NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT

Innovation – How to Tap into Investment, Media, More Investment, Customers, and Success!

Introduced by: Manek Dubash, Editorial Director, NetEvents

Panel:

Janice Roberts, Partner, Benhamou Global Ventures

Jim Lussier, Managing Partner, Coast Ridge Group

Hiro Rio Maeda, Managing Director, Draper Nexus

James Hamilton, President, Valetta Capital

Hot Start-Up IoT award finalists:

Tom Ramar, Global Vice President, Sales & Business Development, H3 Dynamics

Bryan Gale, VP Product Marketing, Cylance

Greg Fitzgerald, Chief Operating Officer & Chief Marketing Officer, Javelin Networks

Hot Start-Up Cloud award finalists:

Steve Garrison, VP Marketing, ZeroStack

Peter Lunk, VP Marketing, Menlo Security

Michael Wood, VP Marketing, VeloCloud

MANEK DUBASH

Don't worry about time, because here at NetEvents we have this special compression algorithm where we manage to compress time. You'll find out how that works later. Basically, what we're going to do here is we're going to

invite three Angel Investor Venture Capitalists to come up to the stage in just a second. They're going to be - then we're going to have six altogether, into two categories, IoT and cloud, entrepreneurs to come up and pitch to those venture capitalists, and then basically the venture capitalists will get together and decide who wins in which category. My job here is just to kind of moderate that process. So, I'd like to invite the - sorry, the four Angel Investor Venture Capitalist people to come and join us. Onto the stage please. So we've got Janice Roberts, Jim Lussier, Hiro Rio Maeda and James Hamilton. Good to see you.

So, which one of our entrepreneurs is going to win the coveted awards, which will be announced tonight after their deliberations. We will find out. So the first category we're going to do is the Internet of Things, the IoT, and we have three competitors here to come and pitch for five minutes - no more than five minutes. If you go over your five minutes you will hear this music. No you won't, you'll hear Jaws, is what you'll hear. It certainly won't be silence. Cylance if you'd like to come down and be the first to come and pitch to our panel.

I think you have - what you'll do is you'll grill each of them for three minutes after they've pitched. Yes, that's what you're getting if…

Then after each category, I'd like you each to do a quick summing up. That's the five minutes music, yeah. Okay, great. Okay, first one. Cylance come on down. Five minutes. He's in makeup. Okay, well let's move on to H3 Dynamics first, then. Tom Ramar - go for it.

TOM RAMAR, H3 DYNAMICS

So this - check. Okay. So sharks can - can you see this? Are you going to turn around? I have a lot of graphics here. I don't lose points because your neck hurts at the end of this? You guys want to tee up H3 Dynamics? Okay, just a precursor. I've got a lot of information to say in a very short time, so if English is you - if that's your second language, please approach me after this. I'm happy to go through it again, but I'm going to talk fast and move fast, because this mic will go off. So let me know when we're going to start.

Tom Raymore, H3 Dynamics. We are based in Singapore. Again, recently opened up an office here in the US.

So who and what is H3 Dynamics? So in addition to designing and developing an autonomous drone, DRONEBOX, we are working to connect self-

sustainable field robots to the cloud to develop domain expertise. So fundamentally, DRONEBOX is a mobile sensor for the Internet of Things, so you've got your data gathering, power independence, data communication, mobility, all under the field of - all under the umbrella of telerobotics, very similar to the Mars Rover which is another platform for telerobotics which everyone in this room, I'm sure, is familiar with.

How did we come up with DRONEBOX? So you take the example of cell phone tower inspection. Historical example is technician shows up, puts the safety harness on, climbs up the cell phone tower, does the inspection, comes back down, safety gear off, back in the truck and gone. That evolved into commercial UAV operator shows up in a truck or van, launches a UAV, conducts a similar inspection. But now DRONEBOX is out there 24 hours a day, seven days a week, scheduled flights, unscheduled flights, doing analysis, whatever you need it to do but it's on-site 24/7. As an IoT device DRONEBOX is going to change the face of the commercial UAV industry.

Two main value propositions of DRONEBOX and H3 Dynamics. The first is automation of drone inspection for services. Now, we're going to talk about that a little bit more in just a moment. I see some inquisitive eyes here. The second is 24/7 availability, as I mentioned. So most drone service companies specialise in a single vertical. For example, commercial UAV operator shows up to a farm, goes out to the field, scans the field, provides the data analysis to the farmer and leaves. However, through DRONEBOX, H3 Dynamics wants to develop domain expertise. So what does that look like, domain expertise? We started to categorise this into oil and gas, inspection, agriculture, so on and so forth. I won't read all those. What we want to do is, through our SDK platform allow people to upload their domain expertise. For example, inspection. A commercial UAV operator in Spain does solar panel farm inspection. That person can upload their domain expertise into our app environment and a similar commercial UAV operator in Arizona can access that, download that expertise and perform the same solar farm inspection in Arizona. Every time that happens, if you look up here in the upper right, that original owner of that expertise is actually paid a royalty fee, and the person downloading it and using it and subscribing to that domain expertise in Arizona, in this particular example, only pays a small monthly subscription.

Looking to the future, again we want to remove the hardware piece as a barrier to entry. So the hardware eventually, as we see it, be free, and the revenue model will come from subscriptions and analytics as a service from domain expertise. Our go to market plan, rather - there's more opportunities than time and resources, people and money, so therefore our go to market plan is focus on a few opportunities now, become very strong experts at those, and over time grow that expertise again, rather than be average at a whole bunch.

A glimpse into the future. Not only will we have DRONBOX as an IoT sensor, but like I mentioned in the last - in the panel, ground robots, human robots, marine robots, fixed-wing aerial robots too. This kind of ties to the first speech

that we had, or first informational lecture that we had. Artificial Intelligence. DRONEBOX will scan the field, look for overwatering, under-watering, over-fertilization, look for disease, tell another drone where the specific area of mitigation is. That drone will launch, apply the fertiliser, apply the water, whatever's necessary, but it's all conducted by drones.

Recently our customers have asked us for how drones go from box, to box, to box. Powerline inspection, pipeline inspection, positive train control. It's a bit of a pony express for DRONEBOX, going from one box to the next to recharge and back, so this is a business concept that we have for the future.

A quick glimpse into some of our IoT go to market partners, customers and pending customers too. We are H3 Dynamics, we are working to connect self-sustainable field robots to the cloud to develop domain expertise. Thank you.

JANIC ROBERTS

Can I ask a quick question about…

TOM RAMAR

Yes please.

JANICE ROBERTS

…go to market? So in the last session you said you were working on this and it was more of an exercise. Here you talked about, really - and you talked about analytics. Here you talked about really as a service. Does that mean that ultimately the hardware's going to be free, owned by you, and you're going to be really an analytics company, and how does that influence the sort of cash needs that you might have, do you think?

TOM RAMAR

Yeah, great question. So the DRONEBOX as it stands right now is not cheap, so that's not going to happen within the next two years, but we'd like it to become free to remove it as a barrier to entry. Even the government contacts we're speaking with now, they want to give more of a sass, a lease. Government offices aren't actually extending the CapEx programs that they've had in the past. That may be through a partner, if it's not through us. Maybe GE Capital. We're working through all those details now, but yes.

