

Orca Security: Deep Cloud Inspection



The cloud security market is highly-competitive, diverse, and often confusing. There are over 2,000 IT security startups out there, so what makes Orca Security so special? In this video, Eric Gold interviews Avi Shua, CEO and co-founder of Orca Security about SideScanning, a radically new approach that secures the entire cloud estate and helps meet compliance mandates, but without disrupting business operations in live environments. With it, Orca is able to read your cloud configuration and workloads' runtime block storage out-of-band, giving you workload-level security across AWS, Azure, and GCP — without the gaps in coverage and operational costs of agents.



Transcript

0:00 Eric: Hi, there. My name is Eric Gold and I'm with Orca Security. I'm here with Avi Shua, the CEO and founder of Orca Security. Today, Avi is going to talk about the very innovative novel technology of work called SideScanning. But before that, Avi, I'd like you to provide a little bit of background—how did you become a cybersecurity expert?

Orca Security Ltd.
Exhibit 2133
Wiz v. Orca
IPR2024-00863, -00864, -00865
Ex. 2133-001

0:00 Eric: Hi, there. My name is Eric Gold and I'm with Orca Security. I'm here with Avi Shua, the CEO and founder of Orca Security. Today, Avi is going to talk about the very innovative novel technology of work called SideScanning. But before that, Avi, I'd like you to provide a little bit of background—how did you become a cybersecurity expert?

Avi: Thanks, Eric. In fact, I have been involved in cybersecurity during my entire adult life, even before it was called cybersecurity. I started in high school, this area really excited me. I moved to the Israeli intelligence, and served in unit 8200 for almost a decade. And after that, I moved to Checkpoint. I've worked in various roles over the last four years. During this time, I was always excited about how attackers are really penetrating things, and more importantly, what is the best protection from them.

Eric: And my understanding is that when you founded Orca, you actually did that with a few other people from Checkpoint as well.

Avi: Yes. In fact, we are a pretty unique group of founders. We are eight co-founders. All of us are executives and architects from Checkpoint. In terms of experience, we have more than 150 years in combined experience in building a cybersecurity product that protects the vast majority of the Fortune 500 companies.

Eric: And when you started Orca, you actually received quite a bit of seed funding, \$6.5 million. Is that a record for Israeli cybersecurity companies?

Avi: I don't take benchmark but it's certainly on the high line.

Eric: Okay. I mean, for seed funding and not even series A, that's quite impressive. So, Avi, today what I'd like you to do is just explain to us, you know, there are so many security companies out there, what's so special about Orca?

Avi: Okay. So definitely when you look at the cloud security market, you think that one thing that the world doesn't need is another cybersecurity company focused on the cloud. There is, I think, dozens of these companies. But when I looked at this product together with the other co-founders, we haven't asked how many companies out there this question, but a more basic question, is there a solution that they can simply deploy? And will alert if I have, let's say, a vulnerable asset in my environment? And it must always work, not after I run through four months deployment, it will cover 80%. Is there a solution that can alert if I have a machine with even known malware in my organization that I can trust it will always work? And unfortunately, the answer is no. There is no single solution out there that can generally answer this question for all of your cloud environment. All of them overlook disclaimers. It will work if you've done that, it will work if you integrated that, and these are the processes that organizations simply cannot follow. So we wanted to create something really unique that can answer this question and work 100% of the time for all of the assets.

Eric: Avi, I am quite literally sitting on the edge of my seat right now. I want to know what is so special. What is the secret that you're alluding to? What is the tech behind this?

Avi: Thanks. So let me show some slides that might explain. So one sec. Okay. So essentially what we've created is the Orca cloud visibility platform. It's a five-minute one-time integration, which is not of the kind of let me change something in your system and pray that everything will work afterwards. It's an impact-free, read-only-based integration that you can do without any concern for all of your environments and get the full-stack visibility. And when I say full-stack, I mean, both the control plane like other solutions, but and this is the unique part to the operating system, application, and data. And it's not only for a subset of the asset, it's for all of the assets for now and forever. Everything that will run on the cloud environment will be visible. And this is truly a value proposition as we are the only company that can provide this. And as I said, it's based on a unique technology, which we call SideScanning. I am the inventor of this and it's in patent-pending phases. The idea is that SideScanning, like other solutions, collects cloud configuration, but unlike them, we integrate with cloud infrastructure to read the virtual machine's runtime block storage. This is the unique part about

run on the cloud environment will be visible. And this is truly a value proposition as we are the only company that can provide this. And as I said, it's based on a unique technology, which we call SideScanning. I am the inventor of this and it's in patent-pending phases. The idea is that SideScanning, like other solutions, collects cloud configuration, but unlike them, we integrate with cloud infrastructure to read the virtual machine's runtime block storage. This is the unique part about it. We do not rely on the machine themselves to report the posture, we do not rely on something running on them, we read it from the side and this is why it's called SideScanning. Does it make sense?

