanced portfolio of investments, continued automation, data analytics and good security practices will continue to be the pattern.

There are many ways to get in touch - @dvellant on Twitter, david.vellante@siliconangle.com, comment on LinkedIn as we always appreciate the feedback from the community. These episodes are all available as podcasts so you can listen while you multi-task and don’t forget to check out ETR for the survey action. Have a great Thanksgiving, be smart, stay safe and we’ll see you next time.

Watch the full video:

Photo credit: fongleon356
Breaking Analysis: Sparked by COVID, CISOs see Permanent Shift in Cyber Strategies

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.