JIM LUSSIER

I think it's a great idea, and I think there may be some defensibility around the apps, but on the hardware itself, I mean - and I think it's a cool idea, but fundamentally this is a drone, it's a solar cell, some networking technology, some wireless technology. It's an aggregation of some conventional technologies. How are you going to - what's defensible about that? How can you actually make money on that? Or are you going to have to outsource this to others, and if so how are you going to be able to control the software there?

TOM RAMAR

Great question as well. It's, from a hardware - I break it down into two parts. So fundamentally, from a hardware perspective, it's not defensible. Over time it will become more commoditised. We're already starting to see more people come into this field. It's not just a metal box that a drone flies into. There's a lot of engineering, a lot of technology that goes into it. To make it defensible, to answer your question sir, it's through the analytics and the software. Whether we develop that internally or through partnerships like DroneDeploy, they have an amazing software out there that uses the service, that's the future of the market. Integrating many IoT devices to our platform.

HIRO RIO MAEDA

I have a question on [inaudible], and that this inspection and maintenance market is actually a big market. It's about a $4 billion market in the next few years. But the problem is that many of the inspection on cell tower, the wind turbine, it's actually not by - it's not done by the GE's of the world. It's actually done by the smaller companies, fragmented across geographies. Those companies are not large enough to buy a company like this one. So how are you seeing the exit opportunity in this market?

TOM RAMAR

So are those - just to make sure I understand answering the question, those smaller companies are commercial UAV companies that go out and have pilots, correct?

HIRO RIO MAEDA

No those - if you go out after the inspection market for the cell tower, wind turbines, the inspection and maintenance companies are the ones who's going to be using your services, right?

TOM RAMAR

Got it. Okay, so great question again. What we've been told is that a key differentiator for H3 Dynamics is two-fold. One, it's the DRONEBOX itself, which other people are creating, but in additional that it's also - it's methanol-based hydrogen two type of fuel cell, right? So to be clear, methanol-based fuel cell, off the grid power, so we can put these in remote areas where other people cannot. You can use the same drone for more than one use. You can use it for inspection, you can use it for conservation management, you can use it for security. So that's what we've been told. A big differentiator is off the grid power that we provide to an autonomous DRONEBOX to be clear. Does that answer your question?

HIRO RIO MAEDA

Not really, but I think since there's limited time I think…

JAMES HAMILTON

So you put up a quick go-to-market slide there. If I'm a farmer and I want this amazing drone-collected data, how am I going to find out about it? How are you going to get to me?

TOM RAMAR

So great question again. So we're starting to attend agricultural type of events. We don't actually develop the sensors that go onto the drones. Rather, for example, we have a partner called MicaSense. They're out of Seattle. We put their sensor on our drone, and we use our software to deploy. So we're going to specific events, and from that we get more - whether it's an air show, farming, security, inspection, we get more leads than we know what to do with.

[Music]

MANEK DUBASH

Thank you very much.

GREG FITZGERALD

Good to see everybody again. I am now with a new company called Javelin Networks. So if you want to - if we want to - tell me when time to go. Thank you Mark. Okay, Javelin Networks is a cybersecurity company designed to stop - detect and stop attackers in the act of attack on any device, anywhere, at any time.

Now, the company started - if you go to the next slide, two slides please - the company was started by some ex-military incident responders that spent over a decade chasing attackers, anywhere in the world. In particular, one of the places was the Vatican. What they recognised was that using all the tools, the defence technologies and security technologies they have today, that the effort to do that, to collect information, aggregate the information, report on the information and then analyse all that, the attacker had already come and gone. They'd already covered their tracks. So they said there had to be a better way.

So actually using the concept around Artificial Intelligence and Machine Learning, and a mathematical principle called randomisation, they recognised that they could actually make it so that the attacker reveals himself. Hence they created their product, which the company is launching today out of [stealth], that's called [Zero Move]. You can go - so what they recognised here too is when they stop attackers in their tracks, no matter where they are - on an oil and gas pipeline, on a monitoring device, on a laptop or a server, that the attacker, once he compromises a machine, has to do one of two things. One, they've got to look around and see where else they go, and the second is they need to figure out how they do that undetected, and the number one way that's done is through stealing credentials. A valid username and a password of an actual employee. Go to the next slide please.

What you see - the top cyber-attacks of the past three years, as you can see on the right column from the back, it's around topology recon - reconnaissance, trying to understand what's going on with the topology, and credential theft. That's it. So what we're finding is that while an attacker might use a variety of tactics to get onto a machine, they have to do one of the other two things to proceed in that attack to be successful. Go on to the next slide.

So what has - you guys have heard about the kill chain being kind of external. To attack a machine has now become the focus of the internal kill chain, meaning once they're there, they have to do internal reconnaissance. They have to exploit the systems that are there, they have to escalate privileges a la user to get the right access, to get beyond that machine and again move laterally or the concept of getting off that machine to someplace else. Because the further they start to burrow into the network, the harder it is to find the attacker.

So if you go to the next slide, what happens - next slide. So what happens with Javelin, is that the domain that has all your active directory users and your topology, is known. So instead of disrupting that network and asking the IT departments to put more systems or fake items into it, they allow an Artificial Intelligent agent to analyse it and to create its own mask.

So what happens is, before Javelin you have a definitive, known, computer server person, which may say ten. After Javelin, it looks like 100. So now the attacker looks at a volume that's exponential, and doesn't know which one's legitimate and which one's not. The minute they move to take an action to

either ping a topology element, or to understand an individual's credentials, they set off a silent alert. Kind of like walking into your house, right? An attacker comes in, sets off a silent alert. Now you can either have the police shut them down, get them off that system right then and there, or an IT department might say let's see what's happening? Is he going after the safe, with the money and the jewels, or is he going after the file cabinet for the information?

Because I want to know two things. What's the purpose, and what are tools and the tricks of the trade that they are using to get there. Because if they can understand that, one, they can shut him down and contain him to only that device, and two, they'll have information and knowledge to the go look anywhere else in the organisation for the information they need.

Now, what's beautiful and unique and different about Javelin is that this is all done seamlessly. It's done with one server and a small memory item that sits on the server, or on the devices that is automatically deployed. So it's not an agent, it's not chewing up processes, it's not impacting end-users or the network or administrators, and is giving factual information that is forensically sound, meaning that when an attacker actually attacks or touches something it's an actual action that's caught. It's not what we know today as collection of information for indicators of compromise. Thank you.

JANICE ROBERTS

I have a question. I'll start again, I'll jump in because we don't have much time. This is a longer question, I think, but what intrigues me - and it's sort of a simple question in a way - is I think companies now, we all know that attacks will happen, but how do you market this? What's the story? You're saying trust us. Lot of trust here. Let them come in, find out what they're doing, let them wander around and then you'll - basically then secure them. I mean, just explain that a little bit, because I think the marketing sell is sort of interesting here, right?

GREG FITZGERALD

That's why I've been hired.

[Laughter]

Because honestly the technology is there. The actual answer to the question is interesting, because we're not trying to convince people that they have been compromised. The customers that they have already today are the ones that are like, no matter what I do I know I'm going to get compromised. So we're not having to sell on the front end that convincingly. What's really nice is what they're looking at is how are you better than all the other technologies I've been buying and using today. That's where hopefully the simplicity is, instead

of chasing the attacker, let the attacker reveal himself. Then you can get into the how, but that's more of a try - try the effort. Which is interesting, so let me answer your question on that one. A POC takes less than an hour. So very much like Cylance - I love Cylance as you guys know - you could test that and within 15 minutes you'll know whether you have malware on your machine. Well, in Javelin's case, within an hour you'll know whether you have an attacker in your system somewhere.

