Security Automation

A Strategic Imperative for Federal Agencies

SWIMLANE

Table of Contents

Cody Cornell
Co-Founder & Chief Strategy Officer, Swimlane

My time working in IT and security roles at the Department of Homeland Security (DHS) and the U.S. Defense Information Systems Agency (DISA) gave me a firsthand look at the challenges security practitioners face in the public sector. It showed me that the cybersecurity issues at-hand cannot be solved if the security industry continues to push burdensome solutions that lean heavily on security teams performing manual tasks.

As a nation and society, we are at a crucial juncture with a multitude of significant cybersecurity challenges confronting us, from threats to our critical infrastructure, to increasing and changing risks posed by nation-states like Russia and China. These challenges have put cybersecurity in the limelight for the federal government, as those elected to protect us realize that cybersecurity is a matter of national security.

To combat this unprecedented threat landscape, the Biden Administration issued a series of executive orders that seek to improve the nation's cybersecurity posture. As part of Memorandum M-22-09, government agencies are now mandated to move towards zero trust cybersecurity principles by the end of the government fiscal year in 2024. This executive order is no small task for federal agencies, as these government-wide cybersecurity requirements directly impact the outlooks and roadmaps for individual agency security initiatives.

From my experience, I realized the need for solutions that are powerful enough to solve the most sophisticated security challenges while remaining easy to navigate as organizations continue to grapple with cybersecurity talent shortages. At Swimlane, we want to ensure the public sector is empowered by the proper strategies and solutions that will keep our country protected while staying on top of regulatory compliance. So, we surveyed over 100 security professionals and executives at U.S. federal agencies to learn more about the challenges they face and how they are working to implement a zero trust architecture ahead of 2024.

We hope this report brings a level of confidence and reassurance to federal agencies as they navigate the path to cyber resilience. Additionally, I hope it sparks more conversations about the optimal technology to enable security teams to respond swiftly and effectively to incidents in order to safeguard national interests and public trust.

Sincerely,

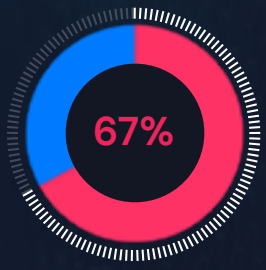
Cody Cornell

Executive Summary

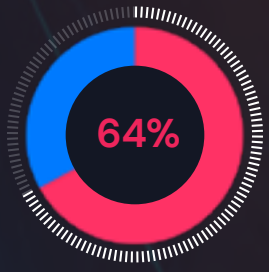
With the 2024 deadline approaching for federal agencies to meet the Zero Trust executive order from the Biden Administration, we sought to understand how prepared federal agencies are to meet the requirements. Swimlane partnered with Dimensional Research, a leading independent research firm, to survey over 100 security professionals and executives at U.S. federal agencies. Together, we investigated the confidence level of these agencies in meeting the memorandum's security automation requirements and the tools leveraged to overcome challenges in adopting the key components of a Zero Trust architecture. In this report, we explore some of the key findings from our survey.

Key Findings

Security Automation is a Necessity. Are Federal Agencies Ready?

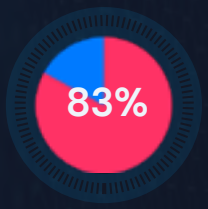


67% of federal government agencies are confident or very confident they are prepared to meet the Zero Trust requirements laid out by the U.S. government.



64% of federal agencies said they are choosing low-code security automation solutions.

Grappling with Security Team Vacancies



83% of federal agencies have security team positions currently open.

64% of federal agencies said it takes longer to fill a security position than it did two years ago.

1 in 3 (35%) of federal agencies don't think their security team will ever be fully staffed.

Turning to Optimal Technology

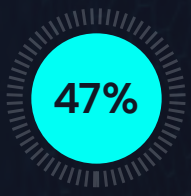
Almost all participants (99%) cited benefits of low-code automation solutions:

49% of participants said it leads to less reliance on coding to automate.

40% of participants said they were able to address all security automation requirements.

38% of participants said that the capabilities of these solutions scale with the experience of their security team.

On the other hand, nearly all participants (99%) cited drawbacks to no-code security automation, which included:



47% of participants said that no-code solutions lack features like reporting and case management capabilities.

44% of participants said these solutions do not support all environments, including public cloud and hybrid environments.

43% of participants said that no-code tools will have to be replaced in the short term.

