NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT

INNOVATORS IN CLOUD, IOT, AI & CYBERSECURITY

Conference Debate Session IV - NetEvents Shark Tank Session

Chair: Manek Dubash

Editorial Director, NetEvents

Panellists:

Janice Roberts	Partner, Benhamou Global Venture Partners
Siddhant Trivedi	Investor, Omidyar Technology Ventures
Hiro Rio Maeda	Managing Director, Draper Nexus
Curtis Feeny	Partner, Silicon Valley Data Capital

Manek Dubash

Now I hope we're going to get to perhaps a little bit of entertainment, as well as being quite serious about these matters. We're going to run our own little *Shark Tank* here and we're going to have four venture capitalists who are going to come down and they're going to judge some start-ups. The start-ups are going to come down, they're going to pitch, if the VCs would like to come down and join me on the stage here, that would be great, the four of you, Hiro, who else have we got here? Janice of course, yeah here we go. Come on. Then we're going to have some start-ups and they're going to pitch to the VCs.

Okay, so the start-up people are going to pitch to the sharks and the result of their deliberations will be announced this evening over dinner. There will be awards and there will be winners and there will be losers and hopefully not too many tears. Okay, so without further ado, the first one is AISense in the category of IoT cloud start-up data centre. AISense, you have five minutes maximum, absolutely maximum. Go.

Sam Liang, Founder and CEO of AISense

Hi, my name is Sam, I'm the founder and CEO of AISense. We are a start-up in Silicon Valley. The problem we're trying to solve is that there are billions of people in the world who talk a lot, especially in enterprises, people spend tonnes of money and time talking in meetings. There are a lot of statistics that show that in a lot of enterprises people spend maybe 30 or 50 per cent of the time in meetings, phone calls and videoconferences, however people forget things really fast, within 24 hours people forget 70 per cent of the conversation.

So we are a group of AI experts, coming from Google, Stanford, MIT, we are building these technologies to understand what is conversations. For myself, a little bit of background, I used to lead Google Map Location Service, we built the blue dot iPhone, Android and the web. I got my PhD from Stanford, David Cheriton was my PhD adviser and David Cheriton is a strong supporter of our start-up as well. My first start-up was previously acquired by Alibaba and this is our second start-up here. As I just mentioned, David has always been an extremely strong supporter to this and also Tim Draper and other investors.

We are building technologies to recognise human-to-human conversations. This is multi-party, multi-speakers, long form conversations, it's actually much more difficult than Amazon Alexa or Siri where they only have one single speaker asking short questions.

So let me just do a quick demo to just show how this works. What you see right now is a real-time transcription, it's done in the cloud while I'm talking here. It's all done by our deep-learning speech recognition. I bet you have probably never seen this before, you might have seen dictation built by Nuance, but this is actually much more sophisticated because again, it's long-form conversation, it's far field because I'm actually not directly speaking into the microphone. This is a system that you can use already today, if you go to Otter.ai, you can sign up and use it. I guess there are a lot of journalists here. You can use it for your interviews. Everything will be available immediately and you can search everything really fast.

Let me pause and go back to see and old conversation. Suppose, as I mentioned, if I search for a key word like Tim Draper, I scroll down and I can quickly find all the conversations related to Tim Draper. He actually is a strong supporter to this and he uses this himself a lot. I just found this part. This is a previous speech by Tim Draper.

[Audio playing]

This is basically how it works. You can use it on iPhone, you can use it on Android. Let's see. We also partner with Zoom, one of the hardest videoconferencing system, they licence our technologies and all your Zoom meetings, if you turn on this option, you can get automatic transcription right after the meeting. So that's it. I don't know how many minutes I have.

Manek Dubash

Okay, so now the sharks have five minutes to grill you.

Janice Roberts

I have a couple of questions. So the first is, in a room where there's lots of people talking over each other, how does it work then?

Sam Liang

Right. That's one of the major challenges we're trying to solve. When you have multiple people, we have technologies called diarisation that separate the voice from one speaker to the other speaker. The next step, once we separate it, we use another technology called a voiceprint to match the name to the speaker, so if there are five speakers here, we separate them, speaker one to five. Then we use a voiceprint technology to label a few sentences from each speaker, then you can match the rest of the meeting and you can figure out this one is Janice, the other one is Sam, and it remembers the voiceprint the same way it remembers the face in a photo. So once you label a few photos, you can match 100 other photos. Same here, once you label a couple of minutes of one person's voice, you can match the rest of the speech and the future speeches as well.

Curtis Feeny

Could you talk about your revenue model and also the traction in terms of number of users and how you're growing?

Sam Liang

Yes, so we have a combination of enterprise, B2B and B2B2C. As I mentioned, Zoom is already our customer, they license our technologies. We are actually processing thousands of hours of meetings every day already. That's already generating revenue and other companies like Bridgewater, one of the largest hedge funds in the world, they have a radical transparency principle in the company, they record all their meetings. They love this technology so much, they actually invested in AISense and we're in the process of providing this solution for them as well.

For the Otter app, it is a mobile app on iPhone and Android. We have a subscription model, anyone can download it and use it for free for up to 10 hours per month. Beyond that, the user pays $10 per month. We do provide some promotion for students, so a lot of the students find this useful for taking lecture notes.

Hiro Rio Maeda

So I'm actually impressed with the accuracy of what you just showed and I have an accent, you have an accent and this morning I was driving up here and because I had to send an urgent message on the SMS, I was just using Apple's voice to text. The accuracy was not there, so it was like, I did a voice to text to drive safely, but now I have to fix it, so it's a bit more dangerous. So what are you doing differently from Apple, Google, Amazon?

Sam Liang

Yeah, there are a lot of different factors. First of all, we have the best AI scientists, as I mentioned, from Google, MIT, Stanford, Cambridge, these are super-talented people. We've caught tonnes of data from the internet from all kinds of different environments; actually every room has different acoustic characteristics that we have to collect tonnes of data with different acoustic characteristics and do the learning training. You mentioned accent, that's actually one thing we did in terms of Chinese accent, Indian accent, Japanese accent and we mix that into the training data in a certain way so that not only it's able to recognise native speakers, it's also able to recognise people with accents.

Hiro Rio Maeda

I see, but not just an accent, but expanding it to other languages, what does it take?

Sam Liang

Right now we are focusing on English only. We do plan to add other languages later. Right now it's English only, yes.

Siddhant Trivedi

Sam it's great to hear the pitch, particularly because I've heard it from Bridgewater, so it's very interesting to hear from you as well. Could you talk a little bit about the competitive landscape? Obviously you mentioned Nuance, but there are also a lot of verticalised voice solutions. So in sales you've got Chorus and GONG, in HR you've got Ambit. What are the top three use cases of - what are customers using?

Sam Liang

We focus on the more general use case, which has a general appeal. As I mentioned, corporate meetings, interviews, phone calls and we do conferences. We don't, you've mentioned GONG and Chorus, I mean they focus on sales conversation. That's the only thing they do, but most of the people here are not salesmen, but we do want all these people to be able to use it. We do do more natural language processing to understand certain key words like action items, names, decisions. In our system actually we can already extract some summary keywords; without looking at the whole thing, you can quickly tell what this meeting is about. The other thing…

Siddhant Trivedi

Maybe to just add, I guess from the data that you are looking at from your customers, what are they using it for? The top three.

Sam Liang

Reporters love it, a lot of lawyers are using it, product managers, actually we know there are product managers in Amazon who use it, product managers in Tinder who use

it for their product meeting. They actually use it to generate meeting minutes automatically. There are students who use it for lecture notes.

Manek Dubash

Time's up, time's up. Thank you Sam from AISense.

The second company in the cloud / data centre category, Cohesity. Come on down, you have five minutes.

Lynn Lucas, Chief Marketing Officer at Cohesity

Good morning, are you guys ready? Give me the sign back there. Go. Hi, good morning, I'm Lynn Lucas, I'm Chief Marketing Officer at Cohesity. Cohesity is based here in San Jose and was founded in 2013 by Mohit Aron, who is known as the father of hyperconvergence. So the previous two speakers on the panel on IoT as well as the gentleman just before, all were talking about an incredibly increasing world of data. Data is now what some call the new lifeblood of the digital economy and yet we don't treat our data as securely and manage it in a way like our dollars or whatever currency you use from around the globe. But it is incredibly important these days for organisations globally.