JANICE ROBERTS

Okay

JIM LUSSIER

I agree, this really is an intriguing idea. That said, it's not a new idea, this whole idea of deception. Just a quick review of the literature, I've identified Allure Security, Ativo, Symmetrica, ForeScout, TrapX who was here, Guardicore, Elusive, Precipient, Shape Security, many other companies that are taking advantage of deception technology. One is, how are you better than the other things they're already using, but how are you different and better than all these other companies that are already out here, and how many customers do you have? You've been around since 2013.

GREG FITZGERALD

We've been around since 2013, so we've got a couple of dozen customers that are all large, which - number 83 on the Fortune 100 list is what I'm allowed to say, as an example, number 10 on the Fortune 100 list. Answering your question, what it is is - what's really nice about our technology is that everybody's already tried the others, so they have a comparison to how difficult, how burdensome, how timely, how intrusive those other technologies are. So I applaud the other guys for trying, but very much like honeypots - like, we hate the word honeypot because the general market hates that general concept. Actually, I'm not a fan of deception. So as you've noticed, I'd never used the word deception because that doesn't seem to be intriguing as a marketing term either. The concept is, again, don't set out traps and hope that the deer comes to it and you can shoot it. It's be in the space where the attacker is going, and let them kind of expose what they're doing to then know for sure that it is a bad thing. It doesn't necessarily have to be an attacker, frankly. It could be a rogue employee, right? An internal attack who's - let's say I decide I want to go and ping the financial servers, just for giggles. Well, that will indicate itself as an invalid activity from my particular domain, because I shouldn't be touching those servers.

HIRO RIO MAEDA

…quick question. So many of the corporate assets, not just sitting on-prem but sitting on public cloud, private cloud, do you have any approach towards those kind of - yeah, outside of on-prem.

GREG FITZGERALD

No.

HIRO RIO MAEDA

So…

GREG FITZGERALD

It's not focused on cloud-based assets. It's only something that - this little mask can make it look like a consistent view of the topology. As it changes, you know, add users, delete users, add devices, it automatically updates itself, which is another differentiator from the other technologies that require some configuration to do that. This automatically updates. But it doesn't necessarily touch the web-based services.

HIRO RIO MAEDA

Got it.

JAMES HAMILTON

So Greg, if the three elements of cyber policy are prevention, detection and remediation, which do you fall in and what are you replacing that I might have today?

GREG FITZGERALD

Good question. We would consider ourselves falling into the detection market, primarily, with remediation being best-practice guidance, I guess you should say. The prevention elements do exist there, but they're after - they're on the compromised machine, so we can actually shut down the attacker on that one machine and not let them go any further. But that's still - that one machine's been compromised, so not in the true sense of that. Now, what we're replacing is frankly a lot of technologies that exist today that are signature based, or heuristics, or behaviour. So today, to achieve the same objective of finding that attacker, you have to aggregate all this information by all these devices. So in our background, like IDS - IPS - [inaudible]

JAMES HAMILTON

Thanks very much.

BRYAN GALE

Thank you. Okay, so Cylance. What do we do, right? At Cylance we have a core product called PROTECT, and it is an endpoint security product that utilises the power of machines, not humans, not people, to process through just the extremely vast quantities of malware that we see newly released on a daily basis. We do that by harnessing the power of artificial intelligence and machine learning algorithms on the endpoint to very, very quickly predict and prevent cyber-attacks in real time.

Now, who are we? So Cylance was really formed by a collection of individuals. The majority of our leadership all very, very steeped in a rich history in endpoint security, coming from big AV, some of the big players in the industry that have been doing this for well over a decade. All of us share one single trait in common, and that is we were very, very tired of our inability to protect our customers with the solutions that we were building. It became very, very difficult to try and change the mindset of the industry, and approach of the industry from within the inside. So we left, and our two co-founders up there, Stuart McClure and Ryan Permer on the right, started up Cylance with the idea that there was a different way and a better way to potentially solve this problem of endpoint security, but the industry was literally utterly failing at doing so.

So a little bit of a business snapshot. We've been in existence now for a number of years. We've been selling product for just under two years at this point. You can see that we focus, obviously, on endpoint security. We are very agnostic in terms of industries, in terms of verticals, whether it's finance, oil and gas, energy et cetera. We do very well in government, DOD, other sensitive types of networks where they're potentially air-gapped networks due to the nature of the product and how it works, and how it's fundamentally different than some of the older solutions in the industry.

We've seen unprecedented market growth in that two years of selling a product. Year-over-year growth for us is over 1,000 per cent from a revenue standpoint, a booking standpoint. We've crossed the threshold now of over 1,100 clients globally, and over five million total endpoints under protection. You see on the slides there there's two million endpoints covered. We also have a number of extensive OEM relationships as well. Appliance OEMs, where a number of endpoints are protected via an appliance in the cloud utilising our AI and ML based technology on the network layer as well.

Now, why is our solution important? What's happening in the market at large? What is that unmet need in terms of what you see out there? So these are some

stats, official stats from the latest Verizon Data Breach Investigation Report. What it really highlights is the continued growth of malware being used in terms of cyber-attacks. So you'll often hear FUD about malware list or file list based attacks, of exploit-based attack happening, but the unfortunate truth is, regardless of the entry point onto a system, 90 per cent of those events still require malware to do the dirty work. To do the data extrusion, to do the lateral traversing inside of networks, and to get the information that those attackers are after out of that environment, okay?

A couple more facts. Just in terms of the different types of attacks or entry points as well. People - our employees in all of our respective companies, they still fall victim to these attacks. Spam and phishing email campaigns, whether it's spear-phishing or very targeted campaign, all too often attackers are seeing a high rate of success with too many users clicking on those emails with those malicious links almost instantaneously with them hitting - with when they hit the organisations' networks. So you see there, 30 per cent of the emails are opened. 30 per cent over all the time. 12 per cent were actually clicked on. In too many cases, that's all it takes for an organisation to become breached, is one single user clicking on an impacted - on an infected link that then allows the attackers to get their foothold inside of that organisation. You see the average click time, or the median click time is less than four minutes. So no matter what type of threat intelligence of other things you're using to react to these changing tactics, you don't have enough time to react hat quickly with how fast your users are opening the door for those attackers to come on in.

So what the continued malware infection cycle does to the company. They're continually chasing ghosts inside of that organisation, trying to continually chase impacted machines and figure out what sort of mitigation needs to take place. There's loss of business continuity where they have to take machines offline, re-image those systems before they get them back into production. Security company - most companies, their security ops teams are relatively small, relatively thin, and those teams are just spread way too thing doing these mundane tasks because they can't literally keep up with the flood of malware that's hitting their environments. So a little bit about where our product, Protect, operates. This is what we call our risk-mitigation cost-control [inaudible].

[Music]

BRYAN GALE

I guess I'm going to be cut off there for the sake of time, so I will open it up for questions. We need a clock, a timer.

JANICE ROBERTS

We seem to be going in order here, so congratulations on all the things that are going well for you.

