

REFINITIV STREETEVENTS

# EDITED TRANSCRIPT

VMW.N - VMware Inc at Jefferies CyberSecurity Conference (Virtual)

EVENT DATE/TIME: DECEMBER 10, 2020 / 3:00PM GMT

## CORPORATE PARTICIPANTS

**Patrick Morley** *VMware, Inc. - Senior VP & GM of Security Business Unit*

**Sanjay J. Poonen** *VMware, Inc. - COO of Customer Operations*

## CONFERENCE CALL PARTICIPANTS

**Brent John Thill** *Jefferies LLC, Research Division - Equity Analyst*

## PRESENTATION

**Brent John Thill** - *Jefferies LLC, Research Division - Equity Analyst*

Good morning, everyone. It's Brent Thill from Jefferies, thanks and welcome to the cyber summit. Today, I'm very happy to have with us Pat Morley, GM of VMware Carbon Black and served as the CEO of Carbon Black from 2017 till the company's acquisition by VMware in 2019; and Sanjay Poonen, COO, Customer Operations.

Just in terms of disclosure, statements made in this discussion, which are not statements of historical fact, are forward-looking statements based upon current expectations. Actual results differ materially from those projected due to a number of factors, including those referenced in VMware's most recent SEC filings on 10-Q, K and 8-K.

With that, gentlemen, good morning. Thank you so much for joining.

## QUESTIONS AND ANSWERS

**Brent John Thill** - *Jefferies LLC, Research Division - Equity Analyst*

The security world is quickly evolving. And I guess maybe Pat and Sanjay, if you could just kind of set the stage of this vision that you're bringing together as a joint team. It's a powerful one and a powerful vision. If you could just maybe, again, just set the stage in terms of the direction that you're going into '21 and maybe just if you could also give us a little bit of background in terms of some of the milestones that you're reaching so far and the things you're most proud of in this joint initiative.

**Patrick Morley** - *VMware, Inc. - Senior VP & GM of Security Business Unit*

Sanjay, why don't you start on that?

**Sanjay J. Poonen** - *VMware, Inc. - COO of Customer Operations*

Yes. Brent, I think this is an important space because we looked at it over the past -- a couple of years as we studied it inside VMware and discussed this with our Board, and we felt -- but if you look at the overall \$50 billion security market, it's filled with lots of vendors, 5,000 vendors, and each of them kind of do small pieces of it, 20 broad segments. And several of those segments were starting to become more and more closely relevant to areas we were investing very heavily.

As you know, we have 85 million virtual machines. So that's a form of an endpoint. We call it a workload. We have about 80 million virtual switches now with NSX, and NSX is becoming, with 20,000 customers, a platform for networking. So networking -- network security is very close to us. We have tens of millions of endpoints we manage with Workspace ONE: laptops, tablets and phones. This was the technology we originally acquired from AirWatch and extended now to all endpoints.

So increasingly, we began to see more relevance in our endpoints where customers are saying, "Listen, we have stand-alone security tools that we add to your endpoints, but they're not as integrated in. They feel bolted on." And I've kind of used this analogy in previous speeches where it's sort of like going to a doctor and she asked you how to stay healthy and she -- sorry, you asked her how to stay healthy, and she says, "You got to have 5,000 tablets."

So we felt like we've got to redo a broken security industry and make it more intrinsic, the analysts also call the zero trust and what that means is taking key security capabilities and baking it into our platforms and making it, such that you don't need dozens and dozens of other tools, agents, consoles, so on and so forth. And that's what we've done.

Another for Carbon Black, we actually began down the journey in network security, and we've built out a full data center networking: load balancing; firewall; SD-WAN, now Secure Access Service Edge. It is the private industry, I think, in a full network security stack. Patrick will talk more about what he is doing for us in endpoint and workload security. We studied that space, felt that was closest to us in terms of what we could do with both Workspace ONE and VSquare, so very excited about that and its road map. And then cloud security is the other area.

So we built a multiyear vision on what we're going to do. We announced last year that we have about \$1 billion in security business. That was last year, and about 20,000 customers who are well in the races. And we think if we can build, over the course of time, a multibillion-dollar security business, in our quest, we were going from 11 to, one day, hopefully, 20, this will become an important space of adjacency that we can pursue.

