The State of the Application Security Workflow

Envisioning the Next Frontier:
Transforming Application Security Workflows

2025 Report

Kodem

Table of Content

A Message from Our CEO

I'm honored to share the journey that led us to build Kodem. Over the years, our team has experienced cybersecurity from every angle—researching code, defending critical systems, and discovering vulnerabilities. We learned a crucial lesson: while digital innovation accelerates, application security often lags behind. Kodem was born from that realization, fueled by our firsthand understanding of protecting critical assets under relentless pressure—and our conviction that, with the right approach, organizations can stay ahead of emerging threats.

We created this report to spotlight the security pioneers who refuse to settle for outdated methods. Across every industry, there are bold leaders shaping a new frontier of application security. By sharing their insights, we hope to amplify their voices and spark collaborative dialogue—one that disrupts complacency and illuminates the future of AppSec.

At Kodem, we aim to be catalysts for transformation, bridging the gap between security theory and practical deployment. Driven by a commitment to solve today's toughest challenges and anticipate tomorrow's threats, our mission extends beyond delivering tools. We strive to empower teams to innovate confidently, knowing their applications are safeguarded from code to runtime.

None of this would be possible without the remarkable community supporting our mission. To everyone who participated in our survey, and to our customers, partners, and investors—thank you for your trust and collaboration. Your insights shape this report and inspire us to continually push the boundaries of what's possible in application security.

I hope you find the report both insightful and inspiring as you chart your own path toward stronger application security.

Aviv Mussinger
Co-Founder & CEO

1. State of Application Security Workflows

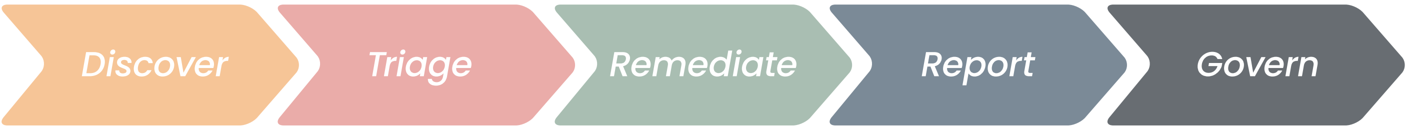
Introduction

Today's application security landscape presents a fundamental challenge: expanding attack surfaces and rapid development cycles outpace traditional security approaches. Application security teams face a fundamental mismatch to secure cloud-native architectures and API-driven integrations while maintaining development velocity.

However, these workflows are often plagued by inefficiencies, fragmented toolsets and manual processes that struggle to keep pace with an evolving threat landscape.

This report explores the state of application security workflows, drawing insights from a survey of Chief Information Security Officers (CISOs), Application Security (AppSec) leaders and security professionals across diverse industries. The research reveals how organizations address security challenges through strategic approaches, while showcasing how automation and contextual intelligence optimize security workflows.

The application security workflow consists of five key stages: discovery, triage, remediation, reporting and governance. This report examines how organizations approach each stage and where they face the greatest challenges.



Discover

Triage

Remediate

Report

Govern

By illuminating the key gaps in application security practices - and highlighting emerging trends and best practices - this report aims to equip readers with actionable insights that can help future-proof their security programs. Kodem, the publisher of this report, purpose built a platform that bridges these gaps by unifying shift-left strategies with runtime monitoring and protection.

Key Findings

The following critical insights provide a snapshot of the current state of application security workflows and the trends shaping the future:

78%
Use more than 5 security tools

Fragmentation in security toolsets

Respondents use **more than five different tools** in their application security stack, leading to inefficiencies and fragmented visibility.

62%
Emphasize slow remediation

Remediation is the largest bottleneck

Respondents cite critical vulnerabilities taking more than **four weeks** to fix, with teams overwhelmed by poor prioritization of risks.

73%
Impliment Shift-left

Shift-left adoption is growing but incomplete

Organizations have implemented shift-left security, but **only half** successfully integrated these practices into developer workflows.