BRYAN GALE

Thank you.

JANICE ROBERTS

I don't think you'll be coming round collecting money while you're here, but seriously, congratulations.

BRYAN GALE

Thank you.

JANICE ROBERTS

This is the IoT section, so could you explain a little more how your solution really extends itself into the IoT world?

BRYAN GALE

Yeah, so a number of factors. So first and foremost, we're fundamentally different than most endpoint security products. We don't have a DAT file, or the concept of a signature that needs to go and reside on disk, or on a device. We work in a very predictive fashion, and we are exceedingly lightweight. So we have a number of our solutions customised to that IoT space, where we work in industrial control systems, other small form-factor devices. I think we've run proof of concepts on Linux and Raspberry Pi devices. Very minimal memory footprint, agnostic to the type of file system being used, and again no need for a DAT file or other large storage media to be used as well. Then the utter lack of updates. We have multiple research briefs where we'll put out, where we'll take a six month old version of our product, against today's attacks, and show that it's 100 per cent effective against some of those attacks. So these IoT or other devices that aren't always connected, you can't always manage them, they can be protected for a very, very long period of time by having thing type of solution on them

JANICE ROBERTS

Related to that, because this is the IoT section, your accomplishments in the non-IoT space are increasingly well-known, and again congratulations for that, but I just saw on August 3rd you announced a service offering around IoT. A lot of times companies announce that when their product isn't quite there. What have you had to do to change your product to make it fit better into this edge-computing, low-latency kind of small-footprint environment, and how much traction are you really getting in the IoT space specifically?

BRYAN GALE

I'd say the traction is just beginning, because the problem I think we have is how do you define IoT? It's such a vast realm, right? So we've had to choose areas of focus. Industrial controls is one area. We've got an Android device coming in soon which is going to go across a whole host of different types of devices. So there's nuances that we have to change in the product in terms of the operating system itself, the hooks that we use in the operating system regardless of the device or the device size, the management infrastructure and some of the protection capabilities of the product that differ from operating system to operating system as well. So the core essence of the product, in terms of the mathematical models being distilled down to those devices, was really a lot of the bulk of the work than some of the nuances for the various platforms and things.

HIRO RIO MAEDA

So I personally use Cylance on my laptop…

BRYAN GALE

Congratulations.

HIRO RIO MAEDA

…so I see the power of it every day. But anybody in this room, especially who has a teenager in your family, definitely use it.

BRYAN GALE

Come talk to me.

HIRO RIO MAEDA

You will find something that you don't want to see, so I strongly urge you to do that. But somewhat related to that, and sorry to digress a little bit from IoT, but what's your plan for going to the consumer side?

BRYAN GALE

So I don't know if I can touch on that too much publicly, but I would say that consumer is an interesting space for us because it's a natural adjacency to the enterprise market that we play very, very well in. You also see that we have a

very strong public relationship with a company named Dell that happens to have a very strong, powerful consumer segment of the business, and I think that's probably a logical area for us to expand into.

JAMES HAMILTON

So Cylance has been very disruptive in the land of the giants. Symantec and McAfee and Kaspersky. How defendable is your machine learning approach?

BRYAN GALE

From what I've seen from both our history, right - so our company's relatively young, only about four years old at this point and I would say that the first really two to three years, we didn't really focus on sales and marketing. It was building that technical, foundational capability of the product itself, which is kind of unconventional in the realm of normal start-ups, where they go out immediately and sell and market something that's just an MPV based product. It doesn't really work. So we took an opposite approach, and so we have at least a two to three, probably four year head start on anybody else that's trying to do this. We watch the competitive landscape. We watch for their job postings, to see - are they truly hiring data science capabilities? Are they truly looking into that ML realm to try and be able to apply that? Then also, too, a lot of us came from industry. We know what they're working with. We know the things that they've tried and failed upon, and it's a tough problem to solve. As Stuart alluded to earlier this morning, you know with two or three features you can get 80 per cent of the way there, but closing the gap on that last 20 per cent is exceedingly difficult and time consuming. We have a number of patents as well that are already granted [inaudible].

[Music]

MANEK DUBASH

Thank you very much. That concludes the IoT section. I don't know if the four of you want to give a very, very swift summing up of what you thought of the three contestants en masse? Or not, we could move on to cloud if you like. Let's move on to cloud, we'll do that later. When it comes to asking the questions, shall we start at the other end first? Start with James and move this way?

JAMES HAMILTON

Well ladies first, I don't mind.

JANICE ROBERTS

That's okay, [unclear] equal opportunity and all that. You start this time.

MANEK DUBASH

We're totally non gender-specific here. So yeah, first let's go to ZeroStack. Steve Garrison.

STEVE GARRISON

Good to see you. Thank you. I've got five minutes, actually. Alright, thanks everybody. I just want to first thank the audience for getting us on the list. Cheers to you, we really appreciate it. So I'm with ZeroStack. We use magical software and some really smart architectures to solve the problem of how to build a private cloud, and - let's hope this works. Here we go. So we are pioneering something called Cloud-Managed Datacentres. You heard Aerohive mention that, I'm going to tie those dots together in a second.

We have a thesis at ZeroStack, that building a private cloud is hard. Starting around 2008, OpenStack started, people started to realise that there might be a different way. Amazon started scooping up customers like crazy though, and proving that if you give people GUIs and make things easy, they will consume it. The private cloud market hadn't really gotten there yet. We still have integration challenges, professional services needs, things of that sort. So we believe in this curve.

We believe the last 10 years of IT have been an outright lie. We can give you agility, but boy we make you pay for it. You have to double your team to get twice the agility, you have to double your budget. That is not a win-win scenario. So we use software and an intelligent architecture to bend the curve. For the football fans, we do want to bend it like Beckham. There it goes. That cost me all of 30 minutes to figure out how to do last night, so I did it, and it worked. Alright. Fantastic. So let's talk about architecture. How do we do this magical bending of the curve to give you agility with much less complexity and therefore much lower cost? Well, my friends, you're going to find out.

First, we believe in on-prem technology. I don't care if you call it hybrid, private, [unclear], containers, cloud, OpenStack, whatever, the point is we know customers want some of the assets on-prem. Why? Because sometimes it needs to be there. Can call it security, can call it governance, it don't matter. People want some things on-prem. So we give you software. It takes your existing, magical, hyper-converged servers or a select group of standard servers, and we make it cloud by simply unloading that software onto that bare metal. No ProServe, no integration, it just works. It's a PXE boot, it just works. We check the hardware, we make sure that the hardware matches, and we tell you when it doesn't. But when it does, it just works after 30 minutes. We have

immediately connected you into your VMware environment, where you can discover and pull things over, or build them on us and then move them to VMware. That's easy.

Now, what we do in the cloud is we have our own cloud. This is the part that's a little strange. We have a cloud-managed technology here. That means that we have a cloud that acts, and behaves and takes out some of that OpEx so that we don't need to do it. We do it for you. We also connect directly into your public cloud environment, so not only are we a private cloud with on prem infrastructure, we are a hybrid cloud to build a bridge between VMware and Amazon, Azure or Google, your pick.

We have a little telemetry that comes out of your - think a call-home device, or a call-home stream of data. It's secure, it's port 443, if you don't believe in that then stop using Salesforce. It's that simple. It's a very well-known technique, very much gated and vetted by many companies around the world. We use that telemetry to again, guide and tell you what you need to know so that you don't have to hire a staff of people to manage that cloud environment.

