**NETEVENTS GLOBAL IT SUMMIT**

***SAN JOSE, USA***

***OCTOBER 3 & 4, 2019***

# DRAFT

## *Shark Tank Session*

### *Lead Judge: Hiro Rio Maeda, Managing Director, DNX Ventures*

VC Judges:

| | |
|---|---|
| Peter Kuper | Managing Director, ClearSky |
| Neil Weintraut | Partner, Motus Ventures |

Hot Start-Up winners:

| | |
|---|---|
| Galeal Zino | CEO, NetFoundry |
| Alice Wang | VP of Hardware, Everactive |
| Noa Shafir | Founder and Chief Product Officer at Odo Security |

**Manek Dubash, NetEvents**

Now before lunch, we have what I hope will be an entertaining session. If our *Shark Tank* sharks would like to come down to the front here and take their seats, we can move to - I think it could be a bit of fun. The way this is going to work is that three vendors have already been voted on as potential winners in three categories in cloud data centre IoT cybersecurity. Those three vendor representatives will each pitch to our sharks - our venture capitalists and they will then decide who's going to get the virtual money that they have potentially to hand out. Hopefully, their conflab will be fairly short, because lunch is after that.

**Hot Start-Up – Cloud/Datacenter Award Winner: NetFoundry**

**Galeal Zino, CEO, NetFoundry**

OK. So, I'm going to start with market. You love big markets, entrepreneurs like big markets. We know business networking is a big market, most of our analyst friends have told us $50 billion or so. I would say it's an under-rated market, an understated market, both in its size and its growth. Why? Today's businesses don't just use software. Today's businesses are software. More specifically, today's businesses are connected software. Business networking therefore has never been more important and I could make that statement five years from now and it will still be true; that's how important networking is, that's what's driving the size of this market.

On the flip side, this hyperconnected paradigm is breaking the legacy network. No surprise, legacy networking is not built for this hyperconnected paradigm. Three quick aspects, I'll break them up :

(1) apps are moving to the edge; apps are everywhere. Devices are everywhere, data is everywhere, networking needs to natively extend to the edge.

Number (2), as we've heard from our friends this morning, security is quite frankly broken. We're doing a horrendous job at security, mainly because it's reactive. A lot of the blame goes right into the network; the complexity of legacy networking. Complexity is insecurity; we fix that.

Number (3), maybe the most important; automation, agility, innovation, that's how folks win in today's world. That means that the practitioner, the developer, the DevOps, the cloud team, they need to control the network. Not the telecom, not configuration; code.

Finally, although we have a large network today - excuse me, a large market today, that's despite ourselves. Telcos have strangled this market forever. That's about to change. There we go. How do we solve this? A lot of problems to be solved that I just mentioned. Fortunately, the solution I think is relatively simple. There are a lot of folks out there building bigger, badder networks and they're doing a great job.

We're taking the opposite approach. We're saying, if the application is the new edge and we really need agility and programmability and automation, let's put the network into the application. This is a path that AWS 38 and Twilio have been down. In AWS, I can go spin up compute, I don't know how AWS allocates the underlying compute box, it just works for me. They manage all that as a service.

NetFoundry, use our APIs, use our web console, you spin up a global private network in minutes and we manage all that infrastructure for you as a managed service. Twilio; put text messaging, put video, put voice into your application without being a 323 or SIP engineer. Fantastic. Same thing with NetFoundry. Put a network into your application without becoming a network engineer.

What does this look like? On the bottom on the left here, you see apps everywhere; clouds, devices, et cetera. Use our SDKs, use our thin clients, to go all the way to the application. Use our containers, in those environments, sidecars. On the clouds, you go to the cloud marketplace, you download our image, put it into your VPC or V-Net and you're done. It is part of your network; it's not just a single tunnel VPN spoke into your network. It's not just a single MPLS connection to a private data centre. It is part of your network.

