ArmorCode

Case Study

How a Mid-size Fintech Company Set Up its AppSec Program From Scratch with No Additional Hires

Maintaining a robust Application Security posture in a world where release cycles are accelerating and threat landscapes are growing is of paramount importance. But applications are getting released without adequate security guardrails as security teams and developers are overwhelmed by, labor-intensive work, and lack visibility into their application security posture or an easy way to orchestrate their inter-team workflows. With no clear visibility into threat posture, security leaders struggle to provide an accurate view of their organization's security preparedness to the leadership team. This case study discusses how ArmorCode helped a medium-sized FinTech company build and scale its application security operations from scratch, provide clear visibility into its risk posture, and enable seamless collaboration between teams.

The Situation

Application security, or AppSec, is a key element in the enterprise's overall cybersecurity strategy. Security cannot be in an afterthought in software design, but teams often assume unnecessary risk while releasing software because they lack visibility, staff to take care of labor-intensive work, and a clear understanding of the risks they are assuming. A Fintech company with 1,000 developers and 15 security professionals based in California, USA, was facing multiple issues, from technical to managerial, when it came to managing the application security posture of their organization; and was looking for tools and processes to build and scale their AppSec program.

> *In the digital era of customer-centricity and "always-on" capabilities, security teams, developers and leaders need to be on the same page and have access to the latest application risk posture. ArmorCode is focused on enabling that collaboration."*
>
> -CISO, Mid Size Fintech, CA, USA

Challenges Faced by the Company in its Digital Journey

Challenges Faced by the Company in its Digital Journey:

Multiple Systems to Flag Vulnerabilities:

As the organization was maturing its DevSecOps program, the AppSec team and developers were using Software Bills of Materials, SAST (Static Application Security Testing) tools, DAST (Dynamic Application Security Testing) tools, Attack Simulation tools, Fault Injection tools, etc. to help them understand their overall AppSec posture. While using these tools, they faced a mountain of findings with duplicate issues raised by different tools and teams, no clear prioritization of vulnerabilities, and no automatic allocation of vulnerabilities to developers.

Lack of a Single Dashboard to Depict Heatmap and Organizational Risk Score:

Vulnerabilities were being identified, but many questions around these vulnerabilities remained unanswered; such as, "What does a specific vulnerability, mean?" "How do a combination of vulnerabilities translate into a "risk score" for the company?" In simple words, many CVEs (Common Vulnerabilities and Exposures) and CWEs (Common Weakness Enumerations) were raised, and how, exactly they would jeopardize the organizational information assets could not be identified. Without this, security leaders were not able to narrate a clear “current state” to “future desirable state” strategy, which in turn impacted their ability to secure the necessary budget.

Lack of a Standardized Knowledge Base to Address Vulnerabilities:

Although the developers knew that there were vulnerabilities present (which included cross-site scripting (XSS), SQL injection (SQLi), etc.) they were not sufficiently trained on how to approach such vulnerabilities or how to patch them quickly. A single vulnerability or defect was being raised multiple times even after it was rectified as there was no systematic way to track vulnerabilities, or their resolutions across tools and teams. False positives created another set of problems, with teams chasing wrong issues. This was impacting the whole SDLC (Software Development Lifecycle) and impacting organizational operations at large.

Absence of a Single, Central Operational Unit:

As the company used multiple DevSecOps tools, services, and programs, there was no proper alignment in vulnerability allocation. Developers were being assigned vulnerabilities without the benefit of a holistic view and without any prioritization. This led to confusion and disparity between developers, AppSec team, and the company leadership.

How the ArmorCode AppSecOps Platform Helped

ArmorCode helped the company address the challenges mentioned earlier and manage the state of their Application Security Operations (AppSecOps) in the following ways:

Operationalizing the Overall Process:

The ArmorCode platform aggregated all vulnerabilities, de-duped, correlated, and normalized them to provide a single pane of glass that showed the company's application security posture. ArmorCode also provided a single platform that automated workflows between the AppSec team and developers, thus simplifying and scaling application security operations (AppSecOps).

Taking Significant Burden Off of the AppSec Team and Developers' Shoulders:

Before ArmorCode, AppSec teams and developers spent a significant amount of time reviewing each vulnerability manually. Many false positives caused them to ignore vulnerabilities, thinking they were already handled, when this may not have been the case. With ArmorCode, both teams now know exactly what they need to focus on.

A Visual & Easy-to-Understand Dashboard:

ArmorCode provided the AppSec team, developers, and security leaders a single reporting dashboard that could be easily interpreted by non-technical members of the Board. It provided a security heat map clearly indicating where risks exist. Prior to using ArmorCode, the company's DevSecOps team was finding it hard to figure out how to quantify the short-term and long-term objectives of their application security program. ArmorCode provided them with a way to assess the security posture quantitatively. For instance, a score of 60 out of 100 was given to the current application security posture. The company could set a target to increase this score from 60 to 80 as a milestone, according to their requirements. Now the security leadership and the Board of Directors review the AppSec dashboard every Monday without any explanation or interpretation needed by technical staff.

Benefits of Using the ArmorCode Solution

The company reported the following benefits and results after deploying the ArmorCode AppSecOps Platform:

No AppSec Program to a Robust AppSec Program Without Hiring Additional Resources:

ArmorCode helped the company put together a robust AppSec program where none existed before. This was achieved without needing to hire any additional security team members. The ArmorCode platform was simple enough to be used by the existing team, thereby force-multiplying their efforts by 10X with powerful automation and orchestration capabilities.

Developer and AppSec Team Efficiency:

Innovation and release agility are without a doubt two of the most crucial aspects of any software company. After deployment of the ArmorCode AppSecOps platform, developers were relieved of the time they were spending on false positives and duplicates, and instead focused their precious time on developing revenue-generating features faster.

Better Resource Prioritization:

ArmorCode allowed security engineers and developers to make the best use of resources, address the most impactful issues first, and prioritize everything appropriately.

No Heat Map to Heat Map:

Without clear visibility into their existing AppSec posture, it was very challenging for the company to set the right roadmap for its future course of action. ArmorCode helped company leadership to get a clear view of their AppSec posture, with clearly visible gaps, heat maps, and obstacles. This became the starting point for a road map to reach their desired end state and helped the security.... This is helping the security team clearly show the ROI of their efforts and provide justification for new initiatives.

Conclusion

The company's journey with application security shows how managing cybersecurity today requires a clear visibility into an organization's AppSec posture, force multiplying the capabilities of scarce security talent by automating mundane tasks, and providing and a clear view of the existing program maturity. With ArmorCode AppSecOps platform, the company has a single platform for Application Security Posture Management, Unified Vulnerability Management, and DevSecOps Orchestration to help them build and maintain a robust application security posture.

ArmorCode

Awards and Recognitions

2022 SINET 16 Innovator Awards Winner

Nasdaq Congratulates
ArmorCode
on their $11M Seed Funding!
ArmorCode
AppSecOps - Your 10X AppSec Force Multiplier
Nasdaq

NASDAQ Spotlight

StartUp Of The Year-Security Software

Hot Company Of The Year-Security Software

TiE50 Awards Winner TiEcon 2022

ArmorCode

ArmorCode is the industry's leading AppSecOps platform. ArmorCode customers reduce application exposure and risk, while scaling AppSec effectiveness and impact by 10x or more across the organization. ArmorCode customers use the platform for AppSec Posture, Vulnerability, and Compliance Management and DevSecOps automation.

ArmorCode: AppSecOps Delivered - Your 10X AppSec Force Multiplier™

Secure Teams Use ArmorCode

Shutterfly snapdocs GUARDANT snap! finance