Enterprise Strategy Group | Getting to the bigger truth.™

Leveraging Observability Data for DevSecOps

Optimize Efficiency by Capturing and Sharing Data for Faster Security Response

Melinda Marks, ESG Senior Analyst

AUGUST 2022

TABLE OF CONTENTS

CLICK TO FOLLOW

Moving to DevSecOps

As organizations adopt modern software development processes leveraging cloud platforms, they are looking to incorporate security processes and controls into their software development lifecycle (SDLC) processes.

Though only 22% of organizations said they have developed a DevSecOps strategy integrating security into SDLC processes, current adoption is low, while a majority (62%) of organizations have a plan or are evaluating use cases, showing significant future growth of DevSecOps.

22%

of organizations said **they have developed a DevSecOps strategy** integrating security into SDLC processes.

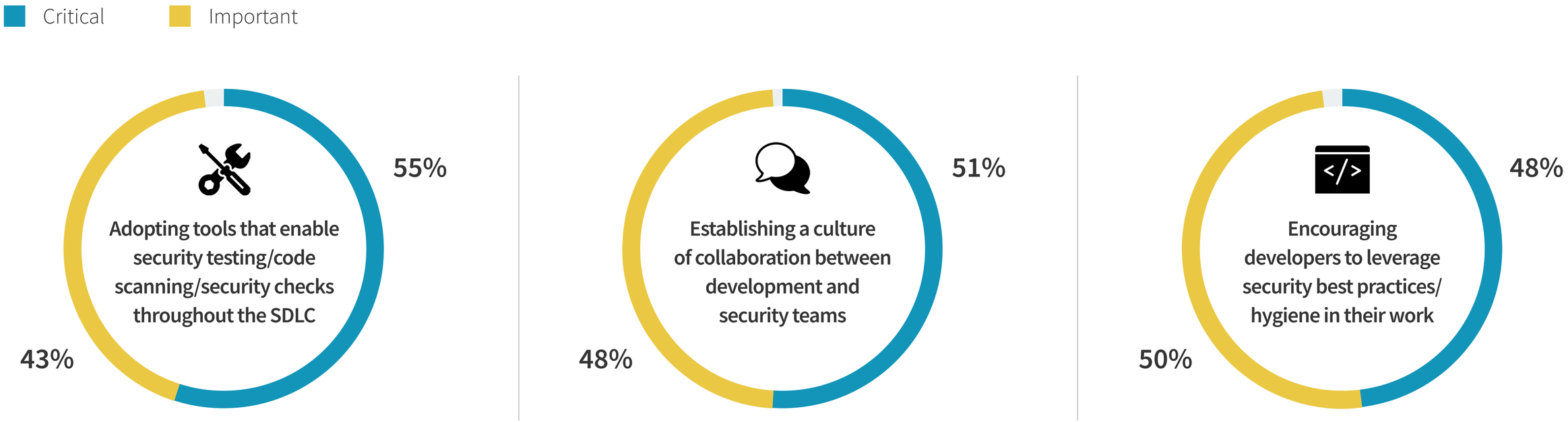
62%

of organizations **have a plan or are evaluating use cases**, showing significant future growth of DevSecOps.

Back to Contents

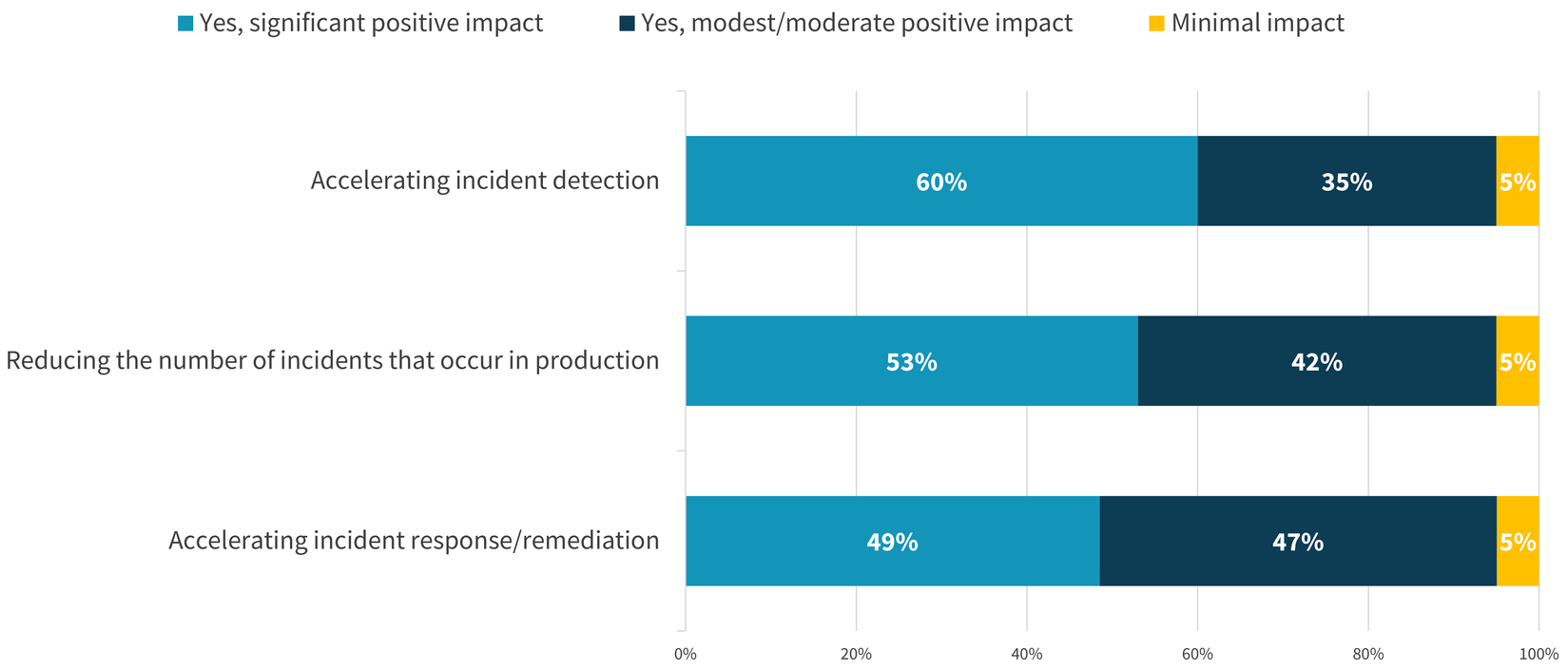
Using tools, collaboration, and secure practices in development