45%
YoY growth in runtime solutions

Runtime security is gaining traction

Growth in adoption of runtime-based solutions which emphasizes the need to **address vulnerabilities missed** during development.

84%
Lean into automated workflows

The push for automation

Security leaders view automation for triaging, risk analysis and CI/CD integration as essential, though 95% express concerns about "garbage in, garbage out" highlighting the need for **contextual insights.**

55%
Faster remediation using runtime

Contextual intelligence is the future

Organizations leveraging contextual insights from exploitability, affected assets and environment risk—achieve 55% **faster remediation** and improved security - development collaboration.

2. Application Security Workflows Today

Mapping the Current Landscape

Application security teams struggle with fragmented tooling and visibility as development accelerates, driving the need for more unified and contextual security approaches.

74%

Operation complexity

Respondents say managing application security across development, CI/CD pipelines and production environments as their top operational challenge.

Despite advances in security tooling, many organizations find it difficult to keep pace with accelerating release cycles. While **73% of organizations** have integrated some form of shift-left security, only **35%** believe these practices effectively reduce risk at scale.

Security tooling adoption may be growing, but many workflows remain disjointed. For instance, **54% of security leaders** still lack a unified platform to manage vulnerabilities from code to runtime, causing redundancies and inefficiencies.

> *When each business unit adopts its own AppSec stack, the result is a fragmented landscape that defies centralized oversight, making security management at scale nearly impossible.*
>
> **Alok Sinhasan**, Head of Cybersecurity Engineering and Solutions at Logitech

Workflow Bottlenecks and Key Pain Points

> *ASPMs make sense, but they don't solve the need for a unified platform. Organizations are still managing five different tools to ensure they don't leave any gap.*
>
> **Nir Rothenberg**, CISO at Rapyd

The Persistence of Remediation as the Primary Bottleneck

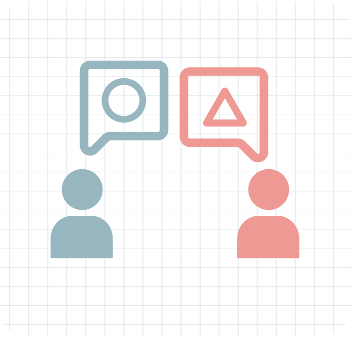
Remediation remains a critical pain point. Even when vulnerabilities are identified early, fixing them involves navigating dependencies, securing developer buy-in, and addressing organizational silos.

It takes 22 days to remediate critical vulnerabilities.

89% of respondents are not satisfied with this SLA, claiming **the attack window is open widely for attackers** during this period of time. 8% of respondents reported **a compromise attempt** during this window.

Delays with remediation are due to unclear prioritization or lack of developer alignment.

77% of respondents express dissatisfaction with the way they **interface with engineering teams**, citing excessive time spent on risk prioritization and justification.



Alert Fatigue and Inefficiencies in Vulnerability Triage

> *Triaging is one of the most frustrating processes security engineers face. It is manual, inaccurate, and leaves security teams unable to keep the pace with development.*
>
> **Ophir Oren**, Cyber Security Innovation at Bayer

Modern security tools generate high volumes of false-positive security alerts, causing alert fatigue and slowing response to real threats.

87%

Respondents are overwhelmed by the **volume of security alerts.**

45%

False positive alerts waste valuable engineering and security resources.

58%

Respondents express **skepticism** about their vulnerability scanning tools' prioritization accuracy.

Balancing Manual Processes with Automation

Despite automation's importance for security scaling, organizations heavily rely on manual vulnerability triage and runtime protection.

77%

Respondents rely on **manual triage process**, using tools such as CVSS and EPSS scores. Most acknowledge these metrics **don't accurately reflect actual risk.**

3. Adapting Application Security to Modern Environments

Shifting from Traditional to Modern Security Workflows

Organizations are shifting from traditional security models to adaptive frameworks, as static scanning proves insufficient for modern threat detection.