Cohesity is here to solve the problem of having management of data and applications across the enterprise and the public cloud in a way that businesses can really start to take advantage of the promise of all the data that is now being generated. This is something that Gartner's been talking about and in particular has stated that two important areas of IT are going to be disrupted over the next three years: one, the storage of the data. There is a dramatic disruption happening in storage where most organisations will move to what's called scale-out storage. Then backup and recovery, this sleepy old technology that was invented more than 20 years ago has now reached the forefront again because of ransomware and that legacy 20-year-old architecture is also not prepared to deal with today's needs for both protection as well as recovery of that data and those applications and those areas are also being disrupted.

So what does Cohesity do? If you think about a data centre for any organisation, what we think about as end users is the primary production applications or the tip of that iceberg is what we interact with, but the vast majority, 80 per cent of the investment and the complexity is underneath the water. That has been now shifted to the cloud. Many companies and public sector organisations ran to the cloud thinking this would help them clean up that very messy, complex environment they had. What they found is that it's just creating more complexity for them. They want the ease and scale of the public cloud, but they are creating that same mess in the cloud these days. What Cohesity does is create a single set of infrastructure, a single operational model across the enterprise data centre and the public cloud and increasingly these remote or edge environments where many of the businesses are placing IoT in our cars, in windmills, oil platforms, so that organisations can seamlessly manage their data and applications and move them across these environments and have one common infrastructure.

Typically most organisations today have upwards of 10 to 12 vendors to manage backup alone, to put this environment together, it's incredibly complex and fragmented. The simplest analogy is that before the advent of the smartphone, you would have had to carry a flashlight, a GPS device, a music player in addition to your flip phone. Now you have one platform, whether Android or iPhone and you've gotten so much capability from it. This is how we're transforming data centre and public cloud operations for enterprises and it's built with the cloud in mind as that continues to grow and expand and become more important for organisations worldwide.

Thanks very much and I look forward to the judge's questions.

Manek Dubash

Okay, you have five minutes to answer the judge's questions.

Janice Roberts

I seem to be starting again. It's not because I'm here, but I'll jump in. So first of all, when I look at what you're offering, I mean it seems to make sense. The value proposition isn't totally clear to me, but what I'd be interested in, I looked at some of your early customers and there's a smattering of different types of customers, e-commerce, universities and so on. How do you start transforming a company to your platform and what are the type of companies that are going to be the early adopters or are the early adopters?

Lynn Lucas

Great question. So data and data centres are a global language, so that's great for a market size. In fact we estimate the total market size to be about $60 billion. Where customers have the most pain today is what's called backup and recovery. Every organisation of any size, say 1000 employees and up, is backing up and having a safety net for their applications. This is the very fragmented and old area, most architecture has been developed 20 years ago and this is where most customers begin and then they can consolidate other storage systems and their data onto a single Cohesity platform as makes sense to them, but we typically see them move to test/dev and analytics next.

Janice Roberts

They can pace it over time, essentially.

Lynn Lucas

Correct, yes.

Curtis Feeney

Who would you be competing with, primarily?

Lynn Lucas

Just a few small companies that you haven't heard of, Dell EMC, Veritas and Commvault are typically the three that we compete against in this legacy backup and recovery area, those being the companies that had created a lot of the existing systems customers have today that are still in place literally 10 to 20 years later.

Hiro Rio Maeda

Well, not just a legacy company, but there are other start-ups, like Druva, Rubrik, [Mac Star]. There are many companies that are trying to aggregate those kind of stories and use it for the little more intelligent backup. How do you compete with such red ocean market?

Lynn Lucas

Great question. I never mention my smaller competitors. ☺ Druva actually is in a different space in terms of backing up the endpoints and we actually partner with them. We are taking care of fundamental - what we call secondary applications - they're - those in the data centre - applications that would back up, say, your Oracle database, your SQL database, your VMware environment. They're focused on a cloud model for your endpoints and we are complementary.

Rubrik is probably the closest in our space, being the only other one that has a modern web scale architecture, the core difference being that it is focused on a better backup solution alone. We extend the capability set to provide more value, to include the consolidation of test dev and analytics and what we would call generic file services use cases.

Hiro Rio Maeda

I see. So if that's the case, maybe you can be more like a open source project, like a Teeid, and that's, like many technical companies started to be using that to consolidate different sources of data and their ways and using analytics and applications.

Lynn Lucas

We'd - I would say that typically, actually what we see as a differentiation is we have large enterprise and public-sector customers - Department of Energy, Air Force, Hyatt - large enterprise organisations. There are many others. Cohesity has been in business, selling about two and a half years, whereas some mid-market, smaller organisations would just look to replace solely the backup. CIOs who are looking to do this digital transformation are trying to find ways to gather all this data into one place, where they can actually take action on it and without putting it in a single platform, a la the smartphone. It becomes difficult for them to realise this vision of digital transformation.

Hiro Rio Maeda

Got it. Sorry, one more question, if you don't mind - do you scrutinise the content and contextual of the data itself, so that you could add extra layer of security or [and other decks] on it?

Lynn Lucas

Excellent question. That's one of the other differentiators from - between us and Rubrik. We index all the metadata of the files as they are brought in. But in addition the platform includes a native map reduce implementation. So for what we would call file data, inside we actually have the ability to index within the files, and per the conversation earlier around GDPR, one of the applications of our platform, we run a secondary app on it that allows organisations to do searches within those files for PII information, like emails, passwords, names and so forth.

Siddhant Trivedi

Why's it taken so long to see innovation in this sector? I mean the public cloud's been around for some time. We've seen cloud adoption happening.

Lynn Lucas

I would - the short answer - since we got the shark noise there - is that I think our founder took a step back and was the one to see that it was time for fundamental innovation and it just hadn't been viewed with his perspective before, but it's certainly very interesting to enterprise organisations today, given today's focus on data.

Manek Dubash

Great. Lynn, from Cohesity, thank you. Now I'd like to invite Dust Photonics to come down, and you've got five minutes starting now.

John Mein, VP of Sales for DustPhotonics

Good morning everyone. I'm John Mein, the VP of Sales for Dust Photonics, the newest optical transceiver company on the planet that's revolutionising optical connectivity for data centre. We're leaving the rest in the dust and not just our competitors, but other technologies, such as copper. So let's get started.

First, I have a question for the audience. What is the most common metallic element on earth? Any guesses? It's aluminium - or as they say in the rest of the world, aluminium. But until 200 years ago, it was unknown to the modern world. How could that be? Because in nature, aluminium does not exist in its pure form. It has to be refined - and you can't just heat up bauxite ore to get it.

In 1808, Sir Humphrey Davy invented a laboratory process, using electricity and some chemicals, to enable a refinement and get - and produce small quantities of aluminium. It was very expensive. Today it's used everywhere, for cookware - it's light, strong, conducts electricity - but it took 100 years for it to be adopted.

In 1850 Napoleon III would host state dinners and he'd give his most esteemed guest aluminium utensils. The rest would get gold. In 1885, when the Washington Monument was completed, they capped it with a six-pound ingot triangle of aluminium. The entire US thought that was way too extravagant. But the very next year, in 1886, two scientists independently, Charles Hall in Ohio, and Paul Héroult in France, developed a manufacturing process, using cryolite and electricity that vastly reduced the cost of producing aluminium.

In 1850, aluminium was $17,000 a pound. By the turn of the century it was a nickel a pound. This enabled vast new industries - it was much like when the laser was invented - it was a solution in search of a problem. They had to develop an industry for this - but aluminium enabled the aircraft industry, through lightweight structures and engines.

The construction industry, the Empire State building used massive amounts of aluminium in its construction. Bicycles - all kinds of applications.

This phenomenon has been repeated again and again. Computers - the first IBM PC in 1981 was $4,000. Today you can get far more functionality for a few hundred dollars. Many other examples of that, including the laser. The first laser pointer was $1,500 in 1963. Now they're $2. Ammonia fertiliser - vinegar even - all through innovations and design in manufacturing were they enabled and became widely adopted by the masses.

Dust Photonics is doing exactly the same thing by reducing the cost of optical connectivity by 90% - and I'll show you how we're doing that.

We are reducing this complex device - it's shown from one of our competitors - to a very simple device shown here, by automating and simplifying the manufacturing process. We're building and perfecting that interface where the fibre interfaces with the laser diode and the photo detector.

Today everyone uses active alignment, where they have to actually light up the fibre, align it with the laser or the photodetector to get the maximum sensitivity. We have completely automated that process.

As it turns out, up to 70% of the building of an optical transceiver is in that assembly process, because of the equipment required, the yield hit and the time it takes to do that. In our factory, in the same floor space, we can produce 30 times as many optical transceivers per hour, as our competitors can do.