The magic of all that is the top of this diagram, APIs and SDKs that gives the developer the keys to this network. Enables the developer to programmatically control the network. We flipped the script. No longer do you put your applications on the network, you put the network into your applications.

The icons here are some of our customers that have done a fantastic job innovating with those keys that we've provided them. The [market's early adopter] but we've been very successful in identifying the early adopter and selling to them. We're over 1.5 million [unclear] in less than a full year of sales. The growth is over 400% on an annual basis.

More importantly, the early adopters we found, they love our product. They are happy. Our growth is mainly on their banks. We spent less than $400,000 in marketing all of last year, as an example.

The best is yet to come. Over the next couple of months, [unclear] will be making a series of exciting announcements that are taking our SDKs, which are right now at the level that an early adopter or an early evangelist could use. We are making them more mass-market friendly, with the bindings for their environments, whether it's mobile, whether it's IoT, whether it's cloud. I'm going to stop there so I don't get the *Jaws* music on me and open it up to questions.

**Hiro Rio Maeda, Managing Director, DNX Ventures**

Tell us about your team.

**Galeal Zino, CEO, NetFoundry**

Sorry?

**Hiro Rio Maeda, Managing Director, DNX Ventures**

You, tell - let's hear about you and your team.

**Galeal Zino, CEO, NetFoundry**

Great. So, one of the more difficult parts of everything I just described has been identifying the team that could make it happen. You need folks who are coming from layer 2 and 3 and think like packets and eat, drink and breathe packets. They can go up the application stack and understand why that needs to be programmable.

On the flip side, I need the application developers coming from layer 7 down, who are willing to learn about life of a packet and make it happen. Our executive team comes from the founder of IoT startup that's now built by PTC. It comes from Juniper, it comes from Cisco, your usual suspects on the networking side and comes from a series of start-ups in cybersecurity and SAS.

**Panel Speaker – Unknown**

There's a waterfall of companies going after the dev-apps area at large. There seems to be a lot to have to do with network management, more of an approach putting a layer over all of the cloud systems. I've seen a lot of management companies trying to do this, so where does - where do the two - it seems like you're taking a different approach.

**Galeal Zino, CEO, NetFoundry**

It is going to be ecosystem. We talked about earlier, the Kubernetes ecosystem which is fantastic. As a software early, API first solution, we're able to integrate in those solutions for a full stack type approach. We want to make it turnkey for the customer. A lot of our customers are actually buying NetFoundry as part of a larger solution that already has a networking piece taken care of. It's not like we're doing everything, far from it but we have the proper API integrations with the security folks, the visibility folks, the monitoring folks to make it simple for you.

**Hiro Rio Maeda, Managing Director, DNX Ventures**

One question. You touched on the software as the main way of today's enterprise run their business and that is true; I tend to agree. At the same time, [unclear] enterprise application is running on SAS as well so my question is, how do you secure that side of the network?

The second question is that relating to that, when it comes to the legacy enterprise of the flip side, it's running actually many of the legacy applications, [unclear] using the binary protocol in a very old way. How do you secure that - how do you secure and authenticate that kind of old classical, traditional software, as well?

**Galeal Zino, CEO, NetFoundry**

Great questions Rio. Two points. Number 1, we certainly don't fit or play everywhere. There are a lot of legacy environments that we plain old avoid and we will wait for them to die their natural death. We're not going to go try to solve a lot of those environments.

On the SAS side, we see basically two models. One is what we call private SAS. It's where I host an application in some cloud; public or private, doesn't matter. It's on RFC 1918 space; it needs to talk to my customer, who is, let's say, a retailer or a hospital, a medical facility. I need a bridge to [unclear]. In that paradigm, today the dominant way to do it is [unclear].

If I take a typical - and one of our examples is OmniSYS, they have pharmaceutical applications deployed in hundreds of locations. Prior to us, they had to manage hundreds of VPNs. If they want to grow - which of course they do, they're a $20 odd million company in Florida, they're looking at thousands or tens of thousands or hundreds of thousands of VPNs. Instead, put the connectivity into the application and now their customer, [unclear] doesn't need to manage a VPN up to their cloud.

