activestate

The 2025 State of Vulnerability Management and Remediation Report

March 2025

activestate

Table of Contents

Executive Summary

Modern software development relies heavily on open source components, forming the backbone of today's innovation-driven world. While open source powers everything from cutting-edge applications to critical infrastructure, it also introduces complexity, risks, and vulnerabilities. Vulnerable and outdated open source components are primary elements affecting organizations' security, and a single vulnerable library can compromise an entire application.

Despite growing awareness and some security measures, organizations face challenges in effectively managing and remediating vulnerabilities, including balancing deployment speed with security, prioritizing critical issues amidst increasing complexity, and a lack of skills within security teams. Furthermore, a failure to integrate security into the software development lifecycle leads to vulnerabilities being addressed after deployment rather than during development.

The financial and reputational repercussions of neglecting open source vulnerabilities can be severe, as highlighted by the Equifax breach[1], which cost them $1.3B. Beyond monetary losses, breaches erode customer trust and damage an organization's reputation.

Vulnerability scans often generate excessive data and false positives, and prioritizing vulnerabilities can be time consuming. Organizations also struggle with complex fixes and understanding breaking changes that push the Mean Time to Resolution (MTTR) from several days to many months. To ensure that organizations can continue their mission without faltering, they must be equipped with solutions that scalably address open source risks. This requires a strategic approach to identifying, managing, and mitigating risks within the open source components and dependencies.

This report showcases the results of a recent survey of DevSecOps personnel and how they and the companies they support deal with remediating vulnerabilities. The takeaway? Most enterprise applications remain at risk due to insufficient mechanisms for prioritizing and remediating vulnerabilities, whether that stems from a lack of resources, skills, processes, or tools. To address these gaps, organizations must go beyond their traditional tooling with vulnerability blast radius assessments, risk prioritization and breaking change analysis powered by AI, and secure and automated remediation that integrates seamlessly into the CI/CD process. The result? A stronger security posture for an organization—and more time for dev teams to innovate.

Vulnerable Components as a Major Threat

According to survey respondents, vulnerable and outdated components are the primary elements affecting organizations' security posture (20.26%).

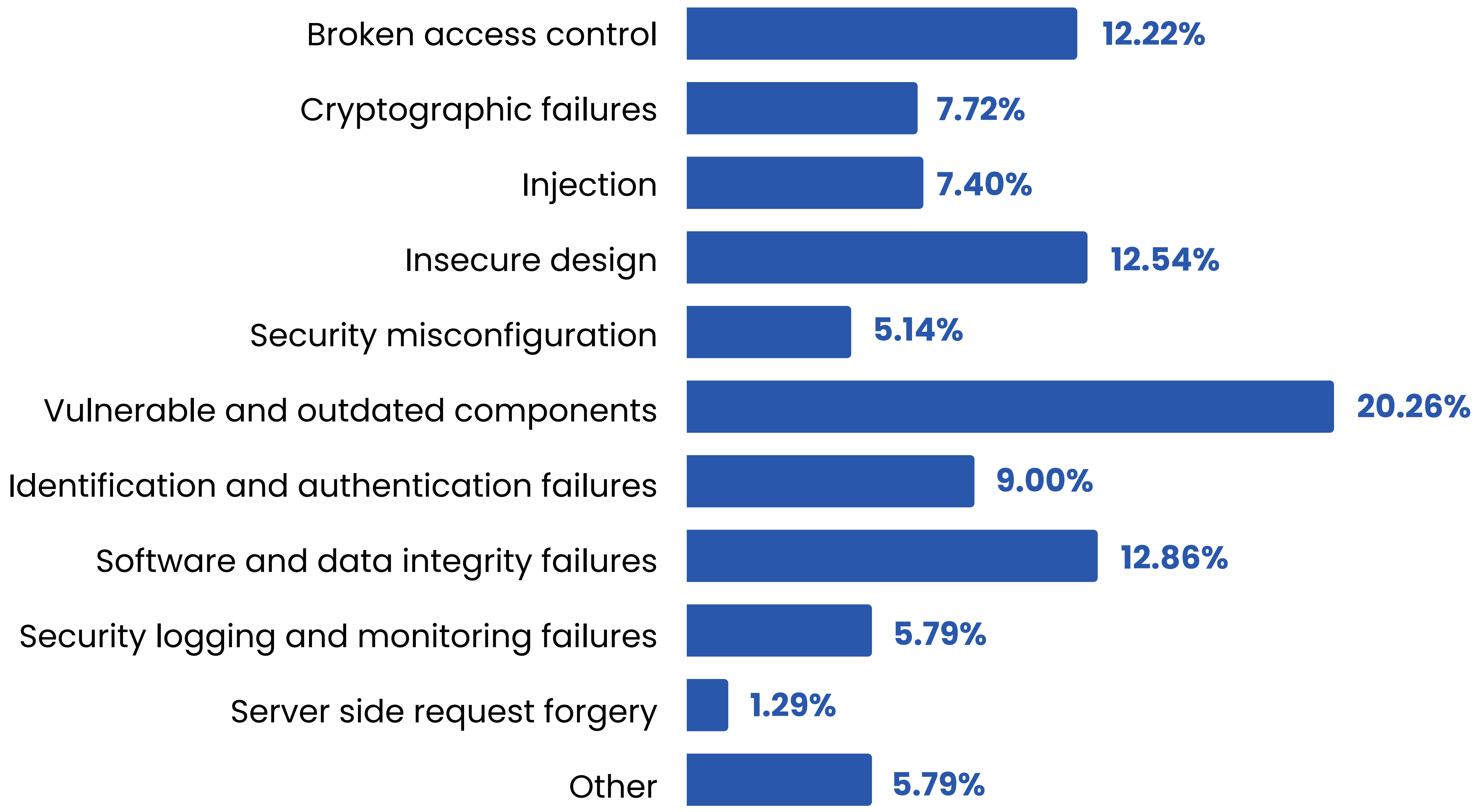


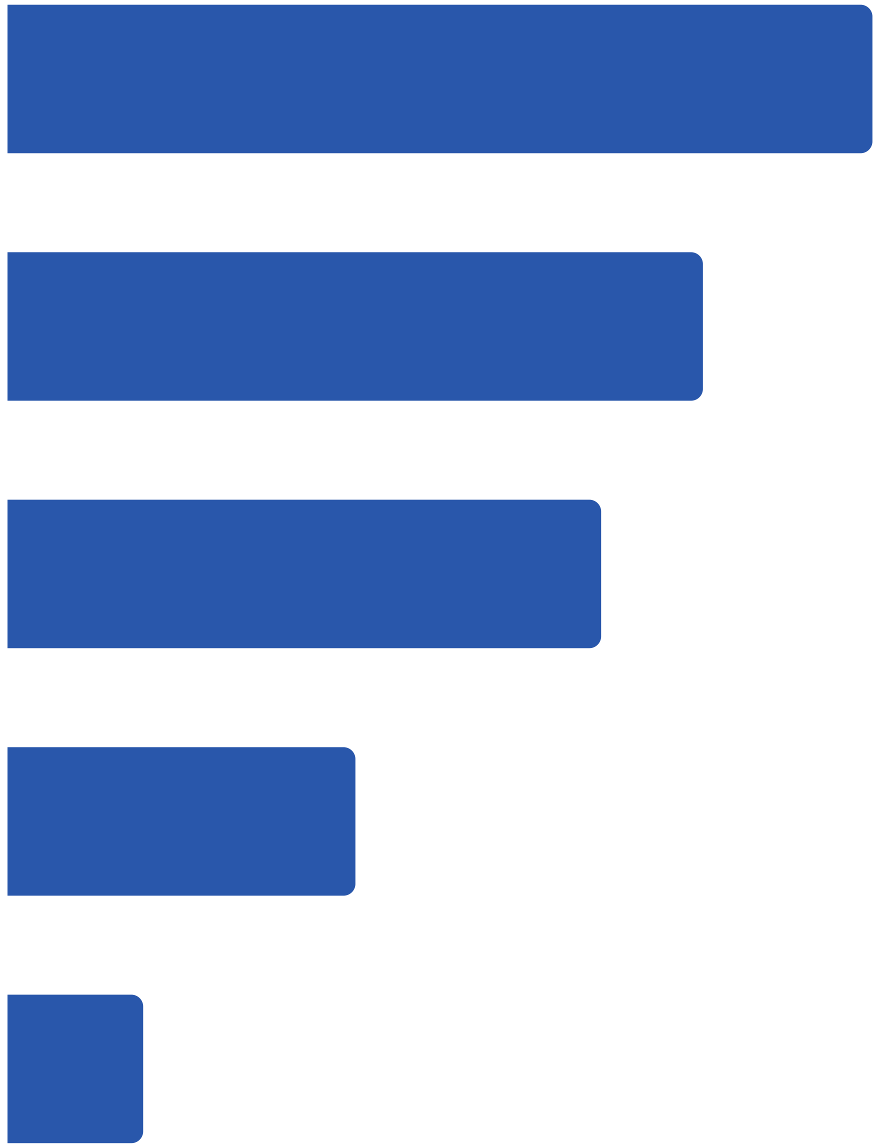
Figure 1:

The top 10 most common vulnerabilities affecting organizations the most

Open source components constitute a significant portion of modern applications, with studies showing that up to 96% of enterprise applications rely on open source libraries, often making up 60-80% of the codebase. These dependencies expedite development and reduce costs but also introduce risks if not properly managed. A single vulnerable library can compromise the entire application, as seen in high-profile breaches like Equifax (2017) and Log4j (2021).

Vulnerabilities in transitive dependencies—those indirectly included—create a cascading risk. Without active monitoring and remediation, organizations leave themselves exposed to data breaches, ransomware, or operational disruptions.

While ~32% of survey respondents stated they use some form of third-party security tools to monitor for and remediate vulnerabilities, **approximately 53% respondents are putting their security at risk** by relying on others to maintain/fix open source vulnerabilities, having limited capability to track and manage their risk, or knowingly using bad open source.



32.80%
of organizations use third-party security tools to monitor for and remediate vulnerabilities

26.37%
of organizations rely on third party and open-source components in their software **trusting the maintainers** to make sure they are free of vulnerabilities

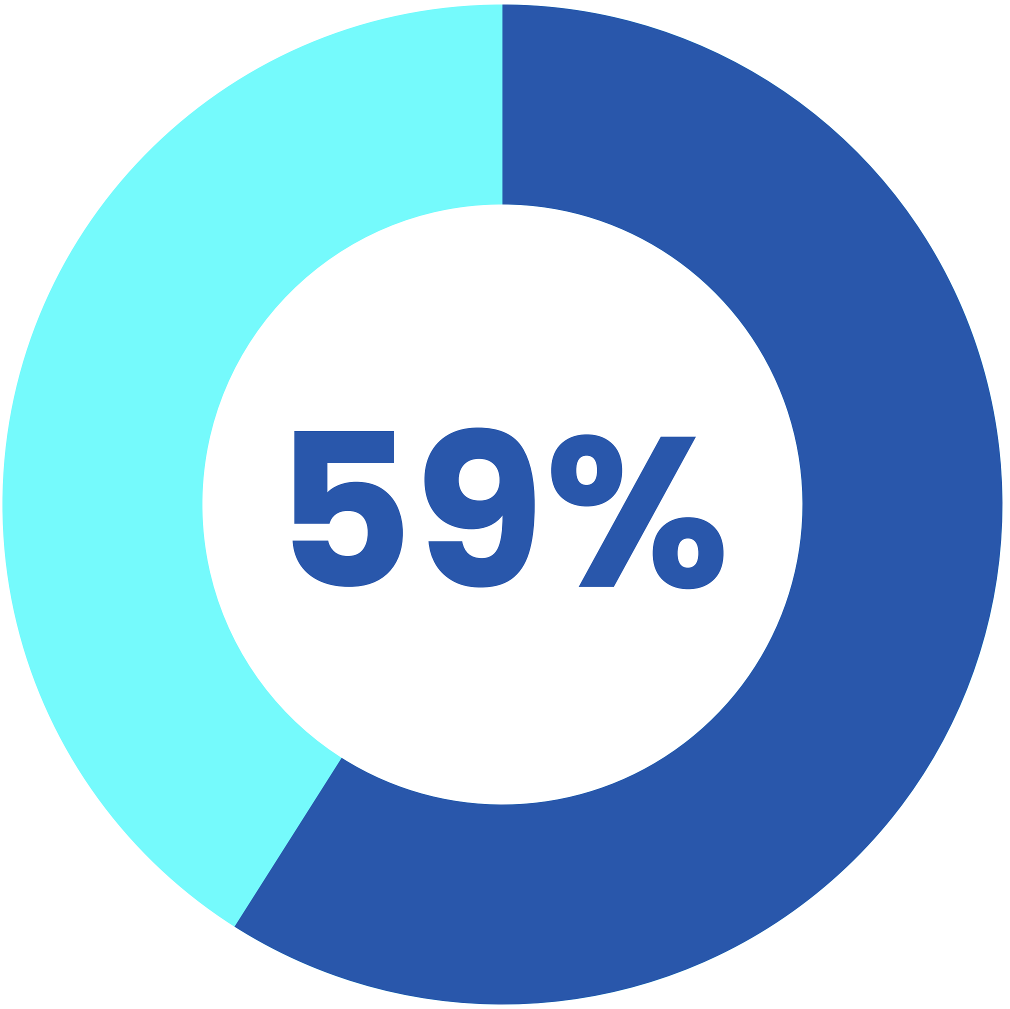
22.51%
of organizations have a **limited ability to track and manage** vulnerabilities in open source dependencies

13.19%
of organizations don’t use open source software because of the risk

5.14%
of organizations often use **outdated or unmaintained open-source libraries**, increasing their exposure to known vulnerabilities

Figure 2:

Third Party software can be a significant vector for vulnerabilities - how is your organization mitigating this risk?

