Enterprise Strategy Group | Getting to the bigger truth.™

Cloud-native Security Maturity:

Using Security to Drive Software Development Efficiency

Melinda Marks, Senior Analyst

MAY 2022

CONTENTS

Research Objectives

As organizations increasingly adopt cloud-native development, they are at various stages of building their security programs to meet the needs of dynamic environments and faster software development cycles. As cloud-native technologies and application components continue to evolve, security teams need to implement the right security technologies, programs, and processes to mitigate risk. ESG surveyed 1,000 cybersecurity professionals knowledgeable about development practices and outcomes at their organizations to learn about the maturity of their security programs and whether they had measurable benefits across different areas.

By looking at how these organizations are securing their applications and their underlying platforms, what tools they are using, how they are gaining organizational alignment, and what they are doing to leverage controls, ESG was able to rank their cloud-native security maturity. Then, ESG was able to evaluate whether more mature security programs impacted security posture, development cycles, and business outcomes.

THIS STUDY SOUGHT TO:

Assess how organizations are securing their cloud-native environments and the maturity of their programs.

Gauge the outcomes and business value organizations achieve with stronger security programs in place.

Explore how mature security programs affected security program effectiveness, software development, and business outcomes.

Validate that security programs drive efficiency across the software development lifecycle, resulting in higher product revenues.

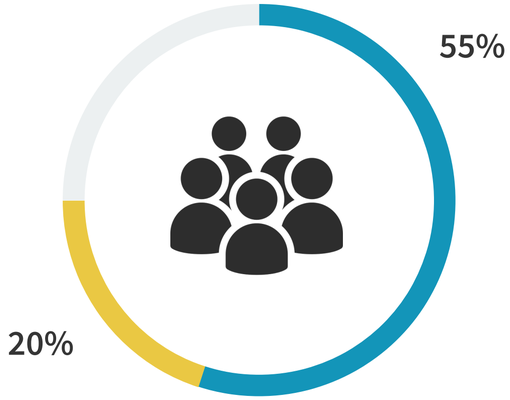
Back to Contents

Cloud-native Security Maturity Trends

For three consecutive years, ESG has studied the maturation of cloud-native security. The most recent report confirmed security maturity trends, including:

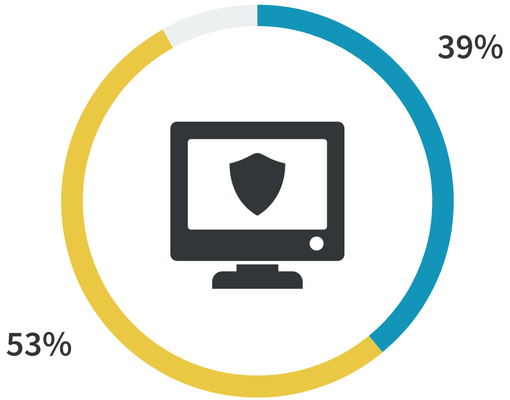
Centralized, top-down buying patterns with executive sponsorship

- We have different teams responsible for securing cloud-native applications, but we plan to merge these responsibilities
- We have already centralized and unified security responsibilty across all our applications and aspects of our environment



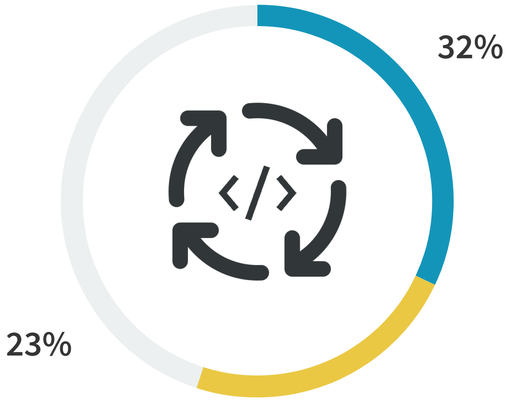
A preference for a platform approach consolidating tools and controls

- We have already consolidated to an integrated platform
- We plan to consolidate to an integrated platform in the next 12-24 months



Security integration with DevOps processes

- We have incorporated security into our DevOps processes extensively
- We have incorporated security into our DevOps processes in a limited fashion

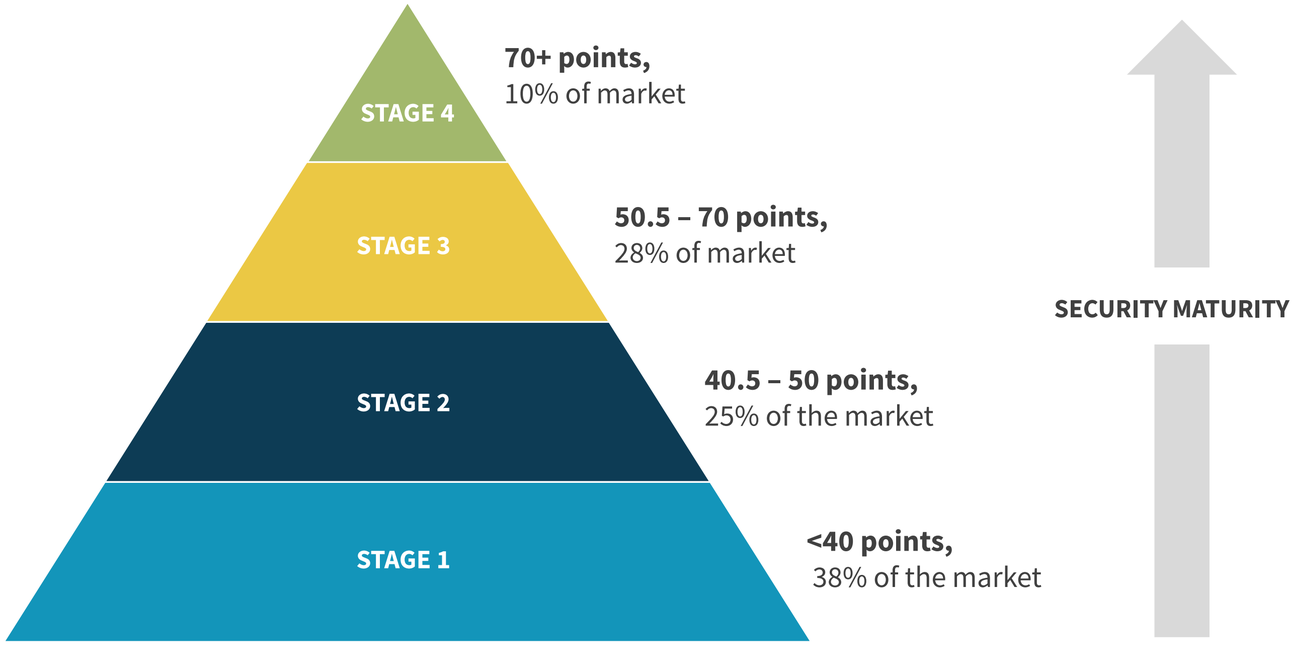


Back to Contents

Segmenting Organizations in Terms of Security Maturity and Looking at the Results

Based on these key cloud security maturity trends, ESG created a data-driven model that segments respondents' organizations into four stages of cloud-native security progress, with Stage 4 being the most advanced. The model used 10 questions from the primary research as inputs to rate the organization's security program in terms of the organization's DevSecOps practices, cloud native security controls in use, security team structure, and executive sponsorship. The more characteristics in place indicate higher security maturity. Then, we looked at how security maturity aligned with modern software development results.

Respondents by Security Stage



CHARACTERISTICS OF A HIGHER STAGE

DevSecOps practices:

An extensive adoption of DevSecOps practices, including:

- Automated security processes for more than three-quarters of internally developed applications.
- Processes that span numerous security workflows, including identifying and remediating vulnerabilities, logging code changes, discovery and inspection of APIs, application of access controls, and more.

Cloud-native security controls in use:

- Current usage of a broad portfolio of controls securing cloud-native applications, including cloud security posture management, container security, API security, entitlement management, web application firewalls, and more.
- A defense-in-depth approach that combines both third-party tools and those provided by the cloud service provider.
- An approach that prioritizes a platform approach delivers the functionality of multiple controls in a single solution for scale and efficiency.

Security team structure and executive support:

- Collaboration between security and development stakeholders throughout the software development lifecycle.
- The organization's employment of cloud security specialists equipped to implement "security as code" approaches.
- Frequent briefings done by the CISO (or equivalent) to the business about the organization's cloud-native security posture.