Eric: It sort of makes sense. But don't the cloud providers give you APIs already that can provide this sort of information? What's so special about SideScanning? I mean, you can query an API of the cloud provider and ask me what instances are out there and for attributes are those instances.

Avi: So, you're completely correct. The cloud providers provide APIs that allow within the metadata. Metadata meaning, for example, the name of the machine, the network it's connected to, even the image that it started from, but it doesn't provide easy access to what's running currently, for example, what application installed, whether it's patched not, what are the files, where the database was installed or even what operations it runs currently in case it was upgraded. It does provide APIs that we are using in quite a novel way that read the underlying block storage and the underlying virtual hardware, and we read these bits and bytes. And from them, we reconstruct the stack to have this kind of full-stack visibility.

Eric: Interesting. So it sounds similar to deep packet inspection because when you're talking about reading bits and bytes, and then reconstructing from those bits and bytes, is it like a deep cloud inspection or a deep cloud acid inspection that you're talking about here?

Avi: So yes, I think this is a great name to put it. This is a great way to do deep inspection, but it's not only deep, it's also seamless and wide. Due to disintegration, we can do it for all of the assets and all of the time, and this is a unique part of that. Let me explain why this is a unique way that wasn't really available before and why I say it is the right way to do securities these days. So please picture yourself as an engineer in a major security assessment company 20 years ago. And this was your world, you're at servers sitting in a dark and cold server room with a hardware CPU memory disk operating system connected to the network and you need to assess them. You don't have a lot of options. One option, there must be the one, is to go from the network sent packets, authenticated, unauthenticated, etc., get the responses, and by that, building the security posture. The other option is to install a security agent. The agent will read the data and will report it back to the mothership.

If you think about it, these are your options. You are bound by that, you can't do anything else. This is a server in a different room. So all of these companies that are, in fact, founded more than 20 years ago, created these solutions, network scanners, authenticated, unauthenticated agents, and has been selling them for the last 20 years. But things have changed, the rule of the game has changed, and they haven't noticed it. And as Abba Master once said, 'if everything that you have is a hammer, then everything looks like a nail.' When the cloud arrived, they simply took the same approach with its cons to the cloud without men noticing that there is a better way. If you look at it, virtualization came afterwards. I know it's, you know, ancient history by now, but when security assessment started, virtualization wasn't a thing. Shortly after virtualization came the concept of virtualization clusters. Why should I care about which physical machine my workload runs? Let us treat a bunch of physical servers as a shared pool of resources. But there was one issue, if you simply take many commodity servers and make a shared virtualization cluster out of them, then when you need to scale up, take a machine out, etc., it's slow because it sits physically on one disk.

Eric: Avi, on this slide, what are these spinning boxes on the bottom here? What are those representing?

Avi: So think of them as the virtual machines that need to move between servers.

Eric: Okay.

Avi: That when you scale up and down, you need to copy and move the virtual machines between the

Avi: So think of them as the virtual machines that need to move between servers.

Eric: Okay.

Avi: That when you scale up and down, you need to copy and move the virtual machines between the physical servers, which is very slow. So, therefore, Dell Critic tool evolved. And if you go to a modern data center, you won't see commodity servers with disks on them, but you'll see a separation of the storage from the compute, and this is one thing that it turns [inaudible 00:09:57].

There is a different server with the block storage and other complete servers connected via high-speed fiber optics. Okay. And this means different rules for the game of security assessment. Because if you go and fast forward in time, this Critic tool became more and more capable and the cloud providers are using more and more capable hardware to perform this multi-tenant virtualization. And what we are doing, and this is the unique part about our technology, we run on the same data center via APIs and read the same data that the workload reads. Think of it as if 20 years ago, you had another interface in each server that the scanner and a magic cable connected to it. And this interface allowed you to read everything, and this is exactly what we have currently. These disks are not physical discs anymore. These machines are not physical machines, they are virtual entities that are provisioned on a virtual data center, and therefore, you can read them from the side or from the bottom depending on the way that you want to picture it to self. But we are reading them without the operation system involvement, without anything on XPLs. This is why we are completely VPC agnostic. We don't need credentials, and we can reassure you it will scan anything. And then...