SWIMLANE

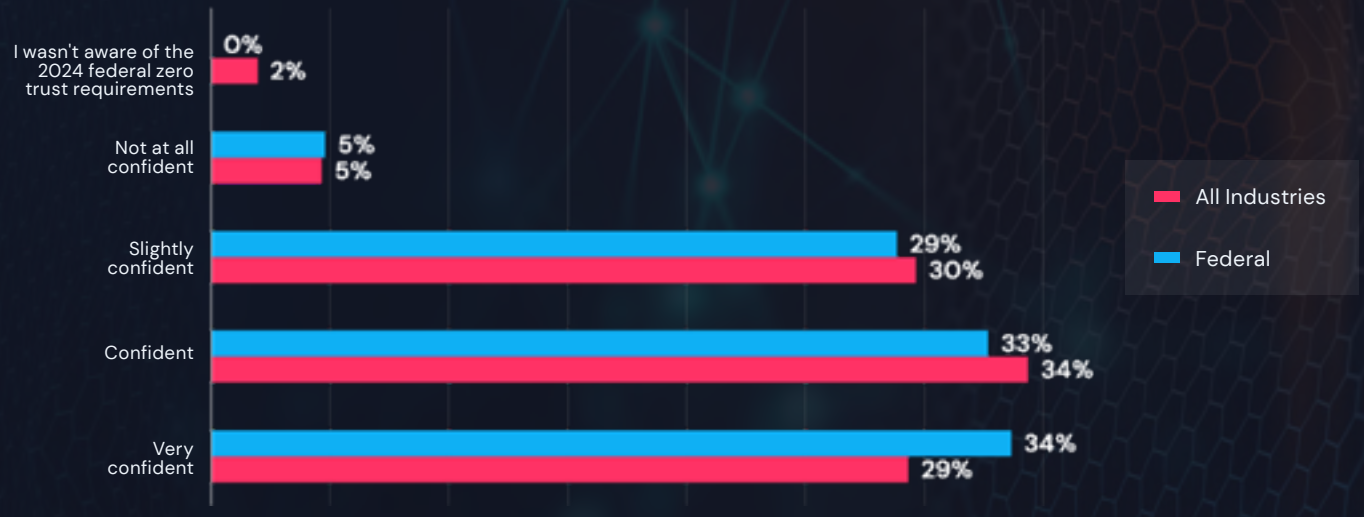
Security Automation is a Necessity. Are Federal Agencies Ready?

The Department of Homeland Security and the Cybersecurity & Infrastructure Security Agency (CISA), along with executive orders from the Biden Administration, have mandated several new security directives around Zero Trust, Logging, and Security Orchestration, Automation, and Response (SOAR). Two of the recent executive orders include M-21-31 and M-22-09, which are government-wide programs that have immediate impacts on expectations and roadmaps for the M-22-09 Federal Zero Trust Strategy public sector agency security programs.

In early 2022, the Biden Administration issued Memorandum M-22-09 requiring U.S. public sector agencies to implement SOAR technology as part of adopting Zero Trust principles by the end of the 2024 fiscal year. In the executive order, the implementation of security automation capabilities is referred to as a "practical necessity" to improve overall cybersecurity effectiveness.

With just over a year until the deadline, **67% of government agencies are confident** or very confident they are prepared to meet the Zero Trust requirements laid out by the U.S. government. When asked how they are arming themselves with the tools that will help to meet all the criteria of implementing a Zero Trust architecture and solve the sophisticated security challenges they face, **64% of federal agencies said they are choosing low-code security automation**.

How confident is your team that it can meet the 2024 federal zero trust requirements enacted by the US federal government?



SWIMLANE

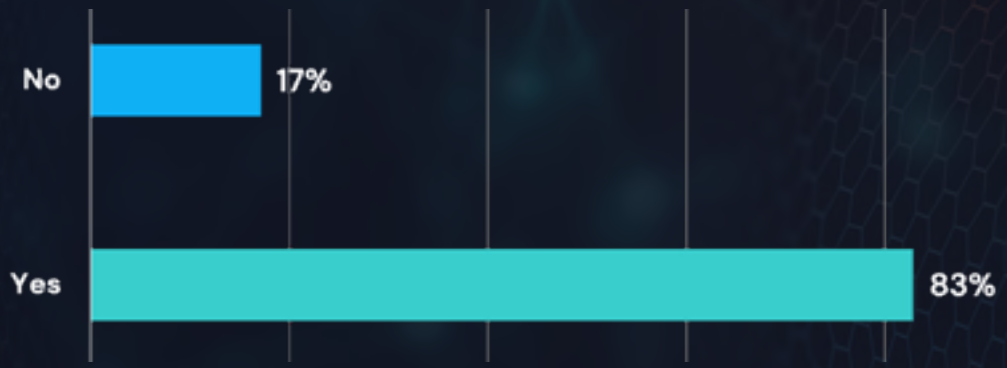
Without security automation, there is simply no feasible way for federal agencies to handle the volume of security alerts and complex processes. The requirement for security automation to address government agencies' pain points is not a new concept, but Memorandum M-22-09 has shined a spotlight on its importance.