Public SAS, different story. Most public SAS is not very relevant for us. It's a built-in isolated ecosystem. I'm not saying all of it is out of scope but a lot of it is out of scope.

**Hiro Rio Maeda, Managing Director, DNX Ventures**

So, you don't go after those public SAS?

**Galeal Zino, CEO, NetFoundry**

As a general rule, no. There are some exceptions, but as a general rule, no.

**Hiro Rio Maeda, Managing Director, DNX Ventures**

Okay, understood.

**Panel Speaker – Unknown**

[Unclear] a little bit about who's the buyer here and is he talking about networking, security ops, et cetera; who's the buyer, how are you getting to them as far as - [unclear] website but is it the carriers, are they necessary and are you trying to eat the lunch of the carriers MPLS and things of that nature. Is that just a [dead] [unclear] in your mind?

**Galeal Zino, CEO, NetFoundry**

Our customer, the buyer, is changing over time. We are making a bet that months, years from now, the new buyer is the developer. It's more of a grassroots buy. That's not the case today. Most enterprises today, the developers might be influencers but they don't hold the budget and they're not making the decisions.

So, our go-to market today is much different than tomorrow. Today, our go-to market has been mainly through ISVs, through SIs, through cloud integrators who take our solution, wrap it up with what they're selling to the customer and solve the networking piece. Tomorrow our big bet though is - like we've seen with SAS, actually, for example; we believe enterprise sales is increasingly becoming grassroots [unclear] the developer.

**Panel Speaker – Unknown**

Do you require some sort of [agents] to the end point?

**Galeal Zino, CEO, NetFoundry**

Yes. There's two basic ways we can get to an end…

[Music plays]

**Manek Dubash, NetEvents**

Time's up - your time is up. I'm sorry. Everyone gets the same time.

**Galeal Zino, CEO, NetFoundry**

Short answer, yes.

**Manek Dubash, NetEvents**

Enjoy your lunch, Galeal Zino.

**Hiro Rio Maeda, Managing Director, DNX Ventures**

Thanks. Do you mind if we introduce ourselves?

**Manek Dubash, NetEvents**

No, of course not. Let's hear from the panel. Who are you?

**Hiro Rio Maeda, Managing Director, DNX Ventures**

I think we actually should introduce ourselves before we started the session. My name's Rio Maeda, I'm from DNX Ventures. We run three funds under a management about $500 million based in Tokyo and San Mateo. We go after enterprise application, industrial solutions, cybersecurity, retail [tax]. Those are the things that we go after.

We tend to invest in industries A and B, [unclear] of the companies. That's me. Pass it on to Neil.

**Neil Weintraut, Partner, Motus Ventures**

Neil Weintraut with Motus Ventures. Motus is our first money - typically first money into the company. We have about 70 investments now related to autonomy.

**Peter Kuper, Managing Director, ClearSky**

Peter Kuper with ClearSky, Managing Director. We are - we have about - just under a billion under management. Very heavily focused on two major sectors, one being security. They're a dedicated fund there and also [unclear] [para technology] from things that are dealing with critical infrastructure; from not just security but also efficiency from your generational transfer.

**Manek Dubash, NetEvents**

Great, thank you very much. Now for our second start-up in IoT. Alice Wang from Everactive.

**Hot Start-Up – IoT Award Winner: Everactive**

**Alice Wang, VP of Hardware, Everactive**

Thank you. Now imagine you are the CEO of a Fortune 500 company; you've got hundreds of factories all over the US, they're pretty happy. They're at 95% productivity but one day you're thinking, what if I could get them to 98% productivity? So, you send out an email to all of your plant managers and you're waiting for their report.

Now imagine you are that plant manager; you just got that email. You're pretty panicked; you're sending emails to your manager; you're sending out calls and trying to get all the data you need in order to push the productivity up from 95% to 98%. I think that's pretty realistic what would happen in today but that's not true in the IoT world.

