Orca Security Helps BeyondTrust Secure Cloud Services Used by Thousands of Customers

BeyondTrust

INDUSTRY
IT Security

CHAMPION
Morey Haber: CTO & CIO

CLOUD ENVIRONMENT
AWS, Azure

> "Orca Security manages all of our cloud-based privileged access management (PAM) solutions today."
>
> **Morey Haber**
> CTO & CIO
> BeyondTrust

Cloud Security Challenges

- Using an agent-based security tool had grown too complex and costly to manage; it had also failed to provide sufficient visibility
- Agents can't load on the company's customized appliance images
- Needed reporting to help assure compliance for ISO, SOC, CIS, and PCI

Cloud Security Results

- Was in full production within two months; fully integrated through Azure Sentinel Security Center – includes ticketing with ServiceNow, Jira, and a variety of other integrations
- Able to secure and monitor cloud solutions sold to customers without adding risk to production environments
- Reduced development and QA time by 1 ½ FTE while providing broader visibility and more actionable assessment results
- Orca reports show compliance evidence pertaining to passwords, firewall configuration, vulnerabilities, and more

BeyondTrust Delivers Cloud-Based Privileged Access Management to More Than 70% of the Fortune 500

BeyondTrust is the world leader in privileged access management, empowering organizations to secure and manage their entire universe of privileges. More than 20,000 customers – including more than 70% of the Fortune 500 – use BeyondTrust's three core solutions to secure their environments and gain the control they need to reduce risk, achieve compliance, and boost operational performance.

Morey Haber fills several roles at BeyondTrust. As CTO, he oversees product strategy. He's also the company's CISO, which makes him responsible for internal and cloud security for over 4,000 cloud deployments used by customers. And he oversees all governance, risk, and compliance efforts.

Twenty of Haber's 20 years in IT have been devoted to cybersecurity aspects. He has authored several books on attack vectors and vulnerability management strategy and was director of security engineering for a company acquired by BeyondTrust. He understands what is needed to detect technical shortcomings that put companies at risk.

Orca Takes a New Approach to Cloud Security

Following a demo of Orca Security, Haber was intrigued. "I was floored. In all my years specializing in vulnerability management strategies and products, this is a completely new approach with so much potential."

Haber and his cloud team ran a trial of the Orca platform. "We had it installed, and it was working for us within a few days. It produced better results and more visibility than competing agents ever gave us. Before Orca, agents only gave us visibility into instance runtimes, but they didn't show us the rest of the environment," says Haber. "We were very impressed. Orca is now fully rolled out, managing all cloud solutions that we sell today."

Orca Secures BeyondTrust's Customer Workloads

BeyondTrust represents a unique use case for Orca Security. While most Orca customers use it to assess their own cloud workloads, as a security vendor BeyondTrust monitors workloads running cloud solutions being used by its clients. Today the company supports more than 4,000 cloud deployments, with many more planned as BeyondTrust continues its rapid growth.

"I've been working with vulnerability assessment solutions for over 20 years. I even wrote a book on how to build vulnerability management strategy. I've never seen anything like the Orca Security platform before. This product is a gem."

Morey Haber
CTO & CISO
BeyondTrust

Haber cites one example of how he's using Orca today. "BeyondTrust's Privileged Remote Access enables third party access to a client's environment to check out things like an HVAC system, make sure printers are working, or whatever the need might be. Our solution performs a credential injection to target systems, so the third parties don't know or see the passwords at all. Once they've logged in, the product screen-records and documents everything they're doing enabling a true zero trust architecture for remote access."

"Orca helps make sure nothing is open or misconfigured, that no instances are missing patches, and that no vulnerabilities exist in our client's cloud environment," says Haber. "Here's another example where Orca showed significant value. We installed a new firewall for one of our products. Orca quickly flagged that a misconfiguration existed in the default settings and we were able to correct it right away. How else would we have seen that? An agent wouldn't have helped since it was on the outside, but Orca caught it. To me, that is invaluable."

> "Orca helps make sure nothing is open or misconfigured, that no instances are missing patches, and that no vulnerabilities exist in our client's cloud environment."
>
> **Morey Haber**
> CTO & CISO
> BeyondTrust

Problems with Agent-Based Solutions

BeyondTrust uses an industry competing solution for traditional vulnerability management of its internal resources and laptops. Before finding Orca, the company attempted its agent-based technology for its cloud-based solutions but ran into numerous problems. "With the infrastructure and knowledge of that tool, we decided to use their agents within our products. The idea was to deploy an agent with each one of our virtual machines," says Haber.

"It takes multiple virtual machines to make up an instance for a client, plus all the backend plumbing. The costs were reasonable, but the DevOps chain – the pipeline to get it certified, build it, have it connected, runtime, update, and everything else – took about six months to implement. And keeping all those agents running as we onboarded hundreds of clients during our exceptional growth was a pain. Very quickly, it became apparent this was going to be difficult to manage."

Haber explains that when it comes to the cloud, if he is given an agent bundle to include in one of his product offerings, it has to be included from the early stages of development, through QA, and into production. "We have to set up the environments to handle the agent in each stage to make sure it works, getting the output of data, and then ensuring it's not crashing. When you start having thousands of agents out there, one or more will eventually break or fail to get updates. Then we have to troubleshoot and subsequently update a customer's production environment. That's a change control and compliance nightmare that is best to avoid entirely."

Orca enables BeyondTrust to avoid those problems. “With the Orca, I’m relieved of the time and investment agents require. I’m not paying for the runtime of an agent hitting a CPU, and I have no change control risk of bringing an operations team member into a production environment.” On cost savings, Haber says, “Agent cost per client is about $20 – $30 per year. When scaled across hundreds and thousands of clients, the cost of using agents becomes significant. With Orca, we don’t have to consider any of that. I’d estimate we save about 2% of runtime costs per client and have reduced our DevOps and QA time by 1 ½ FTEs.”