Back to Contents

KEY FINDINGS

Higher stage orgs remediate vulnerabilities more efficiently

75%+ scan code at each stage of the lifecycle, and they can respond to vulnerabilities 28% faster than average respondents.

Developers at higher stage orgs see security as enablers instead of blockers

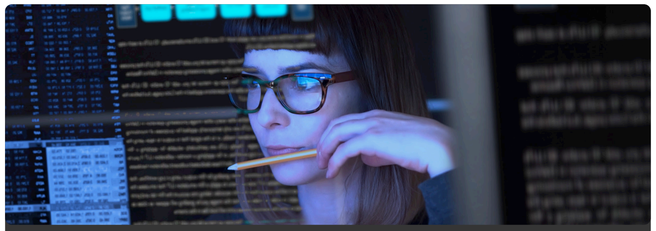
Leading organizations are 4.2x more likely to have development teams that see their security teams as business enablers.

Security stage correlation with operational excellence

Leading organizations are 2x more likely to say their security program has had a significant positive impact on application reliability, observability, and overall security.

Higher stage orgs suffered fewer security incidents

Stage 1 organizations have suffered 31% more cloud-native application security incidents in the past 12 months (despite 3.7x larger cloud-native footprints).



Security maturity impacts product functionality and on-time delivery

Stage 4 organizations are 4.3x more confident about delivering secure code on time and 2.1x more likely to report excellent functionality.

Higher stage orgs beat revenue goals and the competition

Stage 4 organizations exceed revenue goals at a rate 55% higher than Stage 1 organizations and are 3.8x more likely to say their company is in a strong position than Stage 1 organizations. are.

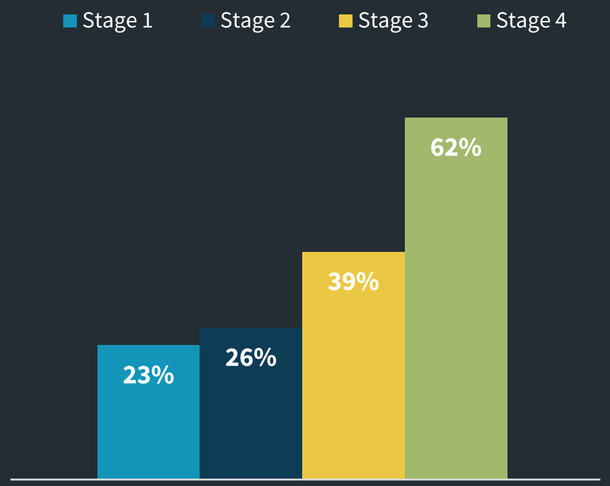
Back to Contents

Cloud-native Adoption Drives Security Progress

Organizations need mature security programs in place as they increasingly move critical workloads and applications to the cloud.

Prevalence of cloud-native applications in production

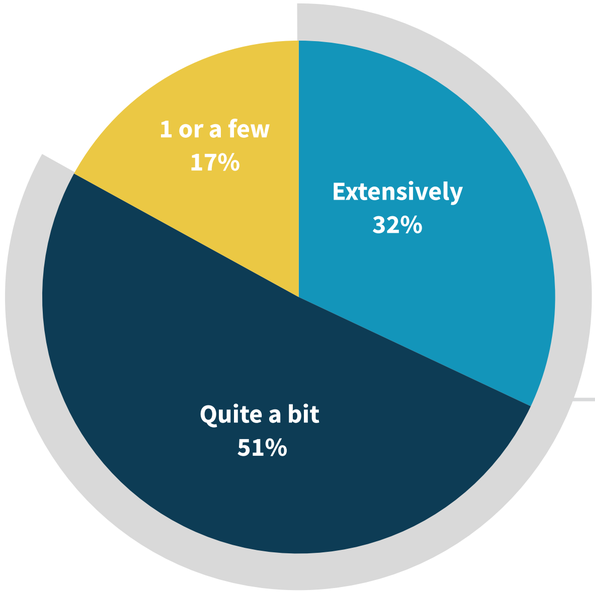
A majority of the organizations surveyed are extensively deploying cloud-native applications in production. When broken down by stage, the Stage 4 respondents were nearly **3x more likely** to say they have extensively pushed cloud-native apps into production than Stage 1 respondents.



Extensively - we have numerous cloud-native applications in production

“Stage 4 respondents were nearly 3x more likely to say they have extensively pushed cloud-native apps into production than Stage 1 respondents.”

Internally developed and delivered cloud-native applications to production.



83% of respondents **have at least several internally developed cloud-native applications that have been pushed to production.**

Back to Contents

Using more containers in production

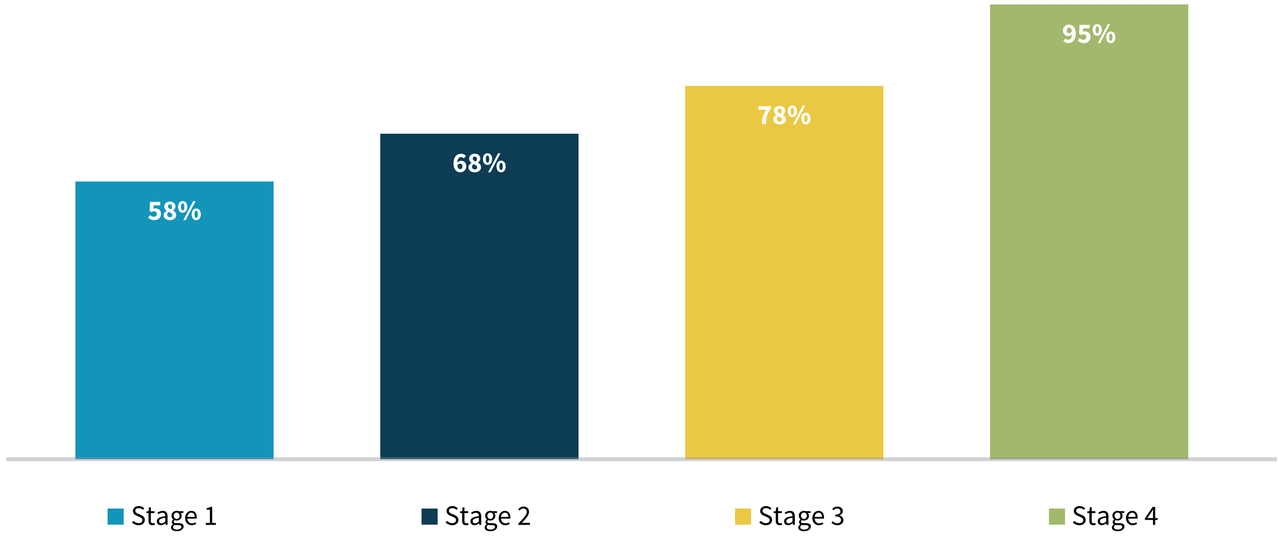
Containerized applications in production are the norm, with widespread usage across all security program stages. There was a higher percentage of usage with each higher stage security program, with 95% of Stage 4 respondents saying they currently use containers for applications in production. Even for Stage 1 companies, container use in production is high at 58%.

70%

of respondents are using containers for production applications.

> **“There was a higher percentage of usage with each higher stage security program.”**

Containerized applications in production.