Eric: So I'm confused, Avi. When I look at this slide if you can just go back one to make that bigger there... So, is Orca installed by the cloud provider? How does it get integrated with these multi-talented to Company B and Company C so it can look at their stuff? It looks like they're all in one box here. How does this get glued together?

Avi: So thanks for the question. In fact, think of the red part as the virtual part. Physically, all come once on the same data center like the customer workload. This is critical for performance. It would never be possible if we ran in a different data center. But logically, it's a side server. It's delivered as a complete side service, sorry, that is getting permissions to the customer environment. All the customer needs to do is to follow a short three-step integration to allow Orca to read its workloads. And then behind the scenes, it launches a virtual scanner. It reads the same data that the customer doesn't need to manage, doesn't seem to do anything about, we simply do it for him. So physically, we are the same, that center logically as a service.

Eric: So this side service, is it sort of accessing the same underlying data as Company B and Company C here but out of band without affecting their performance?

Avi: Exactly, yes. We are reading the exact same data from the side. And it's not the initial images of that to emphasize, it's the one-time data. If B changes, we see it. If the BI changes, we see it. Now regarding the performance, this is indeed something that many people are concerned about. But if you think about it, these discs are not physical disks. You're not bound by the physical hardware of this block device. These are provisioned entities that also have the performance characteristic provisioned. So when the customer launches a workload and ask for, let's say, 1000 tiles, and we launch a different scanner and ask for another 100 high ups for the times of the scan, it doesn't take from the customer performance metrics. It's simply additional performance metrics. You're not within the actual Amazon data center performance limits.

Eric: So it's almost like if someone had mental telepathy and they could read someone else's mind. They wouldn't slow down that person's mind by reading their mind because the person who has the ESP would be using the processing of their own mind when doing that.

Avi: Yes, you're correct. And I can also testify that we tested it in the most extreme conditions of workload that 100% of the time the St. James' random data with CPUs working for 100%, we haven't managed to measure any performance impact. And this is also possible due to improvement to the cloud providers done on there and in the last one or two years.

Avi: Yes, you're correct. And I can also testify that we tested it in the most extreme conditions of workload that 100% of the time the St. James' random data with CPUs working for 100%, we haven't managed to measure any performance impact. And this is also possible due to improvement to the cloud providers done on there and in the last one or two years.

Eric: Interesting. Continue.

Avi: So essentially, if you think about it, these providers are really unprecedented access to data with seamless integration, which is the holy grail of security assessment. You want to see everything seamlessly and this is the way. We see every bit and byte of the system together with cloud configuration that allows us to make in context. We see those binaries, the configuration log files, all of the installed applications, as well binaries configuration logs, the business data on files and databases and we were able to scan recursively into containers as environments. So if you have containers, we simply scan them, again from a virtual hardware side. And another cool thing, this is a much better place to do security, because we do not run on the same things that we assess. So if let's say there is a rootkit or a very capable malware that tries to attack the security mechanism, it doesn't affect us because we don't run on the same machine. So this is a cool side value of that.

Eric: Interesting. Now, when you're looking for vulnerabilities, I remember you telling me that there were some things that you could do that were sort of special for work because of this capability. One of them was to even look for weak passwords.

Avi: Yes. So let me open the UI for a second to show it. We see ourselves as a security assessment... let's see, a security assessment solution in the widest possible way and not vulnerability management because vulnerability management is a critical part, but it's not the only critical part. There's a lot of things that can cause a breach, and a weak password is one of them. If one of your assets is using a leaked password, or a weak password, this is something that attackers can easily use in order to get in. So the way that we do that is when we read the data, we match the local password files with either the common password and leaked password databases. Even if you're using a password that is similar to a LinkedIn password that is leaked, and the username is similar, we'll be able to detect that. We see the username, we look for similar usernames that have leaked so even if, for example, your name is Eric Gold and the username on LinkedIn is called eric2@gmail.com, we'll try the permutations that are an attractive permutation. And if they match, we're able to alert on that because this is essentially what that the attacker will do in order to try to get into the organization.