Organizations prioritize adopting tools that enable security testing throughout the SDLC, but they also overwhelmingly acknowledged the criticality and importance of collaboration between teams and encouraging security best practices in development.



Back to Contents

Organizations that have adopted DevSecOps report significant improvements in incident volume and detection

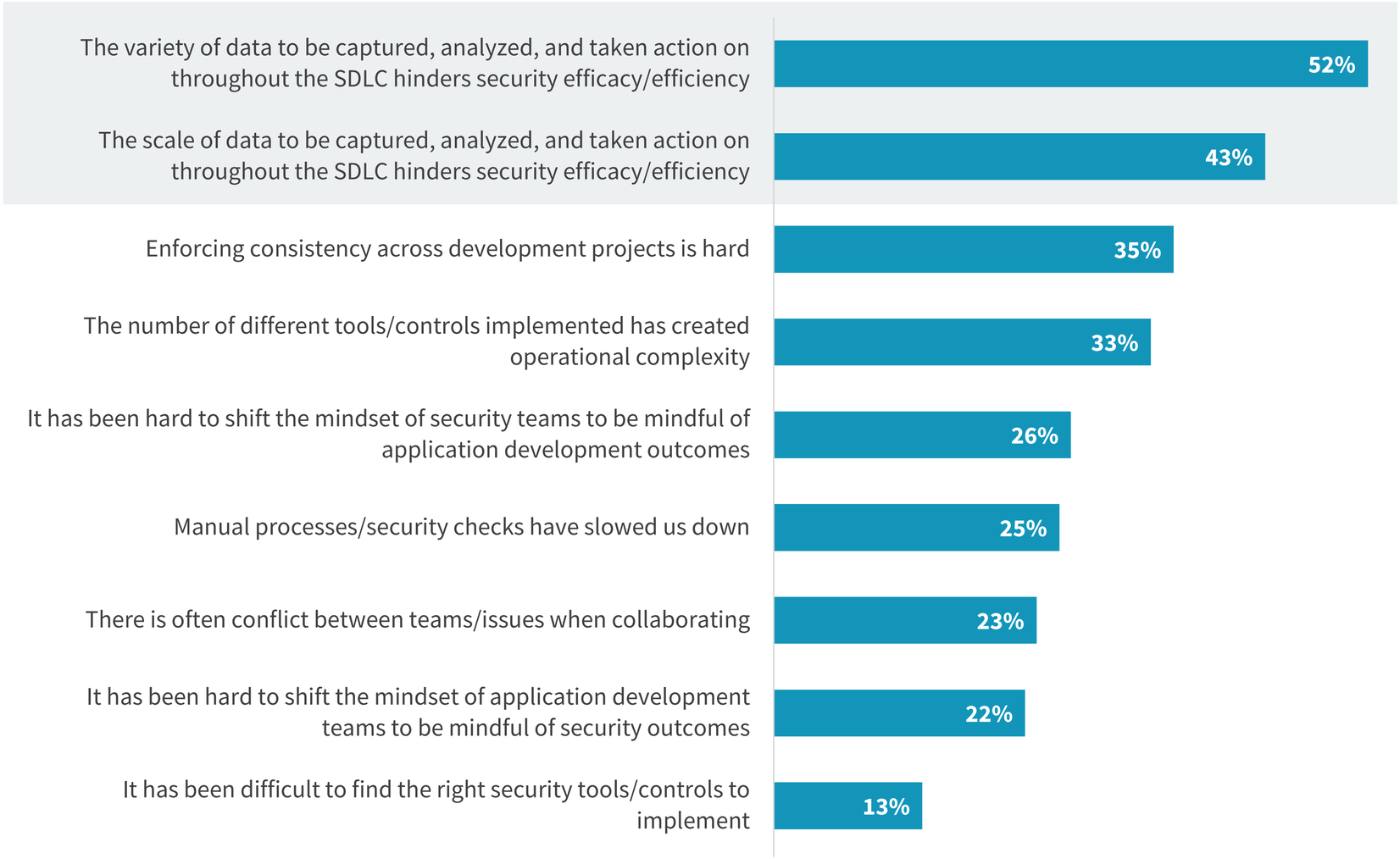


> **DevSecOps has had the biggest positive impact on accelerating incident detection,** while also reducing the number of incidents in production and accelerating incident response.”