The other phenomenon that is happening in data centres is that copper is losing steam. As the data rates go from 100 gigabit to 200, to 400, to 800 gigabits, copper lengths are shrinking and they are becoming ineffective and unusable in data centres. With our technology, we make optical transceivers affordable and we enable that transformation, so we're eliminating the mess of a copper wall like this in a data centre, to a much more simple design with far few connections and less power consumption.

Our device…

Manek Dubash

Time's up.

John Mein

…the [unclear] [20 SR4] is on the market today for 90% of the cost of what it was two and a half years ago.

Manek Dubash

Time's up. Okay. Up to the sharks to give you a grilling. You have…

Janice Roberts

I was going to say Sid should go first.

Curtis Feeny

Wait - I want to ask some questions about aluminium before we jump into - most of the questions that came up for me were about the aluminium history, but back to whatever you do - I think that cost advantage is a manufacturing design breakthrough. Could you give a little more colour on the IP around that? Is it all in the manufacturing process? Was it some breakthrough in technology at the material level or…

[Over speaking]

John Mein

We have patented a little plastic micro assembly that contains micro lenses, prisms and mirrors that's manufactured for us to micron tolerances and that is our IP. Our heart is that light engine.

We have 100% yield with that light engine. It's not too bad if you're building an optical transceiver with just one fibre, if you have to throw 1% of them away, if you have 99% yield - but the 400 gigabit modules use 16 fibres today and if you take 99% yield times 16, that means you have to throw 15% of your transceivers away.

We have 100% yield on all 16 connections.

Siddhant Trivedi

John, could you talk a little bit about the sales process?

John Mein

Our sales process?

Siddhant Trivedi

That's right.

John Mein

Our target customers are everyone building a data centre or supplying equipment to a data centre - Facebook, Amazon, Baidu, Alibaba, Tencent - all the carriers around the world are building massive data centres.

Typically what happens is they evaluate our technology, our sample - they like it, then they buy 30 or 40. They run them through extensive testing that takes about three to six months, and then they ramp production.

Siddhant Trivedi

So it's about six months to sale, is that what you…

John Mein

Mm-hm. We've been sampling since last fall already.

Janice Roberts

I was going to ask the same about is a direct sales model? I'm thinking about how you scale this over time and the size of the market and the opportunity.

John Mein

To date we've been a direct sales model. We've recently hired reps here in the Bay area and China. Our biggest market will be in the US and China, initially, and then that'll spread throughout the world.

Janice Roberts

Where is manufacturing? I know the company's based in Israel.

John Mein

Currently we're using a contract manufacturer in Thailand. There's so little labour in our modules that we seriously considered building them in Israel, where our R&D headquarters is, but we're starting with a fab with them. We'll eventually have our own factory.

Hiro Rio Maeda

I mean you're going after a really, really interesting problem that in many of those hyperscale data centre, the short- to mid-range connectivity is a big issue nowadays. It's not north/south traffic way - it's more the east/west traffic that's being congested. So I think you're solving a big problem there, so that's a good thing.

I think some new companies like IR Labs are coming up with a similar concept, so what do you think, when it comes down to the competition - is it going to be purely the cost per gigabits that you have to compete against?

John Mein

Our first generation of devices are based on chips from other suppliers. For the TIA, the laser driver, and they support multi-mode fibre, which is an easier problem to solve, because the tolerances aren't as tight. But our second generation of products we use silicon photonics, which is being used by other people, but even with silicon photonics, you have the alignment issue. You have to align the laser diode. You have to get the light into the silicon photonics chip. Because you cannot generate laser light inside silicon. It just doesn't lase.

Then you have to line the fibres up to get the information in and out of the silicon photonics chips. Our process will be about to support that as well.

Hiro Rio Maeda

What's your cost per gigabit like?

John Mein

Today we're able to sell the 100-gigabit module for a dollar per gigabit per second, in volume, and with the 400-gigabit module, within three years, we'll be at 50 cents a gigabit per second.

Hiro Rio Maeda

Fifty cents?

John Mein

Half as much.

Hiro Rio Maeda

I guess industry standard's around a one-point something, so if you can get there…

John Mein

I'm sorry, what?

Hiro Rio Maeda

The industry standard is like $1.80 per gigabit per second, so if you can get down to 50 cents that's a - that's great.

John Mein

Okay. All right, thank you. Dust Photonics - enabling the mass adoption of optical connectivity in the data centre.

Manek Dubash

Thank you.

John Mein

You're welcome.

Manek Dubash

Thank you very much. Before we move on to the next category, may I ask the four esteemed VCs to give us a quick, 30 seconds each, maybe, kind of first impressions? I know you're going to do full deliberation over lunch, but a quick 30 seconds each, maybe? What do you think so far? Of this category?

Siddhant Trived

I think we've had a pretty interesting set of companies. Obviously, they're at very different stages, so that's one thing that we have to talk about, and I know Curtis and I were talking about that even before.

Curtis Feeny

I think these are strong technology companies - very strong technology companies, and then when we look at it, it is an investment. Once you put yourself out there with a technology breakthrough in hardware, like Dust Photonics, then you have the competition question of the shelf life is fairly finite. So that's the thing I'm sure we'll talk about.

Janice Roberts

I think when you're talking about this particular sector, [unclear] and so on, they're obviously very broad, so they're hard to compare, but I think it's very clear for all of

them. I would just echo really what Curtis said. Be very clear up front about what your differentiator is and just get to that point.

Some of the real crisp differentiation has come out in our questioning, where really it should come out in the presentation. I think like you brought out more in terms of - the last pitch, in terms of the real cost advantage and what it would mean, and where it could get to.

We need to hear those up front. I should be - our questions should be more clarifying the real meat of what someone's pitching.

Hiro Rio Maeda

It's - this five-minute pitch is very - somewhat difficult, in a sense that we cannot really dive into the specific too much, because I want to let them speak about the entire benefits and inventions that they're coming up, so that's a challenge for us.

Manek Dubash

You're right, here and NetEvents has been working on a time compression algorithm for some time now. We haven't fixed that one yet.

Janice Roberts

Demos are always great.

Manek Dubash

Yeah, absolutely. If the demo gods are smiling on you.

Okay, next category is IoT. NetFoundry, come on down. You have five minutes.

Brian Isaac, Sr Director, Global Business Development, NetFoundry

Good afternoon. My name's Brian Isaac. I'm with NetFoundry. We are headquartered in North Carolina and our founder is Galeal Zino.

We launched the business February of 2017 at Mobile World Congress in Barcelona last year and I came on board in August of last year.

Let me get to our first slide here. For NetFoundry, we are a software-defined network - not to be confused with software-defined wide area networks or SD-WAN. We do operate in three verticals or spaces, but today we're here to talk about the Internet of Things and how you can secure your IoT data cost effectively and with agility.

Where we are unique in the space as we are application specific, hardware agnostic and carrier agnostic. NetFoundry secures and creates a network over any internet or broadband that you provide to the software. This allows you to have the ability to quickly and with agility spin up and create networks.

Someone who is used to using our software and has been spinning up networks can create networks in about nine minutes. From a third party that's been testing our software and giving out to their IT staff, the first time they touch it, it takes them about 30 minutes to create networks and spin them up.

I thought what I'd do is just jump right into this very quickly and give you a use case. At Hannover Messe, a couple of weeks ago, we did a joint announcement with AWS - they just rolled out their IoT analytics and they chose NetFoundry as connectivity partner for them because of the simplicity.

In this example, you have the NetFoundry console, which you can also connect to through an API. This is where your administrator is able to create networks. They then push software to AWS and spin up a gateway. They then send another gateway to where their IoT devices are and then in their console they connect the two together and now they're communicating. That data can flow to AWS and you can leverage AWS IoT analytics.

What's fantastic about this software is you can bring in other clouds. You could have some data go over to AWS and the same or other data to over to Azure.

You can bring third parties in. There's just a lot of flexibility. I know in five minutes we're going to have a hard time getting into all the details.

What I thought I'd also do is just talk about another use case, which is a partnership that we're doing with Micron in the autonomous vehicle space. Micron has a new flash that they've come out with, called Authenta. It provides hardware root trust and NetFoundry can leverage that authenticated identity and use that to create and authenticate the network, going back into Azure to a third party.

NetFoundry's software defined network, compared to a traditional VPN, is dynamic and multi-point versus static and point to point. With our solution, you just have the one client and then you give access to it to anybody. So in the autonomous vehicle example, if Ford needs access and Progressive wants access and any other third parties, you can, through that single software, pass out licences to them, and give them secure access.

