Top security pros say that the SolarWinds hack and the pandemic have accelerated a change in their cybersecurity spending patterns. Not only must CISOs secure an increasingly distributed workforce, but they now must also be wary of software code coming from reputable vendors, including the very patches designed to protect them against cyber attacks. [...]

February 13th, 2021
Top security pros say that the SolarWinds hack and the pandemic have accelerated a change in their cybersecurity spending patterns. Not only must CISOs secure an increasingly distributed workforce, but they now must also be wary of software code coming from reputable vendors, including the very patches designed to protect them against cyber attacks. Organizations are increasingly prioritizing zero trust approaches including simplified identity access management, better endpoint protection and cloud security. While leading solutions in these sectors are gaining momentum, traditional legacy offerings are being managed down from a spending perspective.

In this Breaking Analysis, we’ll summarize CISO sentiments from a recent ETR VENN session and provide our quarterly update of the cybersecurity sector. In an upcoming episode we’ll be inviting Erik Bradley of ETR to provide deeper analysis on these trends. Here we’ll give you a first look and our initial take on what’s happening in the information security sector as we kick off 2021.

The SolarWinds Attack was “Like Nothing We’ve Ever Seen”

It’s been covered in the press but in case you don’t know the details, SolarWinds is a company that provides software to monitor many aspects of on-prem infrastructure, including network performance, log files, configuration data, storage, servers, etc. Like all software companies, SolarWinds sends out regular updates and patches. Hackers were able to infiltrate the update and “trojanize” the software. Meaning when customers installed the updates, the malware just went along for the ride.

How CISOs View the Solar Winds Hack

“The impact of the breach is profound. It really turned on its head a lot of conventions about cyber security…I don’t think the threat has been exaggerated in the media.”

“We’re now in a situation where we have to monitor the monitors.”

“This attack didn’t have any signatures of a previous attack...so you got down to the code level.”

“80-90% of that code is being downloaded from the Internet...it’s bringing DevOps security processes and making us rethink how to reinvent security.”

Summary of CISO sentiment, ETR Venn Jan 2021

The reason this is so insidious is that often hackers will target installations that haven’t installed patches or updates and identify vulnerabilities in the infrastructure that exist as a result. In this case, the very code designed to protect organizations actually facilitated a breach. According to experts, this was quite a sophisticated attack with multiple variants that most believe was perpetrated by the Russian hacker group Cozy Bear, an advanced persistent threat - APT - as classified by the U.S. government.

It is suspected that somehow they phished their way into a GitHub repo and stole username and password access to allow them to penetrate the supply chain of software that is delivered over the Internet. But public information on this attack is still spotty. What is known is that the attackers had been lurking since
March of last year and had nine months to exfiltrate troves of data from the U.S. government and numerous other companies, including Microsoft and Cisco.

**What CISOs say About the Attack**

Last year, right after the attack, friend of theCUBE Val Bercovici of Chainkit said to us on Twitter that he thinks the government hack will have permanent implications on how organizations approach cyber security. CISOs seem to agree. Here are some verbatim comments from the CISO roundtable moderated by ETR in late January:

*The impact of the breach is profound. It really turned on its head a lot of conventions about cyber security...I don't think the threat has been exaggerated in the media.*

*We’re now in a situation where we have to monitor the monitors.*

*This attack didn’t have any signatures of a previous attack...so you got down to the code level.*

*80-90% of that code is being downloaded from the Internet...it's bringing DevOps security processes and making us rethink how to reinvent security.*

**What Can be Done?**

That’s the question every CISO is wrestling with right now. Security pros will tell you they’re rethinking their practices, tools and approaches but there’s no one answer.

Below is a tag cloud summarizing some of what we hear in theCUBE community and in the VENN roundtable from security practitioners:
You hear CISOs talk a lot about zero trust and many are leaning into identity access management and PAM, privileged access management. We’re hearing mandates around two factor authentication. We’ve written extensively about identity and firms like Okta, Sailpoint and CyberArk Software. And Microsoft is coming up more and more in this conversation, especially as Okta is seen as setting a price umbrella – there’s definitely some frustration there amongst CISOs. And Auth0 which does authentication as a service is hitting our radar as well.

