The 2024 State of Secure Development & ATO in U.S. Government Agencies

An interactive e-book publication
Quarterly primary research findings

SecurityCompass

Introduction

In 2024, US government agencies at the federal, state, and local levels face escalating cybersecurity challenges as advanced threats become increasingly sophisticated. As AI increases the threat surface, agencies are moving quickly to expand the opportunity surface at an even greater rate through AI-enhanced cybersecurity strategies. The complexity and scale of threats necessitate continuous adaptation and innovation, including shifting security left in the software development life cycle.

The Authority to Operate (ATO) process remains crucial for maintaining cybersecurity within government agencies. This formal approval process, granted by senior agency officials, authorizes information systems to operate within designated security environments based on comprehensive risk assessments and continuous compliance monitoring. While the ATO process has seen modernization to cope with the evolving cyber landscape, significant challenges persist, including budget constraints. To address both budget and time constraints while ensuring cybersecure software, automated security testing has become critically important. Speeding time to market is now an urgent priority for over half of government agencies. Cloud advancements and ATO Reciprocity are the top two significant developments impacting DevSecOps. The explosion of AI, alongside new and varied privacy and security regulations, is having a major impact on these advancements.

This report, commissioned by Security Compass, follows up on 2021 and 2023 studies, providing key insights into the current state of secure development and ATO processes in US government agencies. It highlights the challenges and opportunities at federal, state, and local levels, examining software development methods, security expertise, developer controls, communication strategies, and ATO-compliant software development approaches.

Commissioned Surveys By Security Compass

Survey Participants

- 150 respondents from US federal (70%), state (23%) and local (7%) agencies
- Targeted individuals at managerial level and above who had self-reported competency in secure coding standards and regulations.

The survey was conducted by Golfdale Consulting

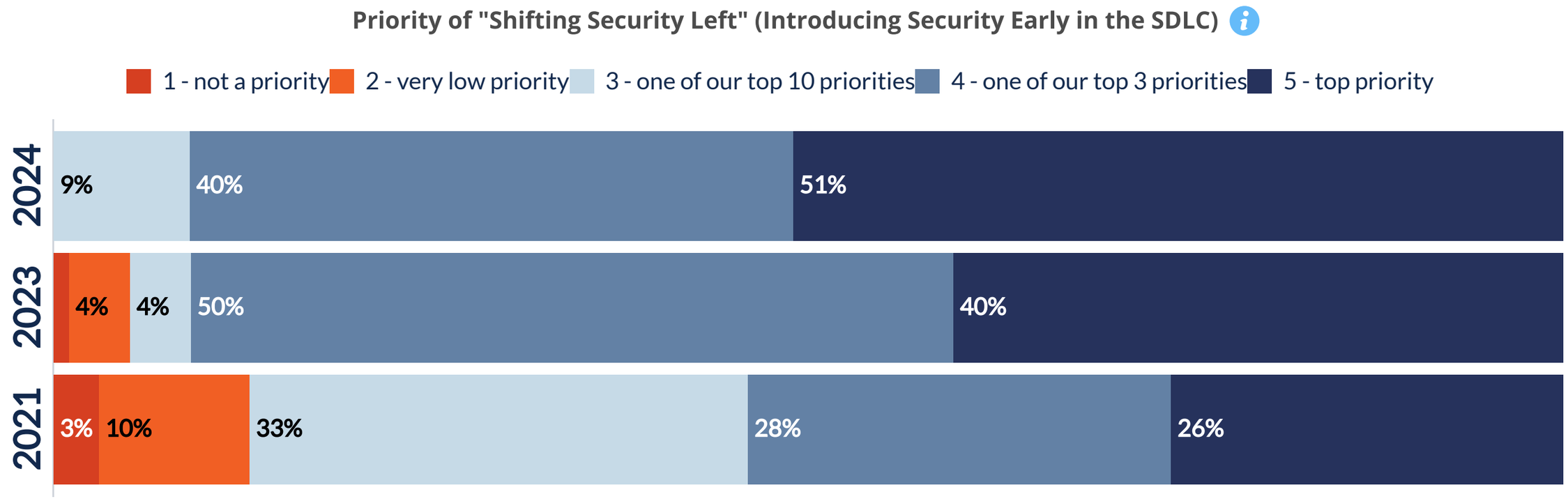
"Through strategic partnerships with federal, state, and local agencies, Security Compass is committed to transforming cybersecurity. We focus on industry leading application security content, robust security controls, and automation to drive greater efficiency and resilience in safeguarding critical information systems. Government agencies are able to automate the ATO process, integrate AI, and shift security left."