Alright, so, I want to make just a pitch that this is a new idea. Cloud-Managed Infrastructure is not unique to ZeroStack. In fact, the Aerohive gentleman mentioned that they're cloud-managed. There's a wealth of companies there that not only went public, they got bought. There's my fellow compadre here from Velo, Mike. I'm going to make a bet here, and a throw-down, that the judges should let us both win because we're both cloud-managed and we're both in different verticals, so let's do that. Alright. Then we've got the security players, none represented here but there are people in security who understand that having a cloud brain that helps manage that infrastructure off-site, which is your infrastructure that's actually on prem, saves you money, and off course we're pioneering the data centre.

Six billion plus guys for VCs. Is there money here? Is there a money pot? You bet. Six billion for wi-fi. We've got over a billion coming out of security already so trust in ZeroStack to give you a huge return not only to our customers, to the VCs here. Alright so just competitive. We think top down. What does that mean? That people want to consume. They don't want to play. They don't want to build. They don't want to get frustrated. We do that by giving them the GUIs and look and feel of Amazon. Our friends at VMware and Nutanix have yet to get that clear and they're way behind.

Then as far as cost, the enterprise wants to know is it cheaper? We offer two to three X better price performance.

Alright, panellists, I made it. I'm ready.

JAMES HAMILTON

Steve, a couple of things. Did you use the term magical? I wrote down magical.

STEVE GARRISON

I did. I'm up in the winery, the hills. The air is thin and there's - you know. It just popped into my head. I'm sorry.

JAMES HAMILTON

Okay, that's good. Just now I know how it works.

STEVE GARRISON

It's magical software with an intelligent architecture.

JAMES HAMILTON

So you need a lot of other vendors to sort of make all this work, right, above you and below you, in applications, in the infrastructure. How do you get that ecosystem together so that you're a big part of this, right? Because...

STEVE GARRISON

That's a great question. Above us we have an app store with over 25 templates in there. Pick Cassandra Jenkins at MySQL, Gitlab, it don't matter. We've basically baked those templates in so you go into the app store just like your iPhone, you click on the template, it automatically downloads itself onto the on-prem infrastructure and you can cloud right there with a few clicks.

Below us it's all about hyper-converged metal or standard servers. We've already announced partnerships with Dell and HP. We'll be announcing Cisco, Lenovo in the future. There we go. I just blew an announcement. What the heck. We're also doing storage integration. You'll be seeing us making announcements for storage vendors because we believe they need a cloud story and they have valuable hardware that the customers want to ignite with cloud.

I definitely see us in the middle of an ecosystem of storage, compute and application partners.

JAMES HAMILTON

Yep, lots of biz network. Thanks.

HIRO RIO MAEDA

As I see all the enterprise is going to be mixed and the converge of on prem, private cloud, public cloud and there's going to be - the total management system is something that is really needed. I think I like that idea but when enterprise look at this kind of solution they look at the costs, reliability and the security. When it comes to security what do you say as a one punchline that you do better than others?

STEVE GARRISON

We scale great. That's my short answer, right?

HIRO RIO MAEDA

No, for the security aspect.

STEVE GARRISON

The security, guys.

HIRO RIO MAEDA

Yeah.

STEVE GARRISON

Well we do have a discussion usually about the call-home technology and we just remind people that any SaaS product that they use is port 443 to communicate so they kind of go okay.

Some customers do want to have the cloud management software on prem and you can imagine carriers who would sell our service as an MTU or private cloud multi-tenant unit service as a managed service itself. They're talking to us about having that software in their cloud so they have total control like a bank might want that total control. We're absolutely willing to do that. In fact some of the other cloud manage companies have to move their cloud brain around as well as you get into a more secure or a larger organisation but that technology is possible.

We're focused on the mid-tier right now as low-hanging fruit and those are the people who can't afford the staff or the budget to do this. We'll be moving upmarket as we grow as well.

JIM LUSSIER

Okay, it feels a little bit like back to the future in some ways. Three, four, five years ago there was any number of OpenStack appliance companies like Nebula which shut down, Piston which was sold and the numbers were low, cloud scaling, so on and so forth.

STEVE GARRISON

Right.

JIM LUSSIER

Some of the knocks on those companies were that hey it's a great way to get started but can you scale this? Also lock-in, now that you have an appliance you're locked in, you can't get off which is one of the real advantages of open stack. How do you respond to that? How do you - it's a good way to get started but how do you scale, what's your largest customer?

STEVE GARRISON

Yeah so we've scaled in the lab to all of our 20 racks which is 20 times 20, 20 units per rack. They're 2RU so that's four - what is that? That's 20 times 20. Let's do the math. We have an English education problem here in the States. Four hundred, thank you Manek. We know that we can scale that far and that's way beyond what most customers are talking to us about. People want to start with one or two devices.

First we're not an over-stacked story in our humble opinion. We bring you the agility, the flexibility but what we're really trying to do is make this accessible and turn a key. Whether you put the software on existing metal in your shop or you buy a preloaded appliance from us that to me is packaging and pricing. It's still the same product. That's one complaint; I don't want to do any integration so that's back to your point.

The second thing is even OpenStack as a platform - you've heard the stories about eBay and Walmart and Comcast. You still have to have a big operations team. We've tried to hide the complexity so that you really are truly GUI-based model just like Amazon. We do have open APIs though so we're not a lock in at least on the integration side because we use open stack or REST for APIs. That is actually becoming an industry-standard connectivity interface today. That's what we preach. Any metal and anything you want to connect through an OpenStack API that's our not lock-in story.

Otherwise we're really competing with people who want to - are challenging the repatriation model or should - when should I pull stuff out of Amazon or Azure. People have told us and we see it when their bill was a surprise, public cloud's easy to get started but you don't have an architectural element there

that you can control and you certainly have out of control cost once you start using a lot of IUPs and storage. This is one of the reasons you see data - 25 per cent of public cloud users are coming back and they're looking for something like what we have.

You're right. I think there was a false start. I think people didn't make it easy enough and didn't package it enough and that's what we've done.

JIM LUSSIER

You got it right.

JANICE ROBERTS

Could you - good questions before me. That's the problem with going last but following on from Jim he did ask you about customers, large customers, whatever but can you just expand a little bit where you're getting customer traction today?

STEVE GARRISON

Sure. We're well over 20 customers and we actually only did GA in March so we think that's pretty fast for an enterprise to take up new technology. That said they are mostly mid-tier market customers right now because I think they have the most pain and the last choice in terms of finding a solution. We definitely are talking to Fortune 500s though. They have a longer sales cycle. We're a little greedy right now. We actually want to raise money next year so we want to get enough of a pipeline to convince folks like you that we're worthy of another big bucket load of cash.

JANICE ROBERTS

Mid-tier and you're selling directly?

STEVE GARRISON

We're selling through three channels actually. We have an excellent channel model right now, companies like [inaudible].

[Music]

MANEK DUBASH

Thanks, Steve.

STEVE GARRISON

Thank you, Manek.

MANEK DUBASH

Good job.

STEVE GARRISON

Always good to see you.

MANEK DUBASH

Is it?

STEVE GARRISON

Is this London or something?