---

**Patrick Morley** - VMware, Inc. - Senior VP & GM of Security Business Unit

And the only thing I would add onto that is that if we look at the progression of what we had at Carbon Black and what we've done now inside of VMware and taking that vision forward, the world we're all living in today is really validation of the strategy. So if you -- the reason we built a platform that we did at Carbon Black, a SaaS-based platform that allows you to consolidate functionality and leverage the power of big data and analytics, the reason we did that was because we felt the cloud allowed us to consolidate functionality but also better find -- see and find and stop the adversary. And if -- and our core premise was that the network was going away. Increasingly, you had distributed users, distributed services across the globe that you were using. The cloud would allow you to consolidate. And, oh, by the way, security was maturing, and Boards and executive teams said, "I can't have 5,000 different products, or for most enterprises, 100-plus different products inside of my organization. I need to consolidate functionality."

And if we look at what's happened this year in the year of COVID, what we've seen is a tremendous validation of that strategy, right? We're all distributed. We increasingly are leveraging distributed services. The IT organizations and security organizations are fully tapped. They can't manage all these different products. And so I think if we look at where we are today, the strategy that we have puts us on a path forward where we're leveraging the trends that the market wants.

---

**Brent John Thill** - Jefferies LLC, Research Division - Equity Analyst

And just, Patrick, maybe talk a little bit about the integration with the rest of the VMware team and how that's played out, kind of where you're at in terms of this vision of the endpoint to network in the cloud? Where are you at from stitching this architecturally together today?

---

**Patrick Morley** - VMware, Inc. - Senior VP & GM of Security Business Unit

Yes. I would not say we're stitching it together. I would say that we're building it in inherently, intrinsically into the fabric of the platforms that we have at VMware. Again, VMware is an \$11 billion company with -- which many people out there know as the virtualization company. But Sanjay already stated, right, we have a number of platforms, in addition to what we're doing on the infrastructure and cloud side, what we're doing in the network side, what we're doing on the end user compute side. So we've got all these control points out there that allow us to take the vision that we had at Carbon Black, which is leverage the power of what you can do with big data and with the cloud and actually even accelerate it more fully.

One of the nice things -- we're a year post the acquisition by VMware of Carbon Black. One of the nice things is that I always think when you go through acquisitions one of the -- fundamentally, culture and people are what matter on the success. Obviously, you need the business metrics, you need to drive the business forward, fulfilling this strategy. But the only way you're fulfilling the strategy is if you have a strong connection on the culture and the people, and we've seen that affinity between the way we ran the business at Carbon Black and the way that VMware runs the business. I think there's a lot of shared values there. So you use that as a starting point and you look at what we've accomplished over the last 12 months and it's what you expect, which is first 6 months or so is, okay, let's establish, make sure we really understand from an operating cadence that we've got kind of a plan going forward that we're all embracing and aligned on. And then the last 6 months, I think we're really starting to see the benefits of what we're doing at VMware Carbon Black and overall inside of VMware.

And those are a couple of big themes. One is helping customers to understand that, as a brand, VMware is a security company. That's one of the big things we're -- I think we're having an impact on right now in the market. And then secondarily, you actually have to deliver on the product side, and we've done that. At VMworld, a month or so ago, we announced workloads, so we've built intrinsically in leveraging the power of the hypervisor in vSphere, we've built security in natively. We announced that, and we've seen great customer reaction on that. And a real excitement about the fact that we can take away a set of agents and a set of complexity from what they're doing right now to secure, as Sanjay said earlier, those 85 million workloads today that are running on our platforms.

And as I said at the beginning, we're also extending beyond just of vSphere into the other capabilities of our platform: network, end user computing, et cetera.

---

**Brent John Thill** - Jefferies LLC, Research Division - Equity Analyst

That's great. Just from -- Sanjay, you mentioned cloud security, and a lot of different names come up when you mentioned that in terms of the competitive landscape. And how are you doing this differently than the Zscalers, the Cloudflares, the others that are going after this from a security as a service?

---

**Sanjay J. Poonen** - VMware, Inc. - COO of Customer Operations

Yes. The term cloud security is a kind of catchall for a number of different areas, and let me sort of parse it aside. We acquired a company several years ago that brought us a cloud security posture management capability. It was called CloudCoreo. We now call it Secure State. It's part of our CloudHealth platform. And basically, what we began to see with many of our customers, they were deeply concerned about both the costs that they were managing in these public clouds. It was kind of getting out of control and they needed ways in which they can [save]. That's, I would say, a CFO type of problem, but CloudHealth is very good at doing that. And then they were also concerned about compliance and security.