Endpoint security of course gets attention with the work from home trend has become much more important. You can see it in the growth of Crowdstrike and as you’ll see in a moment we’re seeing some traction with VMware and Carbon Black in the ETR survey data as well as momentum with Tanium.

CISOs aren’t going to just rip out what they have so Cisco, especially with Umbrella and Duo come up in the conversation. As does Palo Alto Networks. We’ve said many times that they’re seen as a thought leader and CISOs like Palo Alto as well as Fortinet. Fortinet buyers tend to be more cost conscious and often mid-market customers.

And so it goes with analytics and micro segmentation and cloud security with Zscaler and even RPA to automate certain tasks – UiPath has come up in the conversation more and more in a security context.

So you look at this tag cloud above and there’s no one answer - as is the case with cyber - lots of tools, lots of disciplines and a very capable adversary who has learned to – as the saying goes, “live off the land,” using your own infrastructure and tooling against you.

**Security Budgets are not Limitless**

The common narrative is that security is a top priority with CIOs and CISOs and budgets will be up. Boards of directors are aware and willing to spend. So let’s look at that.
The fact is this is only somewhat true. The chart above shows Net Scores or spending momentum for various sectors across the ETR taxonomy and we’ve highlighted the Information Security segment. Yes it’s up relative to the October survey but it doesn’t stand out. Everything’s up as we’ve reported coming off a down year in tech spending – minus 4% – and we’re forecasting a plus 6-7% increase this year depending on the pace of the recovery. But the point is cyber is one of many budget items and organizations aren’t simply writing a blank check to the CISO.

**Firms are Heavily Invested in Security Already**
The graphic above shows several sectors in context and we’ve highlighted security in the red box. The vertical axis shows Net Score or spending velocity and the horizontal axis is Market Share or presence in the data set. And you can see that security has a big presence – it’s pervasive, of course. But it lags some of the top sectors in terms of spending velocity because organizations have lots of priorities. And of course as you’ll see below, like most mature markets, security has some companies with off the charts spending patterns and others that lag.

**Vendors in Identity, Endpoint and Cloud Have Spending Momentum**

Below you see that same XY graphic and we’ve plotted a number of selected security players.
Several points stand out from the above data:

- **First Microsoft**, as usual, is off the charts to the right and amazingly, has an elevated Net Score of 48%.
- **Okta** continues to lead this pack as it has in the last several surveys with a Net Score of 61.5%, up from last quarter’s survey.
- Okta, **Crowdstrike, CyberArk, Fortinet, Proofpoint** and **Splunk**, all up nicely from last quarter’s survey.
- Also we want to highlight **Carbon Black**. The company’s Net Score last quarter was 23.9% with 134 mentions and this quarter its Net Score shot up to nearly 38%. A meaningful and noticeable move for VMware’s $2.1B acquisition that it made in the summer of 2019.

So we see a number of companies with momentum, which stems from a rebound in tech spending generally but also the shift in security spend that we’ve highlighted. And you can see a couple of legacy security firms losing spending momentum – FireEye and RSA in particular, but there are many others in the ETR data set that are in the red zone.

**Microsoft, Palo Alto, Okta & Crowdstrike – Notable Momentum & Market Presence**

Let’s dig deeper into the data and the vendor performance.

Below is a view of the data we first showed you in 2019. The tables depict the Net Score (spending velocity) and the Shared N which identifies the number of mentions within the sector and is an indicator of presence in the market. The leftmost chart is sorted by Net Score and the right hand chart is sorted by Shared N. To make the cut and get into this chart we required a vendor had to have had at least an N of 50 mentions in the sector within the survey.
You can see on the leftmost chart that Okta (61.5%) and Sailpoint (59.5%) lead in Net Score and Microsoft has the largest presence in the sector (518 Shared N) along with Cisco (305) and Palo Alto (278).

**Four Star & Two Star Companies**

Something we started two years ago was if a vendor shows up in the top 10 for both Net Score and Shared N we anoint them with 4 stars. So Microsoft, Palo Alto, Okta and Crowdstrike are the four cyber vendors that fall into the four star group.

