

MANNY: We're going to have a session now. The name of the session is CISO Startup Connection, and it is powered by YL Ventures. The person that will moderate the session, one of the most interesting investors in Israel and a good friend of mine, Ofer Schreiber, and he is a partner at YL Ventures. Ofer, the stage is yours.

OFER SCHREIBER: Hi everybody. As Manny mentioned, my name is Ofer Schreiber. I'm a partner in YL Ventures, and I would like to welcome you to this session, the CISO Startup Panel. I think that you can't really talk about Israeli cybersecurity without mentioning the vast amount of startups, innovation, and technology that is coming out of here, and for us Cyber Week is a great opportunity basically to combine Israeli entrepreneurs and technology with global markets and customers, so this is what this panel is all about. We're going to meet today three early-stage, very innovative startups, and we'll have an amazing panel of four global customers, chief information security officers. And what we're going to have here is a brainstorming session, a discussion Q&A between the entrepreneurs and their customers, and I'm sure it will be very interesting and beneficial to the founders, and hopefully to the audience as well. So, without further ado, I am very excited to bring to the stage our panelists. First is Andy Ellis, chief security officer of Akamai. Bobby Ford, chief information security officer of Unilever. Renee Guttman, the chief information security officer of Campbell's Soup Company and Michael Melly, the chief information security officer of Bank Julius Baer. All right, so let's start with the first company. The first company is Orca Security. Please come on stage, Avi Shua, co-founder and CEO.

AVI SHUA: Thanks, Ofer. One second. Thanks. Thanks, Ofer. So, we are Orca, and we are doing one simple thing, providing full stack cloud visibility seamlessly. Basically, within minutes, providing full visibility of security issues like vulnerabilities, misconfiguration, and breaches in IaaS and PaaS environments. So, a little bit about us. We were founded earlier this year. We are eight co-founders, all of us out of Check Point executive and architects, including me. I was the previous chief technologist in Check Point. We have just announced a \$6.5 million seed, and currently 15 employees, in fact, 16 as of this morning, since I created the presentation, and in beta phases. And we really believe that the cloud migration is not a security issue, but it's, in fact, an opportunity to get better security than you could get in a pre-cloud world. So, let's have a brief look at the typical IaaS or PaaS environment. We see it usually as four different layers. There is the cloud infrastructure layer, the bottom-most layer, that everything is running on top of. And on top of that, there are the various workloads. There are machines, there are containers, but all of them have operating systems, applications, and data. And you need to be able to see and secure all of them. So, in the cloud layers, you need to make sure that you don't have critical misconfigurations like buckets that open to the entire world or a database that everyone can read. This is one thing that you need to make sure. But it doesn't end on the cloud layer. You need to secure also the operating system and application layer. You need to make sure that you don't have vulnerable applications, that you don't have malware running on the machines or any misconfigurations that are sometimes as serious as vulnerabilities. So, this is what you need to know. Now have a brief look at the solutions that are available today. Basically, for the lowest level, there are the CSPMs of the world, RedLock, CloudPassage, and similar solutions that very easily, within minutes, let you know if you have a misconfiguration at

the cloud infrastructure level. People like them. They are very easy to integrate. You get the answers within minutes. But they don't get inside the assets themselves.

[00:05:12]

If you want to know of issues inside the assets of software vulnerabilities, of misconfiguration, you need, as of today, to install agents or deploy network scanners for each and every one of the assets. And this is a process which is both very time-consuming and can cause, in most of the cases, to reach only partial visibility. You can't deploy asset agents on all of the machines. It's an organizational nightmare, especially when it's a large organization or M&As are involved, etcetera. What you really need is to see across the technology stack, to have security visibility for both the control plane, for the operating system, application, and data. And this is exactly what the Orca Cloud Security Visibility Platform does. In five minutes integration, and I really mean five-minute integration, using grid-only access, no changes to the organization configuration, you get full stack visibility of misconfiguration vulnerabilities into your data, without any change in the environment. So how do you do that? How are we able to provide it while all of our competitors require to install agents or to configure network scanners? So, basically, the secret sauce lies in our patent-pending SideScanning technology. When you are working in the cloud, machines are no longer physical. You can approach them also from the bottom, from the infrastructure level. So, what we are doing is that we integrated, using low-level APIs that are open, to the cloud infrastructure level to read the machine configuration and virtual disk and virtual hardware without any integration to them. We read them from the bottom or from the side. It depends on how you want to visualize this. We interpret this data, and based on it, we are able to provide you with full-stack visibility of everything that's going on in your entire IaaS or PaaS infrastructure. Misconfiguration vulnerabilities, even compromised machine, without any need for per-asset integration, network integration, or anything like that. So basically, this is it. Full stack visibility in five minutes with absolutely no impact to the environment.

OFER SCHREIBER: Thank you very much, Avi. And now let's hear some feedback and questions from the panelists.