Eric: But aren't these brute force methods of comparing passwords very expensive as far as CPU? Doesn't that slow things down? And if you're doing that, couldn't that impact the running applications?

Avi: So we're doing it completely on the offline copy. If you think about it, think of an ATM card for example. The reason it's secure to have only a four-digit ATM card is because something will block it after three or four attempts. It's not because it's how to enumerate 1000. And as we are doing it offline, we are in fact bypassing the brute force protection mechanism for the customer. And by that, we can do this thrice without any damage. It's simply done on the scanner CPU.

Eric: So I get that, but I'm assuming besides checking for weak passwords that there are other vulnerabilities that you're going to show us. But does that mean that Orca has to become an expert in developing all these different technologies to look for misconfigured machines, weak passwords, and common vulnerabilities? Isn't it hard for a small startup like yourself to develop an expertise in all of these areas?

Avi: So first, we do have people that are experts in cybersecurity and obvious but, of course, we're not trying to implement everything. This would be completely irresponsible to do. Our differentiator and unique capability are getting into each and every asset and being able to scan it in a seamless way. And we see ourselves as a platform. We combine capabilities from OEM and other providers, like for example, anti-malware scanning. We scan each and every one of the assets all of the time. And we haven't developed our own anti-malware engine and our own anti-malware signature. There are good players that have been in this market for decades of years. The same goes for vulnerability databases.

unique capability are getting into each and every asset and being able to scan it in a seamless way. And we see ourselves as a platform. We combine capabilities from OEM and other providers, like for example, anti-malware scanning. We scan each and every one of the assets all of the time. And we haven't developed our own anti-malware engine and our own anti-malware signature. There are good players that have been in this market for decades of years. The same goes for vulnerability databases. We are not trying to build one by ourselves. And for leaked password databases, we are not trying to source all by ourselves. We've partnered to get it, but it's not an app store. It's not that you need to mix and match. We choose the right things and we integrate them tightly to the kind of data that we have in order to make a solution that makes sense.

Eric: So if I have this right, all this is based upon the SideScanning. The SideScanning is the enabling technology that gives you access to the underlying bits and bytes that describe the running cloud environment. And then from that, you can reconstruct a model of everything, even the instances or cloud assets that the company might not even know about. And then run a series of best-of-breed tests on that model to look for misconfigurations, vulnerabilities, etc. Do I have it right?

Avi: Yes, you have it exactly right. And I think that you've mentioned the assets the company doesn't really know about because, frankly, the most important things that we detect are what we call the neglected assets. The asset that...

Eric: Can you show us some of that in this demo screen here?

Avi: Yes, of course. Let's share, for example, this is definitely a neglected asset, a machine web server that hasn't been patched since 2014. So if you want to see the entire list of vulnerabilities, you can do that. But essentially, the main problem, in that case, is that this machine is out of the patching cycle, it's simply unmanaged. And we see in almost every organization that we'll reach, a significant percentage of assets that no one is maintaining, maybe it is a project that was neglected, maybe it was created but someone who is not into IT never bothered to give the IT the credentials for the machine.

We saw even a case where those in a public-facing SFTP server with customer sensitive data with a weak username and password. And the reason it wasn't neglected from the business side, they've been using this every day for uploading customer logs when the technician was going there, but they never knew about it. If you'll ask yourself, "What tools do they have before Orca to detect it?" The answer will be none. Because it's simply easy to instance that someone created not in the IT department, even gave the keeper to the security. Not because he wanted to do anything bad, he simply didn't know that he needed to do it. He followed the wizard, created an easy-to instance, set an SFTP server rightly because he needed to upload and download customer logs, thought of a password, a four-character common word looked to him like the right one, and it worked that way.

And we said in many, many areas machines that are end of security support, machines that are sometimes already infected by malware by the time that we reach it. And this is why I think that when we talk about detection rate. We shouldn't really focus only on the percentage of the attacks, malware, etc., the distribution can detect once you reach the asset, you should multiply it also by the number of assets, whether it reaches 100% of your organization or 80% and how frequently it scans. It is only a point of time scanning, and many times, this point of time scanning isn't good enough because sometimes, and we saw it also within our customers, something is not known to be bad a year ago, but is known six months ago. So if you scan it only in the introduction time you won't detect it. So if you look at the time limits of the scan, percentage of the organization that is scanned, and the detection rate, this is the true detection rate—the true, effective detection rate that you need to maximize. And this is exactly the reason that we implemented it the way that we do.