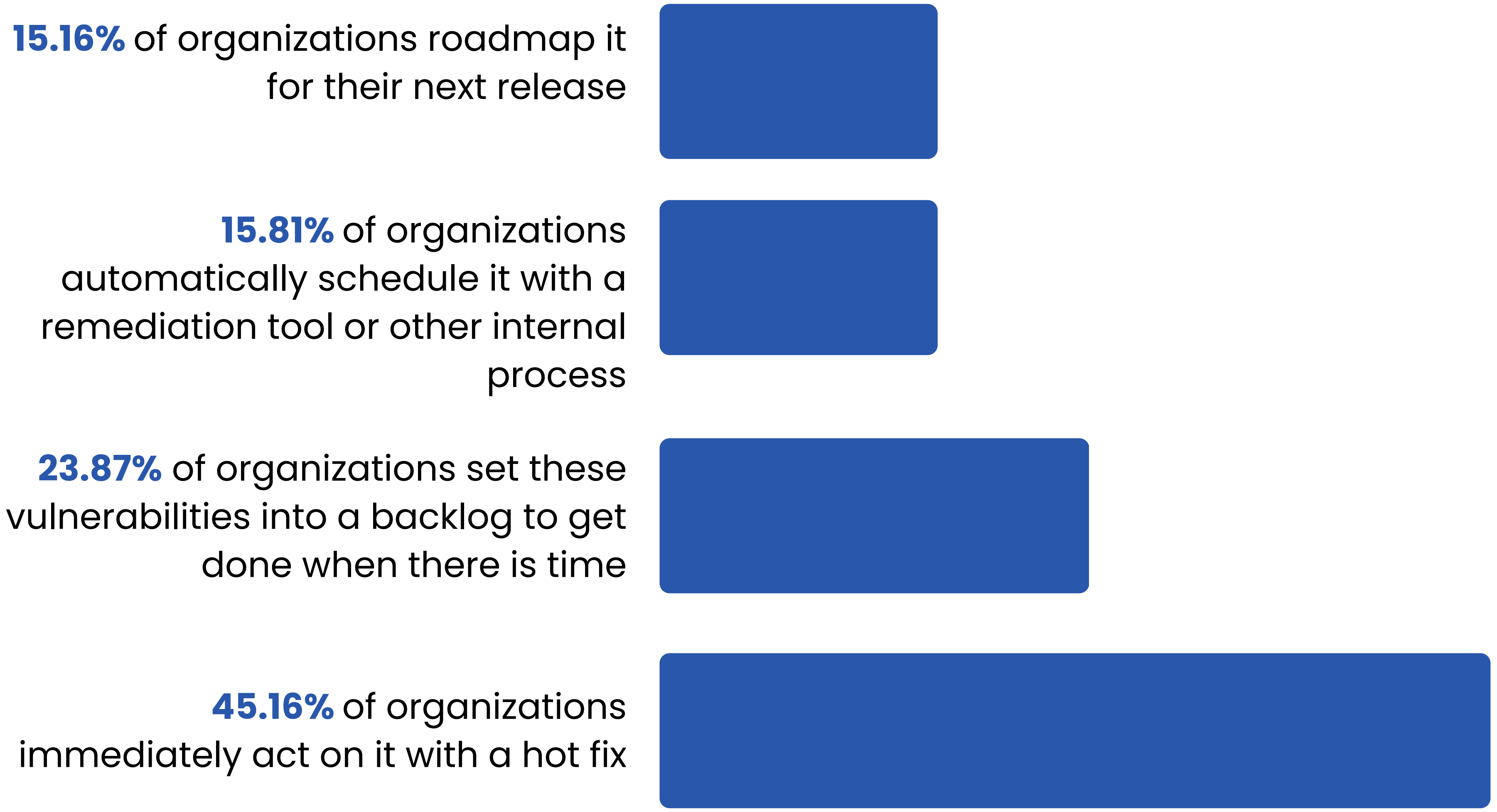


Fifty-nine percent of organizations have deployed Software Supply Chain Security (SSCS)[2] measures to improve application security, yet only 13% of high-risk vulnerabilities were remediated in 2024[2] and there has been a 54% year-over-year increase in high-risk vulnerabilities in application code[2].

Acting on Vulnerabilities

When a vulnerability is discovered, almost half (45.16%) of respondents say their organizations act immediately with a hotfix.

This reflects a **reactive approach** to addressing security threats as they arise, potentially sidelining planned roadmap items and feature enhancements due to the immediate need to address the vulnerability. This mindset also leaves organizations perpetually playing catch up with attackers.



15.16% of organizations roadmap it for their next release

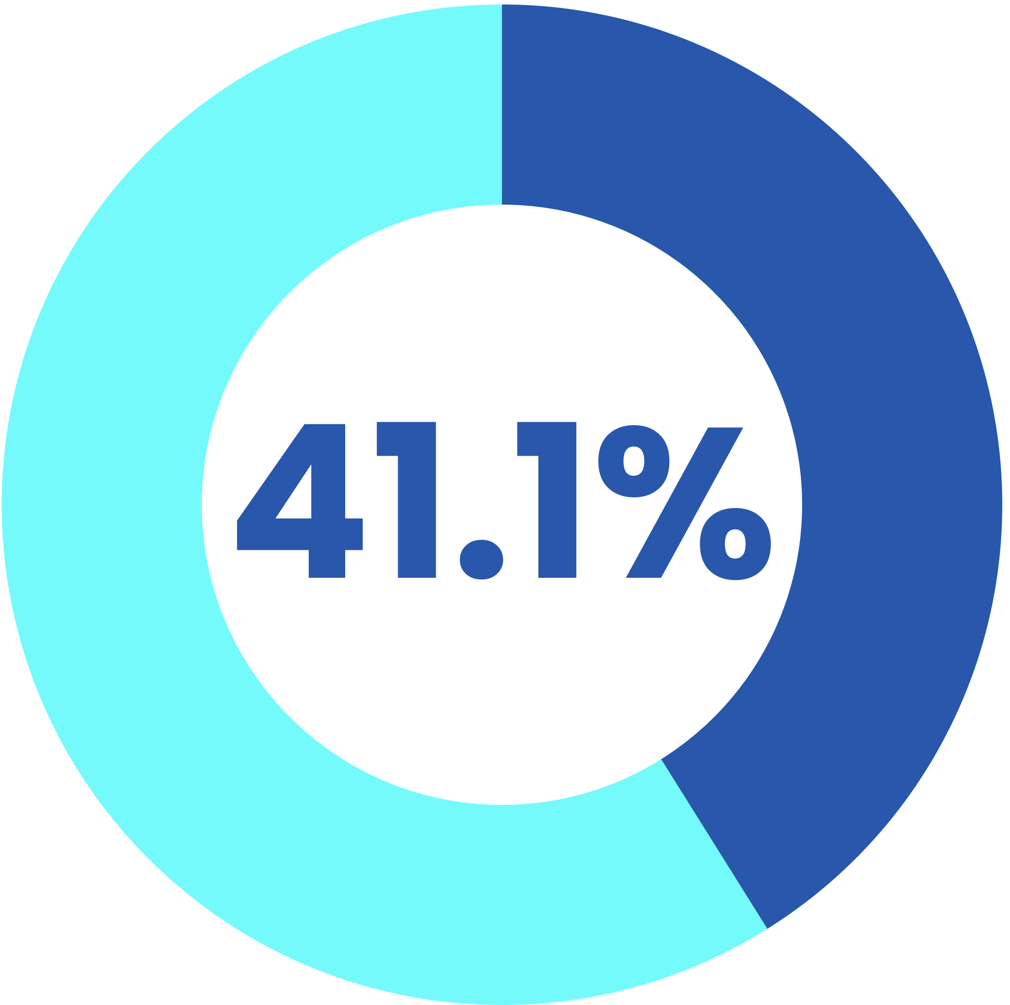
15.81% of organizations automatically schedule it with a remediation tool or other internal process

23.87% of organizations set these vulnerabilities into a backlog to get done when there is time

45.16% of organizations immediately act on it with a hot fix

Figure 3:

When a vulnerability is discovered how is remediation prioritized?



Forty-one point one percent of survey respondents said they measure the success of their vulnerability remediation efforts by Mean Time to Resolution (MTTR).

41.10%
of organizations measure it by tracking **Mean Time to Resolution (MTTR)**

34.30%
of organizations measure it by tracking the number of vulnerabilities found and resolved

13.92%
of organizations don’t track their resolutions or don’t measure the effectiveness of their remediation

10.68%
of organizations claim they don’t have vulnerabilities

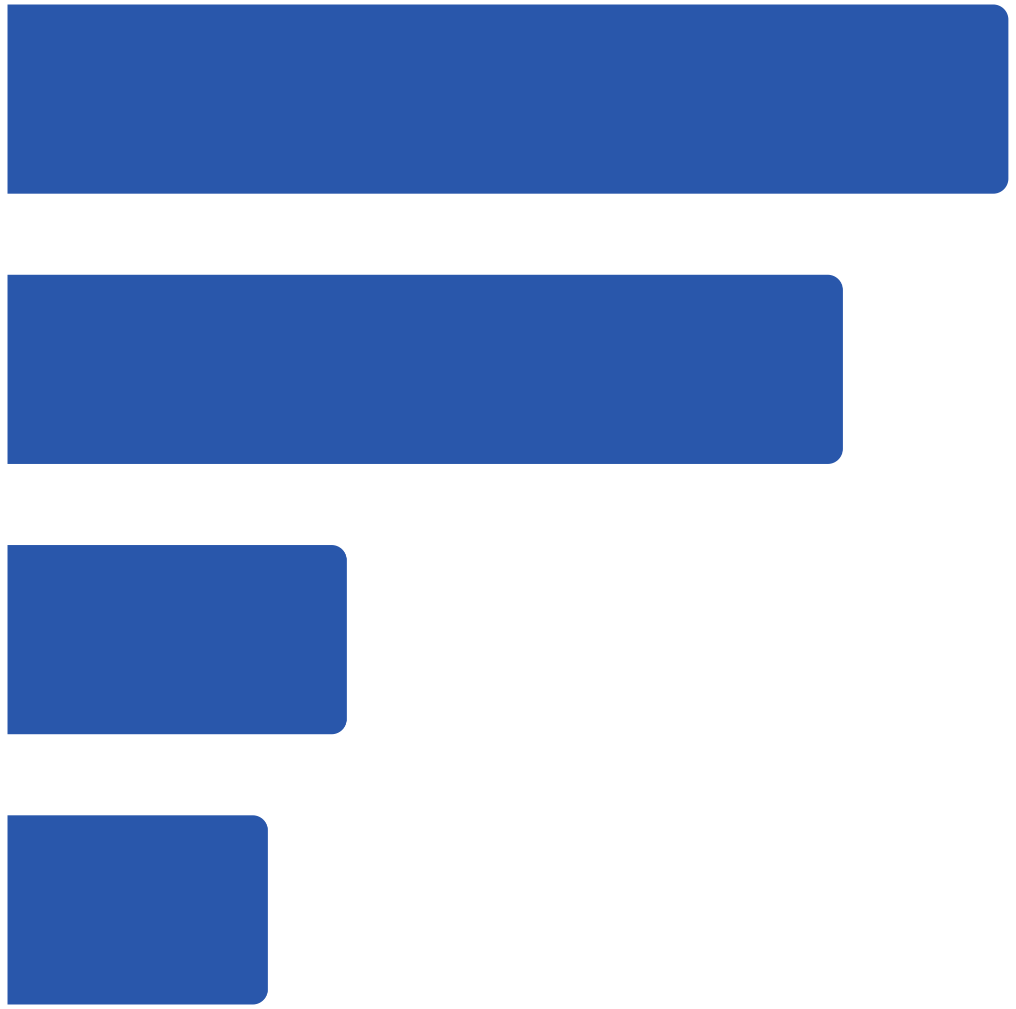


Figure 4:

How is the effectiveness of vulnerability remediation measured in your organization?

Open source vulnerabilities are publicly disclosed, making them easily exploitable if left unpatched. Attackers often exploit known vulnerabilities before organizations can respond: >50% of CVEs have exploits developed and published to the dark web within 7 days of discovery[3]. By contrast, less than 40% [4] of organizations successfully remediate vulnerabilities and it takes them 270 days[5] on average to do so. So while tracking MTTR is important, it is not necessarily a meaningful measure of security posture if it extends beyond the average time to exploit a vulnerability.

When asked about the factors impacting the time to remediate a vulnerability, **41.61% of survey respondents noted the major factor was the complexity of the fix**, followed by 18.39% stating understanding breaking changes most impacting the time to fix.

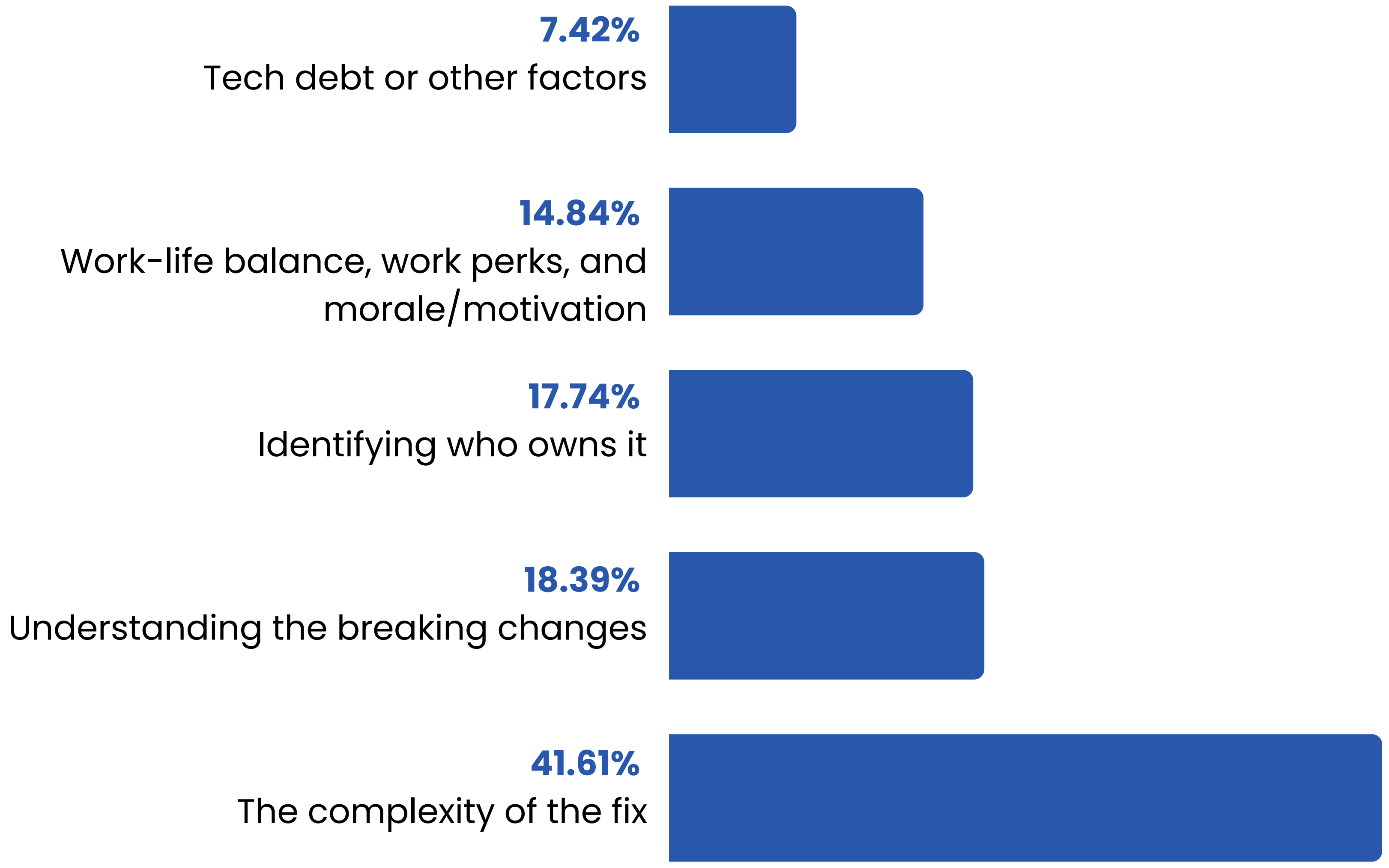


Figure 5:

The major factors impacting organization’s ability to remediate vulnerabilities

A failure to integrate security into the software development lifecycle (e.g., through DevSecOps) leads to vulnerabilities being addressed after deployment rather than during development, introducing additional complexity and increasing the likelihood of encountering breaking changes.

A DevSecOps mindset reflects a proactive strategy to identify and remediate vulnerabilities early in the development process, reducing the risk of security breaches and ensuring that security is a shared responsibility across development, security, and operations teams.

According to a recent IDC study, “Catching security issues earlier, improving the security posture of applications, and improving the pace of app development while maintaining security posture are top drivers for adopting DevSecOps.”

activestate

Balancing Speed with Security

The respondents’ biggest challenge in achieving faster deployments while maintaining security is balancing speed with security controls (34.07%).

This finding underscores the inherent tension between the desire for rapid software deployment and the necessity of implementing thorough security practices.