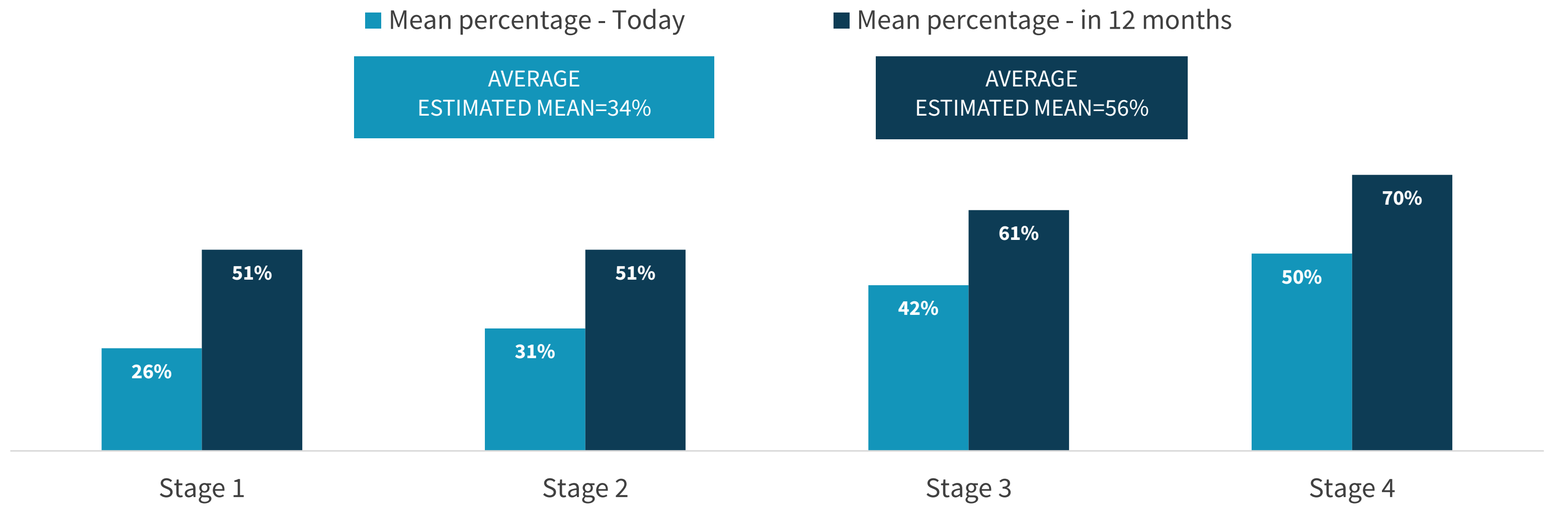
Back to Contents

Growing cloud-native footprints

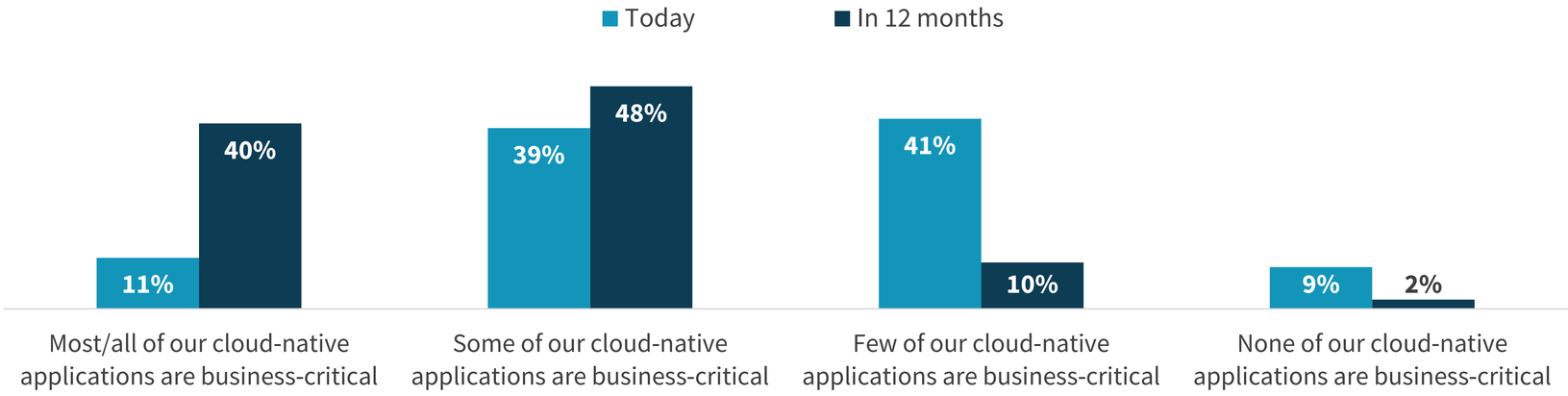
Organizations are expanding their cloud-native footprints over the next 12 months. According to our average survey participant, just over one-third of their internally developed business applications are cloud-native implementations. When asked of our Stage 4 respondents, that number jumps to 50% today. In 12 months, leading organizations report that figure climbing to 70%.

Organizations are also increasingly comfortable putting their critical applications into the cloud, planning to quadruple the number of cloud-native business-critical applications over the next 12 months.

Internally developed business applications that are cloud-native implementations.



Organizations are increasingly running business-critical applications in the cloud.



Back to Contents

Business criticality necessitates stronger security programs

There is a direct correlation between organizations with more cloud-native business-critical applications and higher stage security programs.

Today, 31% of leading organizations say that most/all of their cloud-native applications are business critical. That figure jumps to 77% for the next 12 months. Lagging organizations will have an even larger transformation on a relative scale, jumping from only 6% to having 25% of their business-critical applications in the cloud.

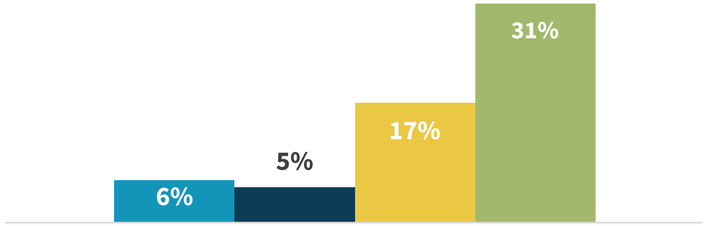
31%

of leading organizations say that most/all of their cloud-native applications are business critical.

Organizations with more advanced security programs have more business-critical applications in the cloud.

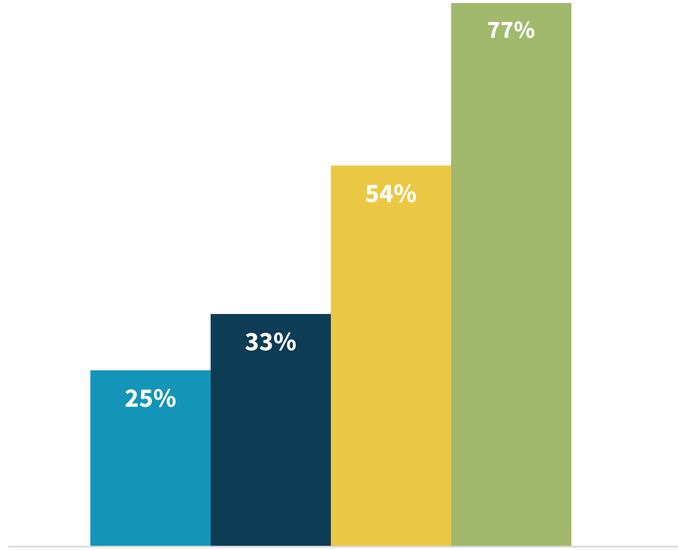
Stage 1 Stage 2 Stage 3 Stage 4

STAGE 4 ORGS HAVE 5.2X MORE CLOUD NATIVE BUSINESS CRITICAL APPS TODAY.



Most/all of our cloud-native applications are business-critical - today

STAGE 4 ORGS WILL HAVE 3.1X MORE CLOUD NATIVE BUSINESS CRITICAL APPS IN 12 MONTHS.



Most/all of our cloud-native applications are business-critical - in 12 months

Back to Contents

Improved Security Results with Higher Stage Security Programs

Leading organizations better utilize people, processes, and technology, resulting in favorable security outcomes.

Higher stage organizations struggle less with skills gaps

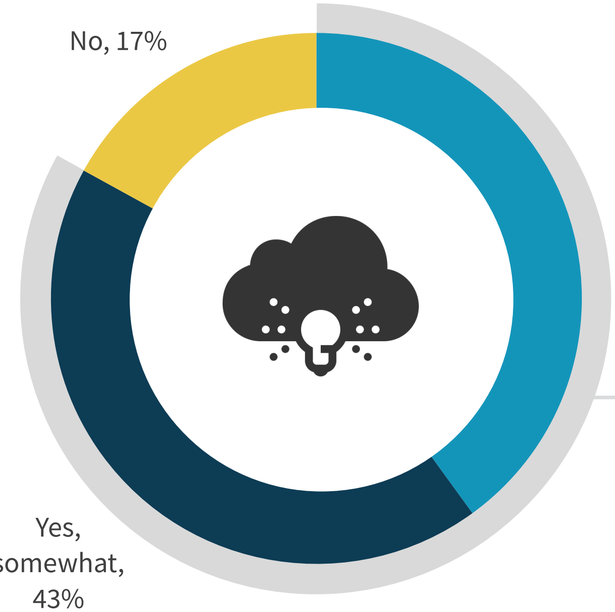
While skills gaps are common across all organizations, the higher stage organizations most frequently said they were not affected by the skills gap. Mature organizations are **47% less likely** to be struggling with cloud security skills within their cybersecurity teams.

