ArmorCode

AppSecOps– Application Security Transformed!

Executive Summary

To drive competitive success, organizations of all types and sizes have implemented digital transformation initiatives. At the heart of these transformations are software applications. And to enable this change, application architecture, development and infrastructure have all transformed themselves, to deliver software faster and more powerfully. Unfortunately, these ongoing transformations have created new and ever increasing application security risks.

This paper summarizes the changes that have taken place in application architecture, development, and infrastructure, and the implications and challenges of these changes on application security and the security teams tasked with managing them.

The paper then outlines a new approach to operationalize application security, AppSecOps, the components and requirements of an AppSecOps platform, and the benefits associated with their adoption.

As you will see, today's Application Security teams are outnumbered and overwhelmed by change, and AppSecOps is the transformative approach to application security that is needed to successfully manage this risk and scale to both the pace and volume of change inherent in today's application lifecycles.

Expanding Application Risk

Everything in the business application world is different than before and faster than ever. Infrastructure has been modernized, applications have been componentized into microservices and the very process of application development and deployment has transformed. All of this change is driven by the need to rapidly deliver software driven innovation, to ensure businesses compete and win in today’s digital age.

These interrelated changes build on each other to enable applications to ship faster and faster. These changes are summarized in Table 1 below

	From	To	Security Implications
Application Architecture	Monolithic, Limited and defined connectivity, Proprietary and packaged code	Componitized, Broad and open API connectivity, Adoption of open source components	• Ever-growing application risk surface
Application Development	Waterfall, periodic release Disconnected from Ops Limited feedback to development	Agile, continuous releases Integrated “DevOps” Continuous feedback to development	• More frequent and discrete changes to both code and infrastructure
Application Infrastructure	Hardware bound, Server-based, Virtualized	Cloud-Scaled, Infrastructure as Code Containerized	• Broader 3rd party risk exposure

Table 1: The Security implications of changes to application development and delivery

As a result, code is released and applications ship, and change, faster than we could have ever imagined. As applications are modernized and broken into more and more microservices, quarterly releases become monthly, monthly become weekly, weekly become daily and even hourly. Competitive success today requires this.

The implications of these changes for application security are tremendous, and can be broken into 3 main areas; an ever-growing application risk surface, more frequent and discrete code and infrastructure changes, and broader 3rd party risk. Each of these factors creates new challenges for Application Security teams.

The Ever-Growing Risk Surface

Applications are now under a constant state of growth, and the business demands for digital transformation and new applications far outpace the ability of manual tracking and processes to keep up. This makes everything in application security harder. From simply knowing the inventory of applications and their associated risk profiles to investigating issues to remediating risk to reporting on success requires accurate visibility into this full risk surface.

Frequent and Discrete Change

Not only are the number of applications growing, but they are constantly changing. Frequent releases with small discrete changes make it even harder for Application Security teams to keep up. There is simply more to know, more to pay attention to, and less time to figure it out. Once a year or even quarterly compliance certifications become meaningless because the moment a new code is released, the certification is invalidated.

Risk from the Software Supply Chain

As infrastructure moves to the cloud, open-source components are embedded into applications, and more integration is done via Open APIs, risk from the software supply chain and 3rd parties increases. Compliance to policy is harder to track, and maintain, and more risk is introduced outside of the control of the organization. Application Security teams must now extend their work beyond the internal organizational boundaries to understand and manage these risks.

All of these changes are not lost on regulators or attackers. Compliance and privacy responsibilities keep growing and do not end at the organization's boundaries. More regulation on more data is, and will continue, to be the trend. And as the risk surface expands, attackers eagerly pounce on new opportunities. Code, infrastructure, and architecture vulnerabilities are shared across the community of attackers, and the cost of performing attacks using available tools and known techniques continues to decline, while the value of the resources exposed continues to grow. So attackers are constantly probing for and pouncing on application and infrastructure weak spots.

AppSec Teams are Outnumbered and Can't Keep Up

Despite this world of growing application risks, business imperatives and organizational priorities often mean that shipping fast takes priority over shipping safe and secure. And AppSec teams simply can't keep up with the pace of delivery for the following reasons:

They are Outnumbered by Developers More Than 100:1

With that many developers creating code, there is simply not enough bandwidth available for them to do the work needed in the time available

They are Dependent on a Set of Disjointed and Siloed Tools and Processes

The amount of manual work and analysis needed to understand, investigate and remediate risk does not scale with the amount of work needed to be done to secure applications

The Development, Operations and Security Teams are Misaligned

The incentives and measurements of the teams simply are not aligned, and "shipping fast versus shipping secure" becomes a point of friction between the teams. Additionally, AppSec teams often lack the tools needed to provide visibility and gain executive sponsorship outside of the security team.

