UNDER PRESSURE:

Is Vulnerability Management Keeping Up?

A Swimlane study conducted by Sapio Research

Table of Contents

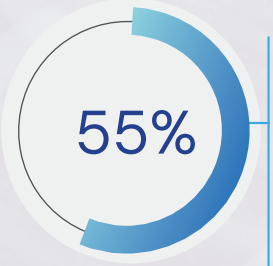
Executive Summary

The relentless surge of vulnerabilities is pushing security teams to their limits, forcing them to manage overwhelming volumes of risk with inadequate tools and processes. Fragmented data from multiple scanners, siloed risk scoring, poor cross-team collaboration, and reactive strategies leave organizations increasingly exposed to breaches, compliance failures, and costly penalties.

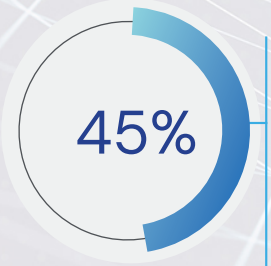
To better understand how vulnerability management teams are coping with these challenges, Swimlane surveyed 500 cybersecurity decision-makers in the US and UK. The results illuminate the critical need for smarter prioritization and automation to reduce attack surfaces, prevent breaches, and ensure continuous compliance.

Key Findings

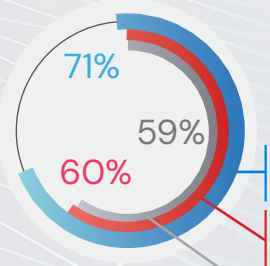
Vulnerability Management is a Web of Complexity



55% of organizations still need a comprehensive system to address vulnerability prioritization.



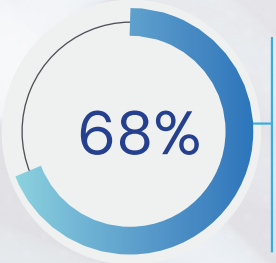
45% of organizations use a hybrid approach to addressing vulnerabilities, leveraging a mix of manual and automated processes.



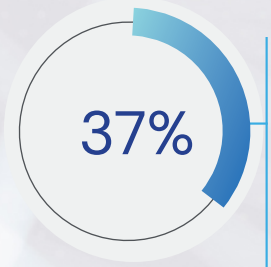
The top 3 vulnerability scanning tools used by organizations include:

- **71%** cloud security posture management
- **60%** multiple endpoint scanners
- **59%** web application scanners

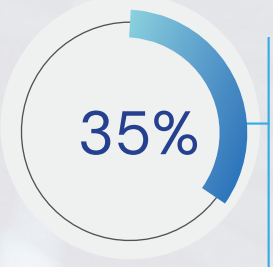
Lack of Context Fuels the Race Against Time



68% of organizations say remediating a critical vulnerability takes more than 24 hours.



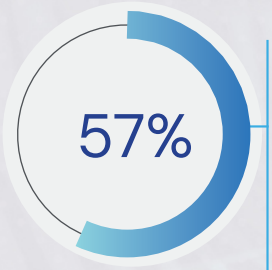
37% of organizations say their biggest challenge in prioritizing vulnerabilities is the lack of context or accurate information about vulnerabilities.



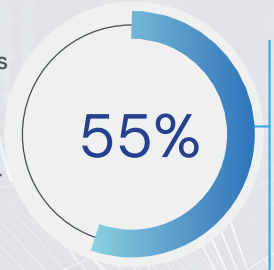
35% of organizations say their biggest challenge in remediating vulnerabilities is the lack of context or accurate information about vulnerabilities.

Key Findings (continued)

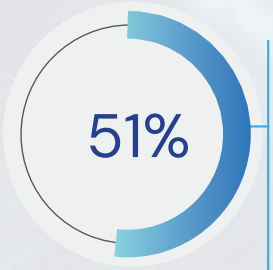
The Hidden Costs of Manual Effort and Inefficiency



57% of respondents said their security team spends anywhere from 25% to 50% of their time on manual tasks related to vulnerability management operations.