Back to Contents

> “For those who have adopted DevSecOps, **data capture and analysis are at the top of the list of challenges related to adopting DevSecOps.**”

Data and Observability Challenges to DevSecOps

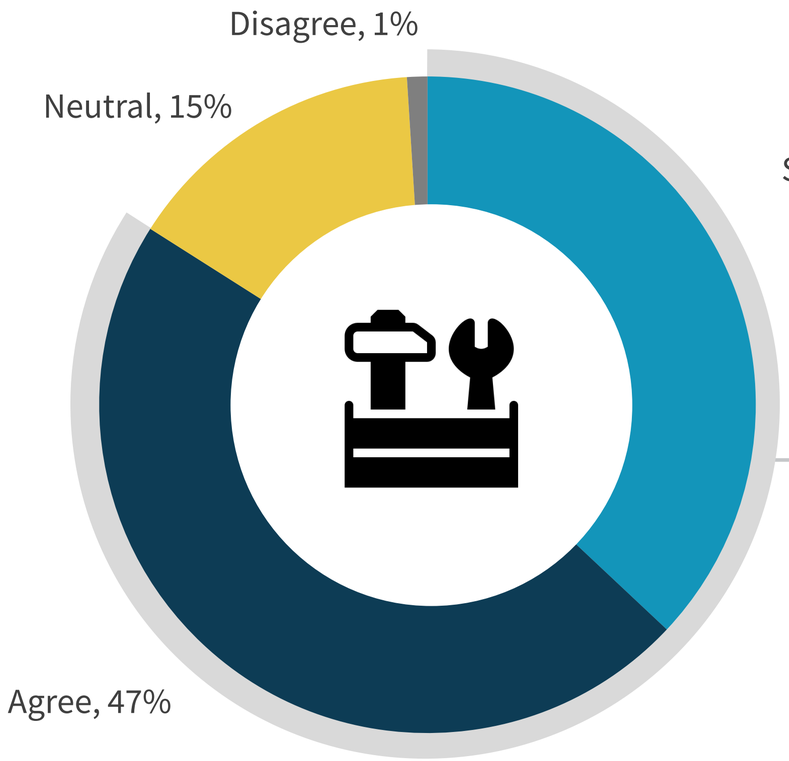


Back to Contents

Getting Data to the Right Person at the Right Time

Developer efficiency is all about shortening feedback loops so that developers can efficiently get the information they need and make needed coding corrections.

It's important that developers can get accurate, timely information throughout the software development lifecycle in order to work efficiently to produce better quality code and to be able to remediate any issues once their software is released.



84% of respondents **believe getting the right data and tools to developers is key to enabling DevSecOps.**

Back to Contents

Using Data for Better Security

Organizations need ways to speed their response to security alerts and incidents because it takes time to collect, integrate, and analyze application and security data in order to triage an incident.

82%

of respondents say accelerating the mean time to resolve security alerts/incidents **is a top priority for their security team.**

17.5

person hours is the average time it takes to understand and triage security incidents.

Back to Contents

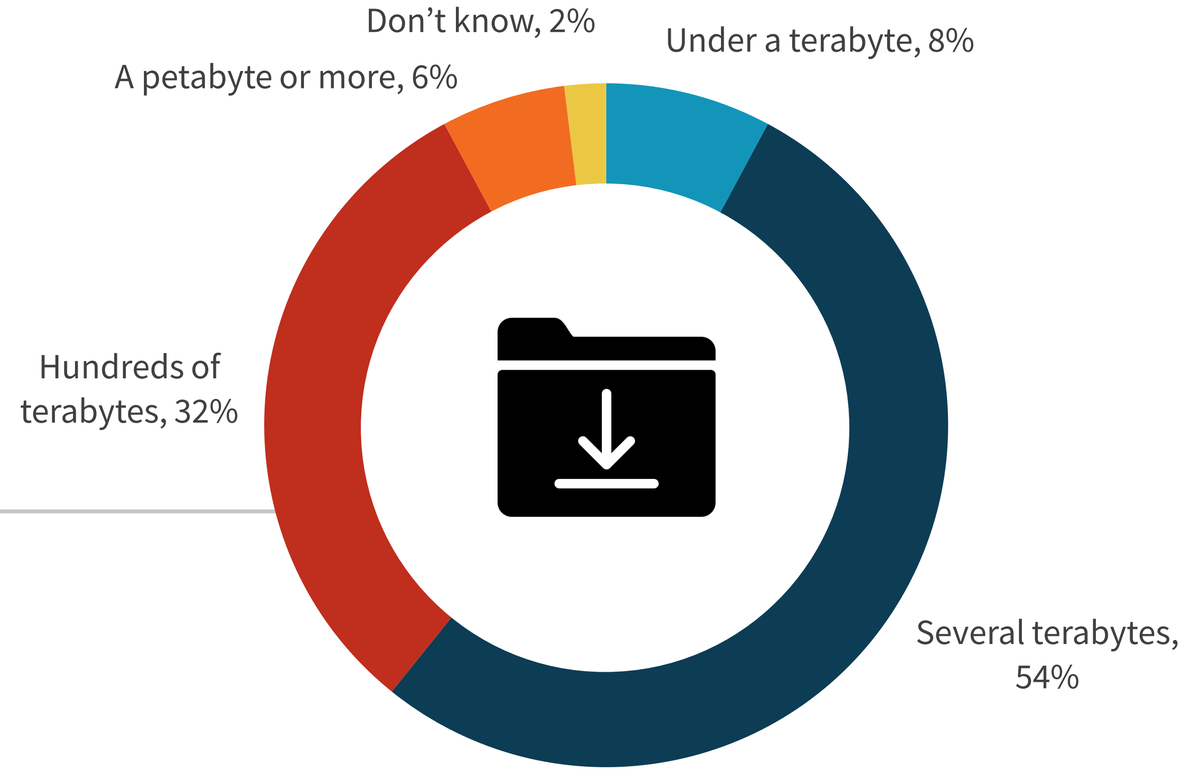
Overcoming Data and Observability Challenges