MANEK DUBASH

Everywhere is London where I am.

Okay, Menlo Security come on down. Where are you? Peter.

PETER LUNK

I guess that's my signal to go. Five minutes are there. Let me jump right into it. That's why Greg was - alright.

Let me talk about the problem before we get into the solutions and what Menlo Security specifically does. If you look at the risk out there from cyber-security we see over 85 per cent of that risk coming in through web and email malware. If you look at the reasons why that risk is there it's really not surprising. We see of the Alexa top one million websites more than one in five are still running outdated versions of software.

On the email side we had someone else do a similar stat here. Despite a lot of money being spent on training over 11 per cent are still clicking on links and attachments even though they've been trained not to do that. It's really no surprise that the real magic of Menlo Security and what we do here is we let you isolate and eliminate the threats coming from email and web.

If you look at traditional approaches to the problem one of the reasons that we see the breaches showing up in the headlines again and again, we see ransomware showing up as a big problem. It's the approach of trying to

determine whether content is good or if the content is bad is really hard and we don't actually believe anyone can do that a hundred per cent of the time.

Whether you look at all the different major product categories that have come out in the security space over the last 20 years; antivirus, we talked a lot about that already today, intrusion detection systems, firewalls, network sandboxes, even artificial intelligence they're not going to get it right every time. They won't be able to keep up with the millions of different variants and eventually some content, some of it potentially malicious is going to be able to reach the user endpoint.

What we're doing at Menlo is to offer a completely new approach to this. We want to isolate content so rather than making a good versus bad decision on content coming to a user we're going to assume all of it's bad and we're going to isolate it rather than trying to say I'm going to either deny or block it. We completely contain that content in the cloud and then we eliminate the path for the malware to go from the cloud back down to the user device.

Let me go a little bit into how that might work. The Menlo Security isolation platform now is able to isolate content from the web, it can isolate content from documents, it can isolate content from email. I'll talk about a specific example here with the web.

Let's say we have a user who wants to connect to CNN to read the latest horror stories on the election. They're going to connect but rather than connect directly to CNN where there's the risk of malicious content coming to the end user device, we're going to proxy through the Menlo Security isolation platform.

What we do in the isolation platform is we spin up a disposable virtual container which has an operating system and a browser which then goes out to cnn.com on the user's behalf, browses the web, fetches the content, executes the potentially dangerous content out in the cloud. But then rather than having that content go down to the end user we use our patented adaptive client list rendering technology to present just a hundred per cent safe visual representation of the data back down to the user's browser.

The beauty of this is that the user gets what is really indistinguishable from the user experience standpoint from being directly connected to the site but now they're a hundred per cent safe from that content. This'll work with any browser, any operating system. It doesn't really matter what you're running on the end device.

The best thing of all here is that we don't have to install end point software on the devices at all. From an IT deployment standpoint that's a really big factor.

If that same user now wants to go check sports scores, say they go to ESPN, what we do is we take that disposable virtual container, we trash it, we fire up a brand new one, brand new operating system, brand new browser so if we did have any malicious content on the previous visit to CNN it's already gone.

They get a new browser, they check the sports scores, they go to a new tab. We dispose of that virtual container too. It's like the IT department handing you a brand new laptop every time you switch tabs on your browser.

If you look at how we're helping customers today our biggest customer's a Fortune 50 bank, one of the kind of top banks in the country. They're currently isolating every link - so every link that comes in on their email system and goes out through our isolation platform and that's over 200,000 users.

We've also got a media giant that's isolating Flash. They got sick of Flash vulnerabilities showing up on their endpoints and trying to keep flash up to date so they took it off entirely. They can run Flash in the cloud on our platform. They don't have to keep it on the endpoint.

Then finally we have a global legal firm that got hit by ransomware twice. After the second time they said let's do something different, we're ready for a new approach. They're not running Menlo Security in the cloud. All their web traffic goes through Menlo.

We've been in production since January 2015. We've got fabulous technology and an experienced team that can help take this to market around the world. Thanks.

JAMES HAMILTON

A couple of quick questions. You're not on the endpoint. Where do you sit? Where do you sit? Where are you deployed?

PETER LUNK

Deployed in the cloud but at the network level.

JAMES HAMILTON

Okay and would you be upset if I said this was a next-gen sandboxing service? Would that be - I know it's limiting but is that a fair assessment of what you're trying to do, sending everything to a sandbox to be deployed?

PETER LUNK

The delta - the only argument I'd have with that, we are - there are some similarities. We're running things in a virtual environment. Even after we see the content - there's no good versus bad decision. We're going to just take visual representation of that information back to the end user device. They never get the actual file that could be infected [unclear].

JAMES HAMILTON

With that you don't necessarily impact the performance per se? It's not noticeable from the user experience?

PETER LUNK

Correct. It's really indistinguishable from the user standpoint.

JAMES HAMILTON

OK.

HIRO RIO MAEDA

Very interesting approach. Basically it is running the corporate's application on your cloud side and basically streaming it to the end point so that they see what they - what's the application is running, right?

PETER LUNK

Correct.

HIRO RIO MAEDA

Is that a fair understanding?

PETER LUNK

Correct.

HIRO RIO MAEDA

In that case what's the coverage of application that you can run, meaning that many of the enterprises have proprietary application, not the Microsoft Word or any of those popular applications but they have their own applications? Can you run those?

Second question is when the user or the enterprise employees are offline without the connection can you still do some of those application opening and running?

PETER LUNK

Okay so let me take those one at a time. The first one was what if there are company proprietary applications. If you look at web for example we're taking the visual representation and passing it back. If it's something that you can see in a browser you'll be able to see it in the - if it's an enterprise application where you've got text input and interaction with that then typically what we recommend people do is we white-list the enterprise applications because those are typically something that you could say are safe in that environment.

HIRO RIO MAEDA

Got it.

PETER LUNK

Then for...

HIRO RIO MAEDA

Offline.

PETER LUNK

Second question was offline and online. If you're offline you're not connecting to the web so the web piece is separate.

HIRO RIO MAEDA

You still want to run emails. You still want to run...

PETER LUNK

If you're running email what happens is on the email side the email comes in, we actually rewrite the links so that the links then reroute through our platform. If you were to click on a link then that link - if you're offline you're not going to be able to click on the link to get out. The links are rewritten and then passed in to the user so that it automatically goes through our platform. There's no way for the user to then bypass that on the security side.

HIRO RIO MAEDA

What about those files that you want to work on like a spreadsheet, Word.

PETER LUNK

On the file side we have a couple of different options for people in the document isolation. We have a safe view. Again it's up to the sys admin to decide how they want to do this but we can take a PDF file or a Word file, Excel file, we can transcode that and give you a safe version. We'll do actually like a PDF rewrite on that so that you have a safe viewable version of the file.

Then depending on who needs access to what you could actually set it. It's configurable by the sys admin whether they want to actually let people pull the original document down.

HIRO RIO MAEDA

Got it. Okay.

PETER LUNK

Typically we tell people not to pull originals down from the internet for obvious reasons.

JIM LUSSIER

I do want to give credit to the press and analysts that pick these companies. I think they're all really unique and original including Menlo Security. At the same time the proof is in the pudding sometimes and you said the user experience is relatively unimpacted. Any time you put a piece of software in a proxy between the user and what they want to get to there's usually some kind of impact. What is the impact on the user experience and how does it compare - the other company that's talked about often sometimes in the same breath with Menlo Security is Fireglass. How are you different from them?