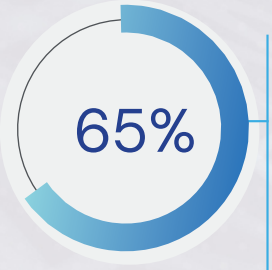


55% of organizations said their security teams spend more than 5 hours each week consolidating and normalizing vulnerability data.

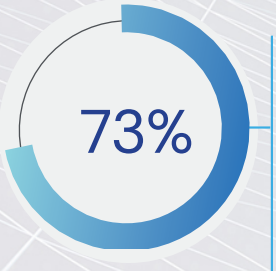


51% of respondents say that the quality of results associated with vulnerability scanners is useful but limited, causing them to need additional tools and processes to prioritize and respond effectively.

The Confidence Shortfall in Regulatory Compliance

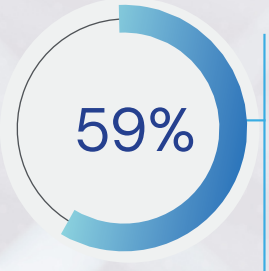


Nearly two-thirds (**65%**) of organizations are not fully confident that their current vulnerability management program would satisfy a regulatory audit.

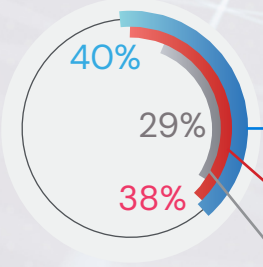


73% of organizations are concerned about the potential for regulatory fines due to inadequate vulnerability management.

Siloed Processes Fuel Bigger Security Risks



59% of organizations said that vulnerability management is siloed within their organization, leading to inefficiencies and potential security gaps.



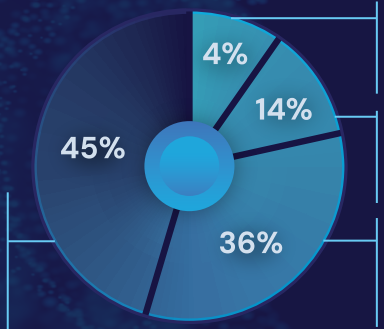
The top three risks organizations associate with poor vulnerability management are:

- **40%** reputational damage and loss of customer trust
- **38%** cite business disruption and operational downtime
- **29%** report financial penalties and fines for non-compliance with regulations

Vulnerability Management is a Web of Complexity

Organizations today face an unprecedented volume of vulnerabilities, forcing them to rethink their approach to vulnerability management. More than half (55%) of organizations admit they lack a comprehensive system for vulnerability prioritization — one that factors in critical elements like Common Vulnerability Scoring System (CVSS), exploit predictability, asset criticality and threat intelligence. This gap contributes to ineffective risk scoring, making it difficult for security teams to focus on the threats that matter most, increasing the likelihood of missed vulnerabilities and exposing businesses to unnecessary risks.

Which of the following best describes your organization's approach to vulnerability prioritization?



4% Don't have a consistent or formalized approach to vulnerability prioritization

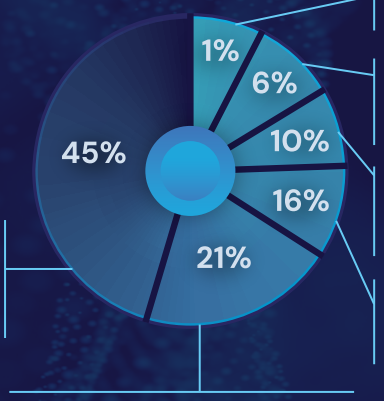
14% Rely solely on CVSS scores to assess vulnerabilities

36% Use CVSS scores alongside additional factors like exploit predictability (EPSS) and asset criticality

45% Have a comprehensive system that factors in CVSS, exploit predictability, exploit availability, asset criticality, and threat intelligence

Despite the presence of sophisticated systems, 45% of organizations still rely on a hybrid remediation approach that blends manual and automated processes. While automation plays a crucial role in improving efficiency, the need for manual intervention suggests that there is still a long way to go in fully optimizing vulnerability management processes.

