
# CASE STUDY

An Online Gifting Company Force Multiplies its AppSec Program

## Company Description

The enterprise is a leading online gifting company where staying nimble, fast, and responsive are essential. Over the years the company has accelerated its software release cycles to stay in sync with changing market trends and innovate faster.

## Challenges and Opportunities

The company utilized 300+ applications, thousands of microservices, and dozens of programming languages. It used 10+ AppSec tools which generated 300K alerts from various scans. This diversity made it very difficult for the organization to get a handle on its AppSec posture.

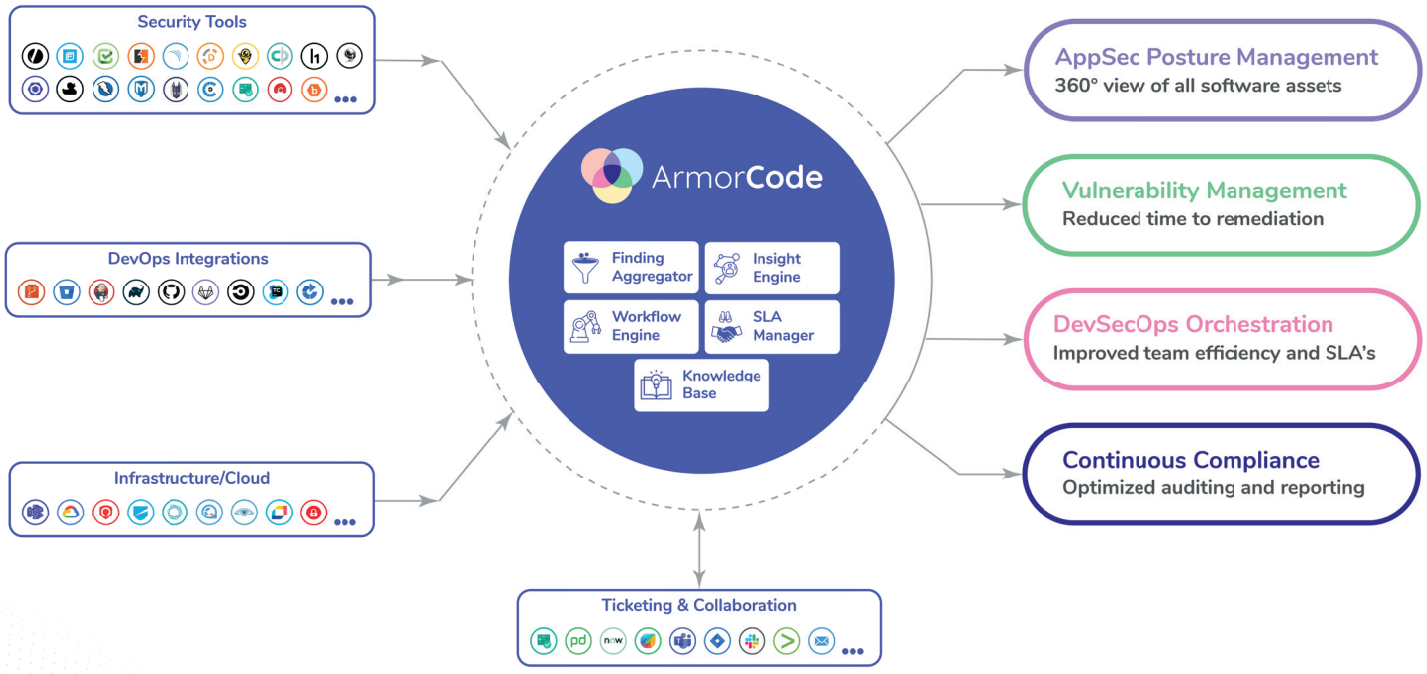
While an AppSec program had been deployed in the company, its small team struggled to address the volume of security issues coming from various tools like SAST, SCA, DAST, Bug Bounty, and RASP; even with a few hundred developers fixing those issues. The consolidation of findings was a tedious process that required the maintenance of several excel sheets. There was inconsistent workflow and ticket process orchestration between tools. This put huge pressure on the small AppSec team and caused alert fatigue. Even after substantial time input, they were not able to track SLAs around findings nor identify which alerts need to be fixed. This led to constant friction between developers and the security team.

# The ArmorCode AppSecOps Solution

With the ArmorCode AppSecOps platform, they now have a single-pane-of-glass to centralize all AppSec findings and normalize them based on each tool's effectiveness. The team now prioritizes findings that matter to maximize risk mitigation efficiency. Leveraging automation capabilities, the team directly assigns the issues to their corresponding developers. With better visibility, they are able to track the health of the environment around their security tools' status. Blind Spots are removed by receiving alerts when tools become inactive for any repo.

The team's AppSecOps program became fully functional after adopting ArmorCode as their comprehensive portal for better visibility, actionable insights, and workflow automation. This has allowed them to ship their software faster and more securely.

## ArmorCode AppSecOps Platform Overview



# Results

1

Total potential savings of ~$10M over 5 years.

2

Continuous and efficient AppSec monitoring: A Single AppSecOps Platform combining AppSec Posture Management, Devsecops Orchestration, and Continuous Compliance.

3

Time for fixing security issues was reduced, and with it, tensions across groups.

4

Integrations with SAST, SCA, SCM, Bug Bounty, CI/CD, MAST, RASP, Infrastructure tools, and others.

5

SLA

Service Level Agreement Automation enabled the creation, sharing, management and tracking of SLAs and automated DevSecOps workflows to effectively “Shift Left” and scale AppSec success.

# What is AppSecOps?

AppSecOps is the process of identifying, prioritizing, remediating, and preventing Application Security breaches, vulnerabilities and risks - fully integrated with existing DevSecOps workflows, teams, and tools.

An AppSecOps platform enables an application security team to scale its ability to identify, remediate and prevent high priority security issues, vulnerabilities, and compliance issues. It also helps identify and eliminate coverage gaps. It automates, manages, and orchestrates workflows enabling developers to fix issues faster and more effectively without specialized training and skills. In short, **AppSecOps 10X force multiplies your AppSec program.**