New cars have multiple LTE SIM cards and Wi-Fi connectivity, which means there are multiple ways to access the car and are potential paths for hacking. NetFoundry runs a software-defined perimeter, which is zero trust, so anybody who is trying to come in, over any one of those broadband connections is unable if it didn't get generated off the NetFoundry network as a known source, we just drop the packets. So you're not ending up with the "zombie cars". We mitigate DDoS attacks.

Really these are very quickly a lot of our strengths about what we're doing and how we're able to fill gaps. A lot of times people are looking at putting us into a category and really, it's where MPLS can give you a lot of private connectivity, but it can be expensive and it doesn't work for all locations.

So for locations where MPLS doesn't fit in, we're a good solution. Where your VPN isn't going to give you that multi-point ability or it's not giving you the performance you want because it puts too much latency on that connection, then we're a good solution.

We're not going to be the solve-all for everything, but we definitely fill a need in the marketplace. What we're seeing out there from our competitors is some people are doing a little bit of some of it, but they're not doing everything that we're doing end-to-end.

So with that I'll open it up to any questions that you may have.

Janice Roberts

First of all, I think the idea of securing IoT networks is obviously essential, particularly for many of the use cases. Is that your big differentiator? Because you talked about a few.

Brian Isaac

Yeah. Our differentiator in the space is - again, we're talking about just IoT here, right. We do apply - but that goes into healthcare and a lot of different other spaces. For us, it's really to take all the work that people are doing on doing that security stack on premise around those IoT devices, and then also what they require from Azure and AWS. They require the same security.

But then we find that people are using traditional VPNs or TLS to connect that, and we're like, why do you have the same rule sets end-to-end on your security? That's the type of connection we're providing.

Janice Roberts

How do you insert yourself into the solution? In terms of the sale - because you're partnering with others, which I can see, but as these networks start to build and get some scale, how do you insert yourself? Do you partner integrators? How do you get to market?

Brian Isaac

Yeah. It's multi-faceted. We're doing direct sales and that's where we're going directly to the customer, knowing that generally speaking that they have an IoT deployment and we know the complications associated with that. We explain the network piece and then they say, oh, hey, that solves our problem. They bring us in.

We're also then working with partners who are out there that are selling. So we have SIs like [Tully] Consultancy Services, Wipro, ACL, Accenture, Cognizant - they're all out there, trying to solve this. Like I was saying earlier on in the panel that this is multi-segmented. It's not just one customer solving - one solution solving the problem. It's multiple and the SIs play a big role in that and they're a big part of our partnership.

Hiro Rio Maeda

Do you have any actual customers in production environment using it?

Brian Isaac

Yes, we do.

Hiro Rio Maeda

In what sector?

Brian Isaac

Currently we have customers in Finance, Critical Infrastructure, Education and Technology verticals. These customers are using NetFoundry for extranet environments,

disaster recovery and data back up. We are targeting healthcare and IoT verticals with some possibilities in Smart Cities and Agriculture.

Hiro Rio Maeda

What about the IoT side and the [auto] side?

Brian Isaac

Yeah, on the IoT side, we're still young, as far as where we are, so we're in the middle of proof of concepts with some of those customers today.

Hiro Rio Maeda

I see. One thing that maybe that many other VCs hate is that we can do everything in every industry kind of things.

Brian Isaac

Sure.

Hiro Rio Maeda

So, as early as you can be, it's - you want to have a laser focus market to go after and improve it there and then expand into other territories. Something that maybe that resonate more, but yeah.

Brian Isaac

Yes, to that point, our focus right now is the finance market and healthcare, along with Fortune 500's.

We're starting to have success on the IoT front. We're working with some of the ISO's or power grids. When you start talking about the power grids, the problem that they're having is you have so many solar farms coming on, and they don't always have the best connectivity, nor can they get those MPLS connections out to where they are, so trying to bring all these third parties into the grid system securely, is important. We can get new solar farms added to the ISO securely, very quickly and cost effectively.

Siddhant Trived

Could you talk a little bit about your competitors and the wider competitor dynamic?

Brian Isaac

The competitors we are generally compared to are VeloCloud, Versa, Silver Peak, but interesting with those, we have the ability to partner with them. They can include our software in their solution to round out their offering. We are a partner with VeloCloud for example.

I've recently learned about a company called Luminate and BlackRidge, but again, they're doing hardware deployments or using BeyondCorp, from Google, as part of their structure. So they are giving you your software-defined perimeters, but then it's not giving you any kind of control through the internet over latency and jitter and the additional security of the multiple paths, like we do. NetFoundry is cloud native.

Thank you for your time. I really appreciate it.

Manek Dubash

NetFoundry. Thank you very much. Applause.

Now, the final company in this category, IoT category is POLTE. I hope I've pronounced that right.

Ed Chao, CEO of PoLTE

Good afternoon. The Internet of Things - one of the key pillars of the Internet of Things is being able to find where your things are. Location is fundamental. POLTE provides location for the Internet of Things.

How do we do this? There we go.

I'm Ed Chao, CEO of POLTE, and I'm going to tell you all about what we do.

One of the big problems of the Internet of Things today is the cost of the device itself. A lot of the modules you see out there cost 20 bucks, 50 bucks. In order for us to be able to scale to the promise of IoT to get to 20 billion devices by 2020, the cost has to get down - down to the level that a lot of these low-power wide area networks are promising, of $3.

Now, you can't get a $3-chip when you're adding a $5-GPS chip to that, right? The economics don't add up. So if you want to have the ability to track an IoT device, such as like in a package - like talking to FedEx, they would love to be able to track - for efficiency purposes as well as for insurance purposes - where those packages are going. Having a $20 module with a GPS chip in it, that has a battery that only lasts a day, does not meet the need.

This is what POLTE brings. We have - what POLTE does, it's a cloud-based location solution for the Internet of Things. We take 4G and 5G cellular signals and we triangulate, based on those signals. What we also do is we ship that calculation from the device to the cloud. By taking it off the device, it simplifies the device for not having to have a complex arm processor or DSP, thus keeping the cost down to just that LTE module and [base pan] modem.

This unleashes a whole new set of use cases, whether it's providing location at the time of a credit card transaction, or a manufacturing line being able to track assets in a private LTE deployment inside an IT enterprise. Being able to provision, very, very cost effectively, smart city sensors, where you don't have to actually know exactly where you did it at the time that you - when you provisioned it. You'd only have to know exactly where it was - we can provide that just with a dip, using our location as a service.

Think about your wearables. How many of you have Apple watches? You have to charge the thing every day. One of the reasons why - it's a GPS. It's draining your battery. Imagine being able to do - having POLTE - which is 50 times more power efficient than GPS.

Containers. There are - I had no idea how many there were - there hundreds of millions of these containers around the world that are shipping our stuff everywhere. These are

high, high value goods that need to be tracked because there are thieves and issues with being able to track where those things are.

The market is huge. Cellular IoT is - based on 4G and 5G is - there's 2.6 billion devices that are projected to be in the market by 2023. It's also projected that the Location of Things market - which includes not only just finding stuff, but the analytics associated with the location of things - is a $72 billion market by 2025. This is a space POLTE is looking to dominate.

How are we going to do it? Our key differentiator is that we have global coverage - indoors and out. Unlike a lot of our competitors who have to have proprietary hardware to be able to deploy their coverage, such as a LoRan or a Sigfox, we're just using the hundred millions - the tens of millions of cell towers that are already out there today.

We have the best accuracy. We provide accuracy both indoors and out. Sub 10 metre, if you're using the macro network, and single metre, when you're using an indoor private LTE network.

We enable the lowest cost. Getting down to that $3-module is no longer a thing of the imagination. It's - you can get there and have your cake and eat it too, with location.

We enable the longest battery life. Because you don't have to have three chips, you don't have to have GPS sitting there looking for satellites for four minutes, or even Wi-Fi looking for your access points all over here. The power to do that is over 20 times more than what we require for our approach using 4G and 5G signals.

We have traction. We have been partnering with key partners in the ecosystem. Sequans at chip level, to be able to pull the radio signals that we need from their chip. It's a very small sample that gets transported to the cloud. We've proven that with them and we're able to integrate with their chip in a matter of several weeks.

The same with Micro - another start-up that does - that is going to enable that credit card capability that we talked about earlier.

We've also done field trials with AT&T. We've proven the technology both indoors and out, both in Dallas, San Jose and in Virginia. So we are a proven technology.

We're also partnering with a company called Rohde & Schwarz, who does test equipment for cellular networks, to be able to continue to improve.