What best describes your organization's current remediation strategy for addressing vulnerabilities?



1% No Defined Strategy: Do not currently have a defined remediation strategy in place

6% Outsourced Remediation: Remediation tasks are handled by a third-party service provider

10% Manual Remediation: Vulnerabilities are identified and remediated manually by the IT or security team

16% Prioritized Remediation: Vulnerabilities are remediated based on a risk-based prioritization process

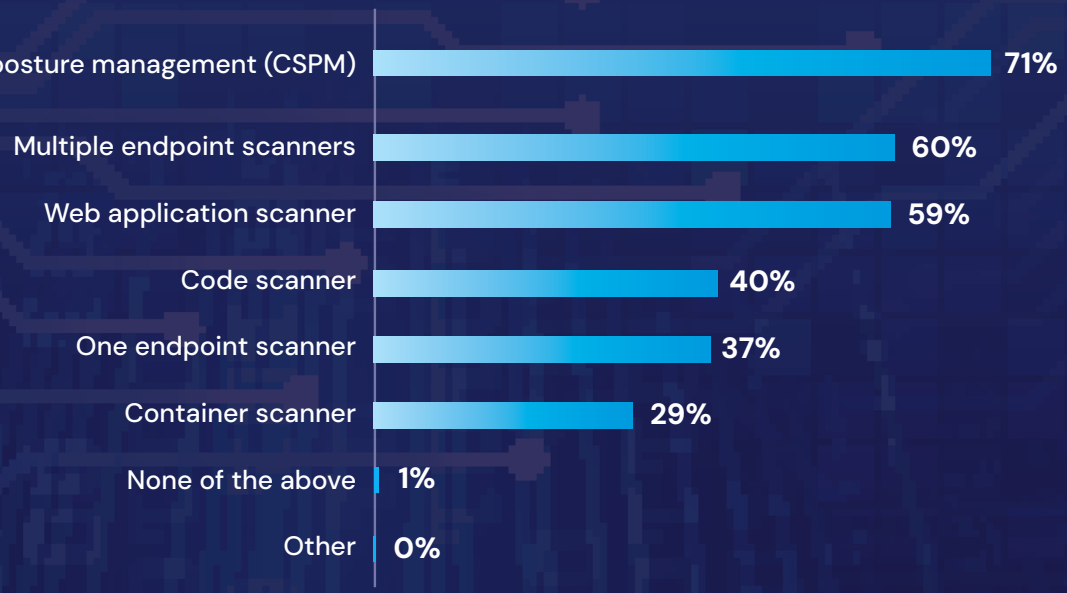
45% Hybrid Approach: A mix of manual processes and automation is used for remediation

21% Automated Remediation: Rely on automation tools to detect and remediate vulnerabilities with minimal human intervention

Vulnerability Management is a Web of Complexity (continued)

Adding to the complexity, organizations are leveraging a variety of tools to detect vulnerabilities, with cloud security posture management (CSPM), multiple endpoint scanners, and web application scanners emerging as the top three tools. The increasing reliance on these diverse tools raises important questions about the effectiveness and integration of current strategies. While these tools are powerful, they can generate fragmented data that complicates decision-making.

What vulnerability scanning tools do you have in your environment?

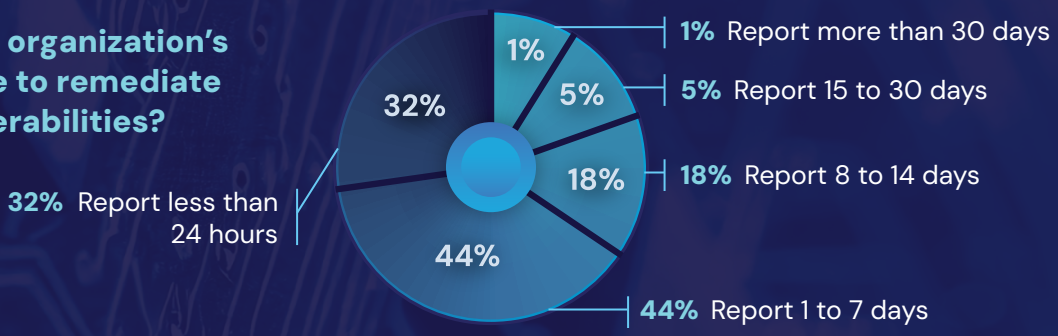


Organizations are leveraging a variety of tools to detect vulnerabilities.

