DARKREADING

Secure SAST. Innovate Fast:
The Future of SaaS and Cloud Security

Executive Summary

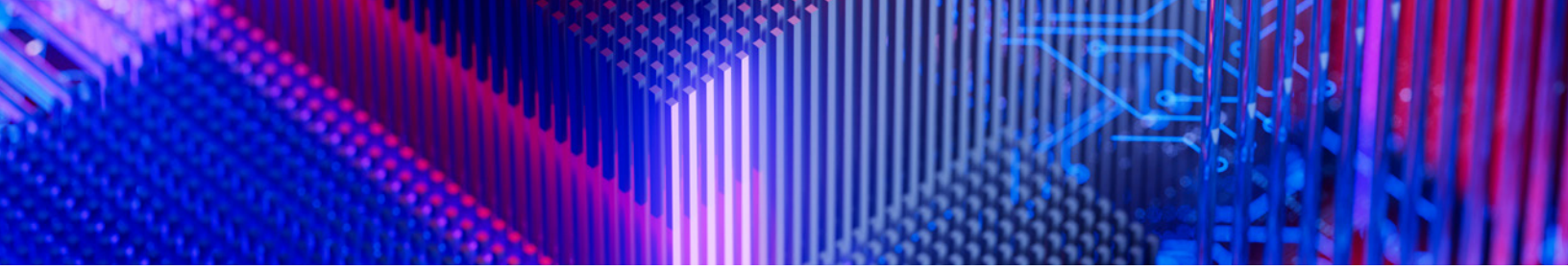
SaaS and cloud developers walk a fine line balancing security, speed, and compliance — yet many still struggle to get it right. Usage of exploits as the initial step in a breach increased by 180% in 2024, primarily through vulnerabilities in web applications.

Software breaches are becoming increasingly severe, with significant financial and reputational consequences. For example, SaaS-based payroll services provider Paycom suffered a breach that exposed 7,000 customers' information. As a result of breaches like this, companies can see stock prices decline rapidly or be subject to class action suits and regulatory fines. In Paycom's case, the company was the target of a $900,000 class action suit following the breach.

This white paper outlines how a developer-first approach to application security (AppSec) can help deliver fast, secure software development in demanding environments. It explores how seamlessly integrating security into developer workflows via AI-powered application security automation can help achieve that goal. It also focuses on what's at stake: competitiveness in a fast-moving sector, safeguarding reputation and preserving customer trust.

Sponsored by

Semgrep



Introduction: The Growing Challenges in SaaS and Cloud Security

SaaS and cloud is one of the fastest growing sectors in technology. According to Gartner, Global SaaS spending will grow 19.2% in 2025, following an 18.1% bump in 2024. Developers must build and release new services faster to stay competitive, which demands increasingly rapid application development while requiring robust security.

AppSec is also a top priority as customers entrust SaaS companies with critical business processes and sensitive data. This has led to calls for security-by-design via 'shift-left' principles, often supported via automation and DevSecOps models.

Key Challenges in SaaS and Cloud development

SaaS and cloud developers face significant challenges as they strive to deploy at speed and at internet scale:

A flood of security software vulnerabilities

Security is becoming more challenging than ever amid the increasing growth of software vulnerabilities. In 2024, almost 40,000 CVEs were added to the National Vulnerability Database, an increase of 38.8% from approx 29,000 in 2023. Excessive false positives from traditional static analysis tools compound this problem, creating "alert fatigue" for many developers.

Legacy AppSec approaches struggle to accommodate the rapid changes affecting the SaaS and cloud sectors. CVSS scores don't offer the context for prioritizing and triaging vulnerabilities, making it difficult for developers to prioritize issues based on their impact. Even the cURL development team, maintainers of a widely used open-source tool, recently abandoned CVSS for this reason. SaaS companies must understand a vulnerability's impact on data and business processes and act quickly.

This lack of context leaves developers processing a long queue of these vulnerabilities, and this inefficiency can be very costly and time-consuming. Research shows that half of developers spend 19% of their weekly hours on security-related tasks, often outside regular working hours. This adds up to around $28,000 per developer per year. It's no surprise that 73% of developers say they've experienced burnout in their career.

Misalignment of teams

Development and security teams often work in silos. Each side feels that the other throws problems over the wall without clear guidance. This leads to miscommunication and inefficiencies. The rift between these teams leads to delays with little coordination in triaging critical issues.

Regulatory demands and pressures are growing

Failing to secure code puts customer trust at stake. It also risks violating compliance rules as regulators focus increasingly on security and privacy. Companies must stay vigilant about critical security and compliance requirements and frameworks, including SOC2, GDPR, SEC breach disclosure mandates, and PCI DSS 4.0 (effective 2024). The EU has the Network and Information Security Directive 2 (NIS2), the Artificial Intelligence Act (AI Act), and the Digital Operational Resilience Act (DORA). Understanding and addressing these frameworks is essential for maintaining security, regulatory compliance, and business resilience.

Supply chain security risks

Open-source software (OSS) is foundational in modern application development, offering developers access to an expansive ecosystem of frameworks, tools, and reusable code. Two-thirds of all organizations increased their use of open-source software last year. Yet, its collaborative and decentralized nature also introduces significant security risks—exposing software supply chains to vulnerabilities that can be difficult to detect and manage.

Security Without Compromise:
Why Speed and Security Must Coexist

While these challenges are widespread, they are amplified by the pace and scale of cloud-native development. However, development teams don't need to trade development productivity for security.

The key is to tackle AppSec with intent. A proactive, developer-first approach to AppSec allows you both speed and security, resulting in greater productivity. That makes development faster, improving velocity and developer morale.