Today's Approach to AppSec is Painful and Not Scalable

While security teams are motivated and incentivized to secure the application at any cost, which inherently slows down delivery, developers are required to ship the software faster and faster to meet the ever-growing business need.

To close these gaps, organizations unsuccessfully try to drive more processes into spreadsheet upon spreadsheet, increase email and chat messages, mandate developer training, create more one-time fixes with tickets and more tickets, drive decisions through change control boards and implement other process "improvements" and bandages.

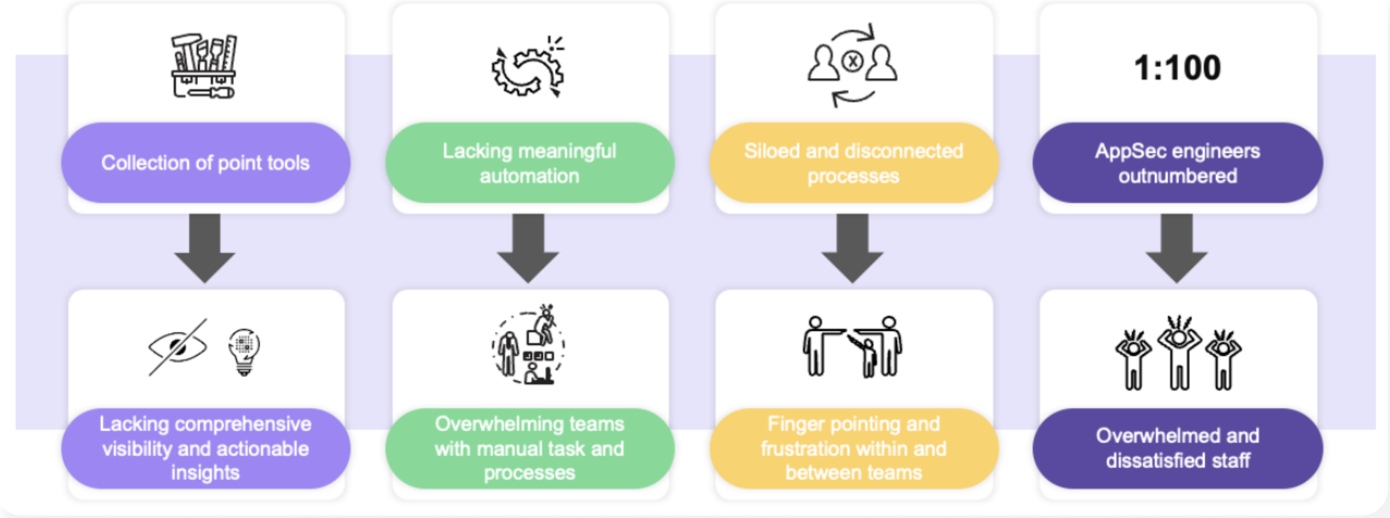

Collection of point tools
Lacking meaningful automation
Siloed and disconnected processes
1:100
AppSec engineers outnumbered
Lacking comprehensive visibility and actionable insights
Overwhelming teams with manual task and processes
Finger pointing and frustration within and between teams
Overwhelmed and dissatisfied staff