ROHIT SETHI - CEO, Security Compass

SecurityCompass

Shifting Security Left

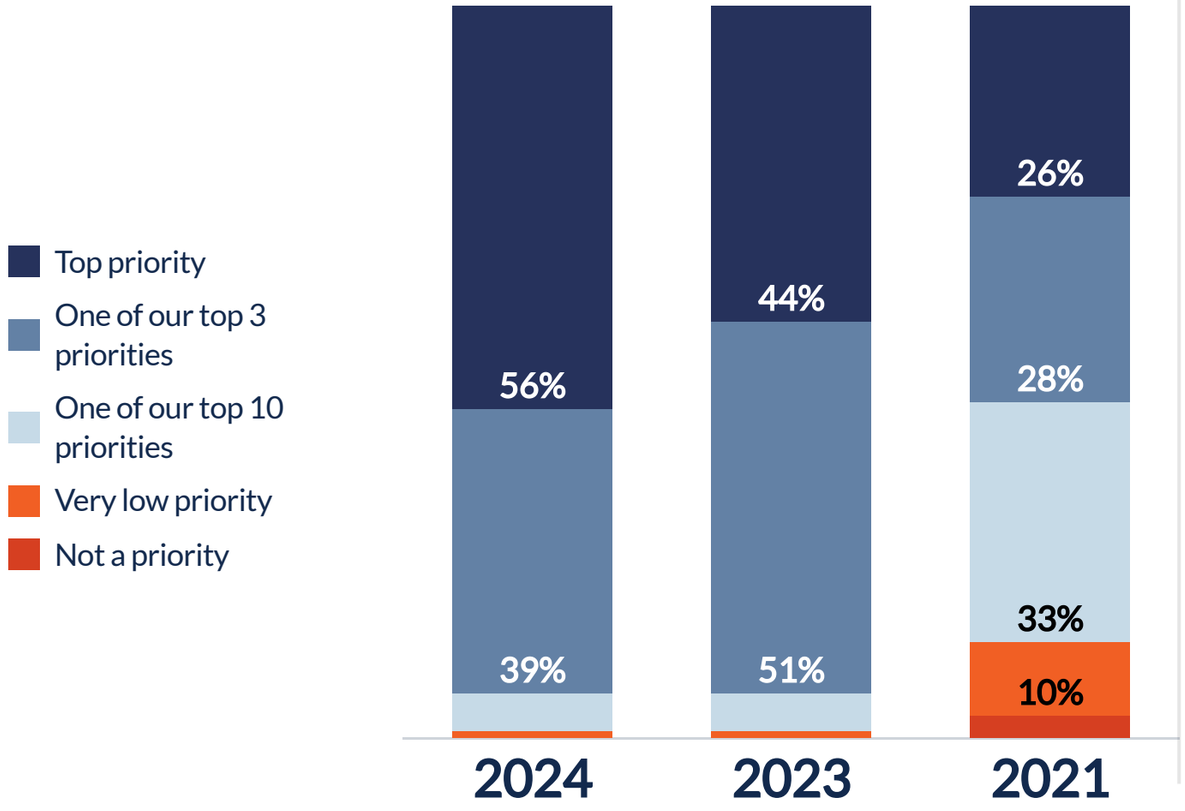
In 2024 we see a continued shift of security "left" by US government agencies, integrating security by design from the very beginning of the software development life cycle. It has essentially doubled as a top priority since 2021.



Improving Software Time to Market

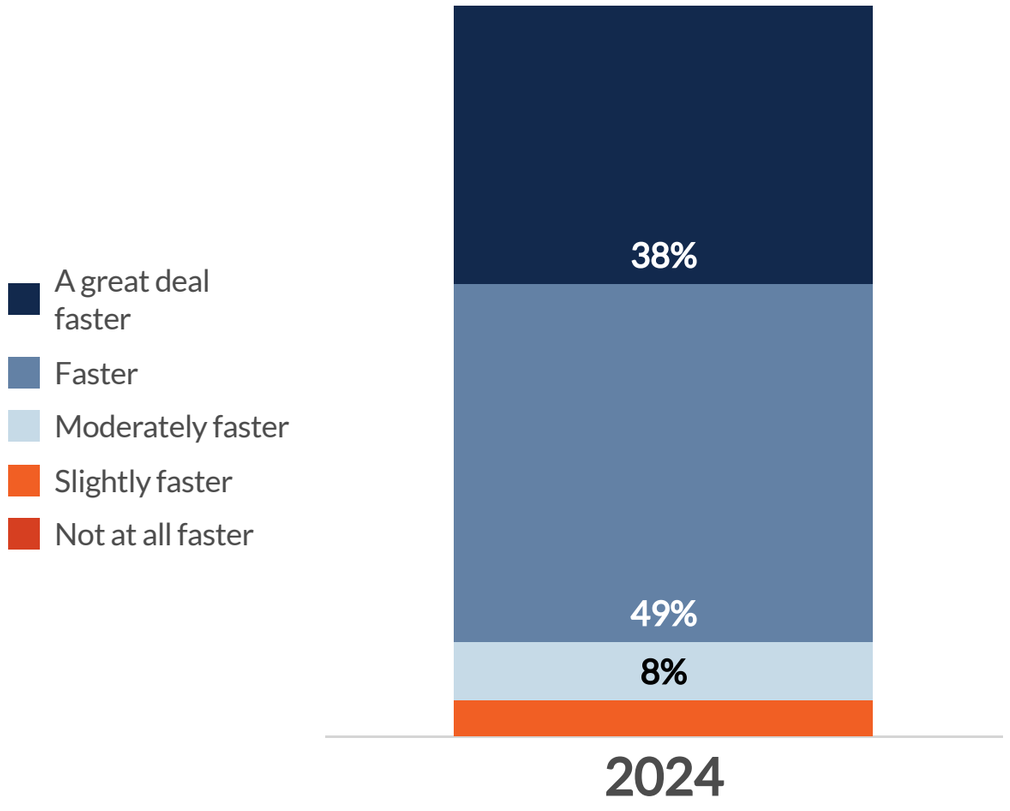
Improving software time to market as a priority has more than doubled since 2021 among US government agencies.

