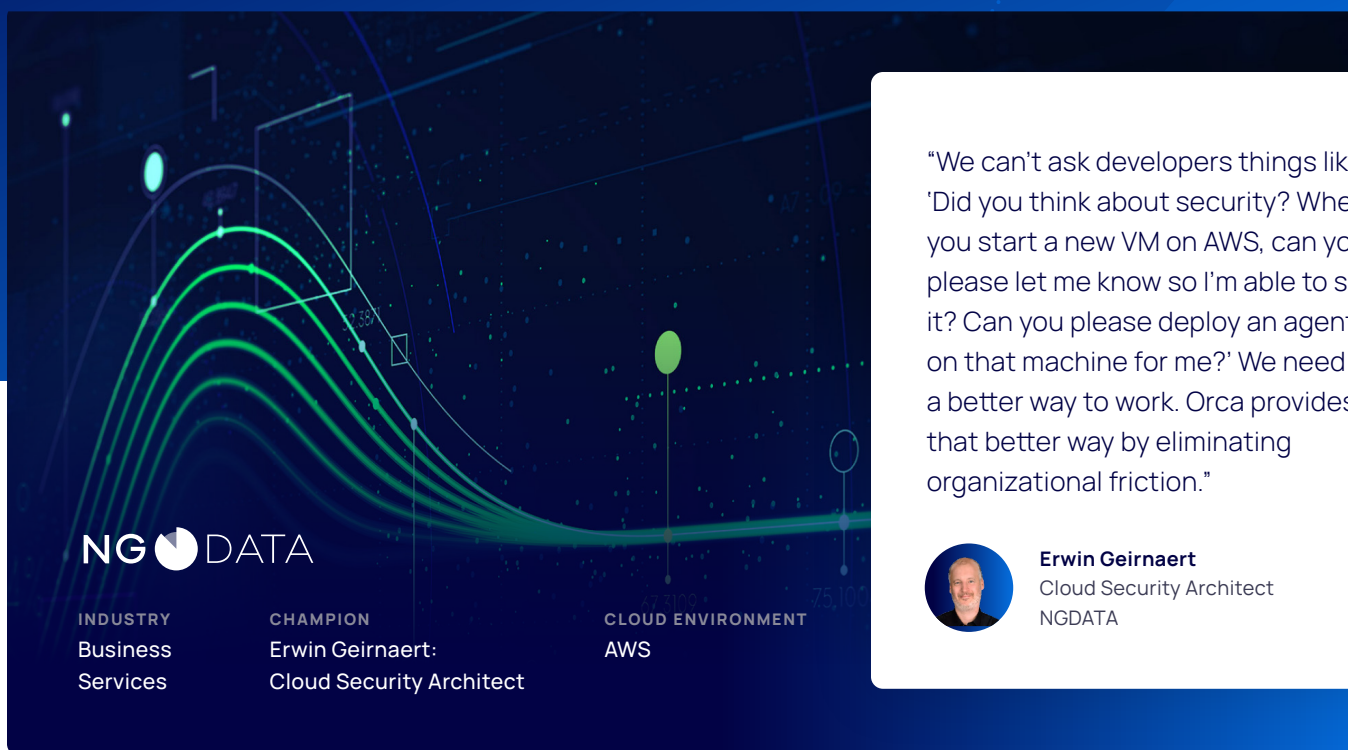


Orca Security Provides NGDATA with One Tool for Security, DevOps, and Compliance




NGDATA

INDUSTRY
 Business
 Services

CHAMPION
 Erwin Geirnaert:
 Cloud Security Architect

CLOUD ENVIRONMENT
 AWS

“We can’t ask developers things like ‘Did you think about security? When you start a new VM on AWS, can you please let me know so I’m able to scan it? Can you please deploy an agent on that machine for me?’ We need a better way to work. Orca provides that better way by eliminating organizational friction.”



Erwin Geirnaert
 Cloud Security Architect
 NGDATA

Cloud Security Challenges

- ✗ Need a global real-time view of AWS assets for a frequently changing estate, preferably without using agents
- ✗ Ensure customer assets and company intellectual property are protected
- ✗ Need tools that integrate with developers’ way of work

Cloud Security Results

- ✓ Attains a full view of all NGDATA assets in real-time
- ✓ Integrated with Jira to automate the vulnerability remediation process
- ✓ Removed organizational friction with developers to move to DevSecOps approach

NGDATA Helps Enterprises Drive More Personal Customer Experiences Through Data Insights

NGDATA helps brands in data-driven industries, such as financial services, telecom, utilities and hospitality, to drive connected customer experiences. Their AI-powered CDP and Digital Transformation Services put people at the center of every business via Customer DNA, which continuously learns from behavior to deliver compelling experiences for brands across the globe. NGDATA is headquartered in Gent, Belgium and has offices in the United States, Europe and Asia-Pacific.