71%

Respondents report their current workflows are ill-suited for the demands of cloud-native applications.

2.3x

More security incidents in hybrid environments compared to fully cloud-native setups.

The necessity of microservices, APIs and continuous monitoring drives organizations to seek integrated shift-left and runtime security solutions.

> *In the cloud, physical limits no longer apply. You might go from a handful of static servers to hundreds of ephemeral ones. This explosion in server count transforms dozens of potential vulnerabilities into thousands, leaving their true relevance uncertain.*
>
> **Rick Doten,** CISO at Carolina Complete Health

The Rise of Runtime

The Criticality of Runtime Tools

While shift-left security identifies code-level vulnerabilities early in development, runtime tools provide a crucial safety net for zero-day attacks, unfixed vulnerabilities and threats in production. APIs, central to modern applications, frequently become prime targets for attackers.

64%

Organizations rank runtime application security as a top priority for the coming year.

52%

Encountered API-specific threats in the last 12 months.

33%

Mentioned runtime tools significantly helped mitigate the threats from above.

Embracing Automation for Security Workflows

Automation's Role in Addressing Discovery, Triage and Remediation

Automation is increasingly viewed as key to efficient discovery, triage and remediation, enabling security teams to focus on strategic, critical tasks.

45%

Reduction in triage times among high automation adopters.

59%

Respondents stated that automation is crucial for real-time vulnerability insights.

Integrating Automation into CI/CD Pipeline

Despite its advantages, automated security within CI/CD pipelines is still underutilized.

38%

Successfully embedded security automation into CI/CD pipelines.

55%

Respondents cite tool compatibility as the primary challenge to embed automations into CI/CD pipelines.

4. Building a Resilient Security Posture

Proactive vs. Reactive Approaches

Rapid software releases in cloud-native and hybrid environments highlight reactive security's limitations. Shift-left strategies help teams neutralize threats before reaching production.

68%

Respondents have begun adopting **shift-left practices**, but the real transformation lies in elevating security to a core development KPI, akin to code quality or performance metrics.

Using Contextual Insights to Prioritize Vulnerabilities

Real-World Exploitability: Environmental context such as API traffic and container datacombine to identify critical threats.

Predictive Analysis: By 2025, organizations plan to use AI-driven tools to anticipate threats and reduce incident response costs.

> *Risk based application security model is the need of the hour. We need a way to identify and apply defense to the business critical applications with an emphasis on risk quantification. This enables us (as an industry) to align cyber security goals with business priorities.*
>
> **Rohit Parchuri**, CISO at Yext

57%

Respondents have **integrated contextual risk analysis** in their pipelines.

82%

Respondents predict **real-world exploitability scores** will replace traditional CVSS metrics by 2025.

5. Looking Forward: Goals for 2025

The Future of Application Security Workflows

1. Autonomous Remediation

Vision: Organizations target autonomous and semi-autonomous systems for automatic vulnerability patching.

Data-Driven Impact: 73% plan to invest in AI-assisted remediation, anticipating **50%** faster fix times.

2. Runtime Solutions at the Forefront

Shifting Emphasis: Runtime-based analysis becomes essential alongside shift-left security.

Continuous Protection: Runtime analysis will become standard across security products. **62%** of security leaders plan runtime solution expansion within 18–24 months.

> *For too long, security vulnerability management teams have forced developers into their remediation workflow and ticketing system, instead of accommodating the development workflow to make it easier for them to remediate.*
>
> **Rick Doten**, CISO at Carolina Complete Health

3. The Developer-Centric Security Model

DevSecOps Maturity: Organizations seek tools that integrate into developer' workflows to speed fixes.

Culture Shift: Incentives and training will encourage developers to take ownership of security tasks, while security specialists provide strategic oversight.

4. Unified Platforms and Consolidation

Tool Sprawl Declines: Currently, **78%** of organizations use 5 or more tools. The trend moves toward unified platforms integrating code scanning, runtime monitoring and threat intelligence.