Priority of Speeding Up Time to Market

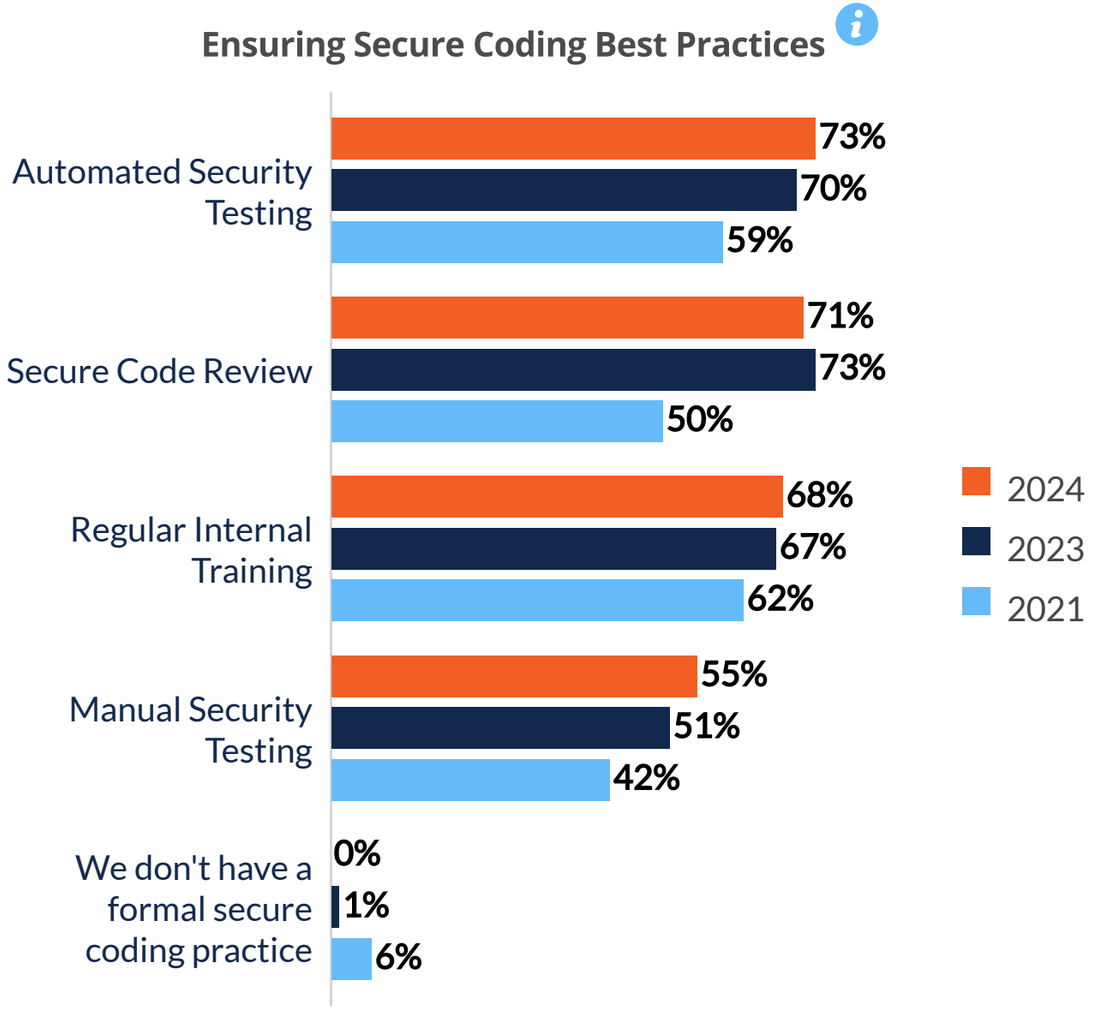


Almost 9 out of 10 (87%) see the impact of tracking inherited security compliance as making their software development either "a great deal faster" or "faster".

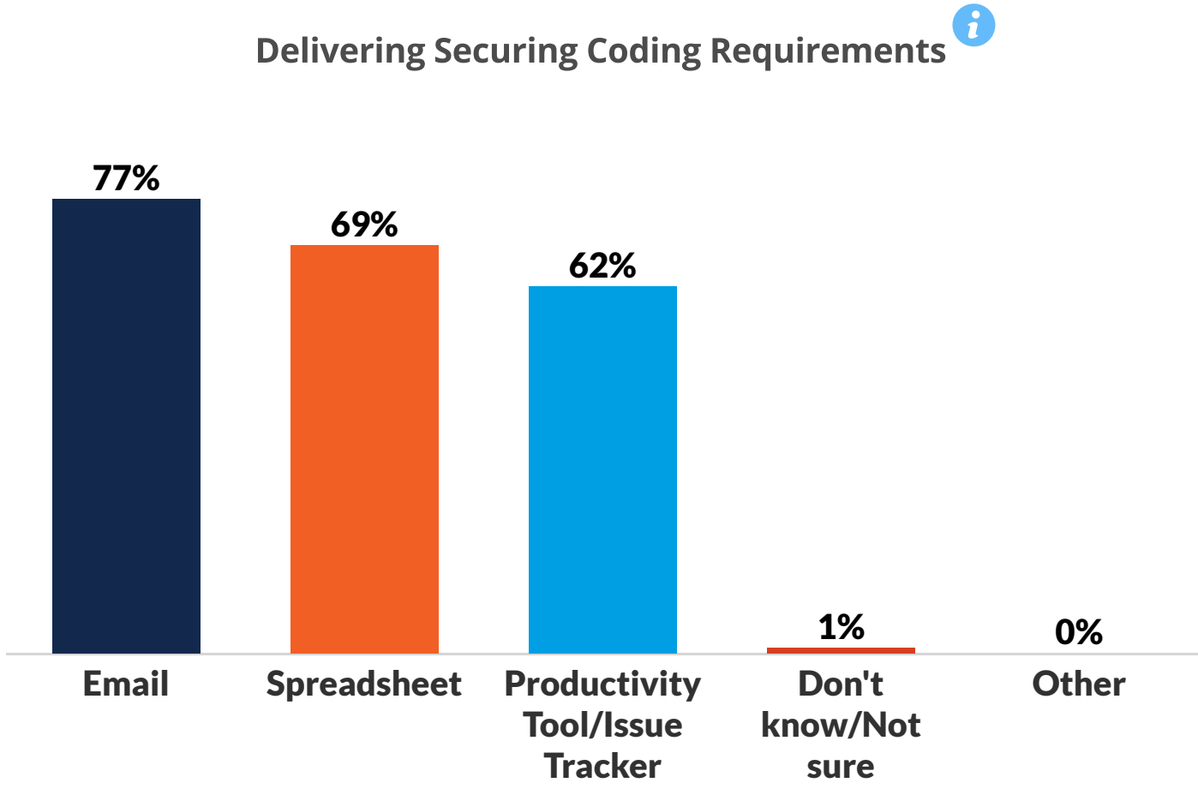
Speed Impact of Tracking Inherited Security Compliance