In the IoT world, you can imagine there are trillions of sensors all over, especially all over the factory so that instead, this plant manager would bring up their tablet, they'd see the whole factory floor. They'd have their pipes, they'd have their machines, everything would be having sensor data and they can easily make that report in minutes instead of hours or weeks or months. That's real money going out the door for the company.

At Everactive, we're investing our technology in making this world, this IoT world, true. I want to show you this plot here, which is the predicted IoT devices and that analysts have come up, in terms of the IoT world that I talked about. Analysts like you guys in the room first predicted that by 2015, we'd have one trillion IoT devices. As you can see over time, the number of IoT devices has decreased and the time to reach the IoT world has also expanded.

I'd like to talk to you about why - why is it have we fallen short? We believe there are two reasons. First of all, when you have a trillion sensors, a lot of these sensors are mobile and probably will have batteries. We've done the math for you; for a trillion sensors, with a reasonable 10 year battery lifetime, that means every day you will have to replace 274 million batteries, per day. That means me, you, all of us will be doing battery replacement management. You can imagine when you're at home and that smoke detector alarm goes off, how annoying that is. That's basically why a lot of these devices are not happening in the near future.

Secondly, we see that IoT is very fragmented, in terms of the different types of appliances, your analytics, different kind of sensors needed. We see different kinds of software in the IoT market. Because of that, there's no consolidated push and so you see a lot of different solutions in the IoT space.

We at Everactive have - believe we have solved these two key challenges. For one thing, we are building self-powered, battery-less sensors so that we can provide continuous sensing of all of your assets and we do not need to change the battery. So, how can we

be self-powered? There's actually power all over; there's power in this room from the lights, there's power in this room from all of the heat in our bodies. There's power just generated from motion.

We are able to harvest that power and do the analytics, machine learning, sensor signal processing and we can send that over a wireless network link up to the cloud so that our customers can reach it through our website and that they will get the data screens. Not just the data but actually insights on the data and that is what adds value to our customers. We provide end to end solutions, meaning we provide the hardware that is able to operate off the - off a very low power. We also provide infrastructure all the way to the cloud and we do this with no batteries required.

This here shows our short-term roadmap of our first few products. We have a platform which is able to use many different types of harvesters and supports many different sensors, so that with this hardware we can support many different kinds of products in the industrial world. Such as steam traps, flare systems and so on. While now we are in the industrial market, we believe that our hardware and our solution can easily extend all the way to consumer and eventually be as small as a stamp so you can put it every single place and that someday, we will soon see trillions of sensors everywhere.

Thank you very much.

**Panel Speaker – Unknown**

Can you tell us a little more of the proprietary differentiation of the technology, is it the efficiency from [photovoltaics] versus [power electric] or is it also on the chip set when you're doing your wireless relays? Give us a little bit more flavour for the tech [unclear].

**Alice Wang, VP of Hardware, Everactive**

Sure, so we do have a proprietary circuit in the hardware that does very efficient harvesting from PV cells and tech cells and motion harvesters. We also are very efficient in how we use that power; it's extremely low power circuits, both analogue and digital circuits.

**Panel Speaker – Unknown**

What kind of network protocol do you use, which I believe it will consume a lot of some sort of - big chunk of energy? With what kind of protocol - how often can you actually transmit and how far can you go?

**Alice Wang, VP of Hardware, Everactive**

Okay. We don't use a proprietary protocol because we studied all the ones out there, such as LoRa, NB-IoT. These are way too high powered in order to support energy harvesting requirements but we are able to transmit up to 300 metres, which is well within a factory floor. Our next generation is trying to go for one kilometre.

We're even working with - going to the [unclear] meetings, because we think 5G will be the right place to go all the way to standard protocol.

**Panel Speaker – Unknown**

How often can you transmit it?

**Alice Wang, VP of Hardware, Everactive**

We transmit once a second and even shorter.

