GraphNode

2024 ANNUAL REPORT

January 2025

Prepared by

GraphNode Research

@graphnodesofware

Table of Contents

01 Letter from the Team

02 The State of Application Security

03 Top Attack Vectors and Vulnerabilities

04 Modern Application Architecture Security

05 Security in the Software Supply Chain

06 DevSecOps Evolution

07 Artificial Intelligence in Security

08 Identity and Access Security

09 Compliance and Privacy Impact

10 Looking Ahead: 2025 Predictions

Letter from the Team

Dear AppSec Community,

As we present our 2024 Application Security State Report, we find ourselves at a critical inflection point in application security. As builders of SAST and SCA solutions and security researchers, what we've observed this year has been both concerning and enlightening.

Our research and daily interactions with codebases have revealed some stark realities. The data tells a sobering story: 91% of applications contain vulnerable components with known exploits, while the average time to fix critical vulnerabilities has reached 95 days. Perhaps most tellingly, 41% of security breaches were traced back to application layer vulnerabilities in 2024. These numbers reflect both the challenges and opportunities that lie ahead.

Our unique position as both researchers and security tooling providers has given us deep insights into these challenges. We've spent the past year analyzing vulnerability patterns, improving detection mechanisms, and working closely with development teams. This hands-on experience has shown us where traditional approaches fall short and where new methodologies shine in the face of evolving threats.

The growing complexity of modern applications, paired with the rapid adoption of cloud technologies, has dramatically expanded the attack surface for many enterprises. Our findings show that organizations need a comprehensive approach to security - one that spans from the first line of code all the way through to cloud deployment.
The insights and analysis that follow in this report are drawn from our extensive research, real-world implementations, and countless hours spent improving how we detect and prevent security issues in modern applications. We hope these findings will serve as both a wake-up call and a practical guide for organizations striving to build more secure applications.

Stay Secure,

91% of apps contain known vulnerable components →

95 days to fix critical vulnerabilities →

41% of breaches stem from app layer →

The State of Application Security: 2024 Overview

Application security landscape continues to evolve rapidly, presenting both new challenges and opportunities. Our research reveals critical insights into the current state of application security, highlighting significant trends and areas of concern.

Business Risk is Rising

Our comprehensive survey shows that business risk is mounting: 91% of organizations have experienced at least one security breach in their applications over the past 12 months. More concerning is that organizations report an average of 2.3 security incidents per year, indicating that breaches are becoming more frequent and sophisticated.

The Growing Complexity Challenge

The increasing complexity of modern applications has created new attack vectors and expanded the threat surface. Organizations are facing multiple challenges:

- The shift to cloud-native development (67% of applications)
- Integration of multiple third-party components
- Rapid deployment cycles and continuous delivery
- Growing API ecosystem vulnerabilities
- Microservices architecture complexities

Time to Remediation Concerns

One of the most pressing issues revealed in our study is the growing time to fix critical vulnerabilities. The average time has increased to 95 days, highlighting the challenges organizations face in prioritizing and addressing security issues efficiently.

Key Challenges in 2024

Security teams are grappling with several critical challenges:

- Limited visibility into application security posture
- Difficulty in maintaining security without impacting development velocity
- Growing complexity of supply chain security
- Integration of security into CI/CD pipelines
- Resource constraints and skill gaps

Top Attack Vectors and Vulnerabilities

The attack surface continues to expand as applications become more complex and interconnected. Our research reveals the most significant threats facing organizations in 2024.

Primary Attack Vectors

The increasing complexity of modern applications has created new attack vectors and expanded the threat surface. Organizations are facing multiple challenges:

1.Supply Chain Compromises

- Third-party component vulnerabilities
- Compromised development dependencies
- Package repository attacks

2. Cloud Infrastructure Attacks

- Misconfigured cloud resources
- Container security issues
- Serverless function vulnerabilities

3. Application Layer Vulnerabilities

- API security gaps
- Authentication/authorization flaws
- Injection attacks

Modern Application Architecture Security

Modern application architecture has fundamentally changed how organizations approach security. Our research reveals that 67% of applications are now cloud-based, marking a significant shift in how applications are built and deployed.

Microservices architecture, while offering great flexibility and scalability, has introduced complex security challenges. Organizations now struggle with securing service-to-service communications, managing container vulnerabilities, and maintaining secure orchestration across their infrastructure. The most telling statistic comes from our survey: 38% of organizations reported container or Kubernetes security misconfigurations as their primary source of security incidents.

The API ecosystem has become particularly vulnerable, as organizations expose more functionality through APIs. Traditional security measures are often insufficient for these modern interfaces, leading to authentication issues and data exposure risks. Our research shows that application teams are especially concerned with securing these interconnected services while maintaining the agility that modern architectures provide.

The adoption of cloud-native technologies has amplified these challenges. Infrastructure as Code and serverless computing have created new attack surfaces that traditional security tools struggle to address. Organizations must now think about security across their entire application stack, from the code level through to production deployments.

67% ↑	38% ↑
Cloud Adoption	Container/Kubernetes Misconfigurations

Security in the Software Supply Chain

The State of Supply Chain Risk

The software supply chain has become increasingly complex and vulnerable. Our research shows that 91% of organizations have knowingly released vulnerable applications due to dependency issues. More concerning is that 39% of organizations lack proper visibility into their third-party components, creating significant blind spots in their security posture.

91% ↑

releasing vulnerable apps

39% ↑

lack visibility

Managing Dependencies and Vulnerabilities

Organizations are struggling to maintain security across their dependency ecosystem. According to our findings, development teams use an average of 38% of their time managing and updating dependencies. Additionally, 88% of applications contain at least one known vulnerable component in their software supply chain, highlighting the scale of the challenge organizations face in securing their software supply chains.