And we give 2 stars to those companies that make the top 20 in both categories. So Cisco because of Umbrella and Duo, Splunk, Proofpoint, Fortinet, Zcaler, CyberArk and Carbon Black (VMware). Carbon Black is new to the two star list due to its rapid rise in Net Score.

**A Quick Aside on Carbon Black**

At VMworld 2019, Pat Gelsinger told theCUBE that he felt like he got a great deal picking up Carbon Black for $2.1B.

His logic was in part based on the valuation of Crowdstrike, a Carbon Black competitor. At the time Crowdstrike as you can see on the chart below, had a valuation that was nine times higher than that of Carbon Black. And you can see from the trailing twelve month revenue that Crowdstrike was a bigger company by more than $100M but the real story was the company’s growth at more than 100%. Crowdstrike at the time was growing much faster than Carbon Black’s 22%, justifying a significantly higher relative value.
Of course the thinking from VMware was that it could pick up Carbon Black at a discount to the market leader and inject growth and profitability into the asset by bundling into VMware’s increasingly capable security offerings. VMware created a cloud security group headed by Carbon Black CEO Patrick Morley, which underscores a commitment to the sector.

Now in VMware’s recent earning call it said Carbon Black had “good” bookings performance. So who knows exactly what that means but if it were significantly more than 22% (Carbon Black’s growth rate at acquisition time), our guess is that VMware would have been more effusive. So let’s assume that since the acquisition Carbon Black growth has been flattish relative to its growth at acquisition as VMware figures out how to integrate the company. Nonetheless, we would still peg its valuation as having increased substantially since the time of acquisition – perhaps in the $3-$5B range. So a nice pickup for VMware in our view, which has a good track record of acquiring companies and monetizing the assets. And we think the value of Carbon Black inside of VMware will likely grow from here.

Further, the ETR data on Carbon Black is encouraging.

Cyber Security Valuations Continue to Skyrocket for the Leaders

Let’s look at how the valuations in this sector have changed since before COVID.
Above is an updated view of our valuation matrix since just before the pandemic hit the U.S. in earnest. You can see the S&P is up 16% from that timeframe and the Nasdaq composite up 43%. Now look at the others. Only Splunk really hasn't seen a big uptick in valuation. And Proofpoint’s valuation hasn’t kept pace. But the others have either risen noticeably, like CyberArk and SailPoint...bounced up like Palo Alto and held nicely like Fortinet or exploded like Crowdstrike, Okta and Zscaler.

So one would think Carbon Black as a VMware asset has done pretty well along with these names and will make long term contributions to VMware.

In addition, we would expect that the tech spending rebound this year combined with the heightened concerns over the SolarWinds hack and the tectonic shifts from the accelerated work from home and digital business transformation will continue to bode well for many of these names...for some time.

**Factors to Watch in Cyber**

As we exit the pandemic and are experiencing a new digital reality, cyber threats have never been greater. Each January if you looked back on the prior year you’d be able to say the same thing for the past several decades. And the reality is that the budget allocations and subsequent spending on cyber are asymmetric to the economic risks. In other words, the $125B or so spent on cyber security doesn’t square with the trillions of in value lost each year to cybercrime. We don’t spend enough as it is and probably can’t spend our way out of this problem.
CISOs have to balance their legacy installed base security infrastructure with the shift to zero trust, accelerated endpoint, new access management challenges and an ever-expanding cloud. And much more. Very few have the benefit of a blank sheet of paper.

Lack of talent remains the single biggest challenge for organizations, which are stretched thin...making investments in automation a trend that is not going to abate any time soon.

In cyber, all the cliches apply – there is no silver bullet. There is no rest for the weary. The adversary is well-funded and extremely capable and they only have to succeed once to create a business disaster for an organization, whereas an organization must succeed every minute of every day. So expect more of the same with no end in sight in terms of complexity, fragmentation and whac-a-mole approaches to fighting cyber crime.

It hurts to state this but it just means the fundamentals for this sector just keep getting better. Bad news but it’s the reality for organizations trying to protect their data. Good news with lots of opportunities for investors.

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, and a slightly new experimental format to our production – let us know what you think:

Photo credit: Ascannio
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