**Panel Speaker – Unknown**

One second.

**Alice Wang, VP of Hardware, Everactive**

Mm-hm, yeah.

**Panel Speaker – Unknown**

What bit rate?

**Alice Wang, VP of Hardware, Everactive**

We're 16 [kilobits] per second. So, it's slower but we think these IoT devices, they don't really need a ton of data. We're actually sending the [insights], we're not sending the data. We're doing the machine learning on the sensor and so we can send more accurate results so that the actual data rate does not need to be very high.

**Panel Speaker – Unknown**

Tell us about the security technology related to it, so bad actors can't get into these.

**Alice Wang, VP of Hardware, Everactive**

Security is very important for IoT so we have to worry about attacks and so we do have, when we're transmitting, [ADS] and those kinds of protocols enabled.

**Panel Speaker – Unknown**

Do you actually have any installs at this point?

**Alice Wang, VP of Hardware, Everactive**

Yes, we do - our first product is called a steam trap monitor. Actually, in many buildings like this, steam is still a primary source of power in factories and so on but when steam - they're only - they're checked once a year or so, so you may be having a steam pipe that's blown, you won't know.

We are currently - our customer base, we have about 10 customers of many different kinds; some are big building, some are food, food and beverage and some are in oil and gas refineries. So, places where it's not convenient to go keep checking the steam traps.

**Panel Speaker – Unknown**

Are most of your market new uses or are you displacing [other] systems?

**Alice Wang, VP of Hardware, Everactive**

I think we - both. Some of them are new, meaning if you go to their factory, they don't have any sensors there but then some, you will see that competitors which have batteries, for example and so there are a couple.

**Panel Speaker – Unknown**

What are your sensors talking to? You have this new data. There needs to be some application, so are you providing them? Are you partnering with someone?

**Alice Wang, VP of Hardware, Everactive**

We are partnering as much as possible. We are also providing. They do talk to our gateway. The gateways then connect to the backhaul, to the cloud.

**Panel Speaker – Unknown**

As for the overall strategy, are you going for the horizontal approach, meaning that you're just providing sensor and APIs and let the other ones or the customers to come

up with applications or are you going deep into the certain vertical and try to come up with application with analytics and maybe getting into predictive maintenance and those kind of value-added application? Which way are you going?

**Alice Wang, VP of Hardware, Everactive**

We're pretty deep. We basically install the hardware. When the customer goes to the website, they see the data analytics, so we provide all that. We're going very deep.

**Panel Speaker – Unknown**

If you go deep, every industry has a really, really different workflow. You really need to customise and come up with a proprietary application catered towards that industry. That becomes really hard to scale into multiple verticals, but how do you solve that?

**Alice Wang, VP of Hardware, Everactive**

We pick generally - like for example, our first is steam trap. There are thousands of steam trap all over United States. The second one is machine health monitoring. That's pretty standardised. You don't need to build a whole new infrastructure just for machine health. You could do the same infrastructure but then for different machines, modify the algorithm. But it's quite well understood in terms of the algorithms. We can also take feedback from the customer in terms of different thresholds for different machines, for example. I think we have pretty big, large markets that [inaudible].

**Panel Speaker – Unknown**

I think we're being attacked.

**Alice Wang, VP of Hardware, Everactive**

Thank you very much.

**Manek Dubash, NetEvents**

Alice Wang, thank you so much.

Now our third entrant in the cybersecurity space is Noa Shafir from Odo. Unfortunately because it's - for us, that is - because it's an Israeli public holiday, she's in Israel, but she is joining us over an audio link. Noa, are you there?

**Hot Start-Up – CyberSecurity Award Winner: Odo Security**

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

My name is Noa Shafir. I am one of the founders of Odo Security. I am here to tell you that you are the network. Every person working from home, every person accessing resources in the cloud, every person who ever sent work documents to their personal emails - just because it was too difficult to connect to the office remotely - represents the new network, a network that is constantly shifting and growing.