PETER LUNK

I'll start with the Fireglass thing. We're shipping product. I'm not aware of them having any customers yet so I'll start with that poke.

JIM LUSSIER

Okay.

PETER LUNK

If you look at...

JIM LUSSIER

User experience.

PETER LUNK

...user experience, one of the things is we are - it's a cloud service so it's based on Amazon web services. We're actually - those AWS nodes are actually located closer to some of these content delivery networks than you might be if you're connecting in through your typical corporate network. We've actually seen some instances - we don't advertise it as a feature but where we actually see acceleration of web performance based on just the fact that we collocated in the cloud with people.

From a speed perspective there's not an impact to user experience that anyone could tell. We have a quote from one of our customers in a small bank in Arkansas. It said by the second day people had forgotten we've done anything and they don't know it's there.

JANICE ROBERTS

I was going to ask the user experience questions as well. There are use cases where there is more of a challenge because if you do have any latency at all in certain [applications] people are going to find a work around because in this instance I think engineers - people can. Is it proven? Are there problem areas where you're still struggling to work that latency issue or not?

PETER LUNK

No, the latency isn't a problem with MSIP. One of the things that really sells people when they see it is - I couldn't squeeze a demo into the five minute pitch but usually it's the demo that gets people believing. People see this and go no it's too good to be true. I've seen previous attempts at this using VDI and it was clunky and ugly but now when they see the demo usually that's what gets people convinced that this is really [inaudible].

[Music]

JANICE ROBERTS

Okay, thank you.

MANEK DUBASH

Okay and now finally one final contestant - candidate. VeloCloud, come on down. Best of luck. Five minutes.

MICHAEL WOOD

Thank you. Okay, start the timer now.

My name is Michael and I'm VP of Marketing with VeloCloud Networks. The wide area network today is broken. It hasn't changed in 30 years and what businesses use today for wide area networking is really designed for the way that they operated, the apps that they ran 10 years ago, not today.

At VeloCloud we've noticed that many applications - you've probably seen the same thing - are shifting to the cloud. We're seeing storage move to the cloud, we're seeing infrastructure move to the cloud, we're seeing security move to the cloud, applications and services move to the cloud. The challenge is that today's wide area network is not adapting to that. Oftentimes IT needs to backhaul those applications back to the data centre taking up bandwidth, valuable bandwidth across the network or they bring in a direct internet connection into each branch office location. The quality there is miserable; a lot of packet loss, delay and jitter that exists.

Ultimately IT is losing control. They have a set of applications that they've sanctioned and then there's a set of applications that all of us use out there that are not sanctioned. Dropbox may be sanctioned but Google Drive is not so why does Google Drive have the same priority as Dropbox when it comes down into their branch office location across the internet or backhauled location?

The internet is a fantastic medium. It's pervasive and there's a lot of bandwidth there but again the quality is poor. It really ends up impacting the performance for my applications if I'm running any traffic across those internet connections. Video's a very good example. Unified Communications as a service is another example. Salesforce is an example. Office 365.

VeloCloud believes the cloud is the network. What I mean by that is finally we're going to move wide area networking into the cloud. We're going to bring it to the front doorstep where many of the applications you use today exist and that is in the cloud. Maybe not all of them but many of them.

The way that we do this is we deliver an overlay network that encompasses a business's existing network if they choose. It exists at every single branch office location and data centre but on behalf of those businesses we extend the network into the cloud using VeloCloud gateways that are distributed around the globe in the internet, multi-tenant, roles based, completely highly available giving assured application performance, bringing management to cloud applications and business policy automation.

The terminology that's been used for this type of activity is SD-WAN or software-defined wide area networking. VeloCloud has taken a very different approach to this. We had the unfair advantage of starting three years ago on this and have produced a cloud delivered SD-WAN architecture that enables us to be the only company that's able to do this in this manner.

IDC believes that this market - Steve, if you're still in the building - is $6 billion so maybe you can update that slide to include that number there.

What VeloCloud does is we have the ability to literally create this overlay network and do it as a zero touch automated deployment model. In other words you don't need to have IT staff in the branch office location to light this

network up. You don't need to have IT staff in the branch office to troubleshoot issues that may exist in the network. You can do it all centrally.

Secondarily, we have the ability to literally pull in multiple links. They might be private links, MPLS or they might be public links like broadband internet. We can steer application traffic between those links at a very low level.

Thirdly, we have the ability to deliver quality of service. Okay, Mike, that's not new, quality of service. We can do it over the internet. Okay, now you've my attention, that's new. Quality of service over the internet, the ability to perform packet loss remediation, jitter remediation and literally repair links, not the entire link but on a surgical application by application basis. In other words the ability to repair maybe Skype for business for Skype for consumer doesn't get any repair work or prioritisation or quality of experience.

Fourthly, we do all this on premise for all the on premise applications you have but then we also extend it into the cloud and take it to the front doorstep of just about every major cloud service that's out there.

The last piece is the ability to have an enterprise maintain investment protection. A lot of enterprises have spent millions, tens or hundreds of millions of dollars on their existing wide area network. We'd never ask you to remove that. You keep it - WAN as you are and we'll create this overlay that incorporates that but also extends and expands your network using the internet and you begin to take back control of your wide area network.

Three hundred customers already are based on VeloCloud and VeloCloud powered. They're doing this because it's great. Thank you.

I'm pretty sure that was four minutes and 30 seconds.

JAMES HAMILTON

Michael, kind of a hot space the SD-WAN. There's been a lot of other tools and apps and companies doing WAN acceleration, maybe not as much in the prioritisation that you do. How do you solve for some of the things that are just traditionally up there? What is it done by? What's the basis of your engineering, development, time and resources?

MICHAEL WOOD

It's a good point. There are a lot of WAN optimisation products out there today. My feeling is that that whole market is beginning to evaporate and decline. In fact you're starting to see a number of those vendors jump on this SD-WAN bandwagon. The challenges that their architecture is designed for WAN optimisation point to point, head end, branch office and they don't have the ability to scale out to the cloud. They don't have the ability to scale down in terms of price running on an x86 platform.

We're a software company, a cloud sales company. We create software, VNF software, virtualised software that literally can run on just about any type of hardware. We run on Cisco routers, we run on x86 based devices, we run on commercial off-the-shelf [unclear] devices so we took that approach of developing the software. We also took the approach of developing it as a multi-tenant. Initially our strategy was to bring this to market directly and not use any partners or any service providers. That ended up working out as a great advantage because that architecture allows SPs and carriers, telcos and large enterprises to deploy on a multi-tenant basis themselves.

Thirdly, a major aspect of this is the cloud component, the fact that it is a cloud delivered architecture for both the on premise aspects but also the cloud component and the distribution of VeloCloud gateways.

JAMES HAMILTON

Is that security - sorry, the service provider market deploying advanced services to their enterprise customers? Is that turning out to be a good vertical?