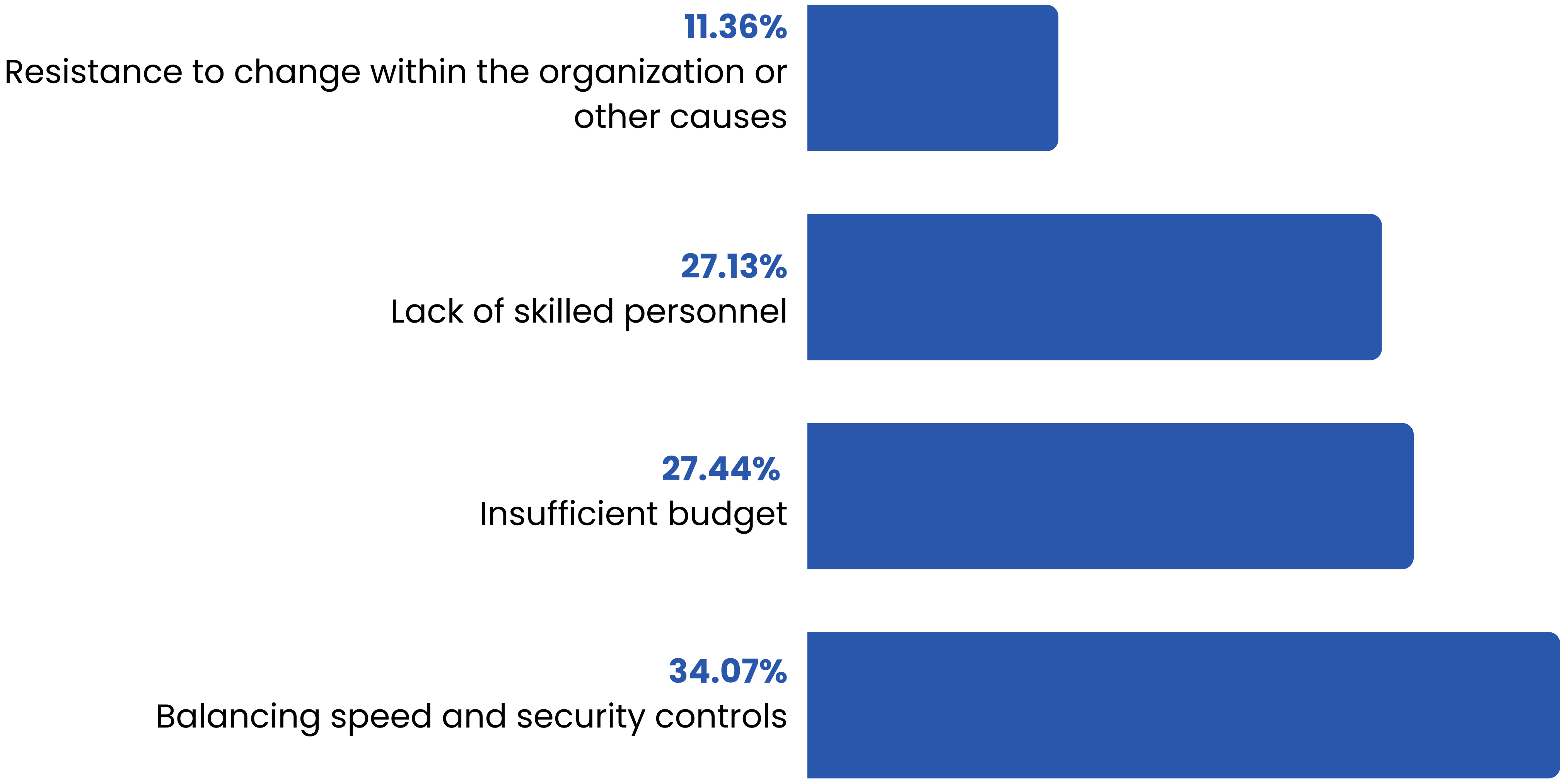


Figure 6:

Challenges in achieving faster & secure deployments

Modern organizations face an ever-growing number of vulnerabilities due to the increasing complexity of software ecosystems and the rapid discovery of new issues. This makes it difficult to address all vulnerabilities effectively, leading to “analysis paralysis” where teams struggle to prioritize and act on critical issues. Many vulnerability scans generate excessive data, including false positives, duplicates, and low-priority issues, which can overwhelm teams and divert attention from critical vulnerabilities.

Vulnerability scanners often fail to provide adequate context about how a vulnerability impacts a specific application or business environment. Without this information, teams cannot accurately prioritize remediation efforts. Tools like CVSS scores may not fully account for exploitability or business risk, leading to misaligned priorities.

In late 2024, ActiveState’s own DevOps team benchmarked the time and effort required to drive all categories of vulnerabilities to zero within our own product environment without a dedicated remediation tool, and found that prioritization of discovered vulnerabilities took more than 25% of the total time for the remediation project (73 out of 280 hours). This involved hands-on research to understand if the vulnerability was reachable and exploitable, and then determining the next step based on those findings (remediate or VEX). Anecdotally, however, the team described this as the most tedious part of the project.

Discover	Prioritize	Remediate	Total
32 hours	73 hours	172 hours	280 hours
13%	26%	61%	100%

Table 1:

Summary of ActiveState’s Vulnerability Management Project hours by stage of vulnerability management, without dedicated tools for vulnerability management and remediation

activestate

Remediation Ownership & Skills

Survey results show that when respondents were asked, “Who owns remediation in your organization?” the most common answer was “Ops, Dev, & Product” at 25.81%, closely followed by “Dev” at 21.61%, “Product” at 19.35%, and “Ops” at 19.03%. Nine percent (9.03%) of respondents indicated that “No One” owns remediation within their organization. This suggests a diffusion of responsibility, where remediation efforts are fragmented across different teams without a single point of accountability, or a gap where no one is clearly responsible for remediation, highlighting a potential area of organizational inefficiency.

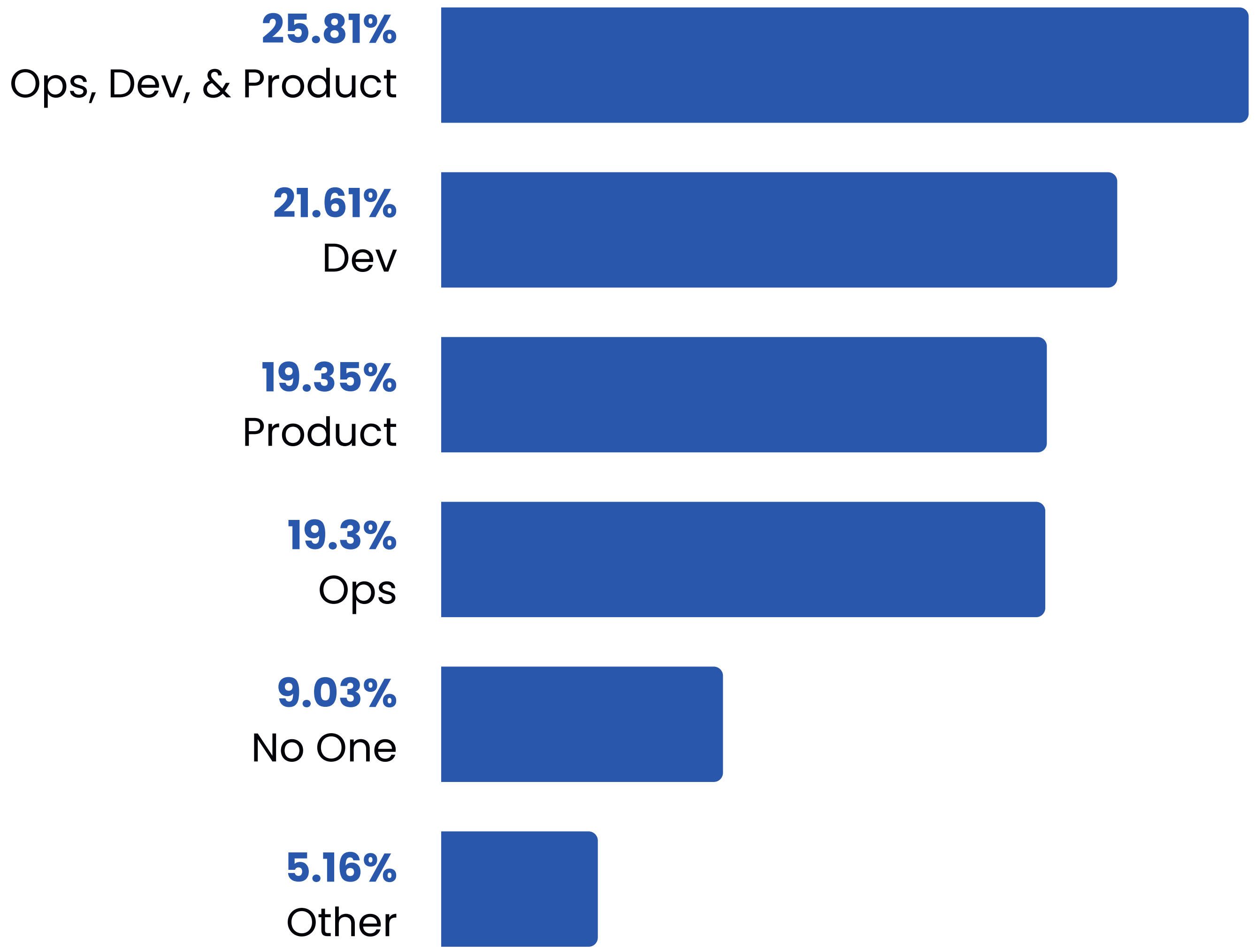


Figure 7:

Who owns remediation in most organizations?

Over 27% of respondents said that their biggest challenge to responding faster and more securely to vulnerability management is a lack of skills within their teams.