Lack of Context Fuels the Race Against Time

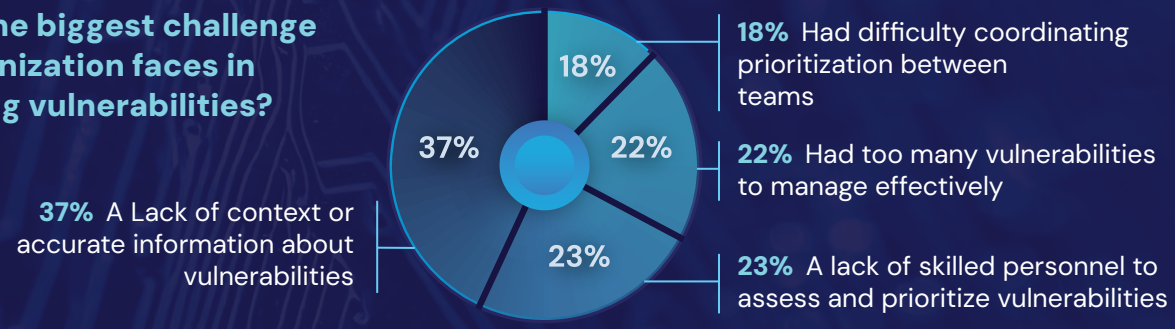
Organizations are facing significant delays in addressing vulnerabilities, with 68% reporting that it takes more than 24 hours to remediate a critical vulnerability. This lag is a major concern, especially when timely remediation is essential to minimizing risk and ensuring compliance.

What is your organization's average time to remediate critical vulnerabilities?

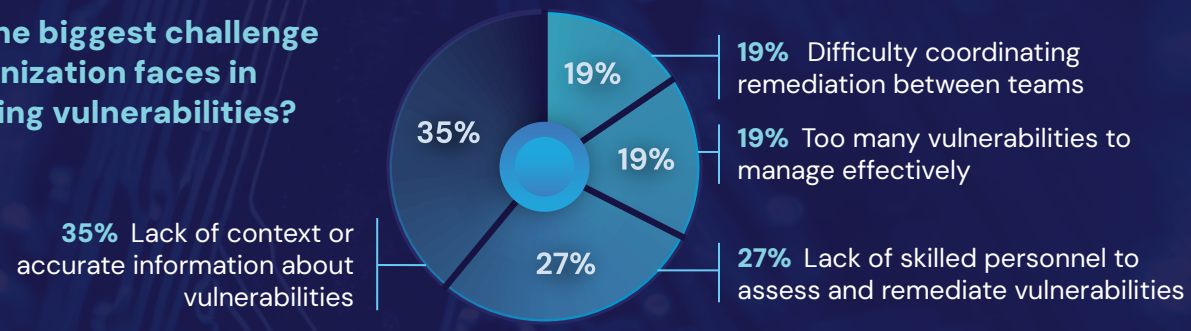


A primary barrier to faster action is the lack of context or accurate information. 37% of organizations identify this as their biggest challenge when prioritizing vulnerabilities, and 35% say the same when it comes to remediation. With over 39,000 new vulnerabilities received by the National Vulnerability Database in 2024, having the right data is crucial to intelligent and fast risk scoring. Without it, security teams are left to work with incomplete or fragmented insights, leading to inefficient processes and slower response times.

What is the biggest challenge your organization faces in prioritizing vulnerabilities?