Figure 1: AppSec are outnumbered and can't keep up

AppSec Chaos and Unmanaged Risk

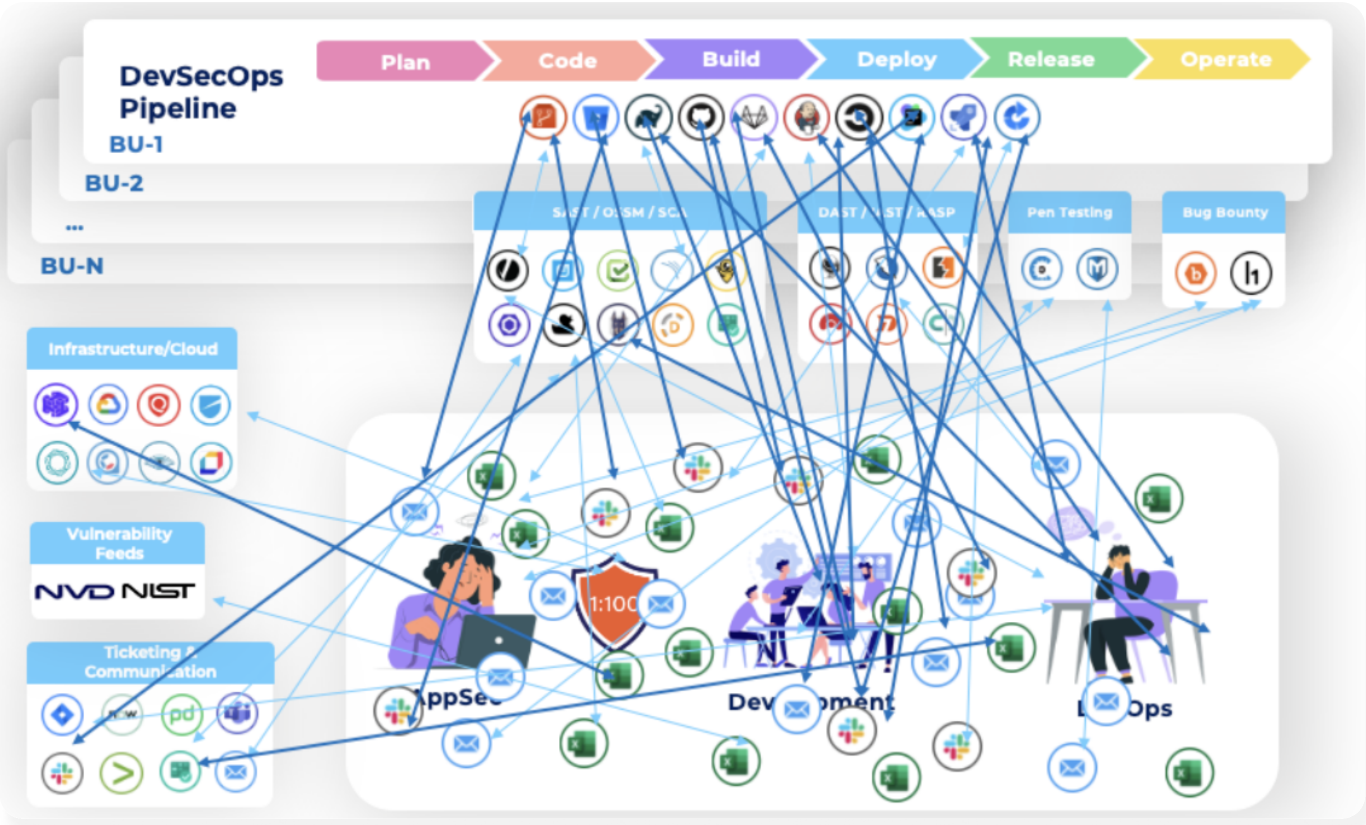


Figure 2: AppSec Chaos and Unmanaged Risk

The application security, development and DevOps professionals are overwhelmed by alerts from SAST, DAST, Cloud, Container, and other security tools. And, in addition to being outnumbered 100:1, the AppSec team needs to cross correlate findings from tools embedded within the pipeline with those that are executed separately and thread intelligence information. This results in “excel hell” and as the AppSec struggles to keep up they become isolated and reactive. While the dev teams keep shipping fast without the needed security guardrails and assurance. Ultimately, the organization is exposed to unacceptable levels of security and compliance risk.

The New Approach, AppSecOps

To protect the ever-growing and changing application risk surface, we need to transform application security to match the transformation that we have seen in application architecture, development, and infrastructure. This requires a new approach, Application Security Operations, or AppSecOps for short. AppSecOps unifies the processes and teams responsible for securing application delivery and operations by:

- Integrating with the existing security, DevOps tools and functional processes,
- Ingesting, normalizing, deduplicating, correlating and prioritizing all of the application-level events, alerts, and data across all scans, tools, and DevOps phases
- Automating critical AppSec workflows across the application security lifecycle

By unifying all of the tools, processes and teams involved in securing today’s modern applications, AppSecOps allows Application Security teams to scale their effectiveness and impact. Implementing AppSecOps requires a platform that:

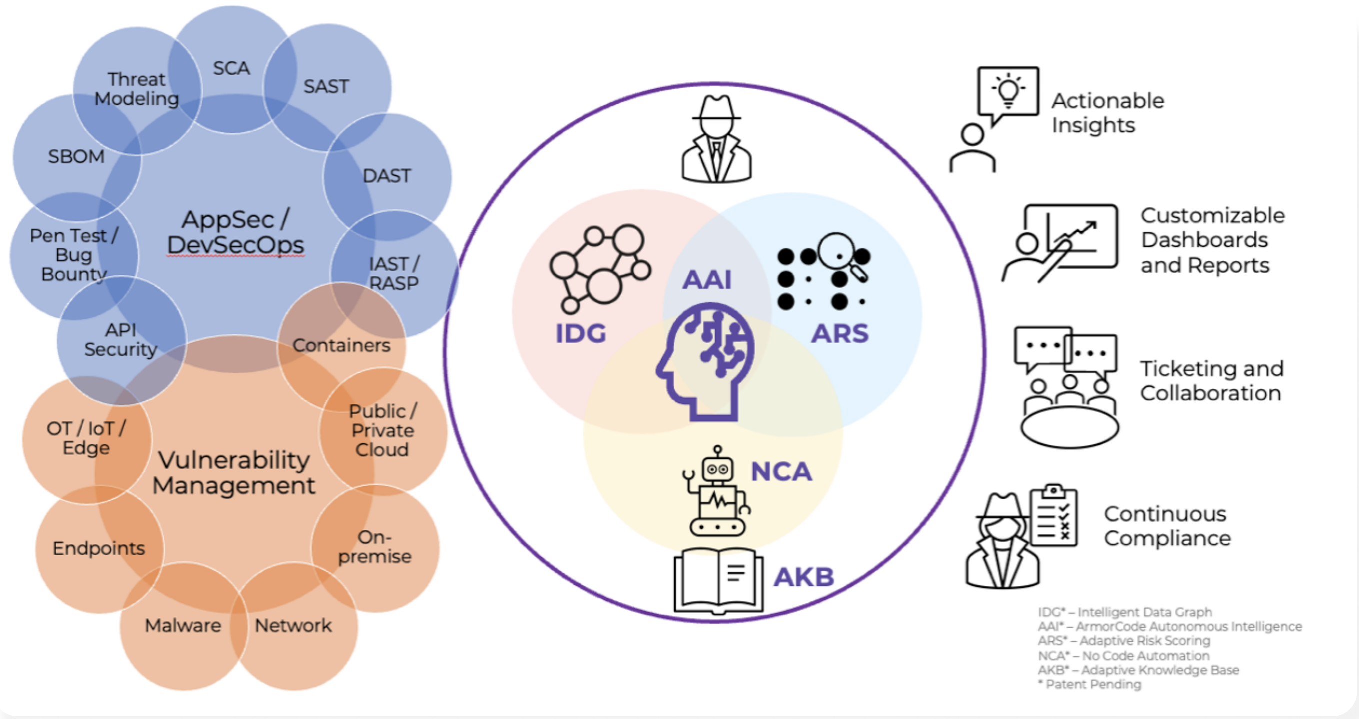
- Automates the critical AppSec security workflows such as
  - Event and alert analysis
  - Triage and ticketing of critical vulnerabilities
  - SLA escalation and notification
- Engages and enables development teams to ship secure code by providing
  - Clear expectations on process role, responsibility and measurement
  - In-process alerting and visibility to code security issues
  - Access to best practices for issue mitigation and fixing
- Provides a single interface and source of truth for all AppSec use cases, including but not limited to posture management, DevSecOps orchestration, vulnerability management and continuous compliance

With an AppSecOps platform deployed, Application Security teams scale their impact by more than 10x, keep up with and secure the constantly expanding and changing application security risk surface, and eliminate wasted time and cost through operational efficiencies. In short they go from frustration, finger pointing and failure, to productive and effective teamwork and success.

The ArmorCode AppSecOps Platform – Components and Deployment

ArmorCode is the industry's leading and most complete AppSecOps platform. The Armorcode solution integrates seamlessly with Security tools, DevOps platforms, Application Infrastructure, and Operational Ticketing and Collaboration products.

The ArmorCode AppSecOps Platform – Autonomous AppSec



IDG* – Intelligent Data Graph
AAI* – ArmorCode Autonomous Intelligence
ARS* – Adaptive Risk Scoring
NCA* – No Code Automation
AKB* – Adaptive Knowledge Base
* Patent Pending

As shown above, in Figure 3, the platform comprises the following 5 components

Intelligent Data Graph (IDG)

Normalizes, Dedups and Correlates data from across security tools and maps to Product/Subproducts (Applications/Microservices) - providing organizations a business centric view of their security posture. Furthermore, by understanding the relationship between the applications and the infrastructure they are deployed on, ArmorCode is able to provide an infrastructure based view of the application security posture.