Ensuring Secure Coding Best Practices

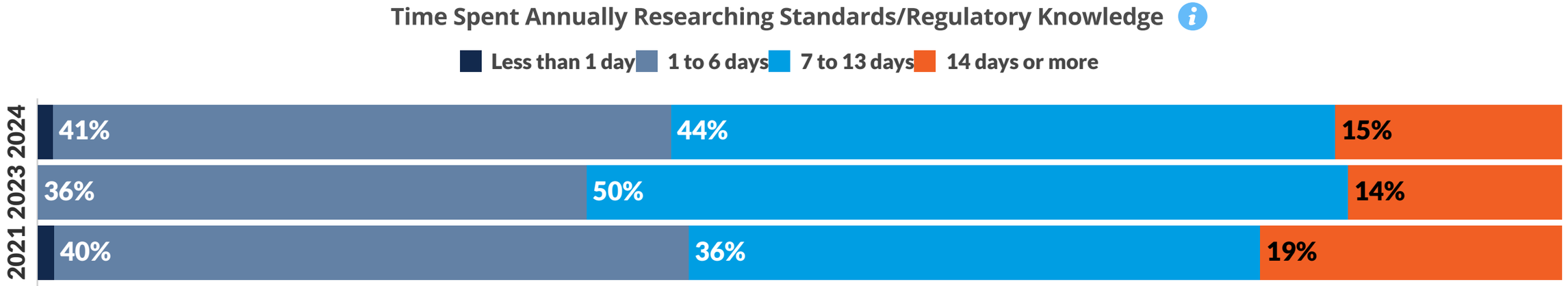


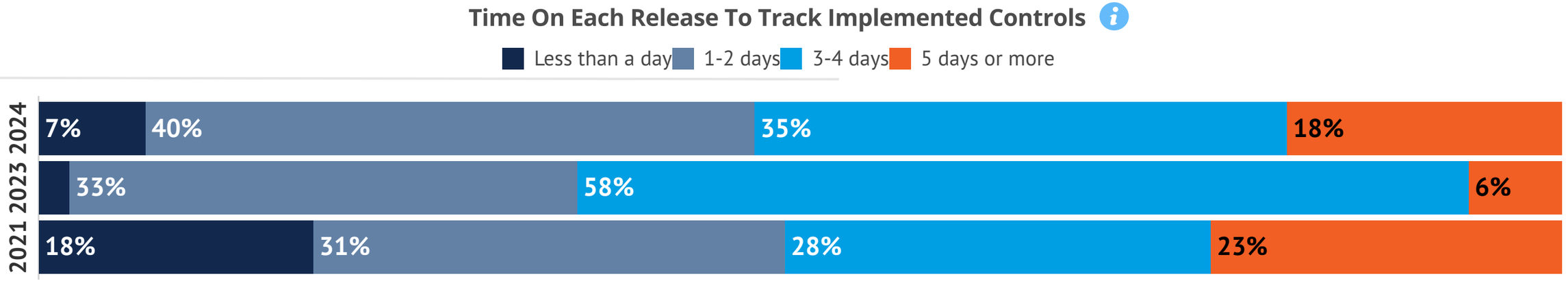
Automated Security Testing continues to rise in prominence to ensure secure coding practices. However, the requirements are most often sent simply in emails and spreadsheets.



Time Requirements to Meet Security Standards

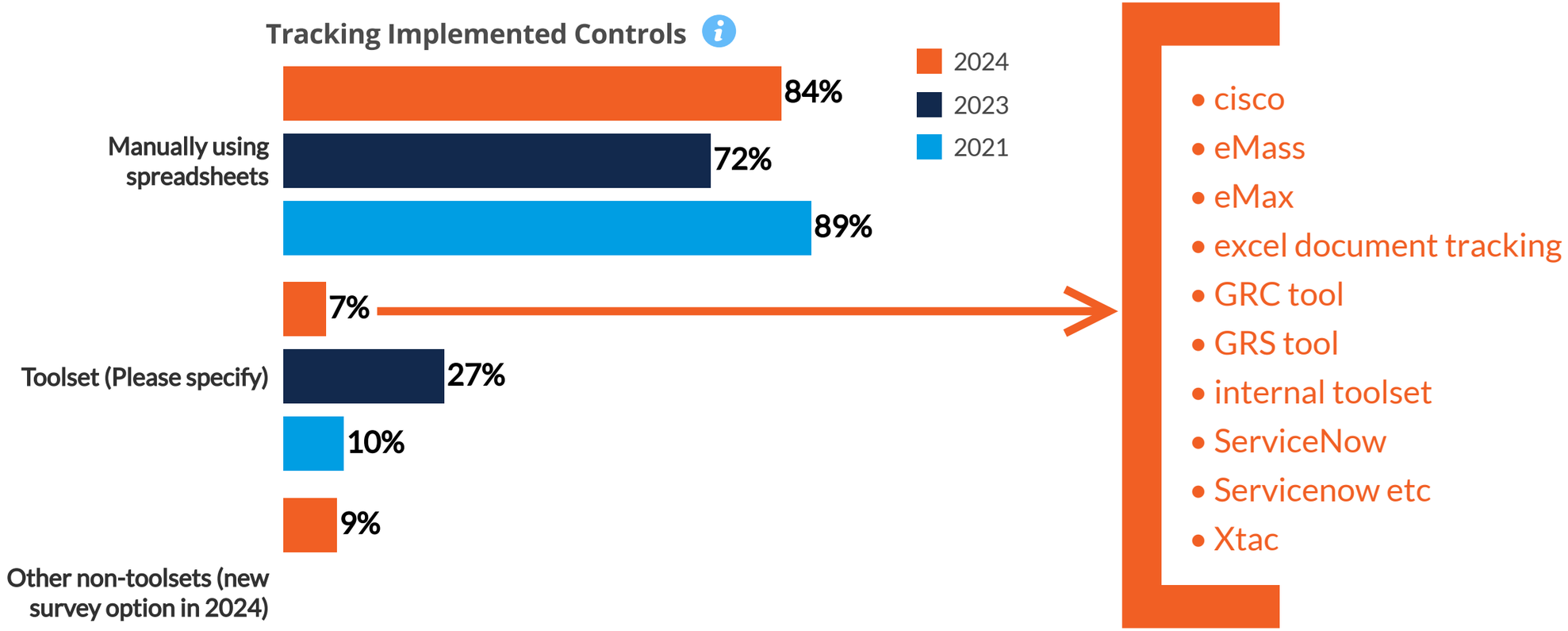
The length of time annually spent building the knowledge to stay current with regulatory requirements varies from several days up to almost two weeks. For each release, tracking implemented controls and creating artifacts to ensure compliance is in the 1 to 4 day range.