38% ↑

time on dependencies

88% ↑

vulnerable components

DevSecOps Evolution

Integration and Automation

DevSecOps adoption has reached a critical phase in 2024, with organizations striving to seamlessly integrate security into their development lifecycle. Our research indicates that 56% of organizations have implemented automated security testing in their CI/CD pipelines. However, only 35% of development teams report satisfaction with their current security automation tools, highlighting a significant gap between implementation and effectiveness.

Developer Experience and Security Culture

The evolution of DevSecOps has placed new emphasis on developer enablement and security culture. According to our survey, 59% of organizations now provide security training and tools directly within developer workflows. Yet, developer productivity remains a concern, with 42% of developers reporting that security measures significantly impact their development velocity. This tension between security and productivity continues to be a key challenge in DevSecOps maturity.

automated security testing

56% ↑

security training

59% ↑

satisfaction rate

35% ↑

productivity impact

42% ↑

Artificial Intelligence in Security

The integration of artificial intelligence into application security represents a significant shift in how organizations approach threat detection and vulnerability management. Our research shows that 58% of organizations have already implemented AI-powered security tools in their security processes, marking a substantial increase from previous years.

The impact of AI in security goes beyond simple automation. Development teams using AI-assisted security tools report a 43% reduction in false positives, allowing them to focus on genuine security concerns rather than chasing false alarms. This efficiency gain is crucial as applications become more complex and traditional security approaches struggle to scale.

Perhaps most significantly, 72% of organizations plan to increase their investment in AI-powered security solutions over the next year. This trend reflects both the growing confidence in AI capabilities and the pressing need for more sophisticated security tools that can keep pace with modern development practices.

The adoption of AI in security practices is not without its challenges, but its potential to enhance vulnerability detection, automate routine security tasks, and provide more accurate threat assessments makes it an increasingly vital component of modern application security strategies.

→ AI tool adoption	58%
→ F/P reduction	43%
→ Planned AI investment	72%

Identity and Access Security

Identity and access management has emerged as a critical component of modern application security strategies, particularly as applications become more distributed and cloud-native. Our research reveals that credential-based attacks remain the primary entry point for breaches, with 62% of security incidents involving compromised authentication or authorization mechanisms. The complexity of managing identities across cloud environments presents unique challenges. Organizations are increasingly adopting Zero Trust architectures, with 47% of enterprises implementing strict identity verification for all users and services, regardless of location. This shift represents a fundamental change in how organizations approach access control and security boundaries.

Despite increased investment in identity security, challenges persist. Our survey indicates that 83% of organizations experienced at least one identity-related security incident in the past year. Most concerning is the rise in privilege escalation attacks, highlighting the need for more sophisticated identity management solutions and improved access control mechanisms.

The successful implementation of identity and access security requires a delicate balance between security and user experience. As organizations continue to expand their cloud presence and adopt modern architectures, robust identity management becomes increasingly crucial for maintaining security while enabling business agility.

Credential-based attacks

62% ↑

Zero Trust adoption

67% ↑

Identity-related incidents

83% ↑

Compliance and Privacy Impact

The intersection of application security and regulatory compliance has become increasingly complex as organizations navigate a growing maze of privacy regulations and industry standards. Development teams must now consider compliance requirements at every stage of the application lifecycle, from initial design through deployment and maintenance. This shift has fundamentally changed how organizations approach security, making compliance an integral part of the development process rather than an afterthought.

Regulatory Landscape Evolution

The compliance and privacy landscape continues to evolve rapidly, presenting new challenges for organizations developing and deploying applications. Organizations are facing an increasingly complex web of regulations, from data protection requirements to industry-specific compliance standards. This shifting regulatory environment has forced companies to rethink their approach to application security, particularly in areas of data handling, user privacy, and security controls.

Inovation

Organizations struggle to maintain compliance while keeping pace with rapid development cycles. The implementation of privacy-by-design principles and continuous compliance monitoring has become a significant challenge, especially in cloud-native environments. Development teams must now balance regulatory requirements with business demands for rapid delivery, leading to new approaches in how security and compliance are integrated into the development lifecycle. The move toward automated compliance checks and continuous monitoring has become essential for maintaining regulatory alignment without sacrificing development agility.

Looking Ahead: 2025 Predictions

The application security landscape is poised for significant transformation in 2025. As organizations continue to embrace digital transformation and cloud-native architectures, we anticipate several major shifts in how security is approached, implemented, and managed. The convergence of AI, cloud technologies, and evolving threat landscapes will drive new security paradigms and challenge traditional approaches to application protection.

Key predictions for 2025:

- AI-powered security tools will become mandatory for effective application security, with automated threat detection and response becoming the norm
- Zero Trust architectures will achieve mainstream adoption, driven by the continued expansion of cloud-native applications and distributed workforces
- Supply chain security will undergo a major transformation, with new standards and automated verification processes becoming industry requirements
- The integration of security into developer workflows will reach new levels of sophistication, with security tools becoming more developer-centric
- Quantum-resistant cryptography will begin to see early adoption as organizations prepare for post-quantum threats
- Privacy-enhancing technologies will become standard features in application development, driven by stricter regulations
- Cloud-native security platforms will consolidate multiple security tools into unified solutions
- Real-time application security testing will become standard practice, replacing periodic security assessments
- DevSecOps practices will evolve to include automated compliance monitoring and reporting
- Security metrics will become key performance indicators for development teams, equal in importance to delivery speed