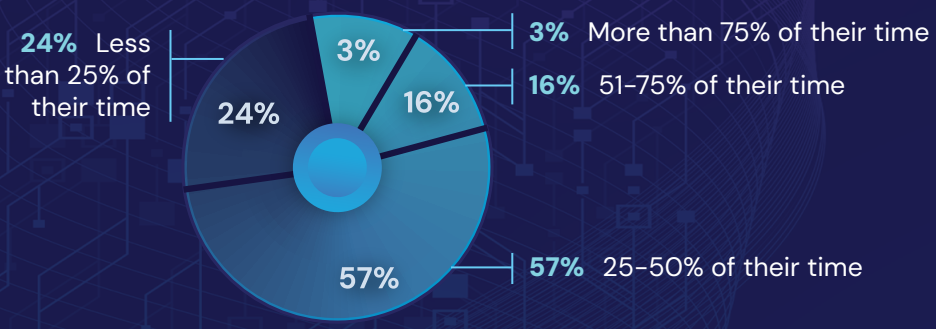
What is the biggest challenge your organization faces in remediating vulnerabilities?



The Hidden Costs of Manual Efforts and Inefficiencies

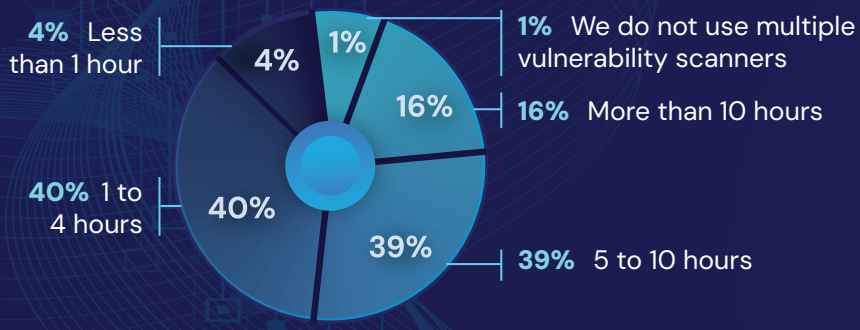
Manual processes are a major drain on security teams, with 57% of respondents reporting that they spend anywhere from 25% to 50% of their time on manual tasks related to vulnerability management. This not only slows down response times but also ties up valuable resources that could be better utilized elsewhere. *Given that the average vulnerability management professional earns $61 an hour, these manual tasks are costing businesses an estimated $47,580 per employee, per year.*

How much time approximately does your security team currently spend on manual tasks related to vulnerability management operations?



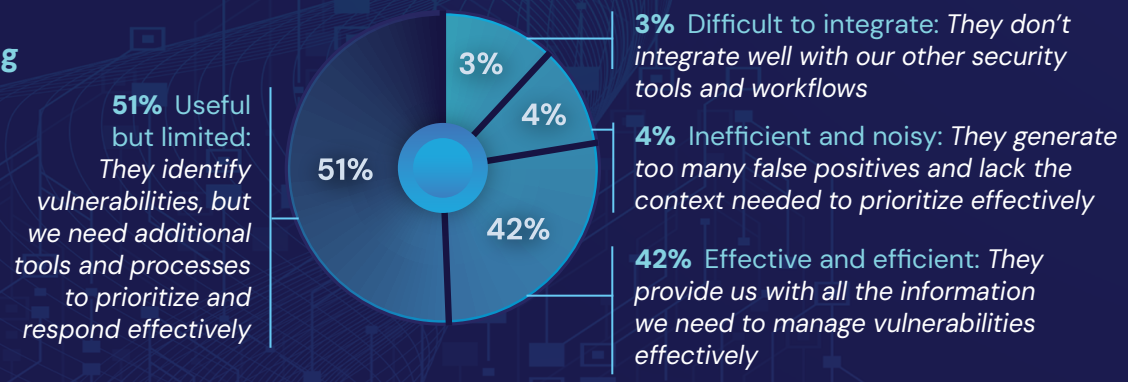
On top of this, 55% of organizations say their teams spend over five hours each week simply consolidating and normalizing vulnerability data. This labor-intensive task adds unnecessary complexity to the vulnerability management process and contributes to inefficiencies that could be avoided. Similarly, these tasks to consolidate data are costing businesses an estimated $15,860 per employee, per year.