MICHAEL MELLY: Well, then I'll go first. What does the traditional vendors, or the first-generation CSPMs, as you call them, prevent them from doing what you are doing, actually? Or why can't they go the way you are implementing nowadays?

AVI SHUA: So, the first-generation CSPMs are reading only the configuration data of the machines. So, for example, if you go for a CSPM, it will see in what network the machine is connected to, who has access to the machine. But they don't go inside the machine. They don't claim they'll do it. They won't let you know if you have a vulnerable Apache server. They won't let you know if you have a machine configured with default credential. They simply don't go into this area. They usually refer customers to integrate a CWPP agent for that. It's outside of their scope.

RENEE GUTTMAN: So the question is, am I displacing other technologies then that I might currently be using? And do I totally get rid of them? I mean, am I going to be able to use your

product inside the company as well? Or am I going to have two different products maybe doing the same thing?

AVI SHUA: So definitely, you are able to replace both the CSPMs and the vulnerability management with a first-generation of the Orca visibility platform. Instead of installing a CSPM and a vulnerability management solution like Qualys, Tenable, or Rapid7, you can get Orca that does both of these roles for you.

RENEE GUTTMAN: Will I still end up running those products elsewhere in my environment, potentially my OT environment or somewhere else?

AVI SHUA: So, in that case, you can replace them for the cloud environment. All of these solutions are sold per seat. So, you can remove the seats from the cloud and use them for the on-prem environment. And in terms of the actual number of solutions in your organization, you can get rid of the CSPMs, which are only for the cloud. So even if you count it by the number of vendors that you are using, you are still not increasing this number.

[00:10:00]

BOBBY FORD: So, I have two questions. The first one is, do you integrate with the SIM? And then the second question is, you say five-minute integrations. Why five minutes? Why not four or three?

AVI SHUA: Can you repeat the last question?

BOBBY FORD: Yeah, so when you say five-minute integration, why five minutes? Why not four or three?

AVI SHUA: Okay.

RENEE GUTTMAN: Because it takes five people, one minute each.

AVI SHUA: So yes, we are supplying the data to SIMs. Regarding five-minute integration, the real reason is because when we say two-minute integration, people think that we are arrogant. It's basically going through 10 steps in a wizard, copying two strings, and giving us access. In all of our beta customers, finding the person allowed to sign the NDA took between 100 times to 500 times of the integration time. Okay, I have a question for you, in fact. We are talking with a lot of organizations, a lot of security professionals, and many times they hear about us and they say, "Okay, that's cool, but I have a CSPM. It provides me cloud security visibility," and they don't understand that they're not protected for the operating system application data layer, that they don't have visibility into these layers. How do you suggest us to approach it from a marketing perspective, from a message to explain that this is simply not enough?

MICHAEL MELLY: Well, I mean, as I understood your solution, on the one hand, you provide effectiveness. You are able to discover the whole lot of the cloud infrastructure that is there that

the other products don't do. And if you don't have a complete inventory, you're always at risk that you miss out something, and therefore, you don't close a vulnerability you effectively have, therefore, effectiveness. And the second thing is about transparency, so you create transparency across the whole stack, and not only on the operating system level, and I do believe that transparency paired with effectiveness -- and those are not two technology-related domains, but they are a big building block in building cybersecurity, and it's not tool-based, but it's a way you're [PH] focused and you provide both of those elements.

RENEE GUTTMAN: So, then I have a question for you. What kind of customers are you targeting, and what does your ideal customer look like right now? I mean, if you have to do that much education, are you prepared to do that, or do you need somebody that's maybe a little more sophisticated? Who's your ideal right now, besides somebody that can write a check?

AVI SHUA: So basically, everyone who have a IaaS or PaaS environment is a potential customer. But we are finding organizations that have large sub-organizations or environments that they are responsible to, but don't have the ability to deploy tools, the most beneficial ones. We've been working with customers that have M&As, that have some subcontractors that they need to audit, that are managing an environment for someone else. And they know that they need to have security visibility, but they simply don't have the manpower and the ability to even start to have visibility inside this environment. So, in these cases, we found it very beneficial because they are willing to jump ship and try it because they understand they have an issue, they understand that they don't have something that can get into the environment for at least a year, and this solves...it's a quick win for them. So, these are our ideal customers currently.

BOBBY FORD: Yeah, that's what I was going to suggest, going after customers that sort of are acquisitive by nature, that have a lot of acquisitions and getting full visibility into those organizations. From a marketing perspective, I would suggest starting with a story, right? Like starting with a story, like how did you come up with the name, right? Why is full stack visibility so important? And then we're all extraordinarily competitive. And if you start talking to us about gaps that we have that our peers, that they don't have, like you'll always have our attention.

AVI SHUA: Thank you.

OFER SCHREIBER: Thank you very much.

AVI SHUA: Thank you, Ofer.