We are a veteran team, with over 150 years' experience in the space of a [netted] wireless and the like and we are [bold]. We enable the Internet of Things.

Thank you.

Curtis Feeny

A quick question on the go-to market. What do you think is the highest pain point market that you will hit first? It sounds like you're very early, but who do you think will get you the real traction, going forward?

Ed Chao

There's two areas that we've seen the most traction on there, when we talk to them in partner - together with our partners. When we ask them, are you ready? They're like, we wanted it yesterday.

One is industrial IoT, where people want to be able to take their - one big trend we're seeing is private LTE networks - going out there with GPRS and other capabilities there, because they want to have that security of private LTE that Wi-Fi cannot provide them. They want to be able to use that infrastructure to locate the goods that go through their factory, as well as all of the tooling that is portable that needs - they need to know exactly where it is at all times, to ensure that there's zero downtime on the factory floor.

There are tens of thousands of components that they want to track. We're able to track it down to the three- to six-metre level that allows them to reduce - increase their efficiencies and their throughput.

The other one…

Janice Roberts

Could you clarify what you're actually tracking? Because in order to track, you have to track something.

Ed Chao

It's a module.

Janice Roberts

So it's a module?

Ed Chao

Yeah. An IoT module.

Janice Roberts

Just to follow on a little bit from this - first of all, I get the need and I think what you have is a vision today, and I'm interested, because you've got - although you're working with partners, you've got a lot of pieces to come together. So, what are the modules and what are the - because a lot of the things you've talked about, one of the issues is the modules and the cost, and the deployment.

Ed Chao

Let me paint a real picture for you. Have you heard of the Amazon button?

Janice Roberts

I absolutely…

Ed Chao

Yeah. So just yesterday Amazon just launched the cellular-enabled Amazon button. That button is far more upgradable in support of POLTE. It is here today. It's just a matter of us - we're a start-up and so it takes a little time to prove this and show everybody that this is real - because it is - but it takes a little time to do that.

Working with our chip set provider, who actually is a chip set provider for that button, we believe we can firmware upgrade those capabilities, using a firmware-over-the-air capability.

So the hardware's here today. If you think about all the use cases for asset tracking - your dog tracker, your child tracker - those are the hardware platforms through our software. We add no new hardware. Our software - firmware being updated on those devices - together with the cloud complexity - all the compute power that's in the cloud - provides location on a thing that didn't have it before.

Janice Roberts

But you've got to build a business, so therefore those are all great ideas, but you're saying industrial IoT is where you're going to really start to build the business?

Ed Chao

Yeah. It's one of the use cases that have hit us really hard and quickly. The other one was asset tracking. So Amazon, UPS, FedEx - they want to have the ability to track their assets through their system, which is highly multi-faceted - as well as provide a value-added service to the customer.

So we're very excited about that one, because it really highlights what we do best, which is indoor and outdoor location, with extremely good battery life and low cost.

Siddhant Trived

Before you go on here, just a follow-up on that question. Just to clarify there - so you have to partner with the chip manufacturers? Is that really how you have to go through and enable POLTE?

Ed Chao

Yes. Yeah, that's one of our biggest friction points. The good news is we're all…

Siddhant Trived

What do they want from you?

Ed Chao

A rev share.

Siddhant Trived

What is that? What does that look like?

Ed Chao

We're still in business negotiations with them, but the way you think about it, is this. The IoT - the reason why Qualcomm, for instance, doesn't get into the IoT chip business - it's low margin. All of these guys that are IoT chip focused are dying for recurring revenue opportunities. So if we're able to charge, say, $2 a year for a device - replacing a $5 GPS chip, which is great value - if they just even had half of that or a quarter of that, that adds hundreds of millions of dollars to their bottom line.

Siddhant Trived

Just to clarify - you don't also need to work with the wireless service providers?

Ed Chao

I'm sorry?

Siddhant Trived

You don't also need to work with the wireless service providers?

Ed Chao

We do work with the wireless service providers. We do need their cell tower almanacs, which are available. We also have technology that allows us to crowdsource and reverse-engineer that without their direct intervention. So that's another key part of our patent - 25 patents that we have that allows us to use a calibration method as well as crowdsourcing. As we scale, our capability just gets better and better over time.

Hiro Rio Maeda

A couple of questions. Are you thinking about adding other kinds of the sensor into the module, such as temperature tracking or moisture tracking or vibration tracking, so that that adds another layer of understanding of how the shipment was being done?

The second question is, what's the cost of module that you're thinking? Depending on that cost, what's your thoughts on limitation to certain - if it's expensive, it has to be only applying to the high value item.

Janice Roberts

Or it goes to the pallet, as opposed to the box?

Hiro Rio Maeda

It goes to the pallet and then can be - has to be reusable, but he has to create the whole ecosystem around it.

Ed Chao

Yeah. We're a platform provider. We're providing other people who are making these modules software - a location as a service. So for them, it's just a software upgrade to their products that have all these multiple sensors.

One thing that we are doing is bringing in location-based sensor information into - in hybridised location. So if you think of an inertial sensing units, to be able to provide tracking, that only improves our capability as - we do location. That's [unclear].

Thank you.

Manek Dubash

POLTE. Thank you. Applause, please.

It's a tough challenge, and yeah, VCs, if you would, a quick 30 seconds - what do you think of the IoT category so far? Because that's the end of the IoT category. Thoughts?

Janice Roberts

I think I just said it with respect to the last person - is it's how you take the vision and build a business, I think. You can't do it all in five minutes, but just give us some pointers. It's how you - when you have this broad vision, how do you start? I think, Hiro, you mentioned this a couple of times - how do you go from the general and the broad to specific?

Manek Dubash

Curtis?

Curtis Feeny

The challenge I think in the earlier start-ups that we're seeing is they don't have the focus yet because they haven't figured out where the best first market is, and that's an iterative experiment. So they're in the experiment stage and therefore I think they really need to focus more on the ROI that they deliver, the specific advantages versus other technologies that will then guide them to those markets.

Hiro Rio Maeda

Basically it's the product, the market fit issue that all the start-ups have to solve, and at a certain stage of the company every entrepreneur has to solve that issue. But before that it's understandable that they want to explore all the possibilities and try to have the one specific one that their technology could solve very effectively. So that's something that I'd love to see in many of those companies.

Siddhant Trivedi

Yeah and I think connecting that to who are you competing against as a result of that, once you do figure out what areas you're focused on, as well as who do you need to partner with and what type of rev share do you have to work with.

Manek Dubash

Right, final category. Three contestants, come on down. We are into cybersecurity. Fyde. Five minutes.

Sinan Eren, Founder & CEO, FYDE, INC

Good afternoon ladies and gentlemen, esteemed judges. I've been in cybersecurity for almost two decades. Never had a dull moment; accumulated a long list of perhaps battle scars. However, the most profound moment in my career I would say was a personal one: my first election, my first ballot cast as a newly minted US citizen, the 2016 elections in our country, where we all witnessed a foreign entity's meddling perhaps or an entity's meddling through the cybersecurity's tradecraft, the most effective since Stuxnet.

This was human-centric, social engineering driven attacks, threats, and I would say that the embodiment of all this human-centric new cybersecurity trend landscape was the John Podesta incident, the chairman of the DNC, and the subsequent disclosure of his e-mails through WikiLeaks. This basically marks the genesis of Fyde where I left my

job at an [IPO bound] cybersecurity company and started the firm to solve human-centric, this new category of attacks for everybody globally.

So today the majority of cybersecurity incidents start with a form of phishing, a variant of phishing. According to Ponemon Institute, this costs about $3.7 million to a large enterprise and about 76 per cent of all businesses suffer one form of phishing every year. Sixty five per cent year over year increase in phishing campaigns were marked by the anti-phishing working group collected by threat intelligence from industry participants.

This is a growing epidemic where the existing market solutions do not offer enough remedy. So for example, the intel - threat intel driven attack triage and site takedown is an extremely slow process where the damage has been long done, or on the other hand, where you talk about active remediation, active prevention, you have internet security gateway solutions and you have personal VPNs which adds a ton of latency and also drains battery. Essentially the last mile is what gets to them.

So today you're sitting here connected to the hotel Wi-Fi; every single one of us has smartphones in our pockets. These are by their very nature perimeter-less; they roam with you wherever you go. So you're going to be hearing a lot of black boxes that solve cybersecurity challenges with magic basically, but ask yourself what is their visibility right now to your laptops. Whatever you're doing, whatever you're clicking, the hotel captive portal that you just clicked through, what is their visibility to that potential threat?