A recent IDC report had similar findings: 11.4% of their respondents ranked developers' lack of security skills and knowledge as a barrier to empowering developers to finding and fixing vulnerabilities, ranking third after limited budget or staffing and prioritizing features over security.

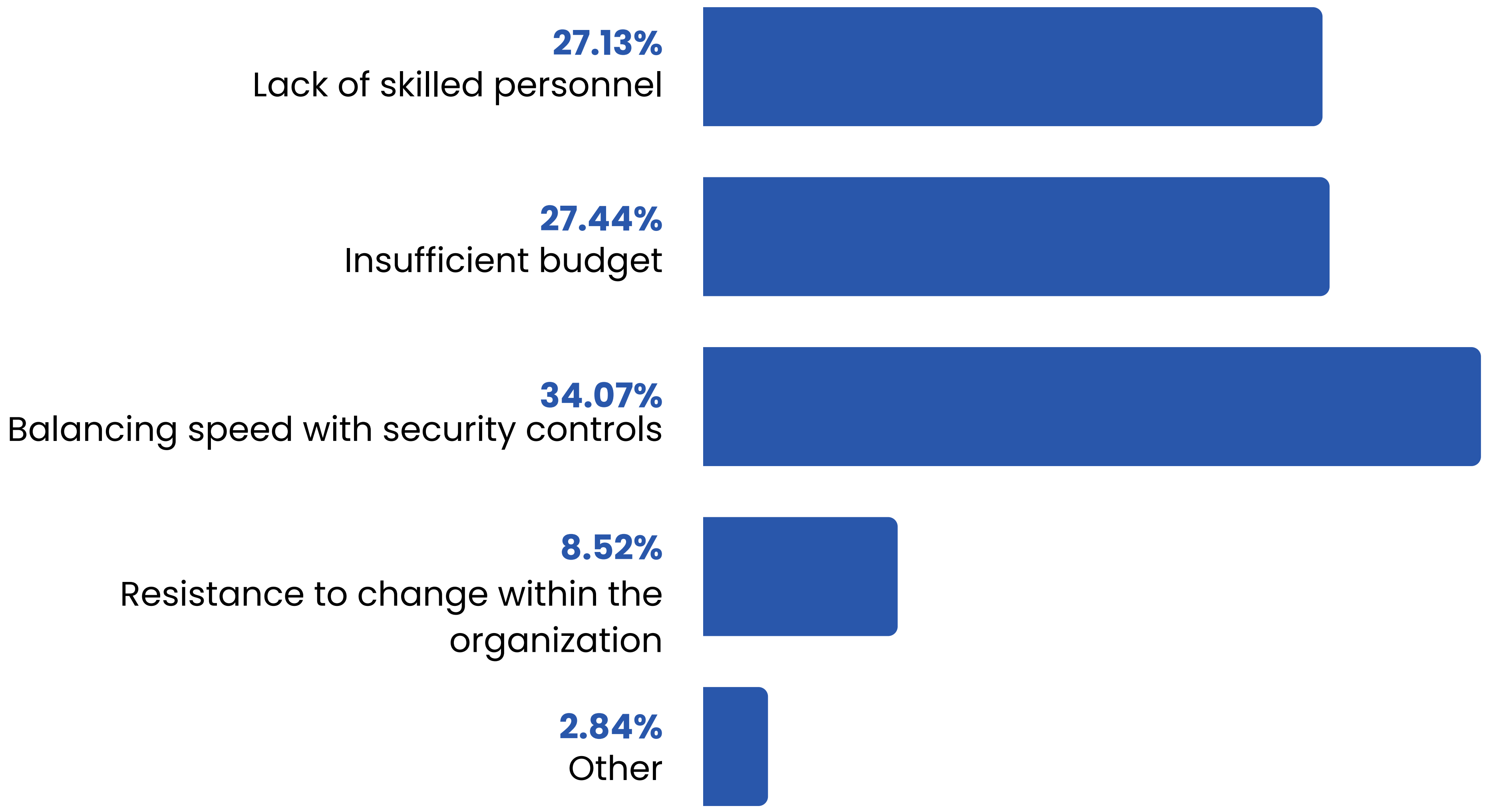


Figure 8:

Which of the following is the biggest challenge in achieving faster deployments while maintaining security

Addressing the Challenges

Open source software is the backbone of modern development. Whether teams are building in the cloud, on-premise, or in a hybrid environment, open source powers everything from cutting-edge applications to critical infrastructure. But with this reliance comes a daunting challenge: managing the complexity, risks, and vulnerabilities hidden within an ever-expanding web of dependencies. For technology executives and decision-makers, the stakes have never been higher.

How do you secure your software supply chain without slowing down innovation?

How do you empower your teams to stay ahead of vulnerabilities while navigating the growing complexity of open source ecosystems?

The ActiveState Platform

The ActiveState Platform was built to answer these questions, address the findings in this survey, and to transform how organizations manage open source security. It’s not just a tool; it’s a paradigm shift in vulnerability management.

By combining deep dependency intelligence, critical risk prioritization, and precision remediation, we deliver a scalable solution that empowers DevSecOps teams to secure their applications with confidence and efficiency.

1

ActiveState helps companies:
Understand the True Extent of Risk with a Vulnerability Blast Radius

Traditional tools often leave teams guessing about the true scope of vulnerabilities across their codebase. ActiveState changes that by providing unparalleled visibility into an organization's open source landscape, leveraging our curated catalog of more than 40M+ components and more than 25 years' experience—so they can understand not just what's vulnerable, but how deeply those vulnerabilities extend.

With ActiveState, teams finally have the clarity needed to identify vulnerabilities at their root and understand their cascading impact across systems.

2 ActiveState helps companies: **Make Smarter Decisions with a Risk Prioritization Copilot**

Not all vulnerabilities are created equal—and not all fixes are worth the disruption they might cause. That’s why the ActiveState Platform uses AI to help teams cut through the noise and focus on what matters most: addressing risks intelligently while minimizing impact on first-party code. With ActiveState, teams are empowered to make informed decisions that balance risk mitigation with resource allocation—without compromising speed or agility.

3 ActiveState helps companies: **Fix Vulnerabilities Faster with a Precision Remediation Pipeline**

Knowing what needs fixing is only half the battle. The real challenge lies in implementing secure fixes quickly and efficiently—without disrupting development workflows. That’s where ActiveState’s Precision Remediation Pipeline comes in. By automating remediation end-to-end—from identifying a vulnerability to delivering secure artifacts into production—we eliminate bottlenecks and give time back to developers so they can focus on what they do best: **innovating**.