In spite of this new reality, companies are still using legacy access solutions like VPNs. The problem is they are nearly impossible to manage at scale, cannot secure a shifting perimeter and provide no visibility into what's actually going on inside the network. Odo replaces VPNs with a zero trust network access where the default state of application infrastructure is dark. Users receive access into internal resources on a need-to-know basis and device [unclear] and health are verified before being granted access to anything.

With traditional VPNs, access is all or nothing. You get authorised to the network based on credentials only. Credentials are pretty easy to steal. Just ask the guy who sent you an email telling you that you've won the lottery in Zanzibar. Authenticated users are logically moved from outside the network to inside. It is all or nothing. Once inside, users have access to everything. Even if a server is protected by credentials, it can still easily be accessed in the network level.

In more practical term, this means that your back office manager, or a malware that he innocently downloaded to his laptop, can attack your servers, get access to sensitive information and even crash your entire system. The worst part of it is that you would not know until it's too late. VPNs are not built to provide visibility inside the network.

With Odo, access can be tailored down to the database query or SSH command. Based on its principle of zero trust, Odo moves access decisions from the network level to the application level, eliminating the ability of attackers to roam freely in the network. Every user is authenticated by a device location and other contextual information and behavioural data and authorised based on preapproved access decisions, permissions and policies before being given access to anything.

After authorisation, users get the minimal level of access needed to do their job. Every other resource is not only inaccessible, it is completely invisible. Also now IT and DevOps teams can actually see what's going on inside the network. Odo provides full activity log and detailed audit trail with alerts in real time on suspicious activity and even logs commands in real time.

It is all delivered as a SaaS solution. This means that for the user the access is seamless. It's as easy as connecting to Gmail. Also it is completely agentless, so there is nothing to install and no need to do changes to your existing architecture. Deployments take three minutes end to end.

Finally we have put together a world-class team, engineer who brings extensive solution and experience in a lead intelligence unit, 8200, and some of the biggest names in

security. We're working with some of the biggest brands in the market and backed by leading investors. I'm happy to answer any question. Thank you.

**Manek Dubash, NetEvents**

Okay, so that actually was - my mistake - a video. Now hopefully while this holding slide is up, we're going to switch actually to a live audio feed where she can answer the questions from the gentlemen on the panel. I'll just keep talking until - ah. Is that a good sound? Do we hear her? Is she there? Is she there? No, she's still somewhere in cyberspace. Yes, I think it's time for someone to tell a joke or two really, isn't it? Or maybe we can speed up the bits somehow at the back there. How are we doing?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

It's very secure.

**Manek Dubash, NetEvents**

It's a very secure connection, so yes, there's a lot of wrapping to be done. Yes.

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Hi.

**Manek Dubash, NetEvents**

Noa, welcome. Thank you for joining us.

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Of course. Thank you for having me.

**Manek Dubash, NetEvents**

The panel, the three venture capitalists, is now ready to ask you questions. Go ahead.

**Neil Weintraut, Partner, Motus Ventures**

Noa, welcome. This is Neil Weintraut. Well, actually a lot of questions related to the technology and its impact on actual usage. We don't have time for that, but I'm trying to understand how you come between the apps and, for example, database access. Are you just monitoring it and are you actually inserting yourself directly in the path?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

We're inserting ourselves directly. We're kind of in the middle [unclear] cloud and all that data is routed through our cloud.

**Panel Speaker – Unknown**

How does that relate to performance? Because [unclear] database level, that would be very performance taxing.

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

We're actually sitting the closest to the data centre, so it provides near to zero latency.

**Panel Speaker – Unknown**

Close to the data centre, but the database could be anywhere in the cloud. How can you be closer to every database - I mean, to the infrastructure?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Yeah, we have a [unclear] of our gateway which is the data part of our solution. It sits closest to your region, so that would be the same availability zone hopefully.