So Fyde is out there to solve this by moving the internet gateway, the proxy, to the edge, to whether that's a smartphone or a laptop, whatever the roaming device you might have. We intercept network traffic in everything that you click and you interact at the edge, at the device level, and solve the phishing problem, the human-centric social engineering driven phishing problem, at the edge.

We are free for consumers for personal use, available from the app store globally, and it will remain that way. And we do sell device licences to the enterprise where we provision through MDM or existing provisioning solutions where the enterprise now gets to control their roaming assets and monitor and detect and prevent security risks with their mobile and roaming assets through a multi-tenant dashboard.

How we achieve this is that we use a combination of blacklist, whitelist and machine learning models that are again compute at the edge. We do not add extra latency; we do not take your private browsing, your private interactions to a cloud gateway and accumulate it there. Everything is done at the edge.

However, on occasion we will run into a borderline incident, a borderline site, a domain, a phone number, a text message you receive, where we cannot make a decision with enough confidence. That's the time we will send that potential threat to our cloud for advanced machine learning and human analysis, so essentially supervised machine learning in the cloud, where we generate a new model and then we will be pushing it out to the edge again to your smartphone and to your laptops for protection of new and advanced threats.

Fyde just raised its funding in 2017. We are - we have launched the company actually as of April and we are based in Palo Alto with our R&D in Porto Portugal. Thank you.

Hiro Rio Maeda

So the mobile phishing has been something that we all know it's been a problem, but somehow nobody was able to crack it. And at the enterprise level or the on prem scene, there's Proofpoint, there's lots of endpoint securities, there's proxies, there's always interception can be happening at the network level. Why is it that any of those guys are getting into the mobile side of it and try to solve this problem?

Sinan Eren

I think we had a unique approach where we were able to figure out an instantiation of a local gateway at the device level. Rather than enduring the last mile latency problem and also the increase in power consumption to route all your traffic from a mobile device to a cloud terminator, we were able to innovate and push that gateway to the edge. I think they basically lacked innovation there and they tried actually, Zscaler, Palo Alto Networks, Blue Coat, they all try to terminate mobile traffic on their gateways. If you look at the reviews, they're universally hated.

Janice Roberts

So can you tell me - so I'm always a little worried if I went and downloaded your app, what would it do for me on a daily basis and would I be - is it easy to use, the UI? Just tell me what it would do for me?

Sinan Eren

Yes super simple, you just install it from the app store, and I encourage you to do that please. It will on-board and disappear. It will be in the background. If you power cycle your device it will come back up transparently. Whenever you engage what we call with a call to action, let's say you receive a text message telling you that your bank account needs to be reinstated because somebody logged in from Ukraine - in the John Podesta incident you got a Google e-mail saying that somebody accessed your e-mail from overseas. The moment you clicked on that call to action, that's where we intercept and warn you that it is not part of the whitelist; this is not a Google asset; this is not a Coinbase asset; you should not be volunteering your information to that site. We could actively block it or we can warn you in real time. Then we go away again. You don't have to launch the application ever again; we're always in the background communicating to you over notifications.

Male

So then how does that impact battery life?

Sinan Eren

Below three per cent on a 24 hour basis.

Janice Roberts

So will it give me more stress or will it destress me by having that?

Sinan Eren

It will destress because we also take on the extra task of removing all trackers and ads from your mobile traffic. You're going to love us. No trackers, none of them will be able to communicate from your mobile device back to their ad servers.

Curtis Feeny

How does your efficacy in stopping mobile phishing compare with what the standard is out there today? What's the sort of [unclear]?

Sinan Eren

That's right. I'm not going to debate the science. Everybody uses what everybody loves to call AI nowadays but regression analysis and commodity machinery models. What we do different is that we don't have blind spots. We're at the edge; we're close to you wherever you are. So we see more, we collect much more granular data, and we use the same computational and regression models and machine learning models. There's no magic there. It's just that we collect better data than they do.

Hiro Rio Maeda

So one of the problems in the phishing problem is that those phishing domains only last for a few days and if they get a couple of customers as victims, then they just go away. So that's why the blacklist never works, but at the most maybe like a week they will survive but how do you solve that issue?

Sinan Eren

Great question. This is why we have a free product. Yes we do give it away to protect everybody. That's us to be a good agent, just to be out there and help protect people. But at the same time they are canaries in the mine. They feed us this attack telemetry. Somebody clicking on that link immediately alerts us about the potential threat that there's a new PayPal domain with a little Unicode character, a little dot here and there. This is how we receive the attack telemetry by giving this product free to consumers.

Janice Roberts

So the free app is really a data source for you or an information source?

Sinan Eren

No, only when we block something for you based on the local model. Yes, if it's bad, we get to have it, because then we can push it out to everybody else. So you're actually sourcing us that threat so that we can share.

Janice Roberts

That's what I meant. I'm a source to you and then you make money how?

Sinan Eren

We make money from enterprise. So we are - our mission is to subsidise this whole thing through enterprise. They want to have control over their endpoints, roaming

devices; this is where we make money. But we will be giving it away to personal use for free forever.

Siddhant Trivedi

And you're anonymising all of that data, right, obviously when you pull it?

Sinan Eren

Yes. The data - threat intelligence is also another additional revenue for us as well. So we'll go to the financial institution where we catch let's say new - I don't want to call it zero day but new phishing attack targeting that brand. We also have some sort of triage link with them. We can detect those.

Siddhant Trivedi

I meant most on the consumer front, anonymising the consumer data.

Sinan Eren

Oh yeah that's right. We're GDPR compliant in that sense, plus, yes, we don't have any sense of user. You just install an application; we have an app ID but we aggregate it; we don't collect it based on application installation.

Manek Dubash

Okay thank you. Thank you Fyde. Number two in the cybersecurity category, Vectra. Come on down. Five minutes. Running. I like running, this is good.

Mike Banic, VP Marketing, Vectra

So good afternoon everybody. My name's Mike Banic and I'm here to speak with you about the Cognito platform. This is the ultimate cyber detection and threat-hunting platform. The problems that we actually address with this are really two. The first is speed. Admiral Mike Rogers gave a speech a year ago and he talked about what they need is speed, speed, speed in order to get ahead of the attacker. When you think about speed, put it in the context of the fact that on average an attacker goes unmitigated in somebody's organisation for 99 days, but it takes them less than three to get admin credentials, which are the keys to the kingdom.

He also talked about another issue which is retaining and finding good talent, and it's said that there's going to be as many as 3.5 million open cybersecurity positions by 2021.

When you think about this industry, it's ripe for transformation, and there's been industries in the past that have been transformed, ones whether it's telephone, manufacturing, auto industry is one of my favourite ones. When Henry Ford introduced automation and new tooling, he increased the speed of production, the consistency of it and the quality of it, and it didn't mean that we eliminated jobs; it meant that we made people better at what they were doing.

In cybersecurity transformation is happening right now, and it's happening in the form of artificial intelligence. We're doing that with the Cognito platform. Vectra is an AI

company transforming the cybersecurity marketplace. The Cognito platform is made of today two software modules, one that's called Detect and another that's called Recall.

Detect does something to solve the time problem as well as the people, the talent problem. It listens to network traffic. It extracts metadata and it then finds the signals of an attacker's behaviour and it triages that behaviour. It listens to it over time, it scores it, it correlates it to the machine the attacker is affecting, and it presents risk information about which machines are the highest priority.

But there's usually more information that you need, which is the reason the Recall module was created. You can pivot from there in order to perform a 360-degree cyber incident investigation around what happened with that signal that got triaged, prioritised and scored for me. From there you can determine where is the expanse of the attack, what other machines has it affected.

We had a customer who actually recently purchased Recall - they were already a Detect customer - and after a three-week evaluation they determined that it was a must have requirement because they had an early signal detection with Cognito Detect. They pivoted, they performed that investigation, and they found the dozens of machines that were affected by a phishing attack and they prevented any loss to their organisation. They happen to be a global investment banking firm.

When we look at the position where we are in the market, people use technologies today to detect cyber attacks, things like intrusion detection platforms. Gartner writes a magic quadrant for this space. They made a strategic planning assumption in the beginning of this year, in January, and they said that by 2020 the majority of these devices will use advanced techniques like machine learning and AI. Of all the companies that are out there doing what we're doing, we are the only company that they added to the magic quadrant; they positioned Vectra as a visionary.

The thing that they said put in human terms, lay terms, the value that we bring over the prior technique, which is that we roll up numerous numbers of alerts and we present an incident, rather than giving alerts that a human then has to track down. It solves the time and the talent problem. We make it easier for people to do their job and actually get ahead of the cyber attacker.