According to Gartner®, "It is commonplace for SOAR technologies to offer low-code-like functionality. This makes programming and workflow improvements more accessible to all members of the security operations team even if they do not have a lot of programming experience. While SOAR continues to offer a lot of features for "power users," these individuals can have broader responsibilities for automation across the organization. Power users can develop their own integrations and often reuse existing code/scripts. SOAR is then used to help build out more repeatable playbooks, allowing organizations to utilize this code based on the building blocks that already exist in the technology."[1]

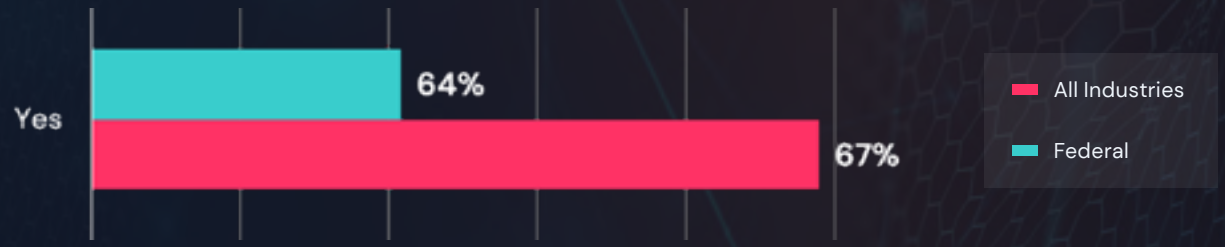
Grappling with Security Team Vacancies

Security teams within the federal government are expected to investigate and remediate thousands of alerts daily while keeping up with evolving mandates. Many are navigating these challenges with chronically understaffed teams, as finding candidates with the right mix of technical expertise, relevant experience, and industry-specific knowledge has become increasingly difficult. Amid these ongoing challenges, **83% of federal agencies report having security team positions currently open**, with **64% reporting it takes longer to fill a security position now than it did two years ago**. This has led **one-third (35%) of federal agencies** to believe they will never have a fully-staffed security team with the proper skills.

Does your organization's security team currently have open positions that need to be filled?
(Federal Participants)



In your experience, does it take longer to fill a security position now than it did two years ago?
(Federal Participants)



In your opinion, will your organization's security team ever be fully staffed with the needed skill levels?
(Federal Participants)

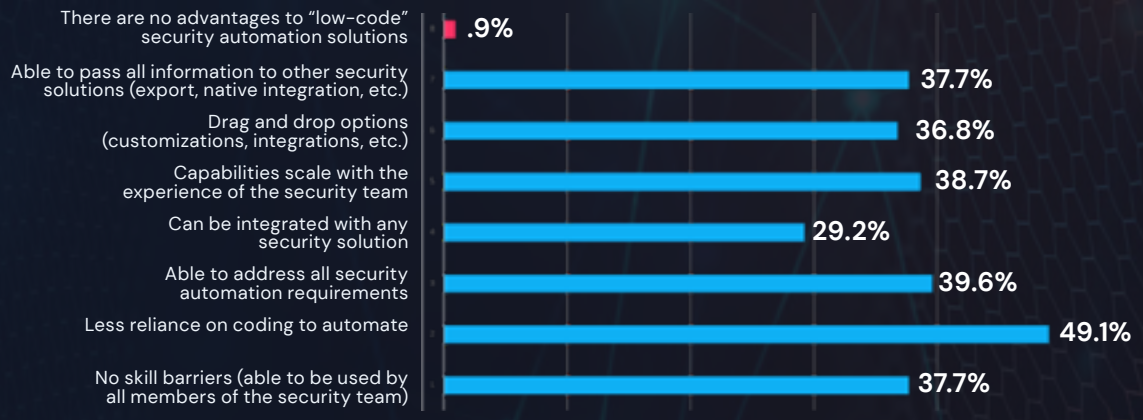
Many security leaders in the public sector have come to the realization that they will likely never be able to fill the open positions on their teams. This has pushed them to ensure they have the best technology in place to meet federal requirements and stay secure.