**Panel Speaker – Unknown**

I see. Relating to that, I have another question. If the data plane goes through your infrastructure for all the traffic, there are many industry which are very sensitive to that. Financial is one of them, healthcare, federal. For those kind of data-sensitive industries, you don't want to be the single point of failure and also you carrying the risk of being compromised and exposing those data to outside. How do you go against those kind of concerns?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Yeah, right, that's actually a great point, because we have been struggling with that. This is why we built our entire platform on top of a [unclear] cluster, so we can actually move the whole thing on premise. Therefore companies have it all self-hosted in their environment, so that prevents the risk.

**Panel Speaker – Unknown**

Okay.

**Panel Speaker – Unknown**

How do you deal with - so what I saw on your materials on the website, SSO for SSH, how do you deal with the key management which is critical there? Between your application authorities, your certificate authorities, et cetera, how are you handling the keys?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Yeah, exactly, so we store it in Hashicorp vault. That's [unclear]. The idea is, instead of users having to hold keys to each one of the servers, they only hold individual keys to Odo. On the other side, the admin is connecting the servers. Then the access decisions are determined logically rather than with keys that can be lost or stolen.

**Panel Speaker – Unknown**

You're tapping Active Directory or something like that for the authorisations necessary or how are you determining that?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Yeah, so that is done as well. This is done for authentication to the other platform and also to the SSH itself to connect to [AD] or other [IDDs] to sync with the SSH account or just connectivity to the platform itself.

**Panel Speaker – Unknown**

Tell us about any customer installs you have at this point.

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

We have about 10, 11 in Israel and in the States and in Europe.

**Panel Speaker – Unknown**

Well, it would help to get a sense of the applications for your - where people have bit.

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Excuse me. Can you repeat that?

**Panel Speaker – Unknown**

What are the actual use cases? Without maybe revealing names, what are customers doing with this specifically? What apps?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

Yeah, sure, so we see three main use cases. The first one being VPN replacement. This is just an easier way to connect, no need to install clients, just easier for everybody in the organisation, easy management. The second being access for DevOps, so that would be the SSH key management. The visibility is very strong over there, the ability to block commands in real time, so that's strong over there. The third one being third-party contractors, so the fact that everything is segmented, no client to install - you can provision temporary users. That's also strong over there. It varies between tech

companies and large-scale companies, so about 200 people would usually want DevOps or [the VPN] replacement and large - we have tens of thousands. [Unclear] they go for the third-party contractors.

**Panel Speaker – Unknown**

Okay. How do you do the mobile side, iOS, Android, Chrome OS?

**Noa Shafir, Founder and Chief Product Officer at Odo Security**

This is all done through a web browser, so it's just a direct connection through the Safari. We don't have anything native for the mobile yet, because there is – are actually also not have been requests for native mobile application. Just through web and then we support seamlessly.

**Panel Speaker – Unknown**

Okay. Understood.

**Manek Dubash, NetEvents**

Okay, Noa, thank you very much for joining us. Now I'm going to invite the venture capitalists to have a little conflab amongst themselves and decide which of the three gets the money. While they're doing that, perhaps we could have a show of hands as to which one you think should get the money. Should it be Galeal Zino, NetFoundry, who is competing from the cloud data centre space? Raise your hands, please. One, two, three, four, five, six, seven, eight. I think - I make that eight. Make that nine. Okay, so that's nine. Someone write that down for me, please, because my maths isn't very good. My head's somewhere over the Atlantic.

Secondly Alice Wang from Everactive on the IoT space, who thinks they should get the money? Whoa, look at this. One, two, three, four, five, six, seven, eight. Keep your hands up. Eight, nine, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19. Nineteen. Twenty. Thank you.

Finally Odo with its cybersecurity system. That's just one, two, three. One, two, three, four. Only one hand, sir. Only one hand. Come on. I make that four. Okay. Thank you.

Well, it looks like the result is pretty conclusive. You're all big fans of Alice Wang's Everactive. How's the conflab going? They're still conflabbing.