Tracking Implemented Controls

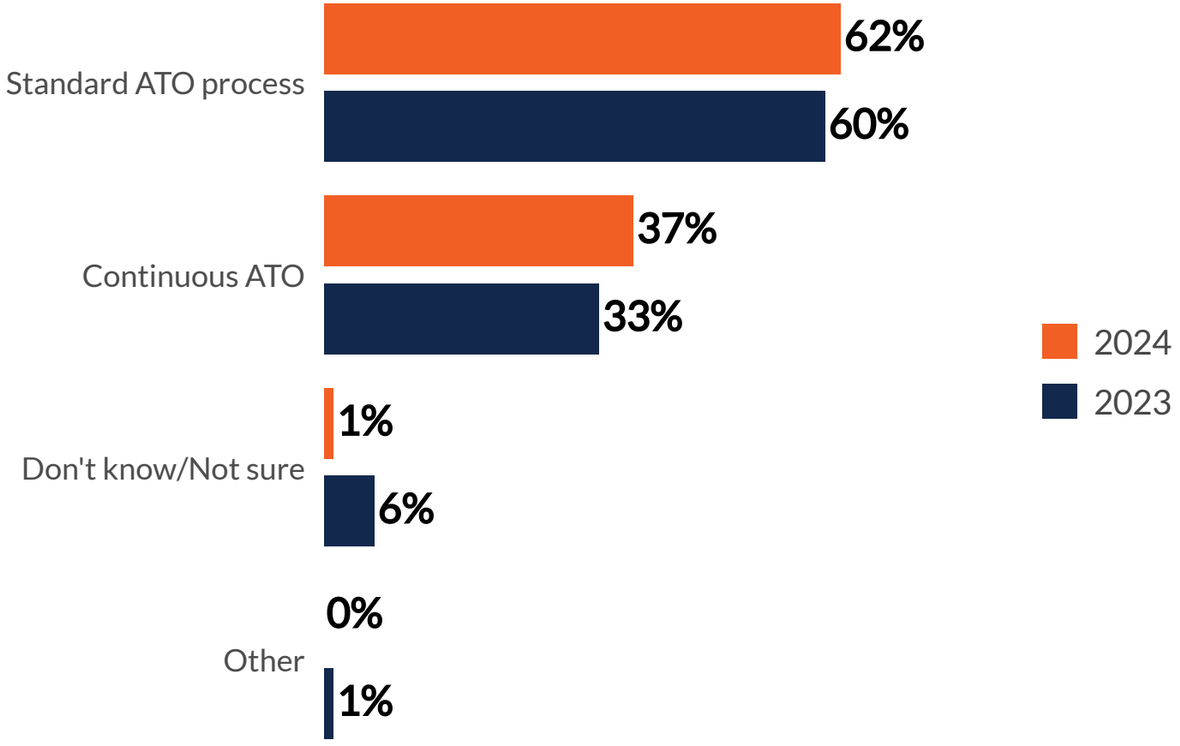
The use of manual spreadsheets to track implemented controls continues to be used by the majority of government agencies building software. That said, there are notable exceptions, as listed below.



Authority to Operate (ATO) and Tracking Compliance

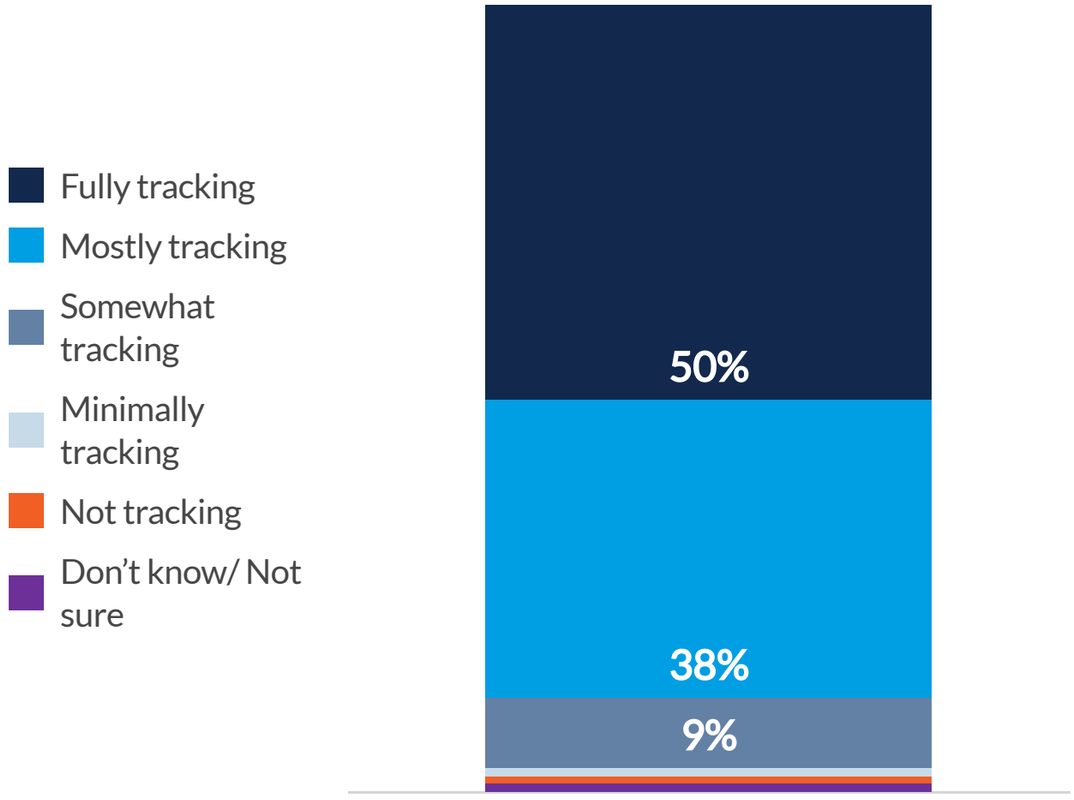
Overall, six out of ten US government agencies use Standard Authority to Operate (ATO) processes.