Summary

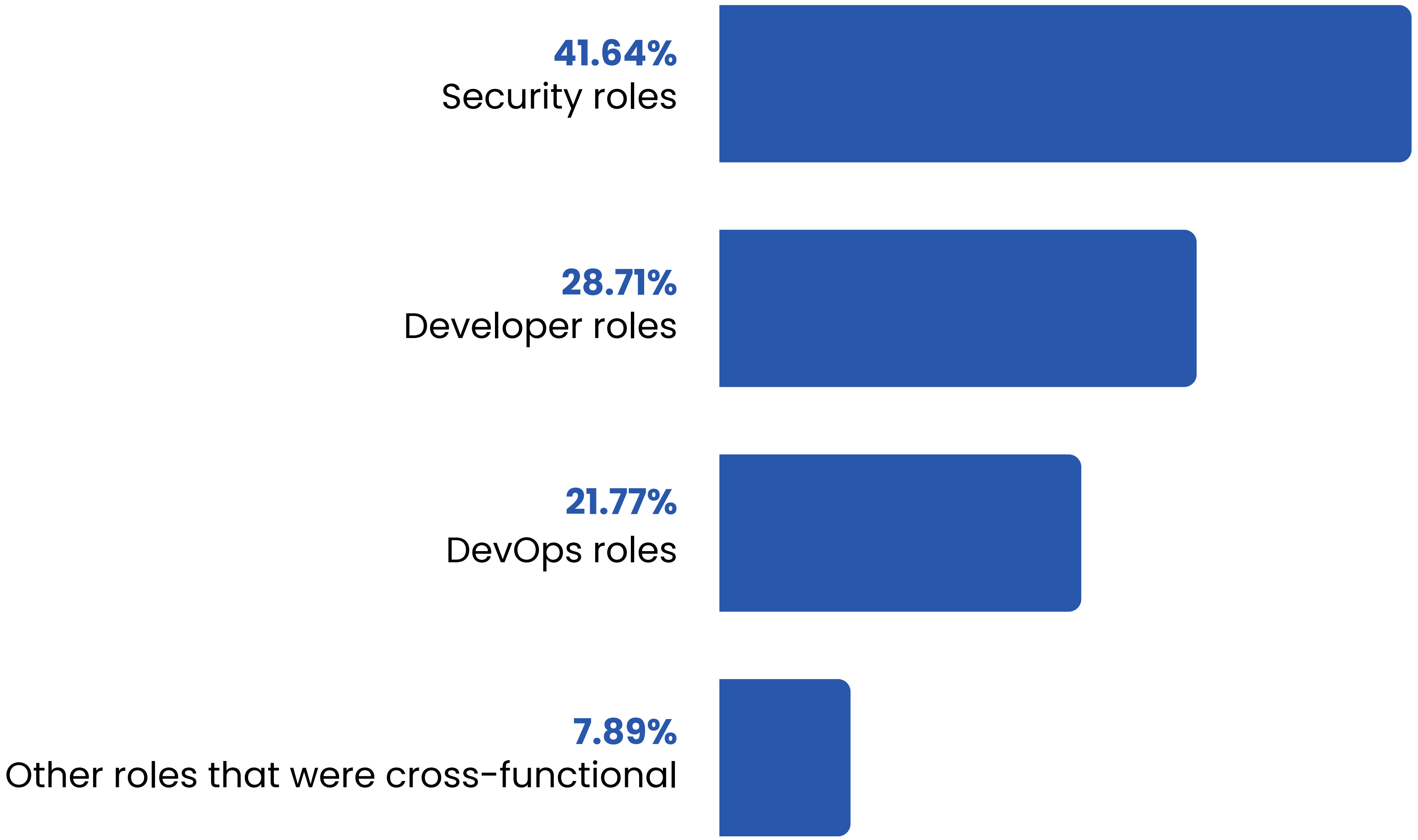
Vulnerability management and remediation is the last mile for enabling companies to secure their applications and improve their security posture. As seen in the survey results, there are still important areas where companies need to invest time and resources to up-level their vulnerability management capabilities and processes.

Tools that address the myriad risks and vulnerabilities that open source introduces can help organizations not only uncover the true risk in their application portfolio, but also directly impact how teams triage and prioritize what to fix, assess the impact of breaking changes when making updates, and securely building and deploying remediations.

About This Survey

ActiveState's Security and Product research team developed a set of 28 questions to better understand the current state of vulnerability management and remediation and the specific pains that companies are experiencing when utilizing open source.

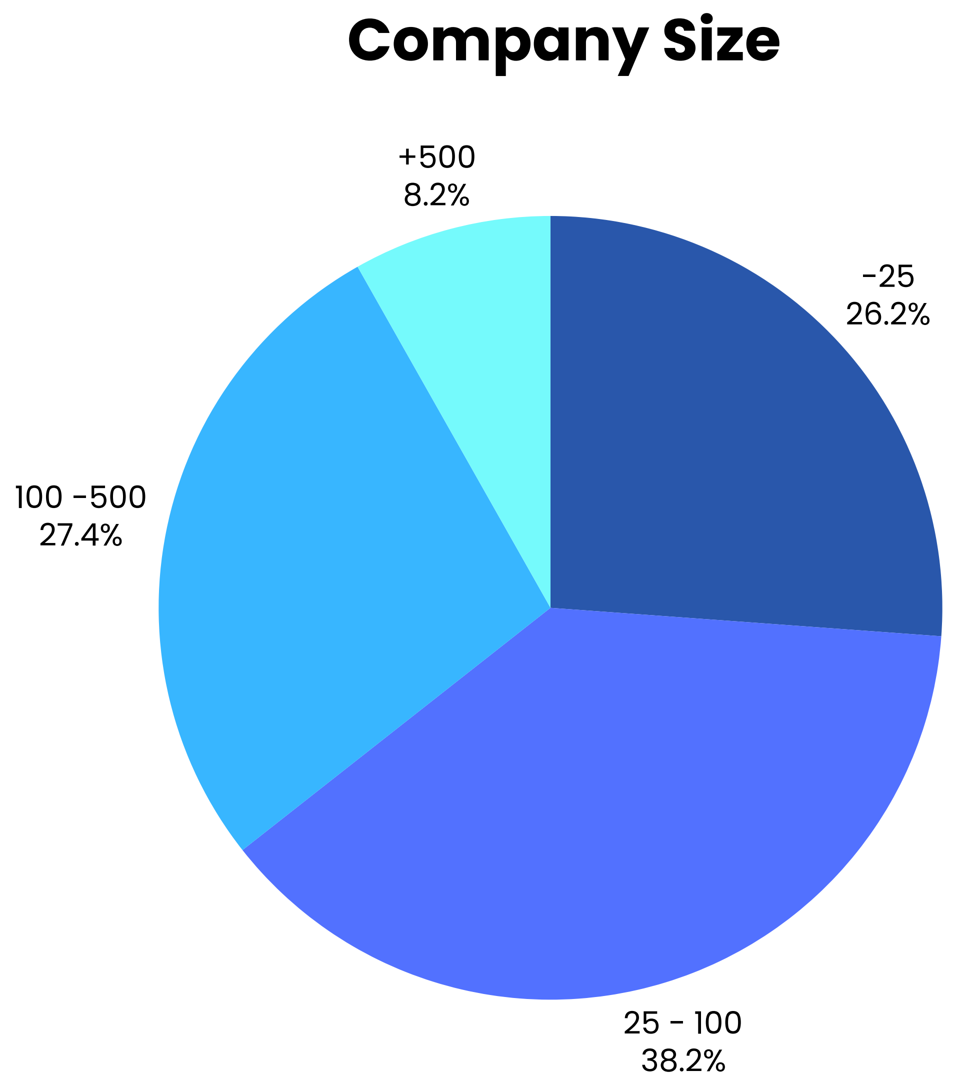
This report features insights from 317 from US-based DevOps, Security, Product, and Developer professionals across a variety of industries and company sizes. ActiveState conducted the survey on February 10, 2025.

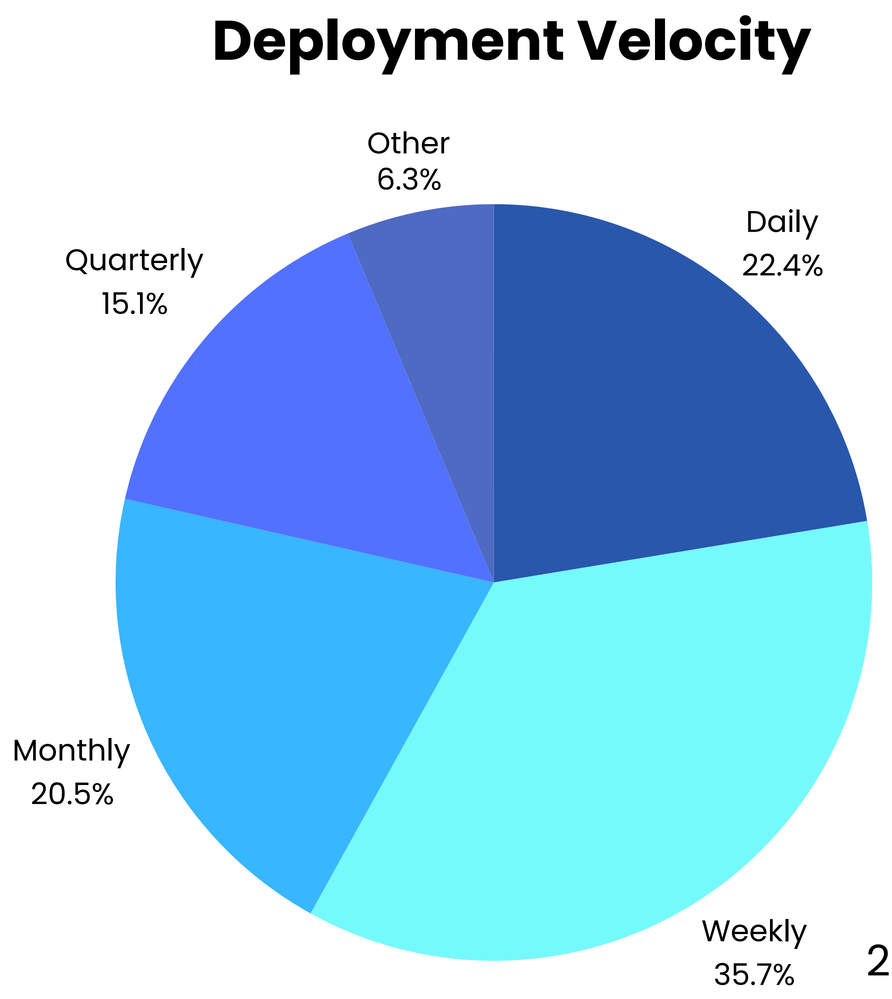


activestate

ActiveState sought out companies with a **diverse number of developers** to understand the pain points and vulnerability management process and ownership at companies of different sizes.