ArmorCode Autonomous Intelligence (AAI)

AAI not only normalizes and correlates data within the IDG but also enriches the IDG with cyber threat intelligence data to provide additional context around the identified vulnerabilities and the risk they represent to the business.

Adaptive Risk Scoring (ARS)

ARS leverages AAI to perform contextual and dynamic risk scoring of findings and assets - helping teams prioritize remediation efforts so they spend their time most appropriately to mitigate risk to the business, i.e. focusing on fixing vulnerabilities that are mapped to business critical assets and are exploitable, or being actively exploited

No Code Automation (NCA)

ArmorCodes no code automation framework automates critical AppSec workflows such as triage, ticketing, escalation and notification. NCA eliminates manual and low value work, to allow the AppSec team to perform deeper investigations and spend more time collaborating with, and coaching, the development team.

Adaptive Knowledge Base (AKB)

Cross correlating knowledge base articles with tickets, findings and code commits to elevate the tribal knowledge within the organization and boost developer productivity. Not only providing developers with the information they need to understand a finding - but also the people to talk to to learn the best way to mitigate a vulnerability.

Working in concert with other tools and across teams, the ArmorCode AppSecOps platform enables the four key AppSecOps use-cases of; Application Security Posture Management, Unified Vulnerability Management, DevSecOps Orchestration and Continuous Compliance - all within a single platform.

AppSec Success

As we have seen, Application Security teams today are challenged to secure a growing and ever-changing risk surface. While Application architecture, development and infrastructure have transformed, integrated and automated to deliver more code faster, Application Security teams are dependent on too many siloed tools and manual processes, suffer misalignment of goals and are outnumbered by developers by more than 100:1. AppSecOps transforms application security to meet these challenges head-on. Teams that adopt AppSecOps and implement a robust AppSecOps platform such as ArmorCode are able to:

- **Manage and Reduce Application Security Risk**

  Through continuous visibility and actionable insight

- **Achieve AppSec Operational Efficiency**

  By eliminating manual, repetitive and low-value work

- **Scale AppSec Success**

  Through full DevSecOps pipeline integration and process automation and simplification

AppSecOps is the future of Application Security, transforming it from a disconnected, largely manual and hard to scale effort, to an integrated, automated and scalable one that dramatically reduces risk while delivering organizational efficiency and effectiveness.

About ArmorCode

ArmorCode provides the industry's leading AppSecOps platform. ArmorCode delivers continuous visibility and actionable insights so that security teams can successfully identify and prioritize the highest risk application security vulnerabilities. Efficiently closing coverage and compliance gaps at a fraction of the cost of traditional approaches - all from within a single integrated platform. ArmorCode eliminates manual, repetitive and low-value work across the DevSecOps pipeline and enables AppSec teams to successfully engage with development teams as security partners.

ArmorCode customers use the platform for Application Security Posture Management, Unified Vulnerability Management, DevSecOps Orchestration and Continuous Compliance - and realize the real world business benefits of;

- More than 10x improvement in AppSec efficiency
- Reduced risk with 100% application security coverage while avoiding 90% of the cost
- Accelerate software delivery through 3x faster remediation time.

Enterprises with 150 developers to 15,000+ developers are using ArmorCode to measure and improve application security posture, coverage, and compliance. ArmorCode empowers development and operations teams to ship and deploy more secure code faster; without increased security staffing, developer training, or workload. With the ArmorCode AppSecOps platform, applications ship secure AND ship fast.

ArmorCode customers include those from Banking/Finance, Healthcare, eCommerce/Retail, Hospitality and Entertainment/Media - from hyper growth digital native companies to some of the most admired global brands across the globe.

In a recent customer study, of a Financial Services client with 5 AppSec engineers supporting over 600 developers, the following benefits were cited

- 90% efficiency gains for AppSec team in reviewing and summarizing AppSec issues that need to be remediated
- 33% reduction in developer time spent on reviewing, remediating, and reporting vulnerabilities
- 66% improvement in overall time spent reviewing and remediating scans, leading to faster releases without increasing the team's headcount

ArmorCode was founded by Nikhil Gupta, former CEO & Co-Founder of Avid Secure, a cloud security startup acquired by Sophos in 2019, and Anant Misra, an IIT Kanpur graduate with 20+ years of software development experience.

ArmorCode: AppSecOps Delivered - ship secure software and ship it fast