So we've added a module, and we've kind of made that part of the CloudHealth platform. So you'll see increasing integration between Secure State, which is part of that CloudHealth platform and Carbon Black so that you get a full view of all workloads have ways by which you can get the full definition of your security posture. That's going well. We have lots of customers now that are being able to manage that cost.

If you know, there was a prominent financial services organization that had a breach, where, in that case, it was a malicious user, but it could also be accidental, was taking advantage of configuration settings in one of the public clouds, was able to exfiltrate data related to credit card and personal information. So you don't want that to happen, whether it's intentional or unintentional.

In the other areas that you mentioned of what also gets called as cloud security because it is a sort of a secure web gateway access into the cloud, we are actually partnering with many of those customers as we build that into the ways in which we think end users will access SaaS applications. So you imagine a user now that goes home. On their laptop, tablet and phone, they typically have like dozens of these agents. We're certainly going to consolidate endpoint management and endpoint security. That's that workspace security concept that Patrick alluded to, the coming together of Workspace ONE and Carbon Black into a unified agent. That's a beautiful concept. That's a beautiful concept of just agent consolidation. That's something we hear about from almost every chief security officer. And none of the other endpoint security vendors have the ability to do that.

Now if you take that same capability and extend it to do some of the things that VPN has traditionally had to do for you and then allow that to then, behind the scenes, go to some kind of secured PoP, if you would, a point of presence, where, in turn, all the cloud security capabilities sit: virtual firewall as a service, SD-WAN, secure web gateway, and then from the -- and turn it to SaaS applications, you're going to significantly simplify the architecture than having to backhaul all that traffic through the data center. And we've been thinking about this for several years.

And with the pandemic, that became something that we were hearing from our customers, we need to accelerate. So we actually announced at VMworld our capabilities in that area, Secure Access Service Edge or what the analysts call SASE. And we will see very shortly, we will be bringing out capabilities that extend Workspace ONE into that area.

Now how are we getting the secure web gateway capabilities through partnerships with 2 companies: Zscaler in the high end because they have a very strong enterprise presence; and then a lot of the browser isolation and some of the commercial market, we'll get from Menlo Security. So we'll partner that.

Now the third category you mentioned were things like CDN, content -- next generation of Akamai of cloud, that's very much a partnership here. It's not necessarily in our -- as we think about edge, maybe we will think about that. It's not in our kind of current landscape of what we're doing in security. So all of those companies are natural partners to us at this point in time.

I think in security, it's very -- as we've been sort of charging that security strategy, it's also very important is you're credible to chief security officers and tell them that you're going to do well and where you're going to partner with a handful of those. I mean I think every chief security officer has a bunch of skepticism if one company is going to claim they're going to do everything among the 20 areas, and they're not good in any of them.

So we picked 3 to 4 areas that we're going to be best of breed. Like, for example, if you pick up the Gartner Magic Quadrant for aspects of network security like SD WAN, VMware is top right. Even as the firewall vendors have gotten to that space, we are further ahead. Some of them are #3, 4 or 5 in the space. We're #1.

So it's very important that we build credibility in the areas and then pick a few partners. Zscaler is one example of that, where Okta is another example, where we will go deep in partnering with them. And they, in turn, are partnering deep with us.

So for example, Zscalers named VMware as the preferred SD-WAN player that they're going to partner with. And that partnership means then that Jay Chaudhry and our teams will go close together at furthering our presence in joint accounts.

---

**Brent John Thill** - Jefferies LLC, Research Division - Equity Analyst

And maybe just expand on the go to market and how this vision is coming together in the field. Are you enabling all the sales reps to sell? Have you brought in a SWAT team to go after this? How has that evolution of the distribution come together?

---

**Sanjay J. Poonen** - VMware, Inc. - COO of Customer Operations

We've had a reasonable success with VMware as we've grown, especially in the last 7 years that I've been here. When I joined the company, it was about \$5 billion or \$11 billion and really investing in specialist teams. It's a model that I've seen successful in SAP. In fact, I ran all the special sales teams at SAP, and we've invested.

And today, we have for each of these key domains that our franchise pillars significantly sized specialist teams. Now they are not bigger than the core team. Think of the core team sort of like the Sun, and are like planets. But they're reasonably sized. And they have to be the expertise. Just like when you go to a hospital, you have a general practitioner and a specialist doctor. They have to be the expert in their area.

For example, in containers and modern apps, we have an expertise around all of the Kubernetes capabilities. Much of it was invested in from the follow-on of the Pivotal and Heptio and organic acquisition -- organic investments we've made.

Networking. We've been building since 2012 and 2013 when we acquired Nicira, sizable network and network security team.