How much time approximately does your security team spend each week consolidating and normalizing vulnerability data?



The limitations of vulnerability scanning tools further compound the problem. While 51% of respondents find the results from these tools useful, they often fall short, forcing teams to turn to additional tools and processes to fill the gaps. This scattered approach creates more work and confusion, ultimately undermining the goal of a streamlined and effective vulnerability management strategy.

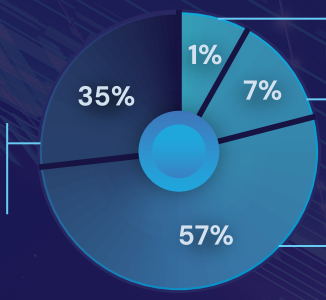
Which of the following best describes the quality of results associated with vulnerability scanners?



The Confidence Shortfall in Regulatory Compliance

Organizations are facing a stark reality when it comes to their vulnerability management programs. Nearly two-thirds (65%) of organizations are not fully confident that their current vulnerability management program would satisfy a regulatory audit. This lack of confidence highlights a significant weakness in the programs designed to ensure both security and compliance.

How confident are you that your current vulnerability management program would satisfy a regulatory audit?



35% Very confident – *we have a mature program and regularly pass audits*

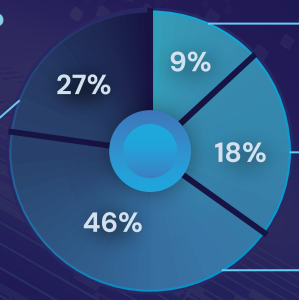
1% Not at all confident – *we are not prepared for an audit and expect to receive findings*

7% Not very confident – *we have significant gaps in our program and are at risk of failing an audit*

57% Somewhat confident – *we generally meet requirements, but there are areas for improvement*

The fear of regulatory consequences is widespread, with 73% of organizations expressing concern about the potential for fines due to inadequate vulnerability management. As regulations grow stricter and scrutiny intensifies, the risk of non-compliance becomes more than just a theoretical threat — it's a pressing concern that could have financial and reputational repercussions.

How concerned are you about the potential for regulatory fines due to inadequate vulnerability management?



27% Not very concerned – we have a strong vulnerability management program in place

9% Extremely concerned – we have already received warnings or fines related to vulnerability management

18% Very concerned – we are struggling to meet compliance requirements and fear potential fines

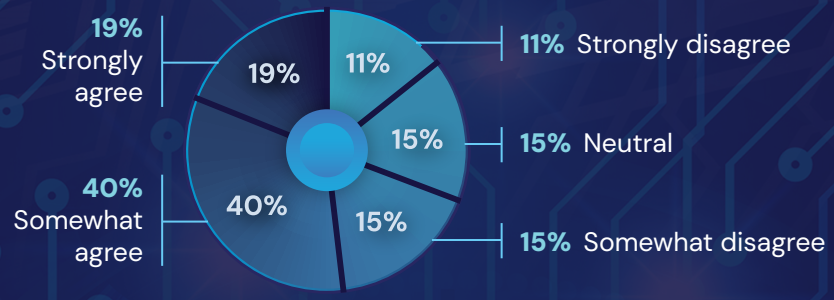
46% Somewhat concerned – we have some gaps in our program that we need to address

The risk of non-compliance becomes more than just a theoretical threat — it's a pressing concern that could have financial and reputational repercussions.

Siloed Processes Fuel Bigger Security Risks

Siloed vulnerability management processes are a ticking time bomb for organizations. 59% of companies report that their vulnerability management efforts are isolated within specific departments, leading to inefficiencies, miscommunication, and critical security gaps.

To what extent do you agree with the following statement: Vulnerability management is siloed within our organization, leading to inefficiencies and potential security gaps?