If we look at how this gets translated into the words of people using the platform day in and day out, Tribune Media, television and broadcasting firm, they say that they were able to use Cognito to reduce processes that took hours into minutes. Texas A&M University and Jackson Health are both interesting in the sense that they're using interns to fill previously vacant positions and give them a brand new set of tooling that's actually accelerating their career track, that's actually getting them farther ahead and making them more skilled, because it's offloading the mundane, boring elements where mistakes get made and things get missed.

By the way, the machine works all the time. People can actually leave work to go see their kid's baseball game or go have dinner with their family. The machine will work all the time in order to tell them information that is the highest priority for them.

Interestingly enough, an intern at Texas A&M University was recognised as Cybersecurity Student of the Year at the SC Media Awards at the RSA Conference earlier this year in April, and a big part of the nomination was how she learned to become an expert in cybersecurity operations by using the Cognito platform.

Part of what allows us to detect the cyber attacker behaviours in real time using AI is the unique combination of security research and data science. Thank you.

Hiro Rio Maeda

So basically you do the network analysis and try to come up with anomaly detections on the traffic.

Mike Banic

So yes, we're looking at network data, and to a certain extent we're finding anomalies, but they're very specific. They're actually things that a cyber attacker must do. In the same way that a square is a rectangle, it's a much more specific version of a rectangle.

Hiro Rio Maeda

Okay, so there's no endpoint sensor that you use; it's just on the network side.

Mike Banic

Correct. There's no endpoint agent. There's nothing that anybody needs to store on the endpoint.

Hiro Rio Maeda

When the user is off grid, not in the corporate network.

Mike Banic

Okay, so if the user is off the network and if they're not in the enterprise environment, then we won't see their behaviour, but when they return, if there's something that's infected with them, then we would see that present.

Hiro Rio Maeda

I see. So when the employee is off grid but connects to the internet somehow, do you partner with somebody so that you can monitor that traffic as well or it's just outside of your boundary?

Mike Banic

So if the - let's say if the user is accessing software that's in the cloud, so it's running in an IaaS environment or software as a service, there is an ability to bring in cloud events in order to detect the potential attacker behaviour that could be present that would only be seen when they're off net.

Hiro Rio Maeda

Got it. One more question. So you have to understand a normal state of the traffic pattern, but what's the learning period like?

Mike Banic

Okay. We use a balance of supervised and unsupervised learning. The unsupervised is what requires the training time. About 60 per cent of the algorithms are supervised so they work as soon as the software is turned on, and the other 40 per cent do require a learning period. It's typically seven days or less.

Hiro Rio Maeda

How is the false positive rate?

Mike Banic

So the interesting thing is it's zero, but that's like an unbelievable figure, right. Anything that we detect actually happened. But I'll give you an example. It's like if somebody - if a car goes through a red light and the camera goes off and takes a photo of it, you then have to, as a security analyst, determine what was that behaviour. If it's a policeman responding to an incident, that's in-policy behaviour that's acceptable. If it's somebody looking at their mobile phone that's distracted, that's a violation. So most of the detections that we present do have a level of ambiguity to them that requires some human inspection, so we keep a packet capture with every detection that can enable that inspection rapidly.

Curtis Feeny

Okay. Can you talk about the scaling of the human element? So you have this augmented AI that is making it instantly usable, but then as you scale does the human element have to scale linearly with the customers?

Mike Banic

It does naturally, but at a much lower ramp than it would with the traditional technique of using reputation lists or signature, because those are alerts. So let's say over time as you deploy this wider through the enterprise, you might have to add three people, whereas if you're adding something that's presenting alerts based on signatures, you might have to add 30 people.

Janice Roberts

So a high level question Mike. You talked about the Gartner quadrant, and if you look closely at that, you've got a visionary sort of position and it sounds quite substantial in terms of how you're addressing things. But you've also got some substantial competition in terms of big companies. The leaders are Cisco or Trend or whatever. So how are you going to break through?

Mike Banic

Yeah it is difficult. We've actually had an increased level of traction with channel partners, both regional ones as well as national and global ones. Last year we experienced 181 per cent growth in new annual recurring revenue, largely because partners were actually bringing us more business. That continued, oddly enough it was about 180 per cent in the first quarter of this year, and I think that channel activity is a big piece of that.

We have a partner, a company that we're partnering with that delivers Red Team services, and we're in a customer network today and the customer is already using Cisco. After the Red Team's been running for about four days, they've reported back to us and said the scoreboard right now is Vectra 11 Cisco 0. So we think that channel model, especially where they're offering Red Team services, is going to be a big factor.

Siddhant Trivedi

What are the two or three big things that show up on your dashboard that are considered KPIs for your customers?

Mike Banic

Yeah so the dashboard itself is - think of it as a traditional [analyst] 2x2, and just like with the magic quadrant you look to the upper right for who are the leaders. Here you look to the upper right for what are your highest risks. It ranks those risks based on the threat level and the certainty. So the more - the combination of behaviours that we see and the types of behaviours are going to drive up both the threat and the certainty score and push it above 50/50 and get it into the critical quadrant. There's the high which is we have a high level of certainty but we haven't maybe seen the threat level drive it into the critical. That helps people prioritise their day.

The one thing we go even beyond that is things that are common about a host that have an attacker behaviour, let's say it's the IP address of command and control, we further correlate that to an attack campaign. So there might be five hosts in the critical quadrant but they're all part of the same cyberattack.

Manek Dubash

Thank you very much. Applause please. And finally, JASK, the final company. Fitz?

Greg Fitzgerald, CMO, JASK

Thank you very much gentlemen and ladies. Are we on? All right. I'm representing Jask. We are an autonomous security operations platform. What we really should be talking about is the problem. We're not solving a problem; we're solving the problem, which is the human impact of cybersecurity. The key is that humans are not scalable; they're now dealing with more than they can possibly imagine in terms of all these alerts and things like that. The SOC itself, the security operation centre, is what we focus on. So as an investor we're looking at companies that are looking at security operations for monitoring their entire enterprise, not just a segment, not just a network or an endpoint or an application, but the combination of them all.

The problem is this is all outdated. So as an investor, what are we doing? We're solving a 20-year-old problem. The incumbents are owning about a $2.5 billion market segment which are really ArcSight, Splunk, LogRhythm, QRadar with IBM, and then it drops off for all the other entities.

So the problem is they have inertia and momentum, no innovation - people are actually leaving those organisations - and they can't keep up with the technological evolution. Adding new technologies that you're seeing today are just exacerbating the problem.

They're doing a great job at their point product, but for the security operations, he and she are concerned about the entire visibility of the problem.

So what we look at, it's time to evolve, just like all of us. We're a two and a half year old company. We produced our technology last June in 2017. We've got about 25 customers already. Very large, everything from 300,000 endpoints down to just a handful of employees.

The unique differentiation that we're offering is two-fold. One, we're ingesting data from anywhere and everywhere. Quite different than a SIEM actually. A SIEM is really log and event files, some records. They're starting to expand into user behaviour and other elements, but the problem is they ingest everything. Here's the bigger problem. They charge on everything.

So the problem is that the more technology and the more alerts and alarms, the more data, the more expensive. It's literally becoming an untenable problem for the customers.

Jask has solved the problem in two different ways. We're applying artificial intelligence and machine learning to ingest the right data. So think about this: you pull in log files, events, and network is a great example because I come from Tipping Point and Sourcefire and Fortinet. We're taking in packet data, metadata, a lot of fluff. You're paying for that with Splunk and ArcSight and those models. With Jask you don't. We're an employee-based model, just like almost every other endpoint and other subscription model that is out there.

We're also doing one other thing. We're taking it from the users, Active Directory or any other LDAP service, every device, so the things that we talked about from mobile devices, laptops, desktops, servers, cloud; we're taking it from the network itself; we're also taking it from applications, Okta and other single sign-on type pieces. And then we're tying in, just like every other SIEM, every other third party that can produce data, whether it's raw data or it has integrations.

So the beautiful piece is that we're taking in everything in a very, very smart way at a lower cost to customers. Now that's value one. Value two is that we're adding an intelligence layer on top. So think about what's happening. In most companies they're sucking in 13, 14 million bits of records or data a day. You reduce that down to alerts that you might see and there's probably 3,500 of those. If you're a team of four in a company, there's no way you're going to get through those.