So what Carbon Black brought to us was an endpoint and workload security team, and we've invested even more. So we took Patrick's organization as he was an independent company and added more. And the first thing I did was added more engineering to him and adding more go-to-market capacity so that we could make that a sizable endpoint of workload security team. Then of course, we have our end-user computing team that's also sizable that we've invested in since the acquisition of AirWatch.

So these teams now have certain swim lanes where they work together. But in this case of Carbon Black, they have some nice adjacencies. They have a very nice adjacency with the network security team as that concept of NDR and ADR comes together. They have a very nice synergy with the EUC team as Workspace ONE and Carbon Black come together, and then they have a very core synergy with the core team. We don't have a special team that sells VSquare. Everybody sells a hypervisor. But as we think about agentless capabilities for workload security, they have a very core synergy.

Then for the core team, what we do is we get them comfortable with the elevator pitch in each of these areas. How does the connected VMware story really bring in the relevance of cloud, of containers, of security? By the way, those are our top 3 priorities for the company.

And that's something Pat and I spend a lot of time on. How do we open the door with a CEO, a CIO or CTO to then have the deeper level of conversation with a line of business developer or a chief security officer. As we've done -- now we're talking to a lot of chief security officers in the hundreds and the thousands. The first thing I hear from them is, "Wow. We love VMware." Now we've been talking about why they love VMware because their boss, the CIO, tells them we should take this meeting of VMware. They're doing a lot with security. They made us successful in the data center or in end-user computing.

So we have a bunch of institutional equity with many of these chief security officers, many of whom were starting to grow our presence and portfolio and relevance with. Patrick and I just did a chief security officer customer counsel. And the amount of feedback and the interest from these are the who's who of chief security officers who are willing to work with us is astounding. And it's because we're building on the credibility and the relevance VMware has already had for many of those customers.

---

**Brent John Thill** - Jefferies LLC, Research Division - Equity Analyst

Yes. Many asked can you do this all in a SaaS environment? Or is this still going to require a lot of on-prem work?

---

**Sanjay J. Poonen** - VMware, Inc. - COO of Customer Operations

Why don't you start, Patrick, on how you've built? Because Patrick is a good example of a leading SaaS asset, and we've leaned forward as we've acquired companies. When we had on-premise, we looked at this space in endpoint security carefully. They were on-prem companies and cloud companies, and we picked Carbon Black as their cloud company. It's very similar to 6 years ago, where we were looking at the end-user computing environment. It is AirWatch and MobileIron. AirWatch was cloud, and MobileIron was on-premise. So we've leaned to cloud very much heavily. But Patrick, why don't you talk about that SaaS capability, about how -- also the hybrid cloud and where relevant on-prem may make sense?

---

**Patrick Morley** - VMware, Inc. - Senior VP & GM of Security Business Unit

Yes. So overall, if you just look at VMware, right, we're pulling the companies pulling the SaaS and subscription. And certainly, on the earnings calls, that's been a discussion that Pat's had and Zane, talking about the pull to SaaS and subscription. And when you look at security, I think security is an area where we're part of the tip of the spear of that, certainly the Carbon Black business, which is primarily -- which is mostly cloud today. Of course, we started -- our heritage was on-prem, and we've pulled the whole organization to the cloud over the last number of years. If you look at the VMware portfolio in security today, it really has a very strong SaaS portfolio.

So in addition to Carbon Black, which is cloud-based, all of our services are in a SaaS-based cloud. Workspace ONE is also available that same way. VeloCloud is also available that same way. And you end up in a situation where a lot of the components that we have today are SaaS-based.

And even when you look at the infrastructure side, as Sanjay said earlier, 85 million workloads out there. Increasingly, many of those workloads are actually running in public cloud. When we look at securing that, again, we offer -- we can offer the securing of our virtualized workloads as a SaaS service.

And as we -- as the company pulls to our modern app strategy, which is Tanzu, so as an organization say, "I want to fundamentally not just shift my workloads up into the cloud, I actually want to build my applications on the cloud," and we look at most of those organizations today leveraging Kubernetes, we have a strategy around that, again, that we call Tanzu. And a big part of our security strategy is also to secure that inherent -- intrinsically via Carbon Black. Again, all of that is SaaS, everything I've just described is SaaS.

So the opportunity ahead for us to be tip of the spear and the security business, I think, is very strong on the SaaS and subscription side.