The risks of this disjointed approach are significant. Organizations identify reputational damage and loss of customer trust (40%) as the top consequence of poor vulnerability management, followed closely by business disruption and operational downtime (38%). In addition, 29% are concerned about the financial penalties and fines they could face for non-compliance with regulations. These risks highlight the far-reaching impact of siloed processes, which not only jeopardize security but also threaten the organization's bottom line and reputation.

What do you perceive as the biggest risks associated with poor vulnerability management in terms of compliance?

Embracing Smarter Vulnerability Response Management: The Path Forward

The growing complexity of vulnerability management is pushing organizations to rethink how they approach organization-wide security, risk and compliance strategies. With the constant rise in vulnerabilities and an overwhelming volume of data, organizations need to adopt smarter, more efficient methods to stay ahead. Intelligent prioritization and automation are no longer just nice-to-haves — they are critical to navigating this challenge.

This shift is about more than just patching vulnerabilities; it's about prioritizing the ones that matter most to the organization's operations. Intelligent systems that blend automation with human expertise provide security teams with the insights they need to act decisively. With routine tasks handled automatically, teams can focus on the most impactful threats, ensuring they remain agile. This approach centralizes data from various sources, offering a unified, real-time view of an organization's security posture. This greater visibility supports smarter prioritization, enhances cross-functional collaboration, and strengthens the overall ability to reduce vulnerabilities, prevent breaches, and maintain continuous compliance.

The clock is ticking, and the stakes are higher than ever. Organizations can no longer afford to operate in the reactive mode of the past. By embracing smarter prioritization and automation today, they can fortify their defenses, minimize risk, and ensure compliance, while regaining time to prepare for the next challenge.

This shift is about more than just patching vulnerabilities; it's about prioritizing the ones that matter most to the organization's operations.

Methodology

The survey was conducted among 500 cybersecurity decision-makers at enterprise companies with at least 1,000 employees in the United States and United Kingdom. The interviews were conducted online by Sapio Research and under the guidance of Swimlane, Inc. in August 2024 using an email invitation and an online survey.

About Swimlane

At Swimlane, we believe the convergence of agentic AI and automation can solve the most challenging security, compliance and IT/OT operations problems. With Swimlane, enterprises and MSSPs benefit from the world's first and only hyperautomation platform for every security function. Only Swimlane gives you the scale and flexibility to build your own hyperautomation applications to unify security teams, tools and telemetry ensuring today's SecOps are always a step ahead of tomorrow's threats.

About Sapio Research

Sapio's passion is giving clients confidence in their decisions, creativity, or storylines—helping them look good and be more productive. We do this by collecting and synthesising insight from qualitative, quantitative, or secondary research data sources. We focus on three key services: audience understanding, brand research, and thought leadership research.

Our high-quality tailored insights help improve lead generation and reputation, get you closer to your audience, and gain an edge against the competition. Through understanding, honest counsel, collaboration, and a swift approach we deliver projects you'll be proud of.

Best new agency finalist, Sapio is adept at opinion polling (we have access to 80 million people internationally), focus groups, face-to-face interviews, telephone interviews, online research, desk research and statistical modelling, to mention just a few techniques. We love B2B research and consultancy. Our business is based on partnership principles inspired by social enterprise.

CONTACT US
swimlane.com

GLOBAL HQ
999 18th St, Suite 2201N
Denver, CO 80202
1-844-SWIMLANE (1-844-794-6526)
info@swimlane.com

LONDON
4 Studley Court, Guildford Road,
Chobham GU24 8EB UK

MALAYSIA
Level 13A, Wisma Mont Kiara,
No. 1, Jalan Kiara, Mont Kiara,
50480 Kuala Lumpur,
Wilayah Persekutuan Kuala Lumpur

JAPAN
1-6-5, Kudan Minami, Chiyoda-ku,
Tokyo 102-0074

INDIA
1st Floor, Wing A, Purva Summit,
White Field Road, Kondapur, Hyderabad.