Turning to Optimal Technology

While adhering to the Zero Trust mandate may seem daunting to federal agencies and their security teams, the correct tools in place can serve as a crucial foundation for meeting the requirements, all while providing the visibility needed to overcome resource constraints and respond to threats faster.

This is why federal agencies are turning to low-code security automation to "lighten the load" of implementing the SOAR component of the executive order. **99% of federal agencies** cited benefits to low code automation solutions, including the ability to address all security automation requirements while relying less on coding skills. These advantages are key to smaller security teams that may not have the required skill set to implement a traditional SOAR solution.

In your experience, what are the advantages of a 'low-code' security automation solution?
(Federal Participants)

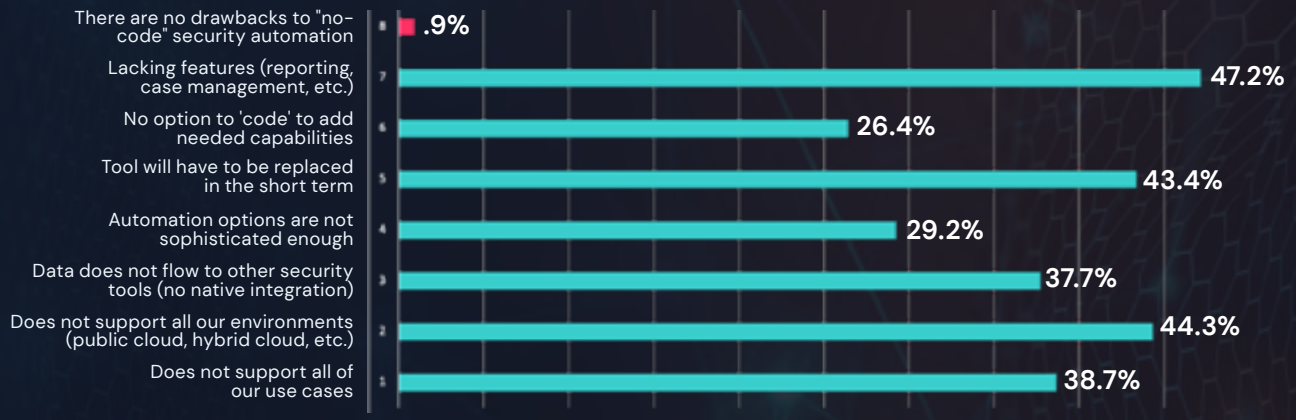


While the absence of coding altogether might seem attractive on the surface, federal agencies are finding that no-code tools don't support cloud or hybrid environments, and tend to lack important reporting and case management features. More importantly, federal agencies cited that no-code security automation tools are **only short-term solutions to long-term issues**.

