

MALE: As the co-founder and CEO of Orca Security, what problems is Orca solving for and how are you differentiating yourself from other solutions?

AVI SHUA: Thanks, so in order to answer that I'd like to explain a bit how we did in fact security posture monitoring before Orca and what are the problems that we are trying to solve. So back in the day before the cloud environments we had hosts. We wanted to secure hosts, and the most trivial answer is to install security agents on them. Naturally they reside on hosts. They can have full visibility to anything that is running on them, detect any rogue activity in the OS, application, detect data that shouldn't be there etc. The main issue, that I'm sure all of you know, is that you need to install them. You need to install, you need to maintain, you need to upgrade them. And if they are not installed and maintained they are simply invisible to you. So, a different approach that we used to have is to try to scan from the network, deploy network scanners. They try to probe things externally, either using authenticated or unauthenticated mechanisms. And these were basically the options that we have on the pre-cloud world. If you think about it, if you want to scan physical machines there's absolutely no alternative rather than installing agents or scanning from the network. So, we've used these two mechanisms, although they are far from perfect. When the cloud came what we actually did as an industry is to copy what we had. We had network scanners -- physical network scanners -- now we have virtual network scanners. We had agents that ran on the environment, on the physical machine, now they are running on the virtual machines. And we simply added another beast, the cloud security posture manager tools that monitor the cloud configuration itself. So, things like the networks the machines are sitting in, the roles etcetera. And we basically ended up with having the pre-cloud tools moved to the cloud augmented by the cloud security posture managers, tools like RedLock, Dome 9 etc. But we saw two main problems that we wanted to solve. First is the problem of agent deployment, that it does not scale. On average, we saw that organizations have less than 50 percent of their assets are covered by all security solutions. It's almost impossible to deploy everywhere. There is a huge intra-organizational friction in order to get them deployed, and even organizations that put people working full-time to deploy that resulted in a very, very limited deployment. And the second problem is there are simply too many security alerts. On average you can see approximately 10,000 vulnerabilities to every 100 assets. And the reason for that is simply because these tools work in silos. They don't really know the overall picture. So I'll just give a very simple example to explain what I'm talking about. Let's say that you have an internal web server which is open only to one person which is vulnerable to critical remote code execution vulnerability. And the same version of code open to the internet. Naturally the machine which is open to the internet is much more riskier than the one open only to the data science team. But when an agent runs on a specific machine, it doesn't see that. So it simply sends all of the alerts to the security team and they need to combine this data manually and they cannot really do that because these tools don't see the overall picture.

MALE: So, talk to me about how Orca is solving this in a different manner. What's the differentiator that you're actually showing in your thought process and in your technology?

AVI SHUA: Okay, so we thought about: is there a way to do it completely different for the cloud? To understand that the cloud is no longer a set of physical machines sitting in a dark cold server room connected to the network, and to utilize the fact that everything is virtual and

running on the shared public cloud providers. And we came with a technology that we call SideScanning. It's a patent-pending technology that we've invented that has several unique benefits. First, it provides complete coverage. The entire cloud estate is covered within minutes and providing superior security -- much better than we had in the local data center. And I know this promises a lot so let me explain a bit how it works. So, first, we don't require any agents, we don't require any network scanner, we don't require any CSPM, nothing like that. And yet we're able to detect the risks within the workloads without any agent, without any scanners, literally without sending a single packet, without running a single opcode in the environment.

[00:05:00]

Instead of interfering with the environment, we collect the data directly from the workloads' runtime block storage. This is in fact the unique differentiator and the "secret sauce" about Orca, and we combine it with the cloud metadata. Instead of integrating with each and every workload requiring network access to it, requiring credentials or installing the agents, we read it from the common shared virtualization environment. And this allows us to gain the immediate understanding of everything, of all of the major risks in the environment. So, in the end you're getting a much more comprehensive visibility because you don't need any per-asset integration. It's complete. We detect everything that exists now and in the future. It's not like you managed to deploy it on 100% of the environment and it's going to go lower because you haven't added people to maintain it. And it's 100% zero impact. And it absolutely doesn't have any effect on the workloads because we don't install anything on them. We don't change anything on them. We had Fortune 500 customers that onboarded their entire cloud estate within a week, and there's absolutely no other technique that could allow that. After they integrate it, we're able to detect the risks that matter most. Things like vulnerabilities in the OS, packages, libraries, misconfigurations; machines that are already compromised. We call it the neglected workloads -- machines that nobody's been maintaining in the organization for years. Many times they're already compromised by the time we see them. And the sad thing about that, it's very easy to detect if you reach this machine. It's always a matter of reachability. Risk of lateral movement, machines that have keys that can allow accessing many others. We see it all the time that due to poor hygiene on some machines, someone left AWS keys that have root access or SSH keys that allow accessing the entire environment, etcetera. And we do all that for all of your environment literally within minutes. So, at the end of the day, we are providing the superior security because it's agentless deep scanning. We're able to see the risks in each host, but we put it within context and prioritization based on the cloud configuration. This is a cool thing that cloud allows us that didn't exist on the pre-cloud world. You don't only see a machine, you understand its location in the fabric. You understand whether it's connected to an internal network or external network. You understand which ports are open. You can get all of this data in a very normalized fashion that allows to provide a holistic prioritization and understand which risks really matter more for you. So let me just take another minute or two to explain how we do that because many people don't really understand how it's possible to read all of this data without talking to the environment, and what was in fact the change that allowed that. So, let's look at machines and environment and how we reach the situation that exists today. Before the cloud was used before virtualization, we had hosts, physical machine with CPU memory and disks on them. And we had on this, running the operation system, application and the data. When virtualization came,

we simply ran on the same virtual host, on the same physical host, a few virtual hosts. And after that came the concept of virtualization clusters. Why should they care on which physical machine my workloads run? Let's just take a bunch of physical machines and treat them as my shared pool of resources. But it didn't scale very well because of many cases you needed to move data. So, the manufacturers moved to an architecture where the storage in fact sits physically on a different box. There is the shared storage box connected via high-speed fiber optics and shared between these physical compute nodes. And what we do in Orca is that we run on an independent host, additional virtual machine, that the setup is done by granting it the read-only access to the account storage. And when we get that, we absolutely don't affect the host because we don't run on the host. We don't talk with them at all. We get the view to the data, the virtual drives, and then we start assessing it. We virtually reconstruct the bits and bytes to the block levels, and then we reconstruct the file system. We build the operation system application and data all on the virtual read-only view and look for any risks that are found in them. So, we in fact have full runtime access to everything that the host uses, meaning it's not only external blackbox view. It's white box. We see every bit and byte on the system.

[00:10:00]

Now we take this view to logically ingest security into the environment. We scan the block storage of the running virtual machines and continuously analyze your environments without any agent, without any effect to it. So, at the end of the day, I truly believe that this is the right way to do security in the cloud. First, you get complete visibility. You see exactly what the host sees. It's run time. It's not initial time. It's immediately attached. New hosts are automatically scanned. No need for organizational friction. Absolutely zero impact. Read-only. We scan on our hosts. We don't have any performance penalty. There is no way it can create any effect to the workloads. Completely VPC agnostic, no need for credentials, no need for integrations with another system for that to work. And another cool side effect, it's tamper-proof. Because we don't run the scanning code on the target environment, even if the host is compromised and has a root kit, it doesn't affect us. So, this is the seamless delivery that we're talking about.