As organizations are increasing the speed and volume of releases to serve more customers, they are collecting huge volumes of data.

But it is costly to collect this much data just for the sake of collecting it.

Instead, organizations should leverage the information to be able to learn from it to improve processes and be able to react quickly when action is needed.

Almost one-third of organizations surveyed capture **hundreds of TBs of application data per month.**

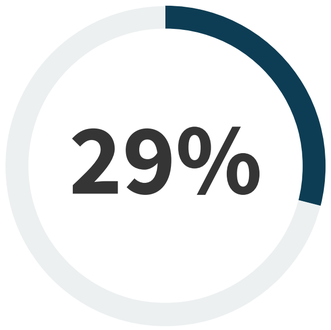


Back to Contents

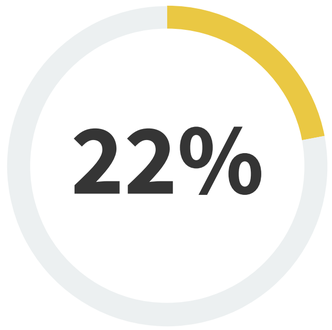
Log data is the biggest component of application data produced, by volume

Log data

Metrics



Traces



Other types of machine generated data

Back to Contents

Getting the Most out of Data

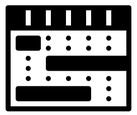
Organizations need to find a way to analyze and use the data. Organizations are using dedicated log analysis tools for storing and analyzing application observability data, but it is also common to use multiple tools (91% of organizations) to get the most out of their data.