Haber explains that when it comes to the cloud, if he is given an agent bundle to include in one of his product offerings, it has to be included from the early stages of development, through QA, and into production. “We have to set up the environments to handle the agent in each stage to make sure it works, getting the output of data, and then ensuring it’s not crashing. When you start having thousands of agents out there, one or more will eventually break or fail to get updates. Then we have to troubleshoot and subsequently update a customer’s production environment. That’s a change control and compliance nightmare that is best to avoid entirely.”

> “For any company considering expanding through regions, Orca provides a streamlined approach. It requires less time to set up, provides quicker time to value, and operates with a lot less risk.”
>
> **Morey Haber**
> CTO & CISO
> BeyondTrust

Orca enables BeyondTrust to avoid those problems. “With the Orca, I’m relieved of the time and investment agents require. I’m not paying for the runtime of an agent hitting a CPU, and I have no change control risk of bringing an operations team member into a production environment.” On cost savings, Haber says, “Agent cost per client is about $20 – $30 per year. When scaled across hundreds and thousands of clients, the cost of using agents becomes significant. With Orca, we don’t have to consider any of that. I’d estimate we save about 2% of runtime costs per client and have reduced our DevOps and QA time by 1 ½ FTEs.”

Another critical reason why agents don’t work for BeyondTrust is that one of its products uses a customized, hardened custom kernel. Agents simply won’t load on that system. Orca’s SideScanningTM technology doesn’t have a problem seeing it.

Orca Compliance Modules and Integrations are Invaluable

Several regulatory or industry compliance aspects are essential to BeyondTrust. To earn customers’ confidence and business, BeyondTrust maintains SOC and ISO compliance—both of which are fully certified across its AWS and Azure platforms. And although BeyondTrust doesn’t require PCI compliance for its purposes, a client might license its technology and use it in a PCI zone. Therefore, having PCI certification is critically important. Orca has built-in compliance modules that help Haber document compliance requirements (e.g., concerning passwords, firewall configurations, PII exposure, etc.).

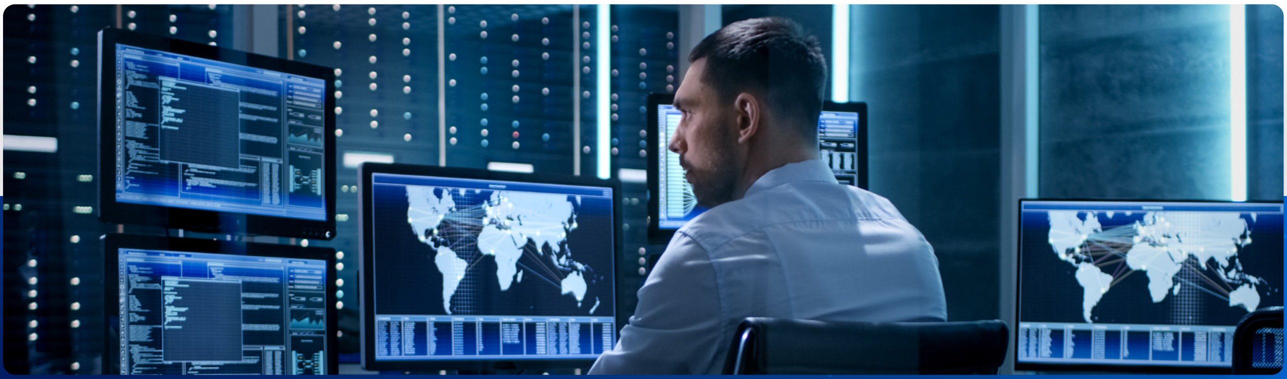
Orca's integration with Azure Sentinel Security Center and ServiceNow makes the solution far more valuable for BeyondTrust. It uses Security Center like a SIEM, so Orca's findings pour right into Azure Sentinel Security Center. Orca Security can kick off a ticket in ServiceNow if an investigation or remediation is needed.

An Azure Sentinel Security Center dashboard is continuously monitored so problems can be quickly addressed. "We stood up those integrations in less than a week, and it works flawlessly," says Haber. "One dashboard chart tells me time-to-triage from the moment Orca detects something. Our average time-to-resolution has been cut in half for anything critical," he says. "Once a ticket is closed, and Orca doesn't see the issue anymore, we have a closed-loop, which is important for our governance team and the people who must ensure we meet our SLAs," Haber says.

The Impact on Security Engineering

Through its integration with ServiceNow, Orca can generate tickets with specific details for security engineering to address. This saves considerable time over using an agent-based tool. "We deploy in multiple regions worldwide – North America, Europe, and South America," recounts Haber. "Per region, when you consider how many components we would need to deploy using an agent-based technology versus a simple Orca connection, you can see where my engineering and ops teams are much happier with Orca."

As for Orca's speed of deployment and accuracy, Haber says, "It's an efficient way to get complex data for actionable guidance. It helps us with vulnerability management, compliance, and secure configurations. After only using it for a few months, Orca has become a very valuable solution for us."



About Orca Security

Utilizing its unique patent-pending SideScanning™ technology, Orca Security provides cloud-wide,workload-deep security and compliance for AWS, Azure, and GCP. After an instantaneous, read-only and impact-free integration to the cloud provider, it detects vulnerabilities, malware, misconfigurations, lateral movement risk, authentication risk, and insecure high-risk data—then prioritizes risk based on the underlying issue, its accessibility, and blast radius - without deploying agents.

orca security

Connect your first cloud account in minutes and see for yourself: Visit orca.security