Eric: Avi, can you show us some other examples or findings that Orca helps you to discover?

Avi: So before I go in and try to explain a bit about the philosophy, we are trying to think like attackers, as hackers, specifically what they will do what are they going to do when they want to breach your network. So essentially, the most important thing that they look is for the neglected assets, for the weak link in the chain, such as machines that are unpatched or have weak passwords. And this is

Avi: So before I go in and try to explain a bit about the philosophy, we are trying to think like attackers, as hackers, specifically what they will do what are they going to do when they want to breach your network. So essentially, the most important thing that they look is for the neglected assets, for the weak link in the chain, such as machines that are unpatched or have weak passwords. And this is naturally one thing that we are focused on. Afterward, you know, you don't want any server to be breached, that's for sure, but it might be. Never assume that servers will not be breached. And if they are, the next things the attacker will look for is for a way to perform a lateral movement, and this is in the way of private keys that are on these servers, access keys, secrets on the same machines. The histories in bash history...password, sorry, in bash history that can allow users to access the different sites and we are looking for all of these. So in that example, there is an insecure private key, a private key that exists near the public key. It allows the attacker to perform a lateral movement.

Another common example is sensitive data in Git Repository. We see it almost always. Machines that are public-facing web server that a developer put in Git Repository because they needed to debug something, etc., and the Git Repository have access keys. So in that case, which is by the way very similar to what happened in Capital One case. The attacker managed to breach a server and then looked for keys that allow him to download everything, in fact, the keys to the kingdom. So this is why we are focused also on the data part. And I truly believe that the, let's say, tier-one idea gen and tier two are the most important. How to prevent people from hacking into each asset and if they manage to prevent them from progressing into the organization. And this is exactly the things that we are looking for.

Furthermore, when we are providing the left, we understand that many times the attacker...sorry, the security team don't really know about this machine a lot. It might be only the name of the, you know, machine that you saw under that and you need to do trials. So we try to provide as much as we can, as lightweight forensics briefcase on the machine to be able to better understand what this machine is about. For example, what application I installed, what Git Repository, if there were logins, what are the recent login attempts, etc. In other cases, if there is, for example, a database server will show the name of the tables on that specific machine and when to test access. Think about it, it has a completely different meaning if this is a server that if let's say a test database or a four terabyte database with customer names and security team need to know immediately. I think that many times...

Eric: Sorry, I guess all this is where, when you were talking about deep, this is where you're going real deep because other tools don't go this deep when they're assessing security risks for cloud assets.

Avi: Exactly. They usually don't do it because they are based on integration that don't allow them. If you only take metadata, you can't see that deep, so you're only based on the metadata. And this is what causes them to go for solutions like trying to go on traffic flow logs, etc., which has very, very limited visibility. In fact, traffic flow logs are like '90s firewall security only [inaudible 00:27:53] we do. It can't really get to the bottom of what data is being transferred, whether there is an attack on the machine. It all boils down to what is the source of the data, you can't make a lot of data if you don't see the right data.

Eric: Avi, when I'm looking at this screen, I see one little menu choice called assets. What's that?

Avi: So one thing we figured, is that besides scanning for alerts, we have a unique view of everything that you have inside your environment. So it's valuable even regardless of whether you want to search how many machines do I have but not only based on the metadata, which machines, let's say, have a one end database server on them? Which machines PII on them, for example? Which machines have databases with more than half a gigabyte? Which are running Nginx web server, for example? So these are all things that we deduce and it's not based on metadata. Unlike other solutions that will show a different similar demo, and it's based on if someone bothered to write in the metadata that this is an engineering server, this is actually based on what's running with no agent, no integration to the credential. Essentially, I haven't shown it but so now a three clicks integration process, and that's it. Three steps, 20 seconds, 24 seconds, and that's it.

show a different similar demo, and it's based on if someone bothered to write in the metadata that this is an engineering server, this is actually based on what's running with no agent, no integration to the credential. Essentially, I haven't shown it but so now a three clicks integration process, and that's it. Three steps, 20 seconds, 24 seconds, and that's it.

Eric: So those are little videos there which help explain how to do it. Okay. Got it.