Dedicated log analysis tools

66%

A cloud-hosted data lake

64%



A security information and event management (SIEM) solution

59%

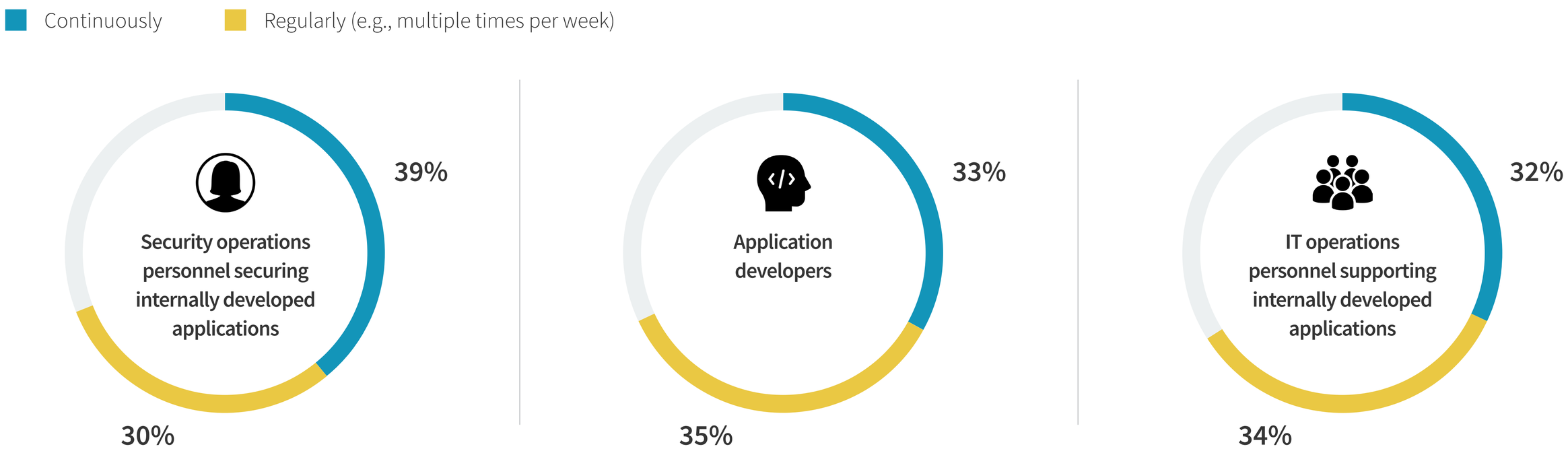
An on-premises data lake

55%

Back to Contents

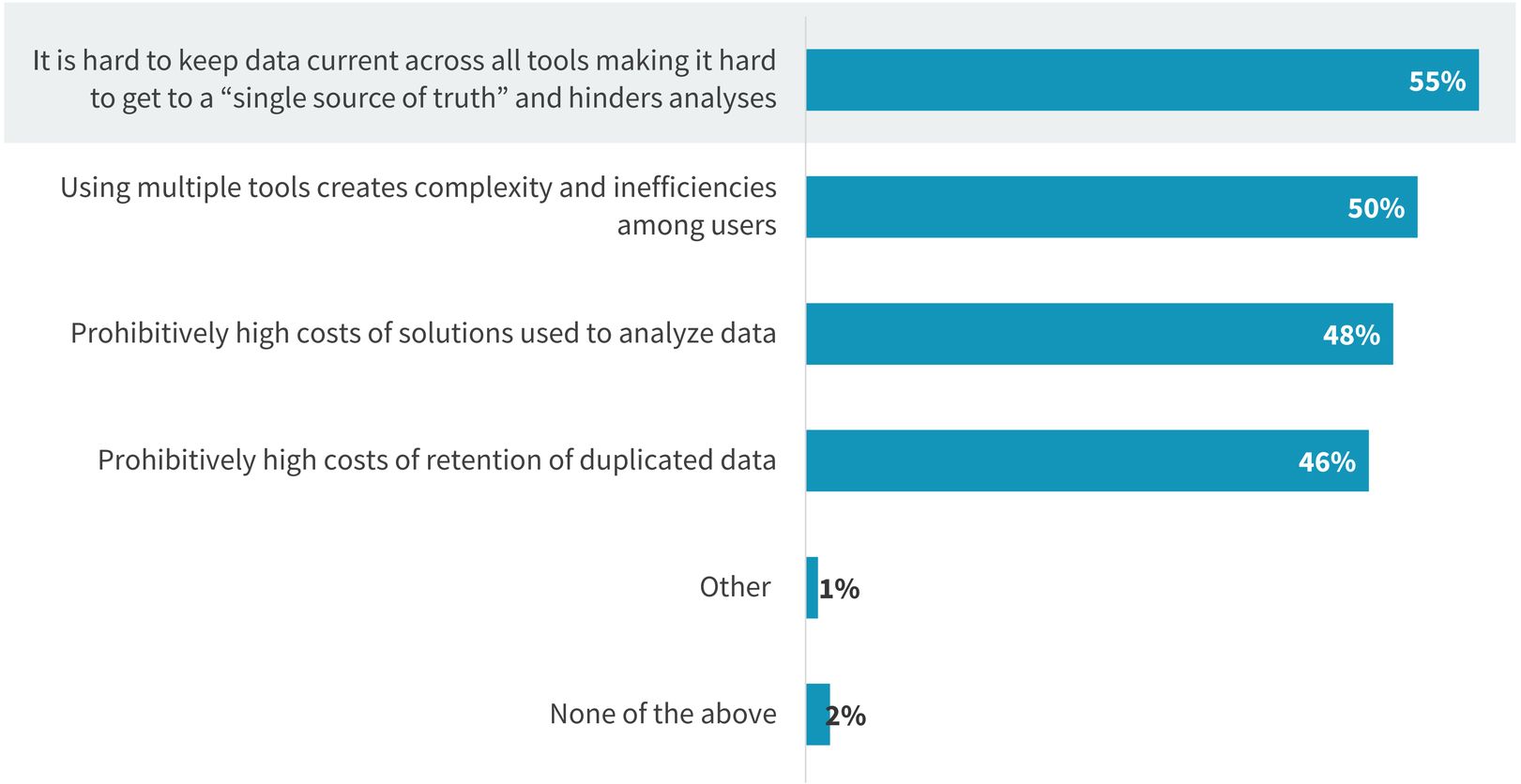
Sharing Data Across Groups

Another challenge is ensuring that multiple groups have access to data to help them in their jobs. **Two-thirds of respondents say that staff across groups—security operations, application developers, and IT operations—need regular access to data.**



Back to Contents

The biggest challenge is keeping data updated for a “single source of truth.”



“For organizations using multiple tools to store and analyze observability data, **it is costly and inefficient.**”