---

**Brent John Thill** - Jefferies LLC, Research Division - Equity Analyst

Patrick, many ask, it seems like right now, there's a big consolidation of the old -- the Symantec and McAfee kind of not doing what their customers would hope, so there's a big opportunity there. But there's -- on the other side, there's a big competitor with CrowdStrike. And many ask how your approach is different, what you're seeing from CrowdStrike? And similarly, what are you seeing from the Symantec/McAfee endpoints?

---

**Patrick Morley** - VMware, Inc. - Senior VP & GM of Security Business Unit

Yes. Well, certainly, the TAM for the marketplace, traditionally EPP TAM was around \$8 billion. As you start to see the transition of where work is occurring, you look at workloads. You look at the -- you look at cloud security. You look at other elements that can be brought into the platform, like vulnerability management, which was part of our recent announcement for workloads, we actually -- with the same sensor, with the same back end, we're actually covering vulnerability management as well. You look at that TAM.

So you start to build out very quickly a very large TAM of security services that can be delivered via one cloud platform with one sensor, or in the case of vSphere and Tanzu, without a sensor at all because we're building it in intrinsically. So it's a really, really big market for us and for more.

So I think CrowdStrike is certainly a very strong and formidable competitor. And if you look at their strategy and their growth numbers, as much as they are doing today to grab share from Symantec and McAfee, we're doing the same thing. We're also grabbing share from Symantec and McAfee. It's a large TAM. You can have multiple winners in the space, but I think the strategy at VMware is slightly different than CrowdStrike. And again, Sanjay touched on this already, right, which is we -- the breadth of offerings that we have at VMware, when we get this right, and by right, I mean, as we build security intrinsically into -- we've already done it with vSphere, as we do it with Tanzu, as we do it with our network virtualization offerings and ESX, as we do it with end-user computing, Workspace ONE, Horizon, it gives us a competitive advantage because we're already there, and we can just -- security is there. If the customer wants it, they can just turn it on.

So our strategy is to deliver great security capabilities for endpoint and workload and at the same time to make sure we're building security intrinsically into everywhere VMware is.

And the only other point I'll add is like one of the really powerful things for me, running an independent software company and then come into VMware, Sanjay said this, but I can't emphasize it enough, our ability to get access at the CIO at the C-level as part of VMware. It's just been phenomenal over the last year. And again, that should be an advantage for us.

And because security is increasingly so critical inside of organizations, Sanjay talked about that advisory council meeting we did a week or 2 ago. One of the interesting things I was surprised at is 1/3 of the CSOs there also owned infrastructure. So you -- now why would that be? Well, that's because security is no longer a thing to the side. Security increasingly is being seen as something that's going to be inherent in the fabric of the



compute for these enterprise companies, and VMware is in the fabric. And so we should be in a position where we can leverage that, again, as an advantage for us as we go to market.

---

**Brent John Thill** - *Jefferies LLC, Research Division - Equity Analyst*

That's great. And Sanjay, many are asking kind of we went into this year. And obviously, it was a total curveball year for all of us. And everything kind of went on ice at the beginning of the year, and things seemed like they're slowly thawing. And I guess from your perspective at a high level, how customers are feeling now, what you're seeing you're most encouraged by as you go into next year. How would you kind of set the stage? And I know you're not giving guidance. But just at a high level, how your customers are feeling and what -- where you're seeing kind of the biggest openings that maybe weren't open before.

---

**Sanjay J. Poonen** - *VMware, Inc. - COO of Customer Operations*

Brent, and just one thing I would add to the previous discussion, you should think of us as like CrowdStrike and Palo Alto in one company if you want to think about 2 big spaces. And if you look at the network security space, many of those companies have never been successful with endpoint security. Even historically, I was 15 years ago at Symantec. The endpoint security guys struggled getting the network security. We're trying to do network security, endpoint security and now the new area of cloud.

Now to answer your question in related environment, we began the sort of pivot to cloud, container, security. These are sort of top 3 areas of focus for the company well before the pandemic. We saw this as very important. As we laid out some of our vision in the last several years, in fact, the pivot to the cloud as we began our VMware Cloud journey with the public cloud vendors and resetting from the acquisition of vCloud -- sorry, from the divestiture of vCloud Air and investing now. This is 3, 4 years down the journey.