Efficiency Gains: Early adopters of unified solutions report **30% faster** remediation cycles and **50% fewer** critical vulnerabilities reaching production

Predictions on Industry Trends and Best Practices

1. AI as the Security Co-Pilot

Real-Time Threat Hunting: Machine learning models will provide automated threat containment.

Adaptive Defenses: AI will learn from active attacks, updating policies and code in near real time.

2. Supply Chain Security Takes Center Stage

Holistic Visibility: Proliferation of third-party libraries, APIs and microservices will drive up supply chain attacks. Making real-time tracking of Software Bills of Materials (SBOM) essential

Zero Trust Integration: Supply chain threats will accelerate zero-trust adoption across network and application layers.

3. Regulations and Compliance as Innovation Drivers

Evolving Standards: Data privacy laws and industry mandates will drive security innovation beyond compliance checkboxes.

Global Harmonization: Broader alignment of compliance frameworks is likely, compelling organizations to adopt advanced analytics for real-time monitoring.

6. Final Thoughts

Application security stands at a pivotal juncture. Fragmented defenses, manual processes and limited visibility can no longer contend with the speed and ingenuity of modern cyber threats. As survey data repeatedly highlights, organizations face an expanding attack surface, underscoring the urgent need for a more unified, automated and context-aware approach.

From Incremental to Transformational

Security must evolve from traditional "bolt-on" to become integral to development as source control or continuous integration. This requires:

Embedding Security from the Start: Shift-left techniques and secure coding practices must become part of standard development workflows.

Embracing Runtime Intelligence: Runtime solutions such as ADR (Application Detection and Response) and advanced API security become baseline requirements.

Unifying Tools and Data: Organizations need consolidated platforms that offer cohesive visibility across on-premises, cloud and hybrid environments.

The Role of Automation and AI

In the next few years, the leap from automated scanning to autonomous remediation will transform how vulnerabilities are addressed:

AI-Augmented Triage: Real-world exploitability scores can replace or augment traditional metrics, sharpening prioritization.

Intelligent Policy Enforcement: Automated policies will adapt in real time, applying just-in-time patches or quarantining high-risk components.

Empowering Developers and Security Teams Alike

DevSecOps will distribute security tasks more evenly between developers and specialized security teams:

Cross-Functional Training: Educating developers in secure coding, threat modeling and other best practices.

Unified Dashboards and Metrics: Providing contextual, role-based dashboards for real-time collaboration and accountability

Actionable Recommendations

1. **Integrate and Consolidate:** Minimize tool sprawl by adopting platforms that manage the end-to-end application security lifecycle.

2. **Automate Where It Counts:** Identify high-value tasks such as triaging, patching and asset discovery that benefit most from AI-driven workflows.

3. **Shift-Left Without Neglecting Runtime:** Security-as-code is essential early on, but real-time defenses are equally critical for threats that slip past development.

4. **Invest in Contextual Intelligence:** Combine exploit data, business impact and usage patterns to focus efforts where they matter most.

5. **Champion a Security-First Culture:** Foster transparent communication, shared KPIs and continuous learning between security, development and operations teams.

A New Horizon with Kodem

Organizations seeking to thrive in this landscape can look to Kodem, which unifies shift-left with runtime analysis in a single platform. Kodem's automation-driven triage, guided remediation and contextual policies empower teams to scale their applications without sacrificing security. For more information you may visit ***kodemsecurity.com***

Kodem

Looking Ahead

This report highlights the critical gaps, challenges and opportunities in application security workflows, underscoring the urgency of moving beyond fragmented tools and manual processes. Key insights reveal that slow remediation, alert fatigue and incomplete shift-left adoption remain persistent bottlenecks, while the rise of runtime solutions and automation offers a path forward.

The journey to a resilient security posture will require organizations to unify their workflows, integrate contextual risk insights and embrace both proactive and adaptive strategies. By investing in high-quality data, automation and seamless collaboration between security and development teams, organizations can not only mitigate current risks but also stay ahead of the evolving threat landscape.