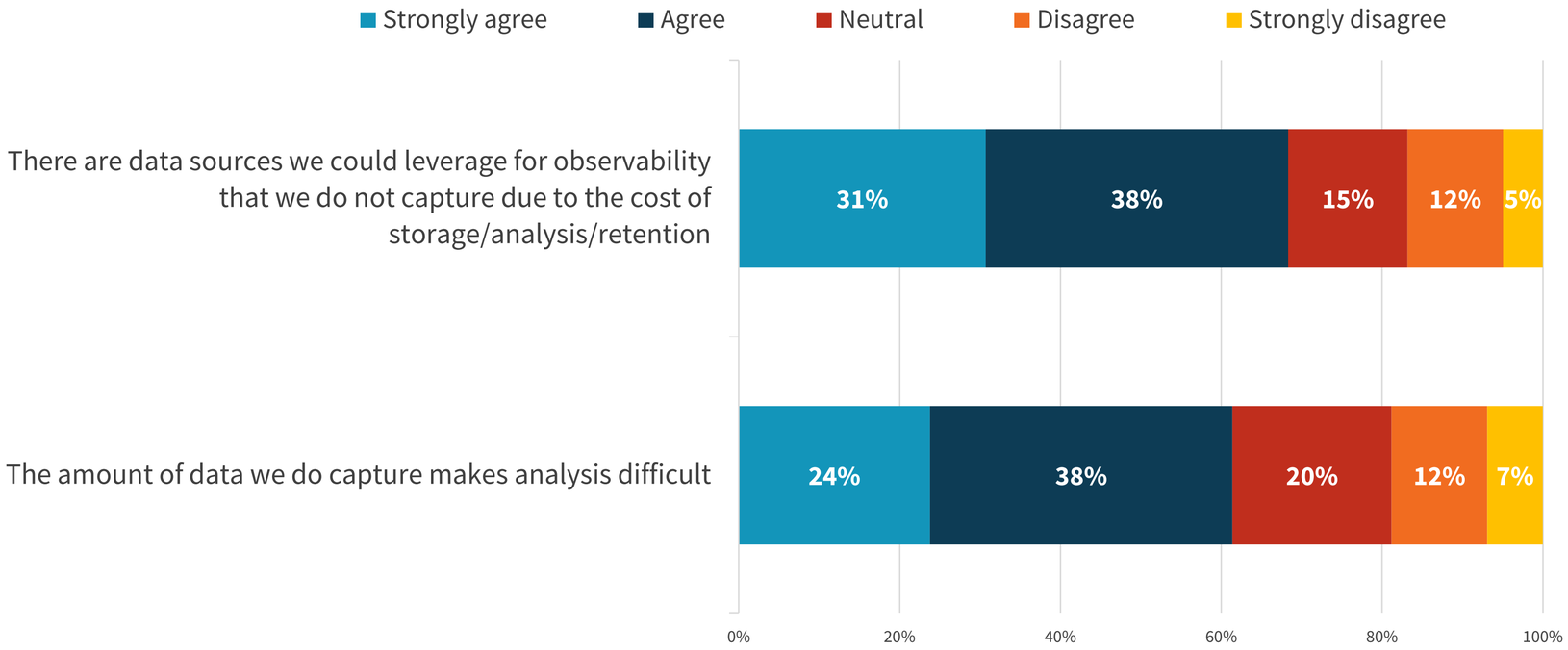
Back to Contents

Getting past cost barriers

The high cost of storage/retention of data can impact application protection if organizations are only able to collect or store data for higher priority applications.

This is problematic if there is an incident and the organization has incomplete data for a thorough analysis and/or timely response.

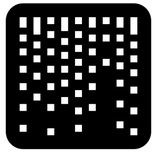
Most organizations (69%) do not capture certain data sources because of the high cost of storage/retention.



Back to Contents

The Need for Better Tooling to Generate Actionable Insights

SIEMs do not empower organizations to distinguish “the signal from the noise” when it comes to application data and observability. When organizations want to speed their mean time to remediation (MTTR), SIEMs are not helpful.



The amount of data captured makes it hard to conduct actionable analysis (i.e., it is hard to distinguish “the signal from the noise”),

73%

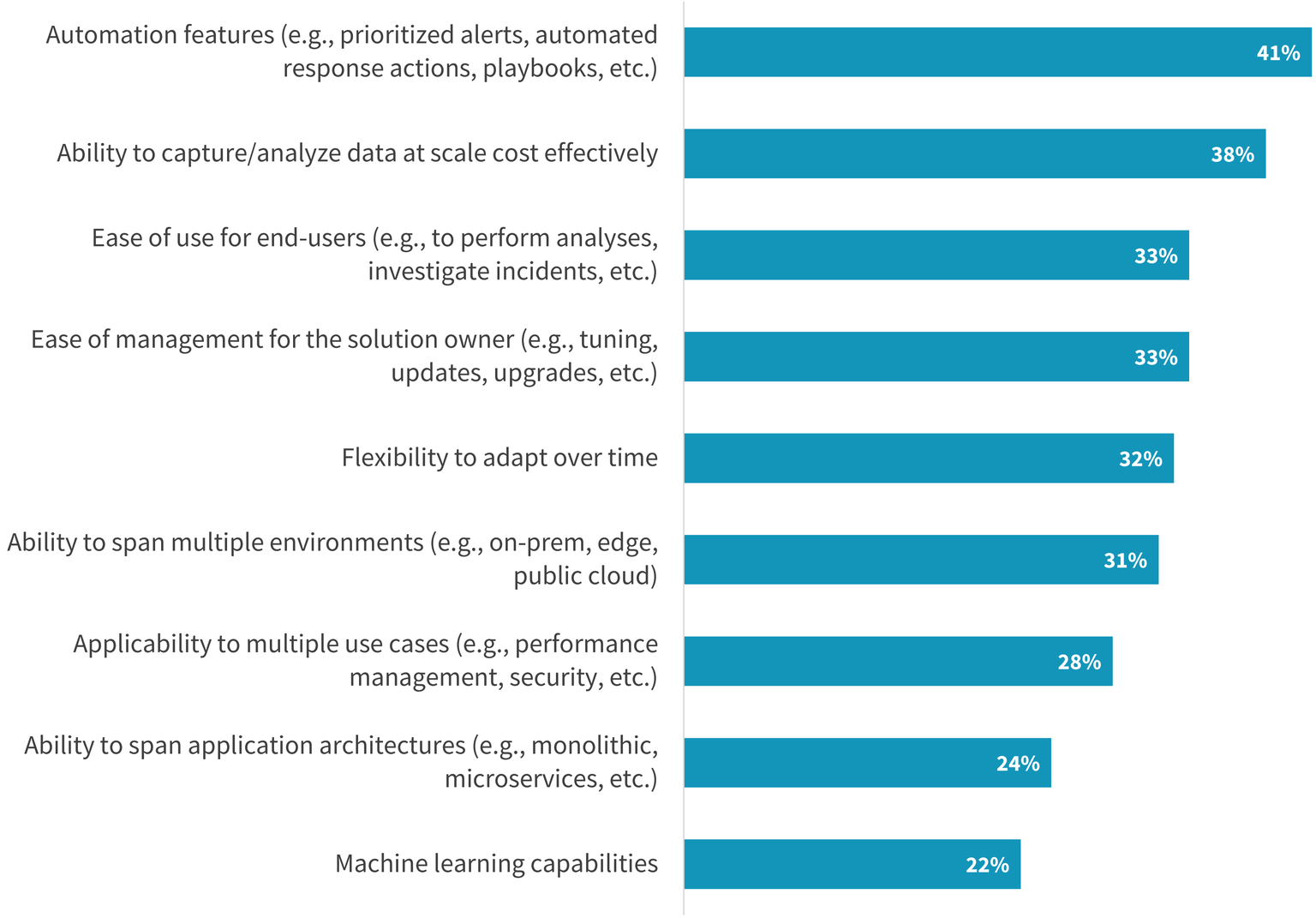
We are constrained by the cost associated with storing/analyzing the volume of data we capture,