Current Approach to Achieving ATO



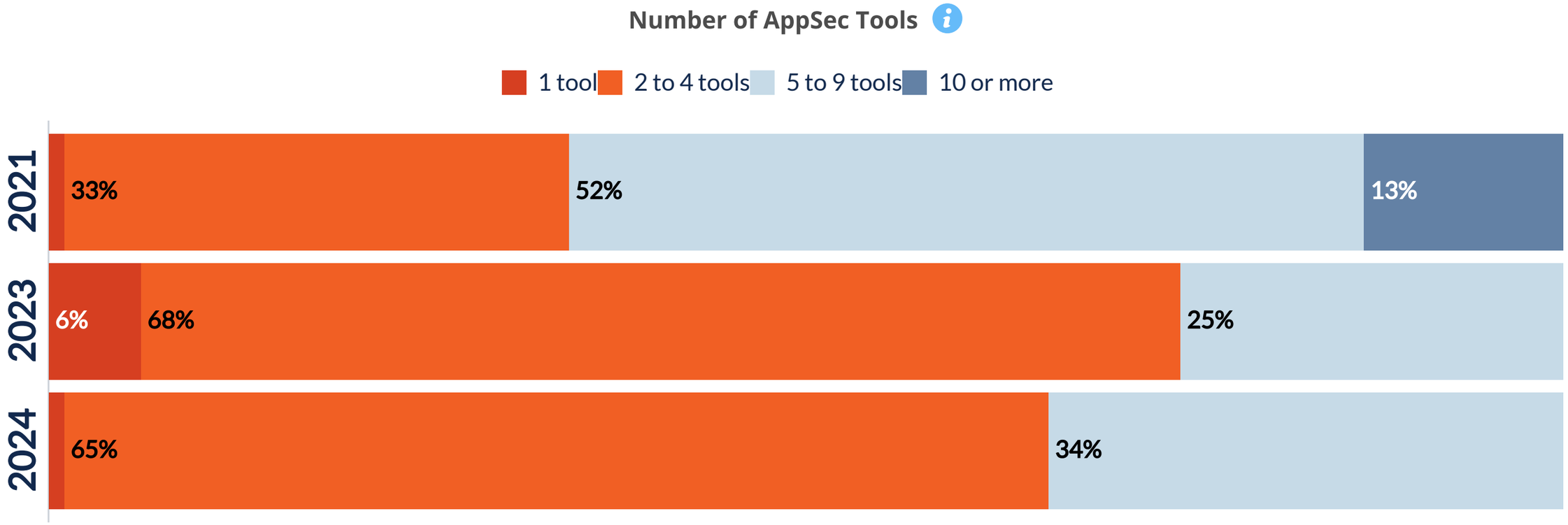
Nine of of ten (88%) are "fully tracking" or "mostly tracking" SSDF compliance.

Tracking SSDF Compliance



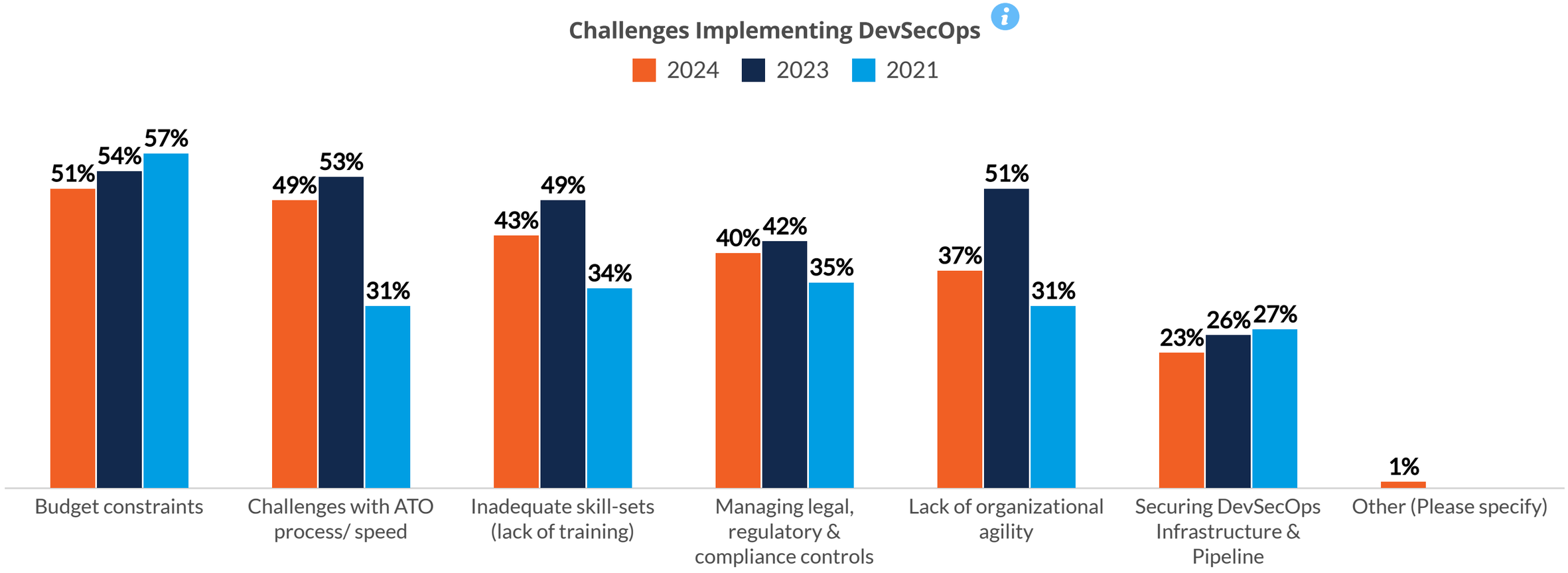
Number of Application Security Tools YoY