MICHAEL WOOD

It's turning out to be a phenomenal vertical. The question is are the service providers turning on the services and advanced service? They're actually taking a couple of approaches. The larger carriers are literally taking VeloCloud gateway technology and integrating it within the MPLS core near the PE or on the PE routers in some cases so that they're bringing SD-WAN and integrating it there at the core and then extending it down to the branch. Their customers are asking them to deliver SD-WAN because it's less expensive. They're able to do that now while still preserving the revenue stream from MPLS but then incrementally increase the bandwidth for SD-WAN at the same time service chaining and inserting services from their own cloud along with third party cloud services. That really dries up their ARPU.

JAMES HAMILTON

Yeah, that's the killer. Okay.

HIRO RIO MAEDA

Just curious, when the customer of yours considers the solution or in the process of evaluation what is ROI that's going through their minds?

MICHAEL WOOD

It's interesting. A lot of times they come because of the cloud problem but they stay because of the very low cost of the solution and the ability to actually get network-wide visibility. In terms of ROI - we've in fact done an entire paper on this - it ends up being pretty dramatic, 3X times savings and in a lot of cases more for a few reasons.

One is they can literally deploy an x86-based hardware in the branch office location is one. They can run multiple VNFs on their hardware along with an SD-WAN VNF from VeloCloud. They can begin to pull some of the services out of the branch into the cloud. So they can now begin to reliably run some of these security services in the cloud instead of having to have a firewall for example sitting there humming away in the branch and a router humming in the branch and a WAN optimisation device humming in the branch and so on and so forth.

There's that ability to really create a leaner branch. Retail, it's huge for them. The numbers are high in terms of number of retail branches and the cost accelerates quickly.

HIRO RIO MAEDA

Makes sense.

JIM LUSSIER

Okay, real quickly, I see that you accepted an investment from Cisco. It looks like you're integrating your product with them. Great partner to have. Is that your exit strategy and how do you get a big - given you're so close to them how do you get anyone else interested to bid on you? What's your exit strategy?

MICHAEL WOOD

I think it's a great - it's a great question. Cisco has a minority investment, a strategic investment in the company. They have no influence over the direction of the company in what we do. It is honestly - Cisco, I was with Cisco for 15 years and ran the branch office routing a product team, [call it] 80, 90 per cent market share in that space.

JIM LUSSIER

Right.

MICHAEL WOOD

I absolutely - if I'm going to be successful and make you successful as an enterprise I have to interoperate with what you have there today. Highly likely it's going to be a Cisco router - nine out of 10 times - and I do that. In fact I do that better than anybody else because I've created a tight partnership. It actually doesn't deter anybody else from - we haven't seen any negatives from that at all because I'm not beholden to them and they're not the only integration point that I've got. I've got integration...

JIM LUSSIER

Who is the most likely acquirer? What is your exit strategy?

MICHAEL WOOD

That's a good question. Our plan is to grow the business substantially, get to the point where it's self-sustaining and we're generating enormous amount of revenue and profit. Right now that's what we're focused on and making our customers successful.

JANICE ROBERTS

I'm a member of the Bay Club so I see that's one of your customers so I'm very pleased about that.

MICHAEL WOOD

Thank you, yes.

JANICE ROBERTS

I imagine - why did they choose you? I know them and I'd be interested because I don't think it's necessarily some of the things you said.

MICHAEL WOOD

Bay Club has - just so folks in the room know, Bay Club is a fitness company. I would say that they've actually expanded much further beyond that. They've got golf clubs and things like that. They operate almost like a place to bring your family and do everything from playing tennis to working out to hanging out by the pool, all those things.

Their strategy was to reduce and eliminate the need for any private lines. They wanted to move completely to internet connectivity but they needed to do it in a reliable way. They don't have much IT staff so they needed to turn up sites

very quickly with low - without having IT staff on site. They're growing and they're also acquiring other clubs. They keep bringing new clubs into the system. They need to bring those clubs up instantly and they need to be part of the family and part of the network instantly. They're able to do that scale aspect.

[Music]

JANICE ROBERTS

[Inaudible] SD-WAN...

MICHAEL WOOD

IOT so we work with Deutsche Telekom for example. They're doing IoT with - I'll just talk louder, is that okay - IoT and robotics and connecting the US to Germany and being able to manage literally things like robotic endpoints and car assembly.

JANICE ROBERTS

Okay.

MICHAEL WOOD

Thank you.

MANEK DUBASH

Thank you. Okay, I'd like to thank all the candidates for being such good sports and joining in with our shark tank. Now the investors will be ruminating over lunch I think is the best word about their conclusions as to who the winners are in each of the two categories. But before we disappear off to lunch I would like to invite you maybe to give us 30 seconds, a minute each on your summing up of how you think everything went and what you thought of the candidates. Who wants to start?

JANICE ROBERTS

Yeah, somebody else start.

MANEK DUBASH

Start in the middle.

JIM LUSSIER

That's the hardest question of all so I get to start.

MANEK DUBASH

Just really quick.

JIM LUSSIER

I think I already said what I think which is that when I was asked to judge this and I looked at the three companies in each category I can see why they were picked. Every one of these companies has a really kind of unique spin, the idea of eliminating the chance of being attacked by isolation or the machine learning applied to just prevention or a new open stack appliance that's immediately deployable.

All of these ideas I think are really, really interesting and it's going to be a really, really tough decision for us as judges to pick which one is the winner. I think a lot of it's going to come down to competitively how do we think these companies are going to stack up? In every one of these spaces they're not the only player so how do we think they can win, how do they think they can be successful? I think each of these companies has a tremendous amount to offer and I was really intrigued to wrap my brain around this and give it a lot of thought and challenge it a little bit.

MANEK DUBASH

Hiro?

HIRO RIO MAEDA

I go next. Very close to what Jim says but very impressive list of companies. The world is moving really fast and the venture is all about solving the problems of the world. Because the world is moving so fast and evolving so fast there are new kinds of problems everywhere in different silo and different niche but every one of them that we saw today seems to be solving a legitimate big problem that they foresee.

By that list I was quite impressed but one thing if I could say to make things easier, I wish the face of the company was in closer proximity because some of them are already succeeding in the unicorn phase and some of them are just seed funded. It's hard to judge, for us to compare but very well done for the list of the companies.

JIM LUSSIER

We will come up with a winner.

HIRO RIO MAEDA

We will somehow.

MANEK DUBASH

Thank you. Janice, any words?

JANICE ROBERTS

I thought great companies. What I always like and you would expect it but there's real passion about their businesses. Here we did talk about some of the challenges but obviously when you present you talk about all the good things, all the momentum. I think we're going to probably spend some time talking about some of the challenges and some of the competition. For me I did get a decent sense.

Again the stage is a little different so I always like to think about how people approach customers whether it's with positioning which often in these busy markets and with the pace of change is difficult, really how companies really position their companies for customers, which sounds obvious but not everybody does. Sometimes it's an afterthought. I think people articulated that pretty well today.

MANEK DUBASH

James?

JAMES HAMILTON

Yeah, since all six companies are at different levels of maturity we'll probably have to come up with some common criteria around disruptive technologies, what business need are they solving for and then the well-defined go to market strategy. I think that would be applicable no matter if they're an early stage start-up or something that's a little bit more mature so we'll try to do that.

MANEL DUBASH

Okay, James, Jim, Hiro and Janice, thank you so much for your time and your energies and hopefully we'll see the results of your ruminations over dinner tonight. That just about wraps it up for the morning session. Let's go and have some lunch, which I think is probably out there in the sunshine and well, see you this evening.

[End]