73%

Back to Contents

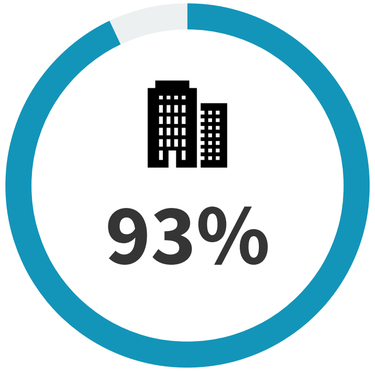
Top Characteristics for an Observability Solution

Because of these frustrations, organizations are looking for automation features and scalability as the ideal characteristics for an observability solution. They are also looking for ease of use, ease of management, and flexibility to adapt over time.



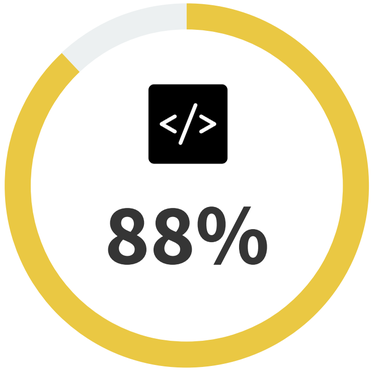
Back to Contents

Flexibility to adapt over time is a must for an observability solution:



of organizations agree

of IT/security professionals agree



of app dev/software engineers agree

Back to Contents

Opportunities and Challenges With Open Source

Organizations often look to open source tools to build customized solutions to leverage their data, but they face challenges scaling them because of the work required to integrate and manage them.

87%

of organizations leverage open source tools within their observability practices.

98%

cite the ability to customize as a key factor in using open source.