Approximately two thirds of US government agencies developing software are using two to four application security tools. The findings also suggest a consolidation of appsec tools among government agencies over the past two years.



Challenges

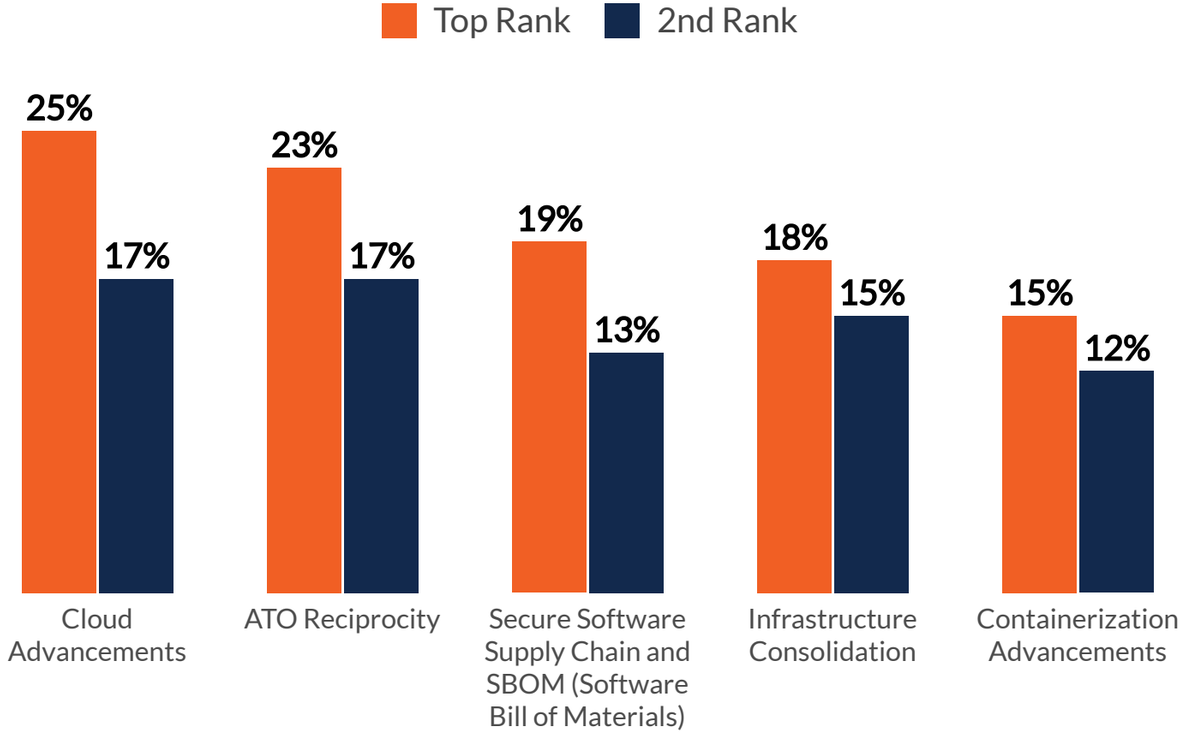
Budget constraints are the most frequently cited impediment government agencies continue to face in implementing DevSecOps, followed very closely by challenges with the speed of ATO processes.



Developments

Cloud advancements and ATO Reciprocity are the top 2 significant developments impacting DevSecOps. With these in particular, the explosion of AI alongside related new and varied privacy and security regulations are having major impact.

Top 2 Developments Having A Major Impact on DevSecOps



Open Ended Comments

We are seeing a significant impact on the future of Devsecops, which is the integration of AI and ML for enhanced threat detection and automated security incident response.

Using of AI tools and new software can make more cyberattacks and harm our security software.

Treating security policies, controls, and configurations as code artifacts that can be version-controlled, tested, and deployed alongside application code in the idea behind the security as code approach.

The key message is about implmenting[sic] zero-trust principles to establish stringent access controls and reduce the attack surface.

The DevSecOps landscape is always changing due to evolving privacy rules and regulatory obligation (such as the CCPA and GDP).

Teams responsible for develops are concentrating on putting in place security controls unique to containers, like access control, runtime protection, and vulnerability scanning of images.