Mature organizations are

47% less likely

to be struggling with cloud security skills within their cybersecurity teams.

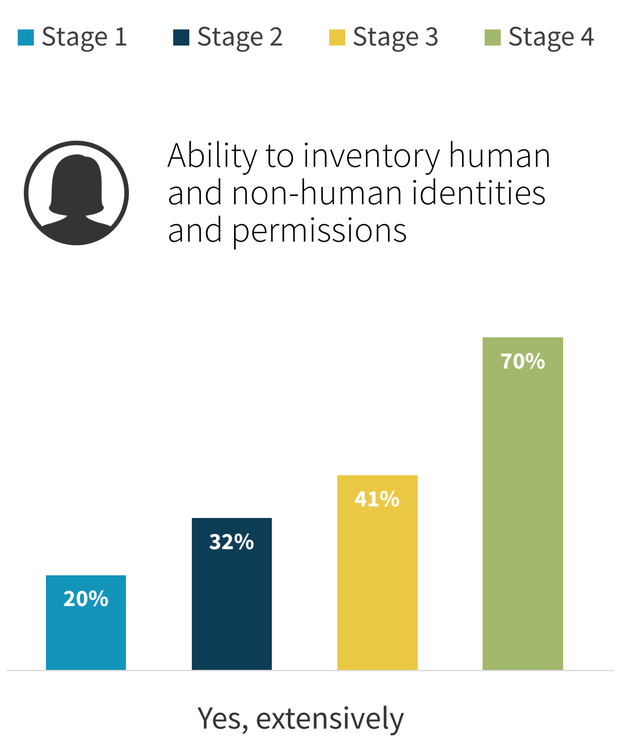
Higher stage companies were less affected by the cloud security skills gap.

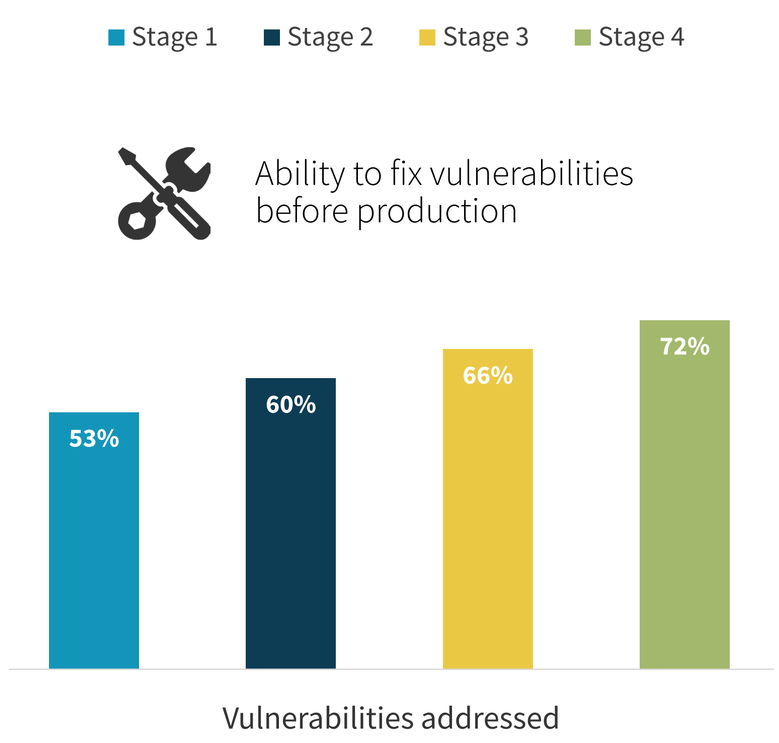


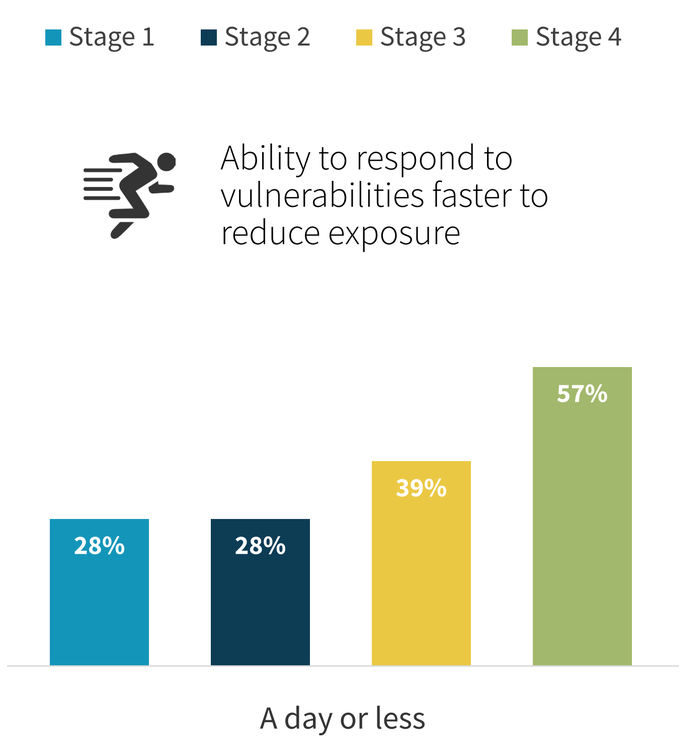
83% of respondents **say that they have at least somewhat been impacted by cloud security skills shortages.**

Back to Contents

Establishing security processes that reduce risk







Back to Contents

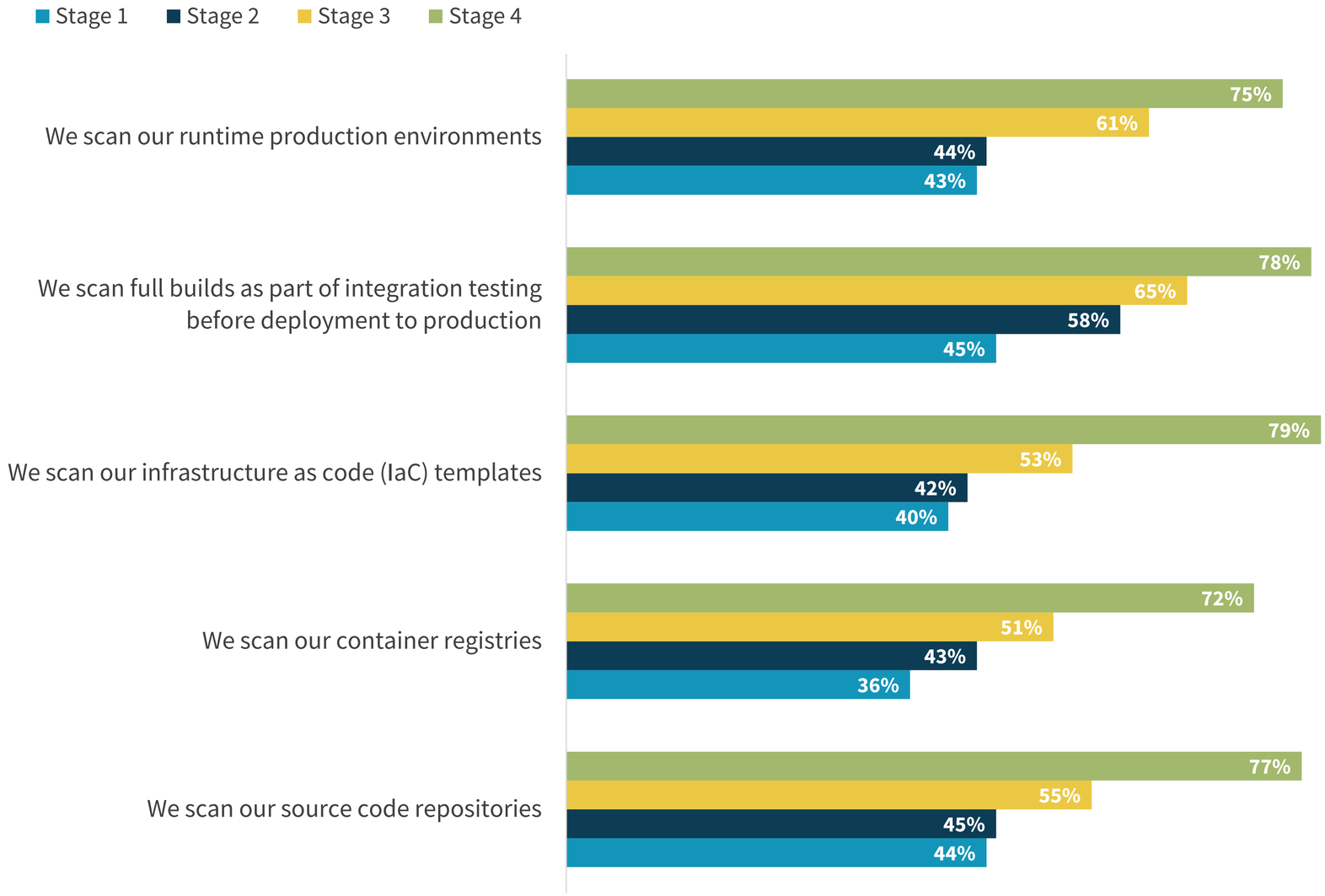
Vulnerability scans by development stage – higher stage organizations cover more ground