So you have to look at where do I start and what do they do, they say I'm going to start at number 10 prioritisation, and they start working down the line. The challenge is the bad guys aren't sitting there letting off the biggest alerts; they're down at the one, two, three level, typically ignored completely and independently don't mean anything.

What Jask is applying is very, very smart algorithms and use cases of what does a DDOS attack look like, what does ransomware, what does an insider lateral movement, what does an Active Directory attack look like. What we've been able to do with a corpus of data that we already have from previous existing customers is build a model that so that now in an organisation it's taking disparate points of alerts, interlinking those, finding the connections that would not be seen physically by a human, not at least

within months or even years even, in terms of making that connection, and instantaneously on a dashboard drawing a timeline that says this is what we call an insight.

So the unique piece about this is that we do believe that humans are a critical element to the one thing humans will always be good at, subjective determination.

Let me put this in an example. You've got a company; you've got an alert that's going off with insider lateral movement. Well we as a technology might alert that into some insight that needs to be seen, but the reality is in one company they're going that's just the maintenance window of a guy moving around. In another company or even at a different timeframe they may go that's a serious problem.

So at that we're moving security analysts from that level one job that really is bad, because all they're doing is collecting data, aggregating data, parsing it up, trying to get a semblance of what is going on from a broader perspective. And then once they do, what do they do, they turn it over to the more experienced security person. So that level one analyst is unexperienced, their job sucks, they're translating all this data that they really don't know much about, and they're burning out, and we don't have enough people. So Jask is elevating the skillsets and the experience very quickly to another level. So that's about it. Thank you very much.

Hiro Rio Maeda

From where within the security budget is this coming out of? Is it the SIEM?

Greg Fitzgerald

That's a great question. So we have actually been selling into the security operations from almost a human element, because they go well I can't hire another person but I've got open headcount and that may be $150,000, $200,000. Well hell, why don't you just buy us and make the people you've got work better. So that's one piece of the budget.

We have replaced SIEM but that's not our strategy. We're augmenting the existing infrastructure. So once piece I didn't mention on unique differentiation, unlike any other competitor is that we're an open platform. Open meaning we take anything, raw log files, rest APIs. We already have either regular integrations with the partnerships of the other vendors or we're doing some customer integration as needed within an organisation. So what we're finding is once we get that integration, it's already set. Does that answer your question?

Hiro Rio Maeda

So obviously you're trying to replace the SIEM and you're trying to be the next gen of the SIEM.

Greg Fitzgerald

In the end I think that's what's going to happen. As I'm an investor, the answer is absolutely yes. If you ask our CEO Greg Martin, he'll be adamant that yes we're going to take over a $3 billion market. So we've just started.

Hiro Rio Maeda

Yeah but there are Splunk, there are ArcSight, there are Qradar, as you mentioned, and also Splunk is not just sitting there waiting for you to take over their positions. So one of the interesting acquisitions that they did recently was the Phantom. They sensed and detected the intrusions but they make it actionable by way of orchestrating automating the incident responses. How do you fill that portion of the gap?

Greg Fitzgerald

Great question. We are actually - we created a line of demarcation for this particular go to market evolution of us to where we're going to let Phantom and Demisto and - I forgot the other gentleman that's out there; there are about three major ones - and we give them all of our data. So it's actually making them smarter. So we have actually really strong integration and relationships with all three of those vendors.

The idea is that's probably a feature later on, as we've seen for Splunk. Demisto probably a future of something else, could be us, could be somebody else, or we've already got some things sitting in the wings for when it's time to - they move to a competitor and we need to produce our own.

Siddhant Trivedi

Sorry, before you go on Curtis. Hiro does mention a good point in that now you have so many different dashboards. You've got the Phantom dashboard, you've got the Splunk dashboard, you've got your dashboard. Aren't you adding more work?

Greg Fitzgerald

Dude, I love that question. You know why? Because we had a reseller that is a dominant reseller for Splunk who said you know what, it used to be a single pane of glass; it's turned into a single glass of pain. That pain is caused by a Splunk in the sense that they have so much data that they've complicated the visualisation and the execution. The reality is they're only one piece, and that's why you often see security operation centres with like 20 screens.

So what Jask is doing is we're kind of aggregating all of that information into one dashboard that now gives you what we call an insight. An insight is taking those 3,500 alerts and saying there's only six. Now within six insights that may have a combination of 25 or 12 or 15 alerts, but they're packaged up in literally - I'm actually putting some marketing terms around - a one click visibility to compromise. Because that's exactly what it's doing: one click.

We've already tested. If you use ArcSight or Splunk or LogRhythm it may literally take you 25 or 30 clicks to get to that answer, where with Jask it's literally one click, and I can show you offline but as an investor it's very fascinating. So that saves an enormous amount of time, prioritise where they need to focus, and yet all the data is still there. So when they need forensics data and other information, it's still available to do to go much further into the analysis.

Curtis Feeny

With 25 customers can you speak to product market fit and maybe tease out a bit what your best customer set is?

Greg Fitzgerald

Yeah so the best product market fit - and that's one of the things we talked about yesterday actually with the press was - I'll give you a little bit of hindsight on that too. The management team here has done three or four companies, as many of you guys already know. The experience, they're coming out of the US Air Force, US Government, and as I say, as SOC operators. So what they've recognised on this fit is that they know the daily task of a security operations and what are the questions that need to be asked. I'm emphasising questions because Jask is Just Ask. You should be able to use the data as your business process rather than the data forcing you to act a certain way.

So what we found in one of the largest organisations - I can't say their actual name but one of the largest healthcare companies in America and I guess in the world - is that there was a workflow process. The workflows before getting a Demisto or a Phantom, but they have a certain workflow process that they love being able to aggregate the contextual data of everything that we're able to pull together instantaneously and then ship that data to that workflow so that the right people within the organisation are getting the information they need for their particular element of the forensics.

So that's been a big asset.

Janice Roberts

My question was really said so I won't ask to repeat that, but what is your sales cycle?

Greg Fitzgerald

It's right now - that's a really good question and we're still early. What we're finding is there's two. One is a six month to nine month sales cycle with the large organisations, and then we're finding some that are saying I've got to replace my Splunk right now; I cannot again cost. So we're getting thrown right in the middle of these transactions. So we closed one within two weeks just recently and that was a $250,000 deal, so it wasn't like a small deal. We've closed others, mostly within a quarter. Thank you.

Manek Dubash

Thank you. Thank you very much and just a little bit more work before lunch. A 30-second overview of cybersecurity. What do you think? Siddhant?

Siddhant Trivedi

Obviously this is a really interesting sub segment of the enterprise market. I think the biggest problem - and obviously it's exciting to see Jask end it - is there's just too any different solutions and too many different gizmos. I think the problem that we saw in IOT and cloud was more around how do you find focus, because there's so many different things going on. Out here there's too much focus into one part of cyber. So I think that's something that we have to consistently think about in security.

Hiro Rio Maeda

So cyber is - yeah it's a very interesting market in the sense that it's a never-ending war that its adversaries just keep coming with more and more sophisticated and creative way and it just - the odds are on their side that they probably can keep winning, but we

cannot just sit here and wait. So then we have to innovate back to them. So that makes it really, really interesting and that's why it gives a chance and opportunity to many start-ups to come up with their own way to face the new problem that existing incumbent cannot solve. So that's why I keep being fascinated by this sector.

Curtis Feeny

So with security it is so crowded that - and I think we saw some good examples here - you have to show your differentiation; you have to show whatever traction you can because it is imponderably hard for anyone to tell what's the difference. So the competitive slide is always helpful. If you're on the Gartner quadrant, that's helpful. How have you differentiated? How has the market verified and validated that you've differentiated? Very important.

Manek Dubash

Thank you. Janice?

Janice Roberts

Yeah I echo really what Curtis says. It's such a busy sector it's hard to really - but of course a very important one again, as Hiro and Sid have said. But it's really hard to identify as an investor the winners. So I think there are lots of good ideas out there and so I think execution is going to be really key because we have to differentiate, customers have to differentiate, and then they have to bring trusted new companies into the network. So it's difficult but I think really understanding the execution piece is really important. A very busy sector.

Manek Dubash

Well you four have a very busy lunch ahead of you, challenging lunch ahead of you, and we'll find out what your - the result of your deliberations over dinner this evening. So Janice, Curtis, Hiro and Siddhant, thank you very much indeed.

Okay, that ends the first plenary session. There'll obviously be another one tomorrow morning. We're going to go now for lunch but take your stuff with you because the hotel has another function going on and if you actually want some lunch, just go that way. It's right out on the terrace. Thank you very much.

[end]