Looking ahead, the next iteration of this research will explore the growing adoption of AI-assisted remediation, mitigation strategies and the future of unified security platforms. As application security evolves, so must our strategies—ensuring that innovation remains secure at every stage.

> *2025 marks a pivotal year for application security. Today's tools generate overwhelming noise, leaving teams struggling to find real threats amid the clutter. The key is delivering actual context and accurate signals—where runtime insights excel—by translating ever-changing technology into tangible risks, helping our teams gauge business impact and tackle the most critical issues first."*
>
> **Alon Hodir,** CISO at Minute Media

7. Demographics

The following demographics outline participant roles, organizational sizes and industries represented in our survey of 82 respondents - showcasing the diverse perspectives that underpin our analysis.

Roles

1. Security Leadership

- Chief Information Security Officers (CISOs), Security Managers, Heads of Security
- Shape security strategies and policies. Their insights reveal broader governance and risk management priorities.

2. Security Practitioners

- Security Engineers, Analysts, Architects
- Oversee day-to-day implementation, incident response and tool management. Their perspectives highlight real-world challenges in triaging alerts and fixing vulnerabilities.

3. Developers and DevOps Professionals

- Software Engineers, DevOps Managers, Site Reliability Engineers (SREs)
- Though a smaller segment, their input underscores the trend toward integrating security into development and operational pipelines.

Organizational Size (R&D size)

Small Enterprises (Fewer than 100 Engineers) – 20%

Operate with tighter budgets and resources, often outsourcing some security functions.

Medium-Sized Organizations (100–1,000 Engineers) – 50%

Transitioning from ad hoc security practices to more robust frameworks. Emphasize runtime tools and compliance readiness.

Large Organizations (Over 1,000 Engineers) – 30%

Possess complex infrastructures and stringent regulatory requirements. Early adopters of advanced solutions like Cloud-Native Application Protection Platforms (CNAPP) and ADR.

Industries

Technology and Software Development
The majority, reflecting tenacious focus on application security for cloud-native and API-based deployments.

Finance and Healthcare
Driven by strict compliance and data protection mandates, placing high emphasis on real-time monitoring and thorough audit processes.

Manufacturing and Energy
Increasingly integrating IT and OT (Operational Technology). Web Application Firewalls (WAF) and perimeter defenses remain prominent.

8. Methodology

This section outlines the processes used to design, conduct and analyze the survey, ensuring clarity and credibility of the results.

Survey Design

Target Audience: Geared toward CISOs, AppSec leaders and security professionals who shape and execute application security policies.

Scope of Questions: Covered discovery, triage, remediation, runtime protection, tool usage (SAST, DAST, SCA, API security, container security) and challenges like compliance or automation.

Focus on Practices: Included open-ended questions to capture nuanced insights on workflow bottlenecks, automation strategies and collaboration across teams.

Data Analysis

Quantitative Methods: Aggregated and examined responses for patterns in tool adoption, workflow bottlenecks and runtime practices. Key metrics included mean time to remediation, alert fatigue levels and usage rates for specific security tools.

Qualitative Insights: Open-ended responses were thematically coded to uncover trends, challenges and emerging best practices beyond the numbers.

Segmentation and Cross-Tabulation: Organized data by organizational size, industry and role to reveal sector-specific or role-specific perspectives.

Data Collection

Distribution Channels: Email campaigns, security forums, direct outreach to industry connections.

Response Volume and Timeline: Gathered over four weeks, ensuring a consistent window for analysis**.**

Limitations

Self-Reported Data: Responses may reflect perceived best practices rather than actual execution.

Sample Representation: While global in scope, some industries or regions could be underrepresented, affecting broad applicability.

Rapidly Evolving Landscape: Application security practices shift quickly due to emerging threats; findings represent a snapshot in time.

find your *Appy* place at

www.kodemsecurity.com