According to the respondents deemed more mature by our model, 75% or more of the respondents code at every stage mentioned across the software development lifecycle (SDLC).

75%

or more of the respondents deemed mature by our model scan code at every stage mentioned across the software development lifecycle (SDLC).

Vulnerability scans by development stage – higher stage organizations cover more ground.

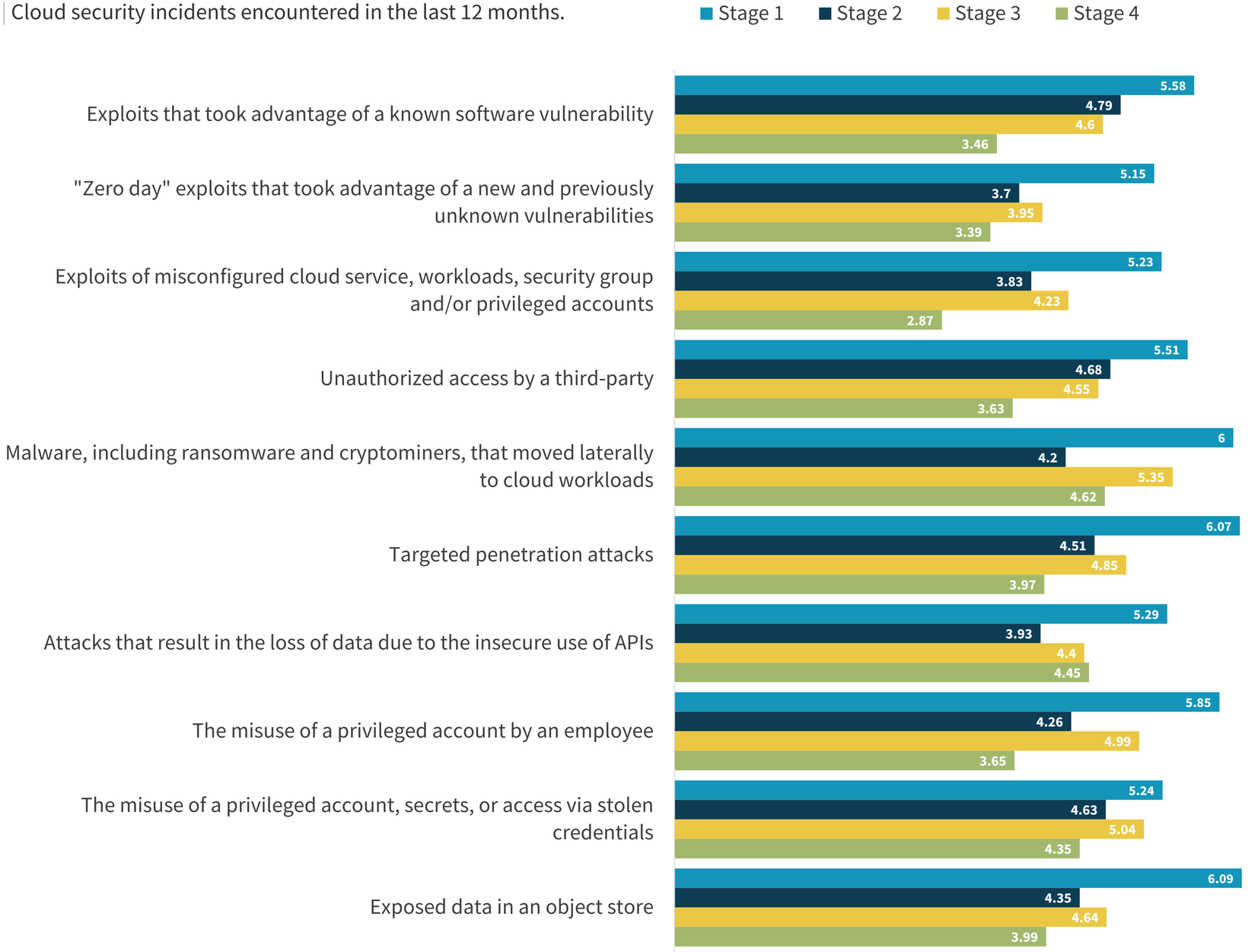


Back to Contents

More advanced security programs help organizations encounter fewer security incidents

With better security processes in place, organizations with more mature security programs encountered fewer security incidents over the past 12 months. In fact, the Stage 1 organizations suffered 31% more cloud-native application security incidents even though the Stage 4 organizations have **3.7x more cloud-native applications in production.**

Cloud security incidents encountered in the last 12 months.



Back to Contents

Higher stage organizations work with development for fast remediation

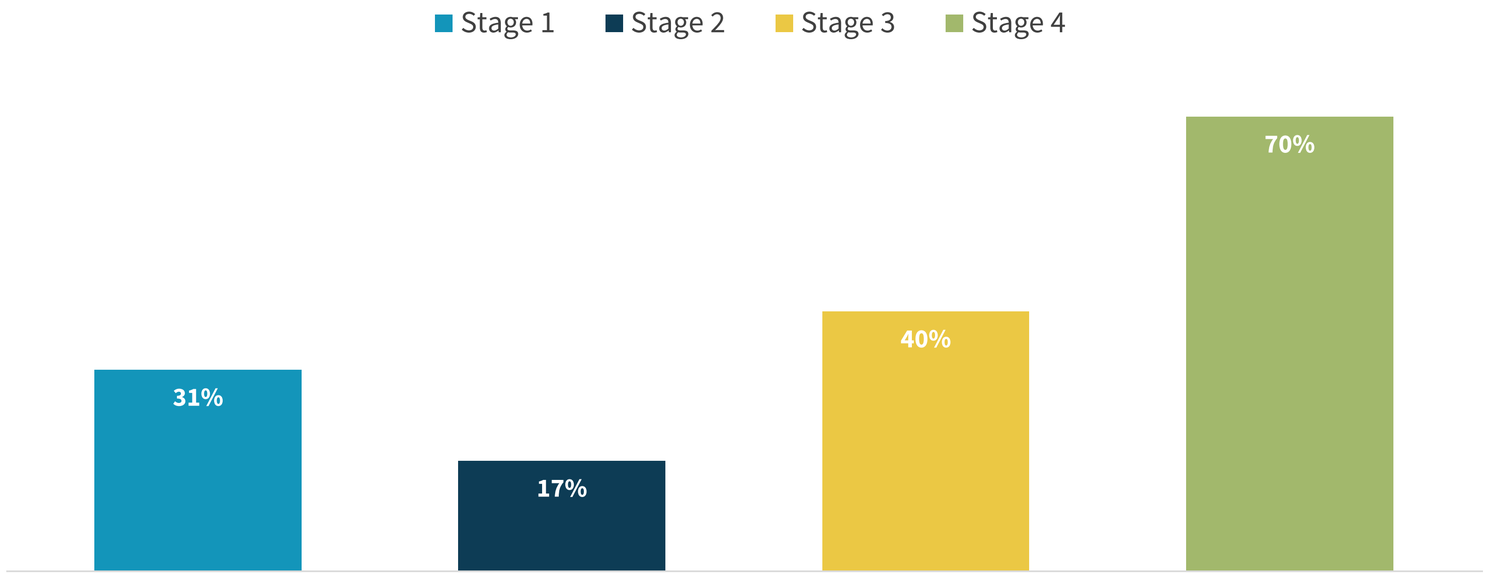
Developers at mature organizations see security as a value prop worth promoting. The marriage of these principles is an understood bonus among the most advanced cloud-native security practices because it helps developers efficiently remediate security flaws.