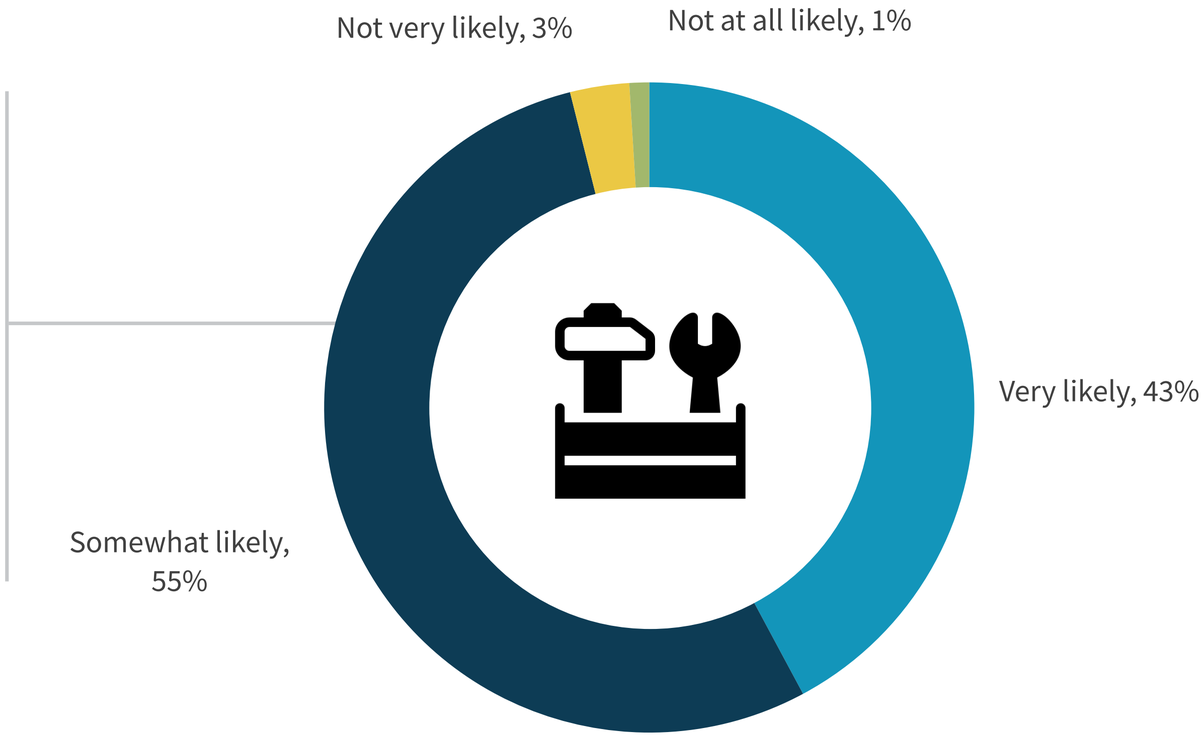
84%

believe it will be challenging to manage, adapt, and scale their open source solutions.

Back to Contents

As a result, organizations are looking for a solution that scales to fully harness their data to drive better results.

Nearly all survey respondents (98%), with titles across teams, from application developers to IT/security professionals, **said they will likely investigate a managed observability solution over the next 12 months.**



Back to Contents

Mezmo, formerly LogDNA, provides an observability platform that helps organizations manage and take action on their data. It ingests, processes, and routes log data to fuel enterprise-level application development and delivery, security, and compliance.

Mezmo saves customers from drowning in data and the high costs of retaining logs. Built for cloud-native environments with modern software development workflows, it provides a single source of truth of what is happening, democratizing the data across groups so they can easily access data to help them in their roles.

This enables collaboration across development, security, and IT teams to create higher quality, more secure products with DevSecOps. Teams can work more efficiently to respond to security alerts and incidents, shortening the feedback loop for developers to remediate security issues and reducing MTTR.

LEARN MORE

Back to Contents

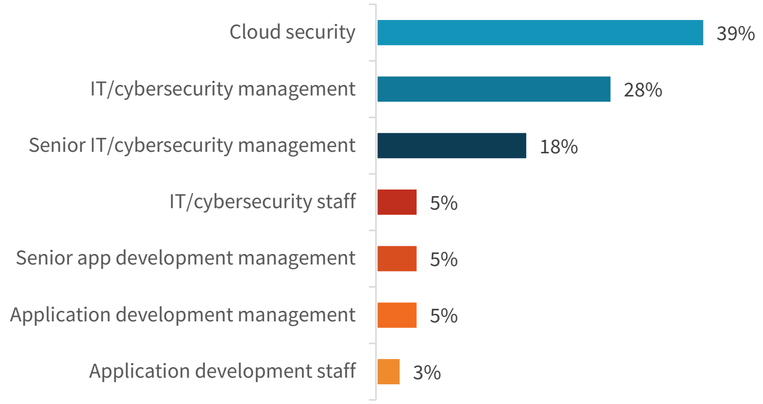
Research Methodology and Demographics

To gather data for this report, ESG conducted an online survey of application developers and security professionals at enterprise organizations (1,000+ employees) knowledgeable about the controls and processes in place to secure internally developed/custom applications. The survey included respondents based in North America (US and Canada).

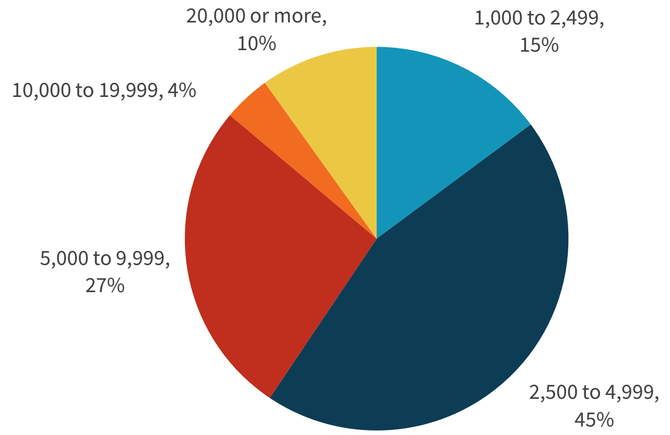
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 200 IT professionals.

Totals in figures and tables throughout this report may not add up to 100% due to rounding.

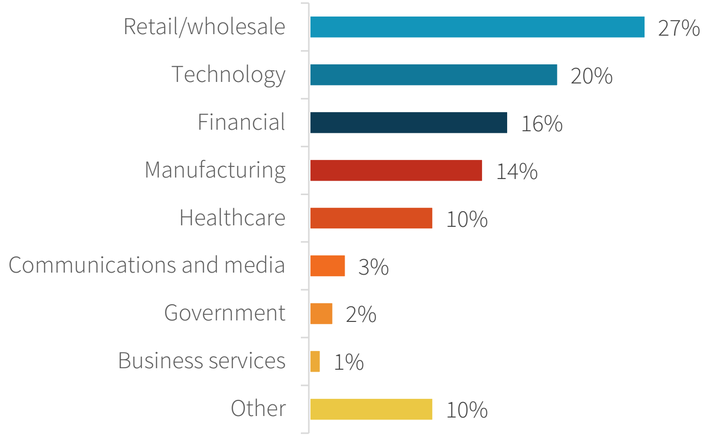
RESPONDENTS BY ROLE



RESPONDENTS BY EMPLOYEES



RESPONDENTS BY INDUSTRY



Back to Contents

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.