Avi: Yes, exactly. And this is essentially minutes and then you're done. And this is very unique.

Eric: And when, when you're using Orca, and this SideScanning to grab the data and then Orca models it and does the analysis, how frequently does it happen? Is it every minute, every hour every day? How often does it run?

Avi: So essentially, if you run continuously, at least daily and we also monitor for events that trigger rescanning. For example, if in your server is launch, or there is a major change in the control plane data, it will cause us to rescan the environment.

Eric: Okay. Avi, I was taking some notes as you were talking here and I just want to ask a few follow-up questions. You know, this UI looks very beautiful, very polished. But once you get into large numbers of cloud assets and lots of findings, it's going to be difficult to scroll through everything. Is there a way to automate this using APIs that it can roll up into other tools?

Avi: Yeah, sure. So definitely everything that you see here goes to the public API. The UI has the exact same capabilities as you can. And furthermore, we integrate with solutions, like JIRA, Slack, and more to create tickets that you can monitor from more than just our console. We understand that people don't want to use the Orca console but editors.

Eric: So you have a robust API that can do everything that can be done in the UI?

Avi: Exactly. The UI in fact uses the same API.

Eric: Okay, got it. Got it. Avi, you know, we could obviously talk about this in a lot more detail. I just have one more question before we wrap up today. What's coming? What direction are you going with this? What new features are you working on?

Avi: So essentially, we are in...we are creating more capabilities into running also within server lists. As of today, we don't run within the server list environment. This is a major capability that we are adding. We are currently supporting AWS onshore (?). Adding GCP support is something that some of our customers are very focused on. We are also creating a mode where this will be fully hosted. The request of some of our larger customers who don't want to use our service, they want to have anything within their account so this is an additional important feature. And last but certainly not least is that we are always beefing our security research team to detect more important capabilities, and another last but not least is visualization. Let me show how it will look within a few weeks. We're going to show in fact, the same findings in a map that will make it much easier to understand the location of this service. In fact, it can affect you based on the environment because it's completely different whether a vulnerable service internal or internet-facing network.

Eric: Can you go back to that SideScanning slide?

Avi: Sure.

Eric: You know, I remember one interesting story you told me about a CSO who said that he was frustrated by the fact that when he needs to audit the organizations that are using the cloud within his company, he has to ask them for favors to install agents and network scanners so that he can do his audit. I guess with this approach, he wouldn't need to ask for any favors. He would just say, "Grant Orca the appropriate privilege and I'll do it myself."

Avi: Exactly. One of the important values that we see is that we dramatically reduce organization friction. Large organizations are very complex and many times they cannot really work together to get out, their priorities are different, etc. It is much harder in cases of M&A subsidiaries. And we saw cases

Orca the appropriate privilege and make it my own.

Avi: Exactly. One of the important values that we see is that we dramatically reduce organization friction. Large organizations are very complex and many times they cannot really work together to get out, their priorities are different, etc. It is much harder in cases of M&A subsidiaries. And we saw cases where the security team didn't even imagine that they'll have visibility into a subsidiary or similar and it's simply because they haven't even established working relations by the time, you know, acquired company subsidiaries that run within different time zones. And then you say, okay, let's simply run Orca and within minutes there you see, and it also creates the baseline of the discussion of not being the panel you see so, "Oh, I need you to check this, I need you to check that because I'm old." It actually sees the risks.

We saw cases where a company was acquired, and the entire database and entire website were running on a vulnerable web server that was simply unpatched since 2016. And it essentially simply gave the answer, and this allows a much better way to progress rather than saying, "Okay, I need you currently to install a network scanner but no, it will delay the integration by two months, let's prioritize it, etc. It's simply a few clicks and it's done, and this is why I truly see the seamlessness as a security feature. It's not only a usability feature instead of putting five days into the integration or five months, it's three minutes. It's the ability to actually see and install it on each and every environment. This is the critical security feature because the environment it runs in is what will likely lead to a breach.

Eric: Avi, thank you very much for that. I think that's a great concluding warning that it's the things that...it's the assets that you don't know about or can't see that will lead to a breach, and Orca helps you to see not only the assets that you know about but also the ones that you don't know about.

Avi: Yeah, this is the important part. Not only knowing, but knowing what's inside, and this is the difference.

