Orca Security Gives Grand City Property the Ability to See Security Risks from Every Angle

GCP

INDUSTRY
Real Estate

CHAMPION
Ran Tenenbaum: CISO

CLOUD ENVIRONMENT
Azure

"Orca Security is truly a single source of truth for complete cloud infrastructure visibility."

Ran Tenenbaum
Chief Information Security Officer
Grand City Property

Cloud Security Challenges

- Needed to get a holistic view of risk and vulnerabilities without using multiple, single-focus security tools and agents
- Diverse teams who maintain the infrastructure are a challenge to coordinate
- Constrained IT resources limit the manpower available to support disparate security tools

Cloud Security Results

- Can now use just one tool to see all cloud security risks and vulnerabilities in a single console
- Gets meaningful guidance on remediation that can easily be assigned to security engineers, IT personnel, or DevOps
- The manpower overhead for Orca is at least 90% less than comparable tools

One of Europe's Largest Commercial Real Estate Companies Trusts Orca Security to Help Protect its Custom Built Cloud ERP System Running on Microsoft Azure

Grand City Properties is a specialist in residential real estate, investing in value-add opportunities in densely populated areas predominantly in Germany. The Group's portfolio is focused on North Rhine-Westphalia, Germany's most populous federal state, Berlin, Germany's capital and Grand City's single largest city in the portfolio, the fast-growing metropolitan regions of Dresden, Leipzig, and Halle, and the largest cities in the north of Germany, Bremen, Hamburg, and Hannover as well as other major urban centers such as Nuremberg, Munch, Mannheim, Frankfurt, and London.

> "For us, the most important criterion was to find a tool that sees different security angles, including infrastructure, applications, and PII. Orca lets us see it all in a single place."
>
> **Ran Tenenbaum**
> Chief Information Security Officer
> Grand City Property

Grand City Property's primary application is known internally as MVA, an ERP system hosted on the Microsoft Azure cloud platform. MVA is being developed in-house because commercial off-the-shelf ERP solutions are not well suited to the unique needs of the real estate industry. A team of about 20 developers is devoted to this mission-critical application.

Ran Tenenbaum has been the chief information security officer at Grand City Property for two years.

The Goal: Find a Single Security Tool with a View of Everything Going On

"We're investing heavily in our infrastructure in Azure," Tenenbaum says. "I've searched for a security solution that takes a holistic approach, providing a review of the entire threat landscape in our cloud environment. We tried various solutions from vulnerability scanning and risk scoring solutions to CSPMs, but none did all I require until we found Orca."

"With a single click, Orca gives us the ability to see where we are with PII, password sharing, and CVEs across multiple platforms. If we have a firewall in place, Orca sees that. If we have Linux containers, Orca sees them. And if we have Windows OSs, Orca sees everything there as well. And It's all in a single view—a real advantage for a small security team like ours."

Grand City Property has performed rigorous evaluations of different security tools to determine which would be most helpful.

Comparing CSPMs and Orca Security

Grand City Property ran a popular CSPM in its infrastructure for two months, then compared the results with what it gets from Orca. "The CSPM has a nice dashboard that lets you see your NIST or CIS scores. But it doesn't give you insights like Orca does with respect to open password hashes or PII that's open on certain locations. CSPMs can't see those vectors." says Tenenbaum.

"CSPMs are solid solutions for configuration compliance, but that's not the only angle we need to look into. Orca also sees application and infrastructure angles to offer a more complete view."

In Grand City Property's experience, CSPMs see VMs but don't see Kubernetes containers very well. Tenenbaum says another advantage to Orca is that it sees the entire environment, including containers and black box security products.

"CSPMs are solid solutions for configuration compliance, but that's not the only angle we need to look into. Orca also sees application and infrastructure angles to offer a more complete view."

Ran Tenenbaum
Chief Information Security Officer
Grand City Property

Comparing Vulnerability Scanners and Orca Security

Grand City Property uses a network-based vulnerability scanner for its on-premise environment. It tried their version for cloud scanning but ran into performance issues. Tenenbaum says, "If we're using a network-based scanner to scan servers, we know a certain number of server scans can impact performance, so we only run it during off-hours. It can take three hours for a single in-depth scan, so it's not something we would do every day. But Orca's SideScanning technology doesn't disturb the production environment at all—a major plus when it comes to scanning."

And network-based scanning is resource-intensive in more ways than one. Tenenbaum explains that Grand City Property does both unauthenticated and authenticated scans with their network-based scanner. This takes time to specify scanning permissions and parameters. "We found that network-based scanning solutions can take 20% or more of a person's time to maintain the scans. This is a drain on resources because we run a lean security team."

Another drawback to using network-based scanners is that they provide limited insights. "We only see CVEs, which is important, but that's not the only vector to consider when it comes to vulnerabilities and threats."

Comparing Cloud Vendor Native Tooling and Orca Security

Grand City Property also evaluated some native tools from the cloud platform vendor. While the tool did an adequate job in finding security issues, its major disadvantage is that it requires an agent that not all security products can install. For example, Tenenbaum discovered his team couldn't install it on a virtual firewall appliance. Without providing full coverage of the entire cloud estate, the native tool leaves gaps that have to be filled in other ways.

Tenenbaum cites two additional problems with using agent-based security solutions. "One issue is performance-related, as agents do require the use of resources on a device. The second, more onerous issue is that we have to have faith that the agent has been installed on all of our endpoints and servers. We have to rely on several people to assure us they've thoroughly completed the pre-check configuration process—that all resources, servers, endpoints, mail relays, and so on are ready for us to perform scans. And we have to rely on IT, DevOps, and others to assure us they're okay with this process."

"This is not an approach I like to take," says Tenenbaum. "I'm trying to limit the footprint of everything involving security to the bare minimum. Anything I can do from the outside, such as with Orca, I'm choosing first instead of dealing with a haphazard agent-based approach."

Grand City Property's Example Use Cases for Orca

For Tenenbaum, Orca helps him coordinate his distributed support staff. "People in different organizations maintain certain portions of our infrastructure. We have internal and third-party DevOps engineers, a development group, a security team, and an IT department. By design, this provides complexity in coordination."

Orca helps Tenenbaum coordinate with the broader infrastructure team. "Orca's reporting gave me the visibility to understand the factuality between the different use of resources," says Tenenbaum.

In one case, Tenenbaum saw an instance with internet-facing access that was a critical vulnerability in the risk posture. He sent a screenshot of the report to the DBA with

> "Network-based scanners can take three hours for a single in-depth scan, so it's not something we would do every day. But Orca's SideScanning technology doesn't disturb the production environment at all—a major plus when it comes to scanning."
>
> **Ran Tenenbaum**
> Chief Information Security Officer
> Grand City Property

instructions to immediately close the hole. In another situation, he saw an unpatched OS within the backup solution. From within Orca, he opened a JIRA ticket to the DevOps engineer in charge of IT hygiene in that environment, who took care of the issue.

No Impact on Production, Complete Coverage, Minimal Overhead to Run

Tenenbaum has found three main advantages of using Orca in his Microsoft Azure environment. One is the non-disruptive nature of the scans. Orca's unique SideScanning™ technology has no impact on his production environment.

A second advantage is the completeness of coverage. "Nothing is being left out of scope," he says. "Everything is covered because Orca sees everything."

The last advantage is the low impact on manpower to support the Orca scans. Tenenbaum estimates it takes at least 90% less time than competing solutions to run the scans and assign follow-up to issues that are revealed. For lean security staff, this concise use of manpower is important.

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](orca.security)