With containers, with the acquisition of Heptio and Pivotal now, that's really gone very well in LAN security, doubling down not just in what we have in NSX, but now with Carbon Black. So that continues, and we see good resonance of those priorities with customers. There is a definitive move to the cloud. Our partnership with Amazon and the other public cloud vendors has done really well. We talked about the cloud business being approximately \$1 billion ARR business. In the last earnings call, the -- we said we were also really pleasantly pleased by the progress at Tanzu. It's actually done better than our expectations, so we feel really good about the progress we're making. And that \$1 billion security business that we talked about, which includes Carbon Black but also includes many other imports, we want to keep growing that.

So I think what we've got to do as we kind of accelerate subscription and SaaS, we've certainly seen during the time of the -- this year of the recession and GDP decline, some freeze in the on-premise and the decline in the license side of it, and we'll see how that plays out because it's not like the environments and the CIOs I talked to, there's a student body left to everything public cloud. They still have 80%, 90% of their workloads in private clouds. There's certainly been an acceleration to the cloud, but that care and feeling of the private cloud, all the move to the edge is going to require VMware technology to help them. And that -- we'll come back in due course as the GDP and the economy improves.

But in the meantime, in the parts that are moving faster, whether it's cloud, whether it's modern applications with containers or whether it's security because of work from home or other areas of security threats, which you've heard some about most recently, we're going to invest, and we're going to invest and we're going to go prosecute that business with both great products, great go to market. It's a good time when there's a lot going on to double down and making our products the best in each category. That's a key priority for the leaders like Patrick and several of the other key leaders who drive security advancements or the cloud or containers, and at the same time, continue to tune and perfect that.

So we've now been using -- we've been using this crisis as an opportunity, so to speak, to continue to tune the machine of VMware and accelerate subscription and SaaS. You've seen that 39%, 40%, 44% growth of subscription and SaaS. And I believe, as we do that, we'll continue to be stay relevant. The key thing though any of these types of challenges is to stay relevant to your customers. I talked about the chief security officer customer counsel we did yesterday, a bigger sort of customer counsel with CEOs and CIOs just last night. And it was amazing to hear how relevant they felt -- still felt VMware was -- as our guest speaker was Stéphane Bancel, who's CEO of Moderna. And of course, we're talking a lot about the vaccine.



But when I reflected on how relevant VMware is to many of them were CEOs, not just CIOs, I think that if we keep going, we're going to get our fair share of the IT spend.

---

**Brent John Thill** - *Jefferies LLC, Research Division - Equity Analyst*

Excellent. Well, thank you so much, both Patrick and Sanjay for joining. Great conversation, and have a great end of the year, and looking forward to staying in touch into next year. Thanks again for joining today.

---

**Sanjay J. Poonen** - *VMware, Inc. - COO of Customer Operations*

Thanks, Brent.

---

**Patrick Morley** - *VMware, Inc. - Senior VP & GM of Security Business Unit*

Thank you. All the best.

---

**DISCLAIMER**

Refinitiv reserves the right to make changes to documents, content, or other information on this web site without obligation to notify any person of such changes.

In the conference calls upon which Event Transcripts are based, companies may make projections or other forward-looking statements regarding a variety of items. Such forward-looking statements are based upon current expectations and involve risks and uncertainties. Actual results may differ materially from those stated in any forward-looking statement based on a number of important factors and risks, which are more specifically identified in the companies' most recent SEC filings. Although the companies may indicate and believe that the assumptions underlying the forward-looking statements are reasonable, any of the assumptions could prove inaccurate or incorrect and, therefore, there can be no assurance that the results contemplated in the forward-looking statements will be realized.

THE INFORMATION CONTAINED IN EVENT TRANSCRIPTS IS A TEXTUAL REPRESENTATION OF THE APPLICABLE COMPANY'S CONFERENCE CALL AND WHILE EFFORTS ARE MADE TO PROVIDE AN ACCURATE TRANSCRIPTION, THERE MAY BE MATERIAL ERRORS, OMISSIONS, OR INACCURACIES IN THE REPORTING OF THE SUBSTANCE OF THE CONFERENCE CALLS. IN NO WAY DOES REFINITIV OR THE APPLICABLE COMPANY ASSUME ANY RESPONSIBILITY FOR ANY INVESTMENT OR OTHER DECISIONS MADE BASED UPON THE INFORMATION PROVIDED ON THIS WEB SITE OR IN ANY EVENT TRANSCRIPT. USERS ARE ADVISED TO REVIEW THE APPLICABLE COMPANY'S CONFERENCE CALL ITSELF AND THE APPLICABLE COMPANY'S SEC FILINGS BEFORE MAKING ANY INVESTMENT OR OTHER DECISIONS.

©2020, Refinitiv. All Rights Reserved.