These organizations also had a diverse **deployment velocity** that was able to inform the decisions and rationale behind the decisions organizations make.

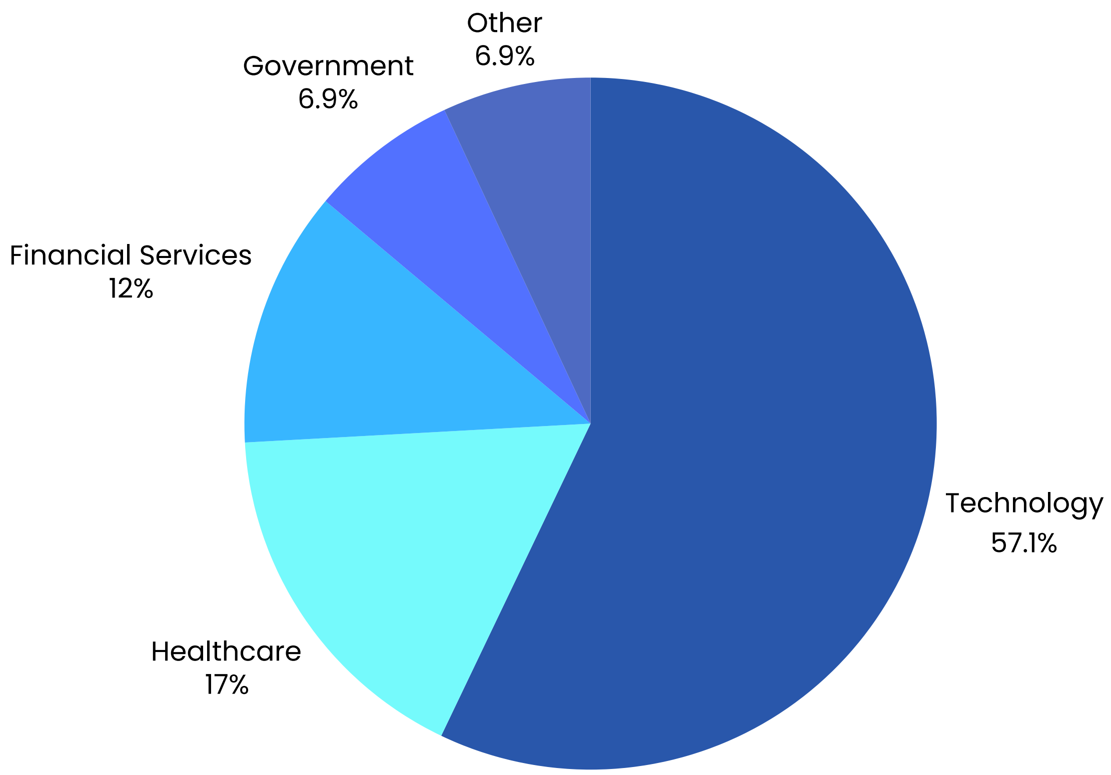




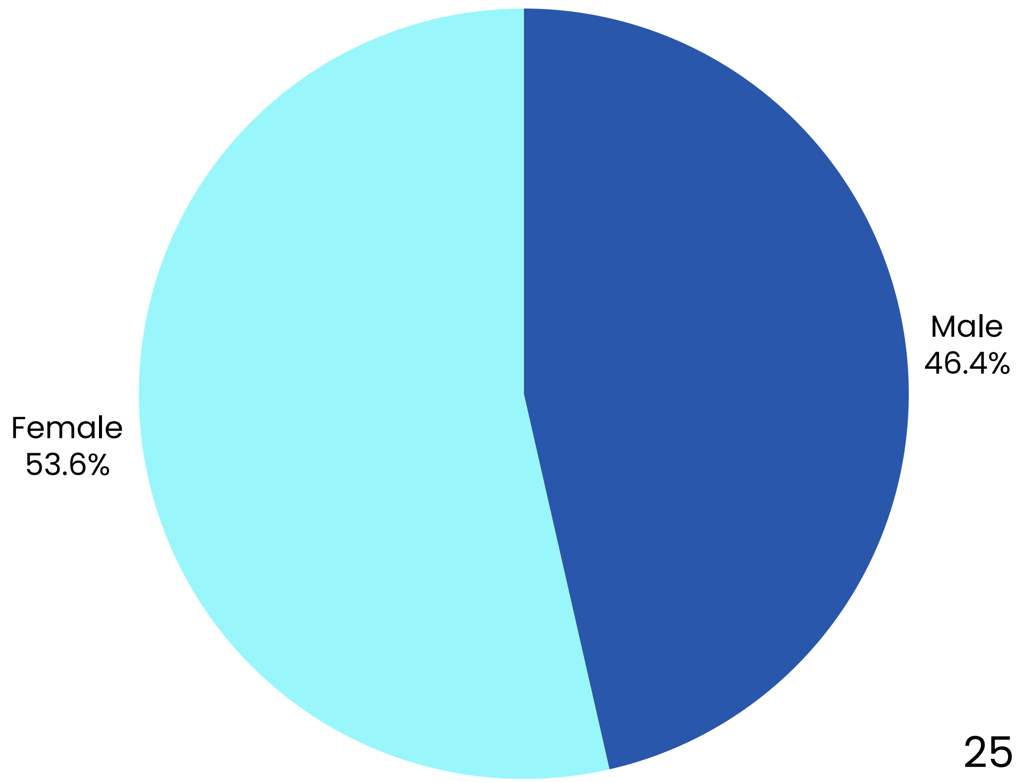
About half of the survey population works for **technology or software companies**. The other half is scattered across Healthcare, Financial Services, and Government and a handful of other industries.

The gender distribution of survey respondents is **relatively balanced.** 53.6% of respondents were female, while 46.4% were male.

Industry



Gender



Sources

1. Newman, L. H. (2019, July 23). 2017 Data Breach Will Cost Equifax at Least $1.38 Billion. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/2017-data-breach-will-cost-equifax-at-least-1-38-billion
2. Gartner, Inc. (2024). Leader's guide to software supply chain security (ID G00807046). By D. Gardner & M. Bhat.
3. Positive Technologies. (2023). *The Consequences of Delays in Remediating Vulnerabilities 2022-2023*. https://global.ptsecurity.com/analytics/the-consequences-of-delays-in-remediating-vulnerabilities-2022-2023
4. Sharma, S. (2025, January 17). Poor patching regime is opening businesses to serious problems. CSO Online. https://www.csoonline.com/article/3804844/poor-patching-regime-is-opening-businesses-to-serious-problems.html
5. Help Net Security. (2024, May 13). Critical vulnerabilities take 4.5 months on average to remediate. https://www.helpnetsecurity.com/2024/05/13/kev-catalog-prevalent-vulnerabilities/

activestate

About ActiveState

ActiveState enables DevOps, InfoSec, and Development teams to improve their security posture while simultaneously increasing productivity and innovation to deliver secure applications faster.

We are the only ASPM solution in the market today that offers Intelligent Remediation, which identifies which vulnerabilities to prioritize, assesses the impact of updates causing breaking changes, prioritizes what to fix first, securely builds open source packages from source, and facilitates the build and deploy process to get fixes into production quickly and easily.

All from the trusted partner that pioneered and continues to lead enterprise adoption and use of open source software.

Request a Demo

www.activestate.com • solutions@activestate.com