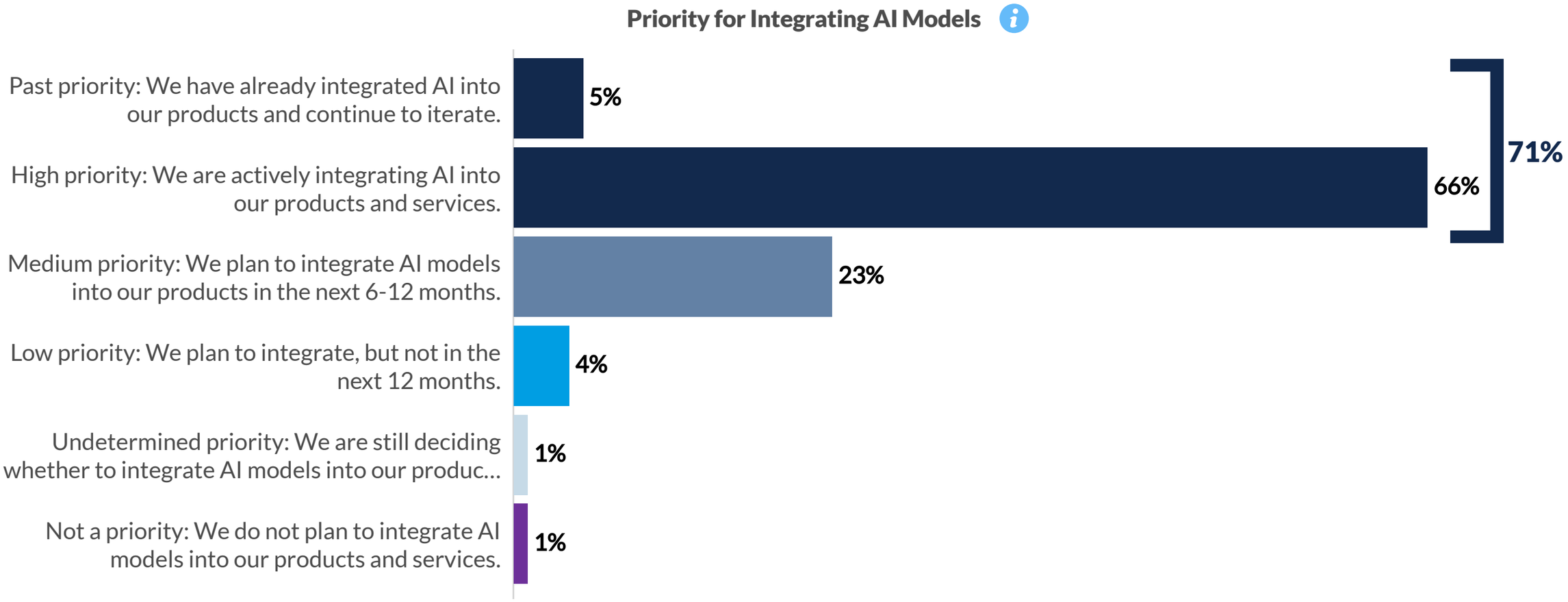
Security can be considered a data-at-scale issue, and teams responsible for observability must also learn to work with massive amount of data.

Our team's threat identification and response have improved significantly as a result of the incorporation of AI and ML into our DevSecOps methodolgy. It's like having an extra pair of eyes constantly watching our systems.

I believe this will have a significant influence on how security teams apply DevOps techniques in the future to expedite response times to security incidents, enhance teamwork, and streamline procedures.

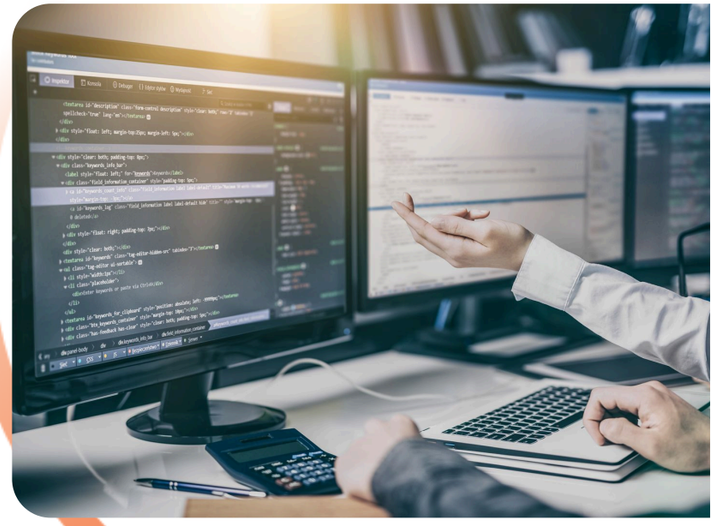
Artificial Intelligence Integration

Seven out of ten government agencies have made AI integration a major priority in their product development. By contrast, just 2% of government agencies that build software have set AI aside and have no plans to integrate it into their products.



Conclusion

US government agencies are progressively modernizing their cybersecurity strategies by "shifting left," integrating security earlier in the software development lifecycle, and adhering to evolving regulatory compliance standards. Alongside the integration of AI into their products, the majority are now prioritizing speed in their software development and deployment processes. Secure code review and automated security testing have become widespread, yet many agencies continue to use spreadsheets for delivering secure code requirements and tracking implemented controls. There is a gradual shift toward adopting more sophisticated toolsets.



As cyber threats increase and compliance standards tighten, the demand for current regulatory knowledge has grown. However, the time required to define security requirements and deploy new software has improved. Achieving ATO has seen enhancement over the past three years. Despite significant advancements, budget constraints remain the primary obstacle for agencies implementing DevSecOps, with the secure software supply chain being a close second. The rapid development of artificial intelligence intersects with all these developments, challenges, and opportunities.

While US agencies have made notable progress, the challenges of meeting modern cybersecurity demands are still formidable. Embracing automation while staying current with new regulatory requirements and addressing new threats is how Security Compass is helping agencies deliver secure software efficiently and effectively.

Secure Development Resources

For more cybersecurity resources please visit: https://resources.securitycompass.com/
Phone: 1-888-777-2211
Email: contact@securitycompass.com

About Security Compass
Security Compass, the Security by Design Company, is a leading provider of cybersecurity solutions, enabling organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its developer-centric threat modeling offering, SD Elements, and Application Security Training solutions help organizations release secure and compliant software to market quickly and cost effectively.

Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defense, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and UK. For more information, please visit www.securitycompass.com.

About Golfdale Consulting, Inc.
Golfdale Consulting Inc., trusted advisors to growth focused business leaders. Golfdale expertise and hands-on approach with senior executives spans three critical areas: 1) global market research and insights; 2) analytics and the application of decision sciences; and 3) advocacy for evidence based regulatory reform and market impact. Follow Golfdale Consulting on Twitter @_golfdale or visit https://golfdaleconsulting.com/