Mature organizations are

1.8x more likely

to rate their development organizations as excellent for the speed of incident response and resolution.

Recognizing the value of better security.



Back to Contents

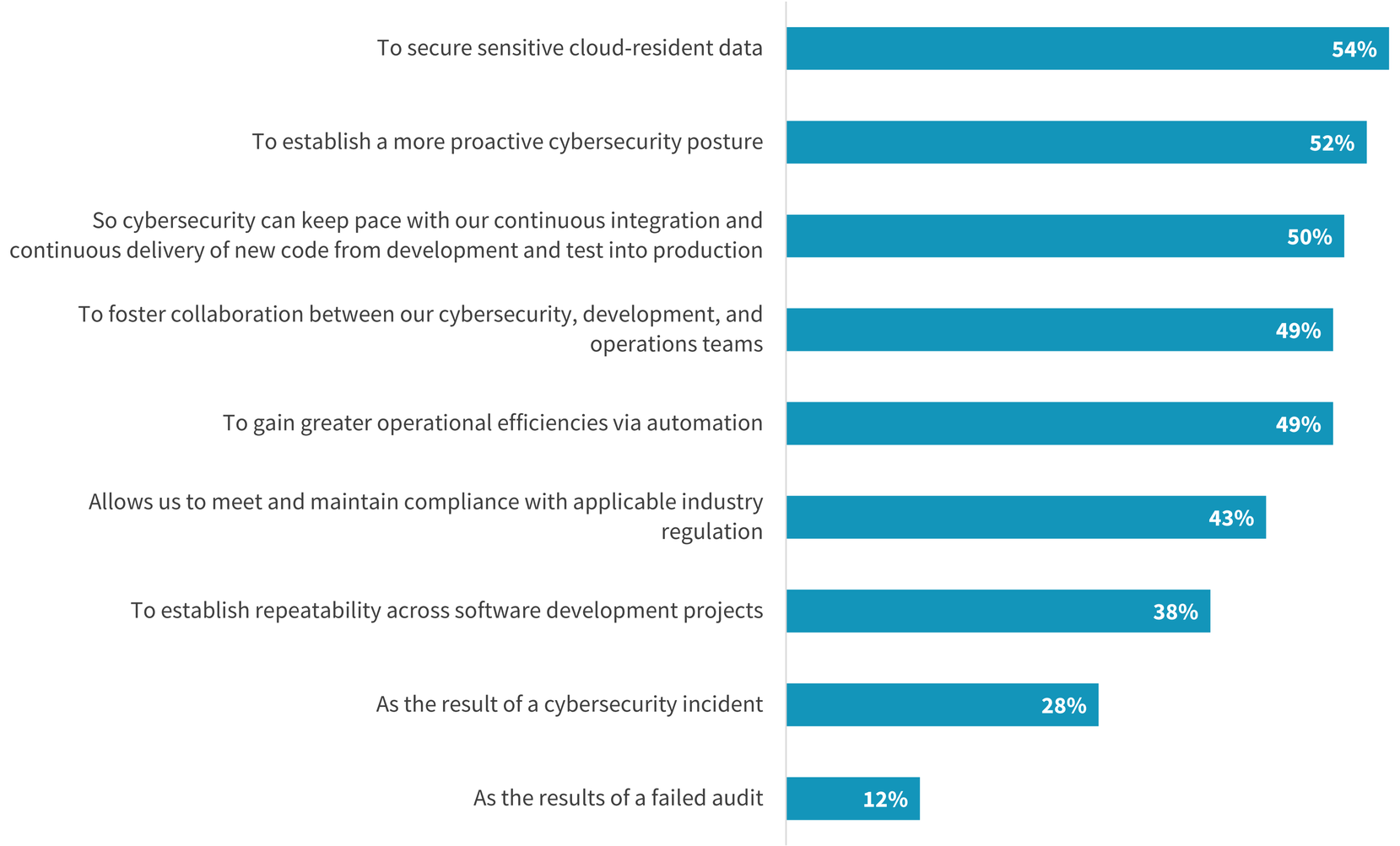
Enhancing Developer Effectiveness

In addition to helping developers address security issues, security program maturity contributes to greater efficiency across the software development lifecycle.

DevSecOps implementation drivers: incorporating security into rapid development cycles

Developers are motivated to incorporate security in ways that can scale with rapid development. Key drivers, including securing sensitive cloud-resident data (54%), establishing a proactive cybersecurity posture (52%), and keeping pace with CI/CD development (50%), were cited by respondents as reasons for incorporating security into the DevOps process.

DevSecOps implementation drivers.



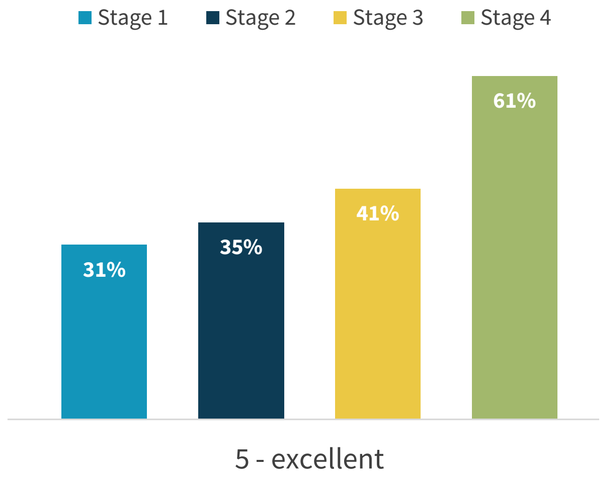
Back to Contents

Higher stage organizations are delivering on-time, secure releases

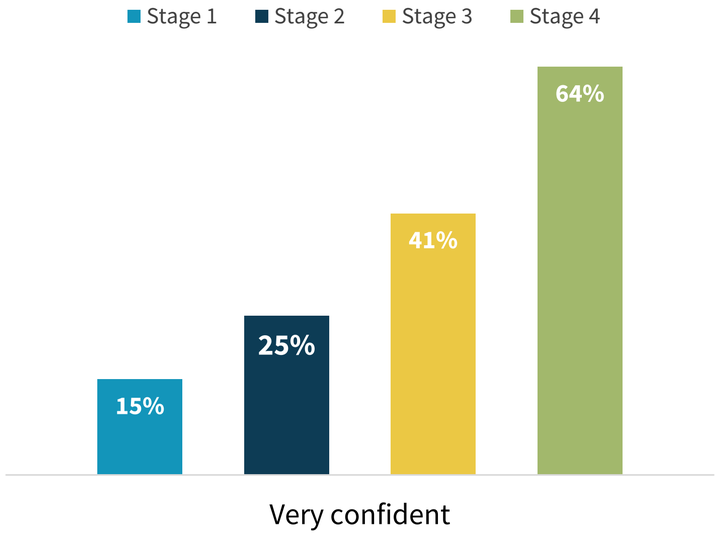
When asked to rate their own development teams, mature organizations had more positive things to say about their development team's speed of delivery. Mature organizations were **nearly 2x more likely** to say their development team's speed of delivery is excellent.

Mature orgs are 4.3x more likely to be very confident than Stage 1 orgs that their development team will be able to ship secure code at the pace required over the next 12 months.

Development team's speed of delivery.



Confidence that development team will ship secure code at the pace required over the next 12 months.



Facilitating better development results

Higher stage organizations reported better results across key development metrics compared to lower stage organizations.

Stage 4 organizations were 2.1x more likely to say the functionality of their code was excellent compared to their lagging Stage 1 counterparts.

Stage 4 organizations were 2.6x more likely to push new code to production environments multiple times a day.

Stage 4 organizations were 1.9x more likely to say the reliability of their code is excellent compared to Stage 1 organizations.