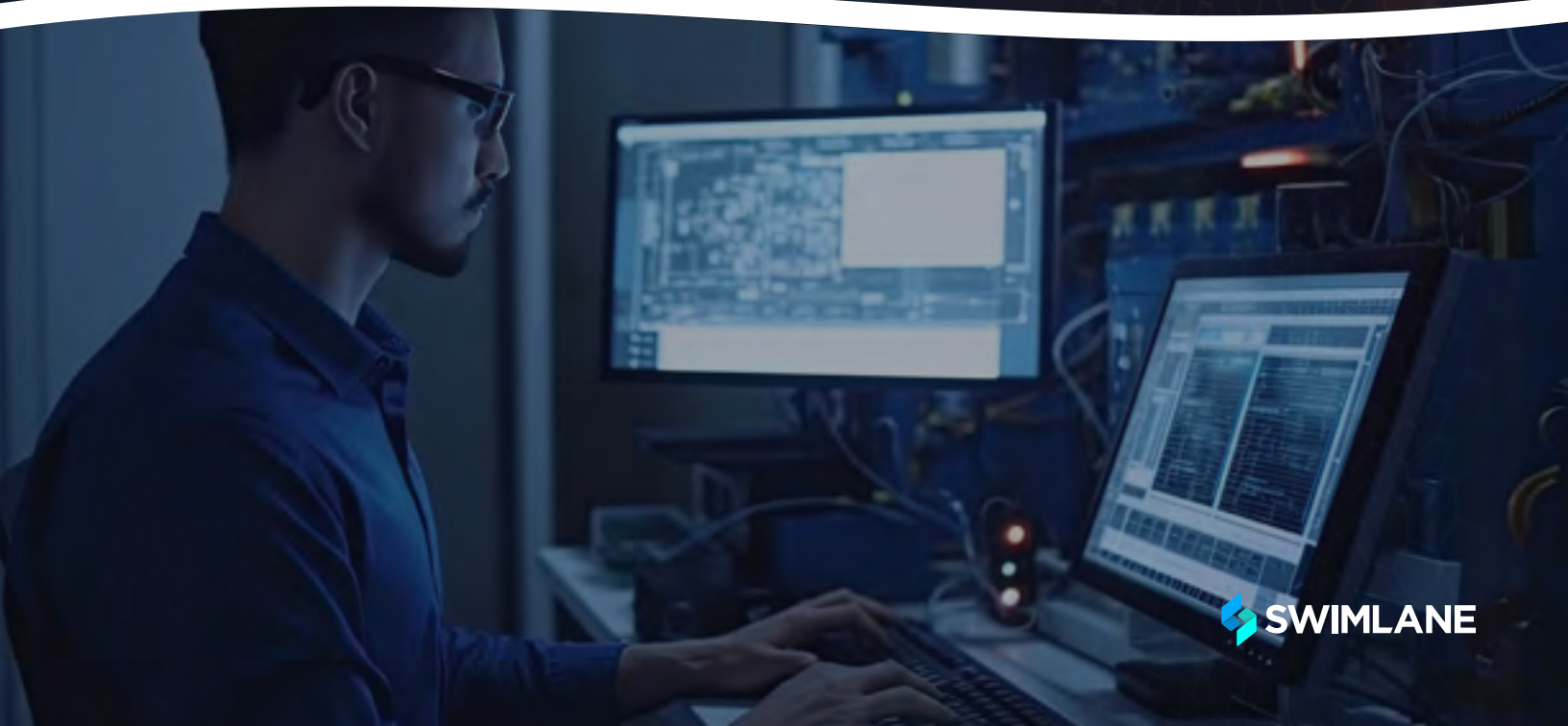
SWIMLANE

In your experience, what are the drawbacks of 'no-code' security automation?

(Federal Participants)



As federal agencies set out to implement the SOAR requirements outlined in Memorandum M-22-09, security operations leaders and teams are turning to solutions that are easy to navigate, integrate with existing security stacks and automate the manual tasks essential to keeping the organization secure. Traditional SOAR solutions can be burdensome due to the extensive scripting required. On the other hand, no-code automation is overly simplistic and often lacks essential reporting capabilities. Low-code security automation offers a solution that is both approachable enough for those with no coding experience yet sophisticated enough to satisfy the most stringent demands of federal agency security operations. These platforms serve as the critical foundation for federal agencies to meet the Zero Trust requirements by the 2024 deadline.



Methodology

Security professionals and executives at U.S. federal agencies were invited to participate in a survey on their agency's security practices. The survey was administered electronically, and participants were offered a token compensation for their participation.

A total of 106 qualified participants completed the survey. All participants had federal agency security responsibilities from roles on the frontline to senior executives.

The following definitions were used in the context of the survey and report:

No-code security automation
Refers to an automation tool that offers a codeless approach to security automation utilizing menu options, taskbar buttons, and drag-and-drop capabilities to create the automation.

Low-code security automation
Refers to an automation solution that primarily utilizes menu options, taskbar buttons, selectable items, and drag and drop to create the automation. It also enables more customization and expansion with the option to use coding or scripting languages to create more sophisticated automation.

Security orchestration, automation and response (SOAR)
SOAR solutions combine incident response, security orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools are also used to document and implement processes (aka playbooks, workflows and processes); support security incident management; and apply machine-based assistance to human security analysts and operators.

---

[1] Gartner, Market Guide for Security Orchestration, Automation and Response Solutions, Craig Lawson, Pete Shoard, June 23, 2023

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission.
All rights reserved.

SWIMLANE

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps reduce process and data fatigue, overcome chronic staffing shortages, and quantify business value.

The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit **swimlane.com**.

About Dimensional Research

Dimensional Research provides practical market research for technology companies. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. Our researchers are experts in the applications, devices, and infrastructure used by modern businesses and their customers. For more information, visit **www.dimensionalresearch.com**.

SWIMLANE