The software platform can be installed on premise or deployed in a private cloud, while all product development work is done in the cloud. NGDATA has contracted cloud security architect Erwin Geirnaert of Shift Left Security to bring order to its cloud

environments, identify and systematically eliminate vulnerabilities, and implement procedures to sustain a good security posture.

Orca Security Succeeds Where Classic Security Scans Fail

Geirnaert's first undertaking was a classic penetration test to identify as quickly as possible the state of the current environment. The scan was only marginally helpful, as it was just a snapshot in time of a constantly changing cloud estate. But even with an authenticated scanner, if it doesn't know what to scan, there's a gap. "It just doesn't work in a cloud-native approach," Geirnaert says.

He then attempted to get information on the IP ranges to scan from the Amazon logs he'd pulled into a Sumo Logic dashboard. This yielded troubling results.



"To find vulnerabilities in a cloud infrastructure, the classic penetration test is dead. Our first scan with Orca was a real eye-opener. We found machines that we didn't know existed, that contained sensitive information, or that had services connected to the internet."

Erwin Geirnaert
Cloud Security Architect
NGDATA

Geirnaert explains how Orca enables the DevSecOps dynamic. “A developer has access to the AWS console, so he can just attach Orca using a read-only policy. He doesn’t need to deploy, apply, or install anything—he just configures AWS and trusts the Orca platform to do the scanning. It takes about five minutes to attach a read-only policy and get it running. And he immediately sees the results coming in from the deep scanning that Orca is doing.”

“With a full compliance view, the developer can ask, ‘Did I miss some security settings in Amazon that could have an impact on my security posture?’ He can immediately see he needs to configure this, enable that, use this, or do that. Orca also updates the compliance. Even without it finding a vulnerability, that alone gives us so much information that we don’t need a security firm to tell us what to do. Orca will tell us what we need to do and how to do it,” says Geirnaert.

“Orca lets us give different users access for different roles. The CISO is interested in compliance. The security engineer looks at vulnerabilities and alerts. The developer can learn from the dashboard why something is a problem.”

Erwin Geirnaert
Cloud Security Architect
NGDATA

This led to looking for a tool that could connect to the AWS API and get a real-time view of all NGDATA’s assets. Such a tool should reveal critical vulnerabilities and whether any PII or intellectual property was at risk. In this quest, Geirnaert found Orca Security.

“Our first scan with Orca was a real eye-opener. We found machines that we didn’t know existed, that contained sensitive information, or that had services connected to the Internet,” he says. Armed with the insight Orca returns, he set up daily scans of all IP addresses and virtual machines, even if they aren’t connected to the internet. “We need a full understanding of what we have to ensure customer assets—as well as NGDATA’s own intellectual property—are protected.”

Orca is a Transformative Tool for DevOps

NGDATA’s developers are spread around the world. Geirnaert says, “We can’t ask them, ‘Did you think about security? When you start a new VM on AWS, can you let me know so I’m able to scan it? Could you deploy an agent on that machine for me?’ We need a better way to work. Orca provides that better way by eliminating all of that organizational friction.

“I strongly believe in a DevOps approach, and then going cloud-native and serverless, because that will help increase security without having to train developers to become security champions. We need to enable them with tooling that integrates with the way they already work.”

Facilitating Compliance with Regulations and Security Frameworks

When Geirnaert first started at NGDATA, he compiled a list of best practices based on the Center for Internet Security compliance framework for AWS. He used the 100-item list like a project management tool to assign tasks. He no longer needs the list.

“When we launch Orca, it dynamically checks for compliance requirements. Before Orca, we wrote such checks ourselves in Sumo Logic. When we looked at the events coming from AWS CloudTrail logging, we would capture and display them in the dashboards. Now we see it all automatically and immediately in a single Orca dashboard.”

GDPR compliance is made easier because Orca looks for PII on servers and in files. Orca helps to find hidden PII and surfaces places where PII is expected to be. As a security person, Geirnaert doesn't have access to production environments, so Orca gives him visibility he wouldn't ordinarily have. Where PII is concerned, this helps steer patching or mitigation of problems.

Orca simplifies the audit process, too. “We can easily filter to show where PII is stored. Since it's all documented, we can show the evidence that auditors ask for with ease,” Geirnaert says.



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.



Connect your first cloud account in minutes
and see for yourself: [Visit **orca.security**](https://www.orca.security)