Back to Contents

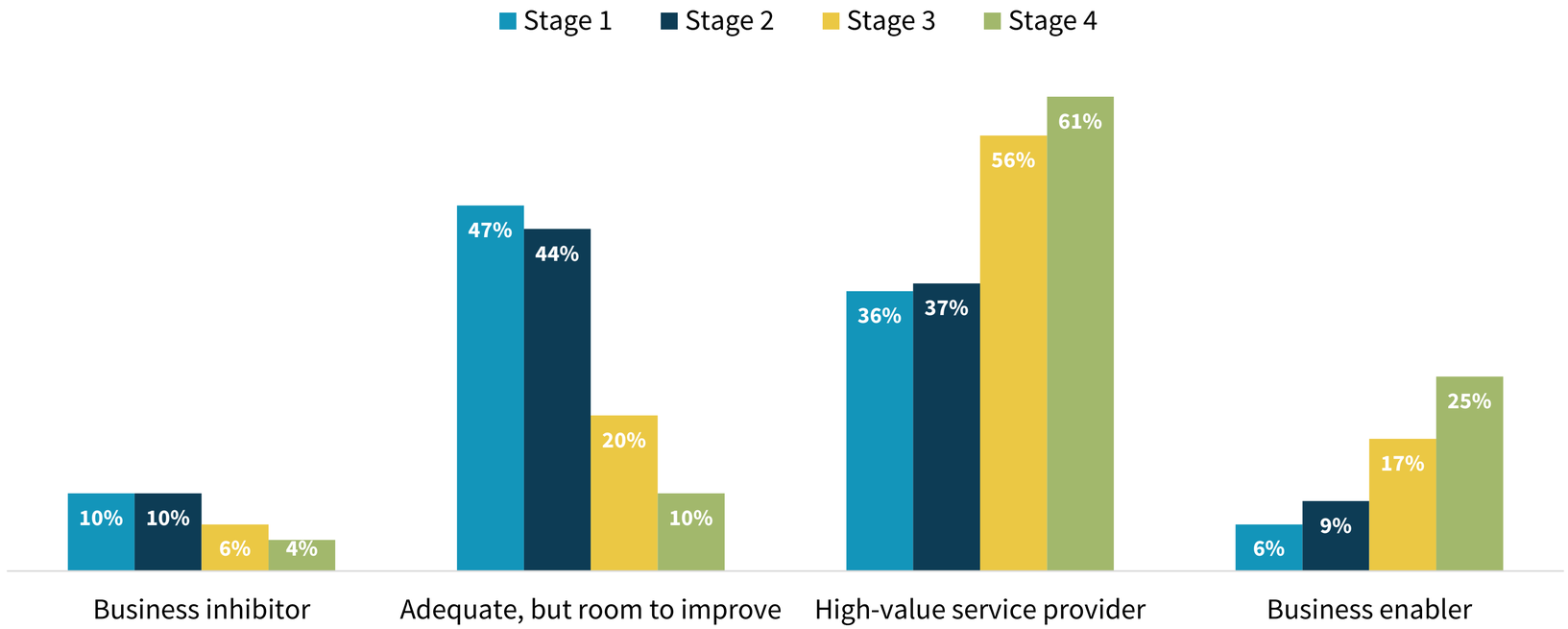
Stage 4 organizations have developers that value the security team

Leading organization are

4.2x more likely

to have development teams that see their security teams as business enablers.

How development views security.

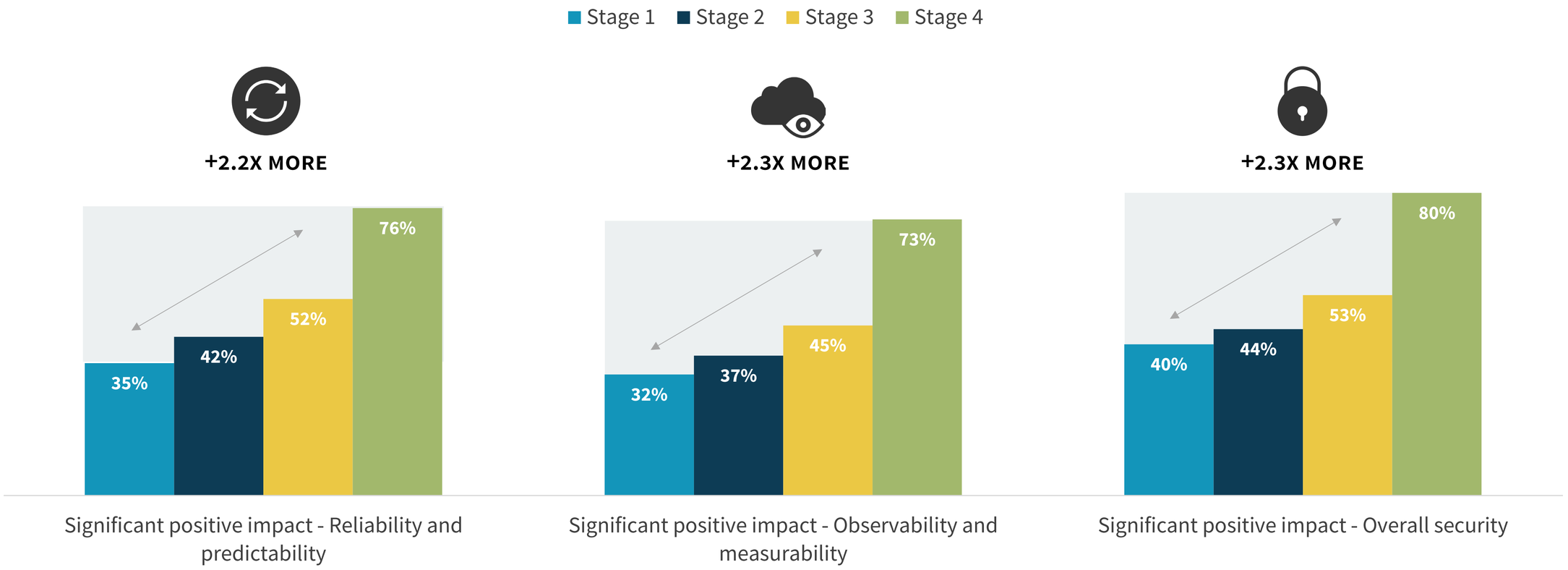


Back to Contents

Mature security programs correlate with operational excellence

When security is incorporated into development processes, it drives efficiency across the software development lifecycle because the developers can work more efficiently within their workflows to deliver higher-quality code instead of wasting time fixing security issues out of band. According to our model, mature respondents are at least **2x more likely** to say that securing internally developed cloud-native applications has had a significant positive impact on key elements of their application and infrastructure security.

How the security approach has impacted applications and infrastructure over the past 12 months.



Significant positive impact - Reliability and predictability

Significant positive impact - Observability and measurability

Significant positive impact - Overall security

Back to Contents

Driving Business Outcomes

Business success today depends on leveraging technology to efficiently deliver products and services. Because security is essential to protecting valuable company and customer data, stronger security programs contribute to better business outcomes.

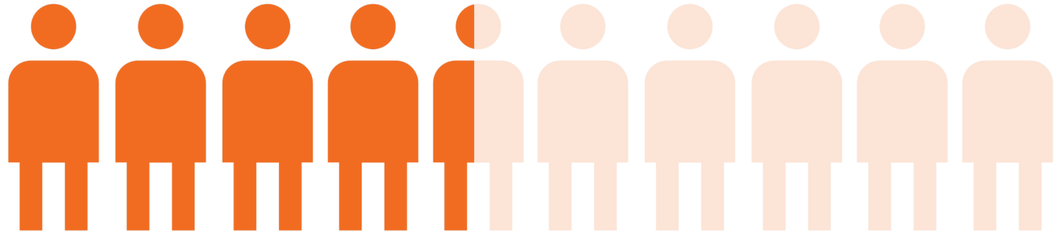
The importance of security in enabling technology adoption

In today's online economy, businesses recognize the importance of technology, whether it's in establishing their online presence, collecting payments, or delivering services. It is no surprise that a majority of respondents across industries consider themselves technology companies.

88%

of respondents consider themselves technology companies.