The Role of AI and Automation in Security

The key to this proactive approach is AppSec AI-powered automation for specific repetitive tasks such as triaging vulnerabilities. While individuals can efficiently complete these tasks individually, their cumulative volume adds up very quickly and becomes overwhelming.

AI can quickly manage repetitive, time-consuming work and serve as a force multiplier. It serves as an assistant that enhances existing AppSec engineers' capabilities, allowing them to focus on more strategic priorities.

Automated AI-powered SAST tools like Semgrep Assistant triage issues automatically to eliminate false positives and provide actionable remediation guidance. As it learns, it evolves, capturing rules and exceptions that developers can customize. One of AI's most powerful strengths is its ability to learn and improve over time. Semgrep Assistant uses "memories" to learn the organization-specific context needed to determine exploitability moving forward. This capability can cut vulnerability backlogs dramatically by triaging technical debt.

Structuring Teams for Secure Development

Automation is a key component of a proactive, developer-first security process, and team structure is equally important. Organizing teams effectively builds strong working relationships and fosters collaboration between developers, security, and compliance. Structural changes include embedding security team members in software development teams and vice versa to encourage cross-team education. Establishing a "security champion" in a development team is a longer-term outcome of this collaboration. Consider joint training initiatives and the creation of agile "pods" that include QA, security, and software development experts in a single team that handles a project from conception through to delivery.

These siloed teams often have competing priorities. They must communicate with each other more effectively by integrating automated systems. This helps them collaborate on AppSec from the early stages of software development (shifting left), moving companies further towards secure-by-design principles.

The Future of SaaS and Cloud Security

Studies show that 58% of companies experienced a SaaS security breach in the past year. The attack surface will grow as code bases and technology stacks become more complex, and the proliferation of cloud services, open-source libraries, and APIs brings new vulnerabilities.

There has also been growing attention on supply chain security. Software bills of materials (SBOMs) are becoming increasingly important for organizations as awareness of software bugs in upstream software grows.

An SBOM is a detailed inventory that lists all the components—including libraries, modules, and dependencies—in a software application, much like an ingredient list on food packaging. It is used to improve software security and compliance by allowing organizations to quickly identify vulnerable or outdated components when security issues arise quickly.

The US administration has mandated SBOMs for federal agencies in an executive order, and organizations like NIST, ISO, and OpenSSF (Open Source Security Foundation) are developing frameworks to standardize SBOM usage.

For these reasons, we anticipate an increasing role for AI and automation. Security leaders have already stressed that AI will be critical and play a pivotal role in safeguarding modern software.

What Next?

Security doesn't have to slow developers down. When integrated correctly, it can be an accelerator and become a competitive advantage. Adopting a developer-first, AI-driven security can transform your workflow, accelerating innovation and compliance while staying ahead of emerging threats.

Here's a quick checklist to get you started:

- **Foster collaboration:** Break down silos to integrate security, compliance, and developer teams early and often.
- **Automate intelligently:** Adopt AI-powered tools to streamline vulnerability triage and reduce noise.
- **Shift security left:** Use these organizational and automation measures to embed security checks early in the development cycle.
- **Focus your resources on what truly matters:** Prioritize threats that matter most, reducing noise and developer burnout.
- **Plan for the future:** Implementing a robust security platform will help you to anticipate future compliance and supply chain requirements.

SaaS and cloud software companies that master these steps won't just survive — they'll lead. Find out more about how developer-first AI-enabled AppSec can get you ahead of the game by contacting Semgrep for a demo.

References

1. "2024 Data Breach Investigations Report." Verizon Business, 2024, www.verizon.com/business/resources/reports/dbir/.
2. "$900,000 Paycom data breach class action settlement." Top Class Actions, October 2024, https://topclassactions.com/lawsuit-settlements/closed-settlements/900000-paycom-data-breach-class-action-settlement/
3. "Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025." Gartner, 2025, www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025.
4. "NVD - Statistics." Nist.gov, 2025, nvd.nist.gov/vuln/search/statistics?formtype=Basic&resultstype=statistics&searchtype=all&isCpeNameSearch=false.
5. "CVSS Is Dead to Us." Daniel.haxx.se, 23 Jan. 2025, daniel.haxx.se/blog/2025/01/23/cvss-is-dead-to-us/.
6. "IDC Report: The Hidden Cost of DevSecOps PPC." JFrog, 22 Jan. 2025, jfrog.com/the-hidden-cost-of-devsecops-ps/.
7. "The State of Developer Ecosystem 2023 | the JetBrains Blog." The JetBrains Blog, JetBrains Blog, 8 Feb. 2024, blog.jetbrains.com/team/2023/11/20/the-state-of-developer-ecosystem-2023/.
8. "Announcing: The 2024 State of Open Source Report." Open Source Initiative, Feb. 2024, opensource.org/blog/announcing-the-2024-state-of-open-source-report.
9. "2024 State of SaaS Security Report Shows a Gap | CSA." Cloudsecurityalliance.org, 2024, cloudsecurityalliance.org/blog/2024/05/16/2024-state-of-saas-security-report-shows-a-gap-between-security-team-confidence-and-complexity-of-saas-risks.
10. "Improving the Nation's Cybersecurity." Federal Register, 17 May 2021, www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.
11. Rundle, James. "Cyber Companies Stress AI as Core Future Technology." WSJ, The Wall Street Journal, 7 Mar. 2025, www.wsj.com/articles/cyber-companies-stress-ai-as-core-future-technology-6944ae93.