



# Online Retailer bol.com Leverages Aqua to Build Secure Cloud Native Applications from the Start

## Customer Overview

Bol.com is the leading online retailer serving the Netherlands and Belgium. It offers a wide range of products in multiple shopping categories with books, music, films, games, electronics, toys, baby items, garden, and DIY items — as well as everything for sports, animals, living, free time, and personal care.

And it is obviously doing something right, as it now has more than 11 million customers and approximately 2000 employees. Bol.com is also recognized as one of the most popular online stores in the region and placed in the top five of the most customer-friendly companies in the Netherlands.

[login](#)  [Mid-Season Sale](#)[Your own living style](#)[Toy Deals](#)[Toy book](#)[So many Select Deals >](#)

## Zóóóveel Select-Deals ook op zondag bezorgd

[Bekijk nu alle deals](#)

## The Challenge: Security and Insight at the Speed of Cloud Native

Bol.com has about 500 developers with more than 100 teams building applications that improve the buying experience on bol.com. Traditionally, it built and maintained this software on-premises, using its own datacenter. But to meet its growing needs, bol.com decided to move to the cloud and adopted agile processes for software development, it also leveraged cloud native technologies such as microservices and containers to build and deploy applications faster.

However, bol.com also wanted to provide its developers with a security platform that supports building more secure code. Bol.com knew this would require a security platform providing granular visibility into container image security issues. By adding this level of capability, its developers could take direct responsibility for remediation by identifying issues earlier in the software development lifecycle. To demonstrate its long-standing desire to empower its developers, bol.com established an internal motto:

*You build it. You run it. You love it.*

With an eye on its goals, bol.com began its cloud journey with test deployments using Kubernetes clusters on the Google Cloud Platform (GCP). Today, it runs a hybrid setup using both the scalability of the cloud as well as running services in its own data center. Bol.com also uses Kubernetes to manage its container deployments.

Although CI/CD methodologies automated its application development and deployment to improve agility and flexibility, it did not fully address the need to help bol.com developers build applications more securely. Thus, the bol.com security team began its search for a cloud native security platform.



*You build it. You run it.  
You love it.*

**bol.com**

## The Solution: A Vital Element of its Security Suite

Bol.com found a partner in Aqua Security – as bol.com wanted a security platform that could deliver cloud native security wherever it deployed.

The Aqua solution provided the bol.com security team with comprehensive, early detection of security issues — when it's easier and quicker to remediate. Although bol.com usually prefers to methodically implement security in small steps, Aqua CSP quickly proved its worth and is now fully deployed within the bol.com production environment. Bol.com uses its own Infrastructure as Code (IaC) and was able to automate the deployment of Aqua in its environment using its existing IaC scripts.

Best of all, once deployed, Aqua's quality of reporting on vulnerabilities is easily scaled to meet the needs of all its development groups. Aqua is now heavily used within bol.com's development pipeline, where bol.com uses its own purpose-built security application for data aggregation and to call for scans from the Aqua CSP.

Once a scan completes, the results from Aqua integrate directly into the bol.com security dashboard. *"Aqua provides our developers with the tools needed to produce secure software and deploy secure images. This was the biggest gain we got by using Aqua,"* said Machiel Pronk of bol.com.

With the Aqua platform, bol.com was able to easily expand security within its existing CI pipeline and integrate with third-party security tools to instantly improve vulnerability coverage:

- Works seamlessly with its home-grown CI/CD security tools
- Prevents vulnerabilities from running in its environment
- Ensures container image integrity
- Provides granular data on vulnerabilities
- Delivers an easily scalable security platform



*"Aqua provides our developers with the tools needed to produce secure software and deploy secure images. This was the biggest gain we got by using Aqua."*

**Machiel Pronk,**  
Cyber Security Engineer  
bol.com

## Customer Benefits: Producing more code, more securely

After implementing Aqua, bol.com has a cloud native security platform that can scale to meet its growing demands. Also, its engineering management team can now easily access vulnerability data and determine which teams are associated with which images. This information is then fed back into development to implement continuous improvement and remediate any production issues. Thus, fulfilling the promise of “You build it. You run it. You love it.” Rutger Prins stated, *“...with Aqua, when we identify vulnerabilities in our images — we can quickly take appropriate action to support our teams and produce code more securely.”*

With its robust security platform, Aqua enables bol.com to:

- Add security capabilities without sacrificing performance
- Confidently detect vulnerabilities in container images and fix them
- Provide tracking and policy enforcement for governance requirements
- Empower developers with precise, actionable remediation information
- Build better, more secure software



***“...with Aqua, when we identify vulnerabilities in our images — we can quickly take appropriate action to support our teams and produce code more securely.”***

Rutger Prins, Security Operations  
Software Engineer  
bol.com