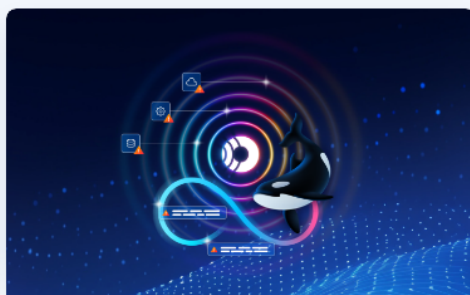
Eric: Got it. Avi, is there anything else you'd like to add today, or do you think you've covered everything you wanted to talk about?

Avi: I can talk for hours but I think that for the sake of time, that this ends on a good thought. Thanks, Eric.

You might also be interested in...



ORCA LITERATURE



BLOG



BLOG

Orca Literature

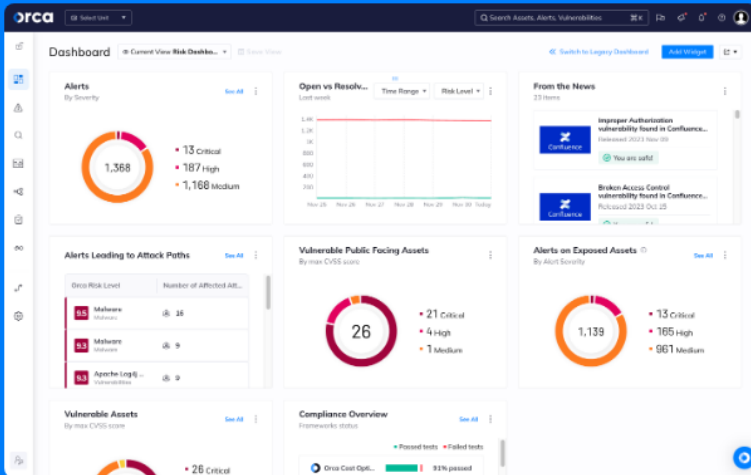
Orca Sensor Datasheet

BLOG

Resolve alerts efficiently with dynamic risk prioritization for the cloud

BLOG

Improved Accuracy and Transparency: Custom Data Detection with Orca DSPM



PERSONALIZED DEMO

See Orca Security in Action

Gain visibility, achieve compliance, and prioritize risks with the Orca Cloud Security Platform.

Get a Demo

Platform

CLOUD SECURITY PLATFORM

- Cloud Native Application Protection
- Vulnerability Management
- SideScanning™ Technology
- Container and Kubernetes Security
- Cloud Security Posture Management (CSPM)
- Cloud Infrastructure Entitlement Management (CIEM)
- Cloud Workload Protection Platform (CWPP)

Solutions

BY SOLUTION

- Malware Detection
- Sensitive Data Detection
- IAM Risk
- Lateral Movement Risk

BY INDUSTRY

- Financial Services
- Technology
- Government
- Media & Entertainment

Resources

Library

- Product Info
- Podcast
- Case Studies
- Blog
- Events

COMPARISONS

- Prisma Cloud
- Qualys TotalCloud
- Lacework
- Rapid7

Company

About

- Partners
- Reviews
- Orca Research Pod
- Careers
- Newsroom
- Media Kit

Contact

Support

Security Portal

Stay in touch

Get cloud security insights and the latest Orca news

* Email Address

Submit

Awards & Certifications

- Management (CSPM)

Cloud Infrastructure Entitlement Management (CIEM)

Cloud Workload Protection Platform (CWPP)

AI Security Posture Management (AI-SPM)

Multi-Cloud Compliance and Security

Cloud Detection and Response (CDR)

Application Security

API Security

Data Security Posture Management (DSPM)

Orca Sensor
- Financial Services

Technology

Government

Media & Entertainment

Healthcare

Retail
- Prisma Cloud

Qualys TotalCloud

Lacework

Rapid7

Tenable

Check Point
- Contact

Support

Security Portal

User Center

Login
- Awards & Certifications

✓ AWS Advanced Technology Partner Security Competency

✓ ISO/EC 27001 Information

✓ ISO/EC 27017 Information

✓ ISO/EC 27018 Information

✓ SOC 2 TYPE II Certified

✓ 2022 AWS Global Security Partner of the Year

✓ Star Level One: Self-Assessment Cloud Security Alliance

✓ CSA Trusted Cloud Provider Cloud Security Alliance

TECHNOLOGY ECOSYSTEM

- Integrations
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- Oracle Cloud
- Alibaba Cloud