Organizations typically see security as either a barrier or an enabler to technology adoption because of the need to protect company data and meet industry regulations. So, it is also no surprise that Stage 4 organizations are 45% more likely to see themselves as technology companies. Their ability to manage security and risk is crucial to business success.



Stage 4 organizations are

45% more likely

to see themselves as technology companies.

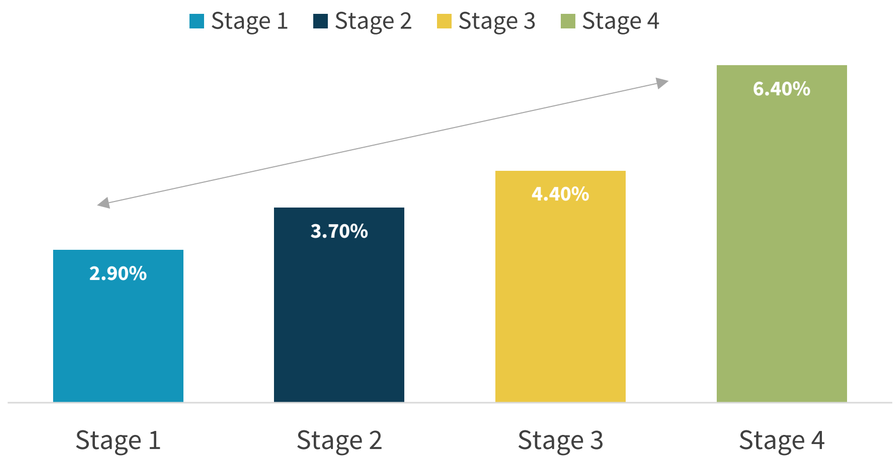
Back to Contents

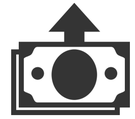
Cloud-native security stage translates to higher revenue

Stage 4 respondents also report better performance relative to their revenue goal than their Stage 1 counterparts. On average, Stage 4 organizations exceed their revenue goal at a rate 55% higher than Stage 1 organizations, which highlights a tangible benefit to cloud-native security practices.

Stage 4 organizations are also 3.8x more likely to say their company is in a very strong position to compete and perform over the next few years than the Stage 1 organizations.

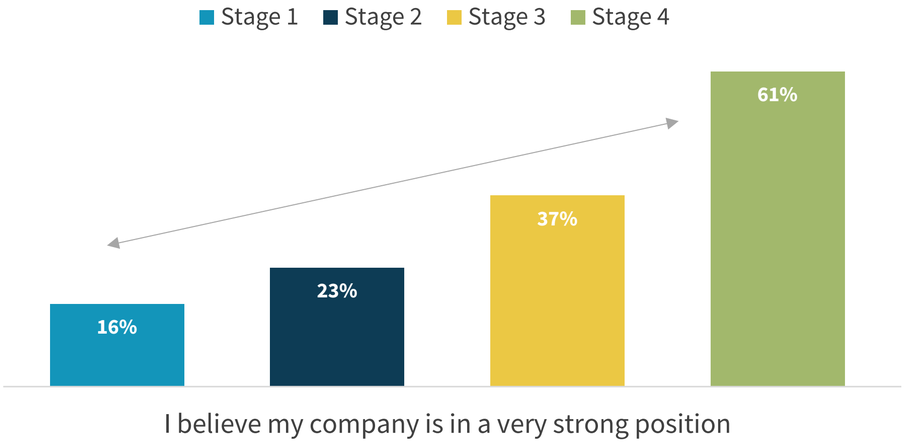
Organizations exceeding their revenue goals.





STAGE 4 ORGANIZATIONS EXCEED THEIR REVENUE GOAL **AT A RATE 55% HIGHER THAN STAGE 1 ORGANIZATIONS.**

Organizations in a strong position to compete and perform over the next few years.



STAGE 4 ORGANIZATIONS ARE ALSO 3.8X MORE LIKELY TO SAY THEIR COMPANY IS IN A VERY STRONG POSITION TO COMPETE AND PERFORM OVER THE NEXT FEW YEARS THAN THE STAGE 1 ORGANIZATIONS.

Back to Contents

PRISMA™
BY PALO ALTO NETWORKS

Prisma Cloud is the industry's most comprehensive Cloud Native Application Protection Platform (CNAPP) with the broadest security and compliance coverage – for applications, data, and the entire cloud native technology stack – throughout the development lifecycle and across multi- and hybrid-cloud environments. Our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate secure cloud native application development.

Explore our Prisma Cloud Security Boot Camp and get hands on with cloud native architecture and cloud security. Learn the processes, tools and roles you need to successfully adopt DevSecOps.

LEARN MORE

ABOUT ESG

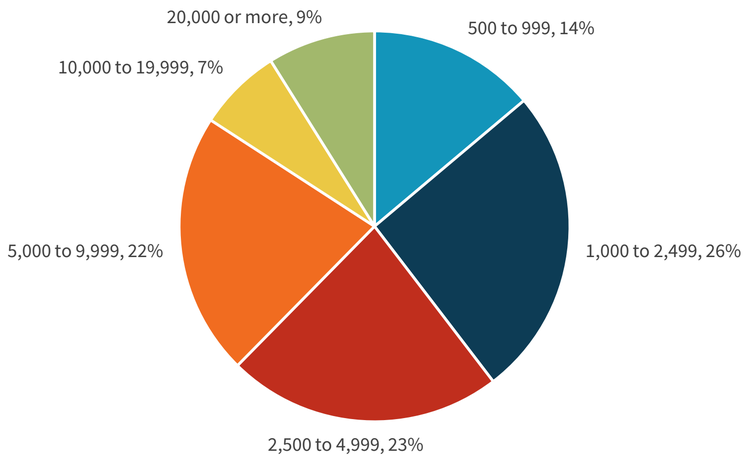
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

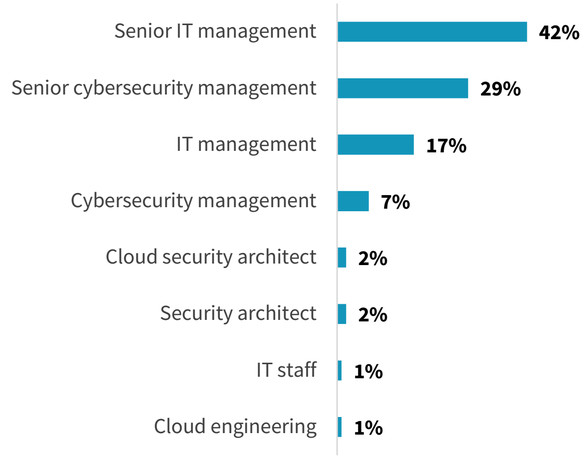
To gather data for this report, ESG conducted a comprehensive online survey of 1,000 IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada; 50% of respondents), Western Europe (UK, France, and Germany; 26% of respondents), and the Asia-Pacific region (Australia, New Zealand, Japan, Hong Kong, and Singapore; 25% of respondents) between November 3rd, 2021 and November 26th, 2021. To qualify for this survey, respondents were required to be personally responsible for the policies, processes, or technical safeguards in place to secure their organization's internally-developed applications. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

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 1,000 IT and cybersecurity professionals.

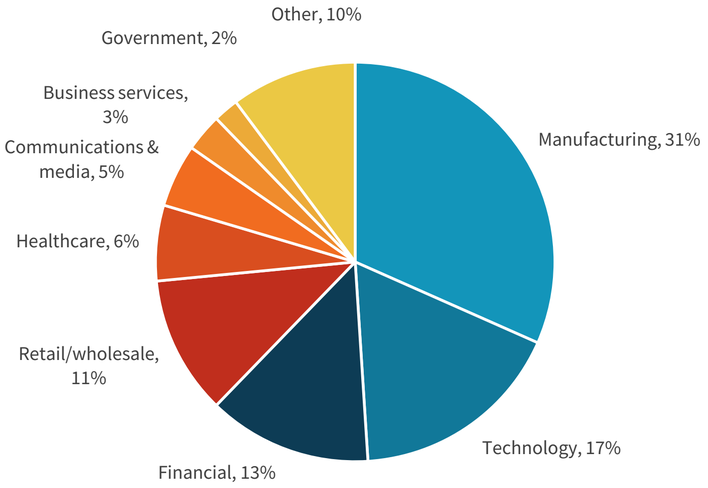
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY TITLE



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.