Time for me to tell you a little bit about what's going to happen this afternoon for those of you who haven't been through this before. Basically the press and analysts will be meeting with vendors. You'll be discussing the issues that the vendors have raised. You can ask them questions directly. You'll be getting their press releases and all those other sorts of information after the event. Lunch, on the logistics front, will be out there, I understand. You'll be getting your schedules and all the details from our wonderful staff out the front, pretty much probably as you leave or over lunch. That's pretty much all really I have to say from a kind of - oh, yes. Yes, yes. Ah, yes, tonight, the Innovation Leader awards dinner tonight. At 6:15 we have a drinks reception at the [Hayes

Ballroom Terrace]. The award winners will be getting their prizes. We'll be also having another awards ceremony in the Innovation Leader category. That's going to be fun here tonight.

How are we doing on the conflab, gentlemen? They're still conflabbing. Do we have a result, white smoke, puffs of smoke? No white puffs of smoke? Do we have a result, Rio?

**Panel Speaker – Male**

I guess one of us could give a comment.

**Manek Dubash, NetEvents**

Over to you.

**Panel Speaker – Male**

Okay, great. Thank you. It's a limited time. Both the presentation and also the discussion among the judges is very much limited, so it's hard to make a call under this circumstance. Whenever the VC looks at any of those entrepreneurs' and the start-ups' pitches, we look at many different things. What is the market? What is the technology? What is the team? What is the business model? What is the - how the urgency and the demand is created? We look at all of those. To make judging smooth, we did the scoring on each of those categories. We generally sum it up among three of us. Based on that, we - three of us - chose Odo Security for this year's Shark Tank.

**Manek Dubash, NetEvents**

Hey.

**Hiro Rio Maeda, Managing Director, DNX Ventures**

Maybe it might be worthwhile each of us to give a comment on why that's the case. It's a very known problem that today's VPN is really legacy and becoming problematic to many of the enterprise. If you look at the latest breach - that was the DoorDash case - it was breached by the third-party contractor accessing into the cloud infrastructure of the DoorDash, legitimately, but it was compromised. All the customers' information got leaked out. If they had that, something like the Odo Security, it could have been avoided. Knowing that kind of incident is happening even today in a continuous basis, we believe that something like this - there are many other ones that's trying to solve the similar problem, but Odo could be one of those companies that could solve this kind of problem. That was my take.

**Panel Speaker – Male**

Yeah, I'll echo Rio's comments. I think a great example of all the major - not all, but many of the major breaches we've heard about [be a] target on the HVAC contractor access all the way through, it's usually an access problem, right. Hackers gain access to

[unclear] credential otherwise and off they go [unclear] what have you. Something that has scale to it, that can prevent wild access and stealing information people should never have access to has been an ongoing obvious need. Some solution like this is definitely going to be part of how you finally counter those attacks.

**Panel Speaker – Male**

I think we'll just offer a calibration on all of them that it's - all of these companies were the type of companies that VCs fund. There's a bit of a synthetic exercise in any panel trying to say this one's, quote unquote, better than the others. But at the same time, it's indicative of some of what goes on when you're trying to raise capital in that often, if you will, your competitor is not even in the same market sector.

We can only invest in so many companies a year. We, well, look for the areas that seem to be the most lucrative, including the easiest to take off, which I think is part of the reason there was a preference here for Odo. First they showed a great end user focus. The market is clearly there. There's an enormous number of entrants in this space in their particular case. But at the same time, all three clearly had great teams. They earned good markets. Each had very special technology to talk about. I actually would like to recognise that all three were very impressive companies. Odo edged out in terms of our selection though. [Unclear].

**Manek Dubash, NetEvents**

Thank you very much indeed. Thanks to our panel...

**Panel Speaker – Male**

Thank you.

**Manek Dubash, NetEvents**

...for sparing the time out of their no doubt extremely busy schedules. Thank you so much for doing that. Okay, that's it for this morning's session. Let's go and get some lunch. See you in the afternoon.

[end]