OpsCompass

2021 STATE OF CLOUD SECURITY POSTURE MANAGEMENT REPORT

TABLE OF
CONTENTS

INTRODUCTION

Cloud infrastructure is growing quickly, and organizations need to keep up.

With multiple assets in multi-cloud environments, multiple pipelines deploying into the cloud, and multiple entities accessing cloud resources, organizations can't let things like comprehensive visibility, asset inventory, and security get out of hand. They need to have a plan for how to manage it all.

Cloud Security Posture Management (CSPM) solutions make it easier for organizations to monitor the state of their cloud environment, and make sure they're staying proactive about cloud governance and policies.

But are developers, engineers, and ops teams actually using the tools at hand to keep themselves secure? Additionally, what challenges or issues are they still seeing that are threatening their security? Are they missing potential threats that could cause massive breaches, simply because they're not looking in the right places?

We wanted more insight into current cloud infrastructure management, so we sought out those who manage cloud infrastructure to better understand what they're seeing, what they're concerned about, and what they want improved.

METHODOLOGY:

On January 27 through February 8, 2021, we surveyed 253 full-time, US-based, IT professionals who deploy, develop, and/or manage cloud applications or infrastructure.

KEY FINDINGS

Here's what we found about their cloud environment:

38%

38% want to adopt CSPM solutions for the first time, and 29% want to switch CSPMs. They're looking for better visibility, better incident response management, and better compliance assessment in their CSPM solution.

They're most worried about configuration errors, malicious insiders and compromised accounts. They fear a breach will come from malicious software or malicious actors, as opposed to human error.

68%

68% are highly confident in their security posture, and 29% are somewhat confident. Throughout, we found a high confidence in security, visibility, and compliance — but that incidents were still occurring.

Identity and security baseline management is a challenge. They're also concerned about data loss or leakage, and misconfigurations or configuration drift.

55%

55% have seen a cloud-related breach at their organization. Additionally, over one-third reported that they wouldn't be surprised if they saw a breach had occurred.

Priorities for 2021? Better real-time monitoring. They also want to be more proactive about their security posture and increase automation.

86%

The positive perception of CSPM has grown. 86% report having grown more favorable about CSPM, and many are hearing about it more from colleagues and influencers.

PART 1:

PROFILE OF WHO WE SURVEYED

For our survey, we interviewed 253 full-time US employees working in IT, with 92.1% in Services and Data and 7.9% in other areas. 74.7% work in companies with 1001 to 5000 employees, and 25.3% work in companies with over 5000 employees. All respondents consider themselves "very involved in the cloud operations of my organization."

The majority — 63.6% — are between the ages of 35 and 44, with 11.9% being younger, and 24.5% being older. 72.7% are male, and 27.3% are female.

They're involved in developing and implementing policy and best practices.

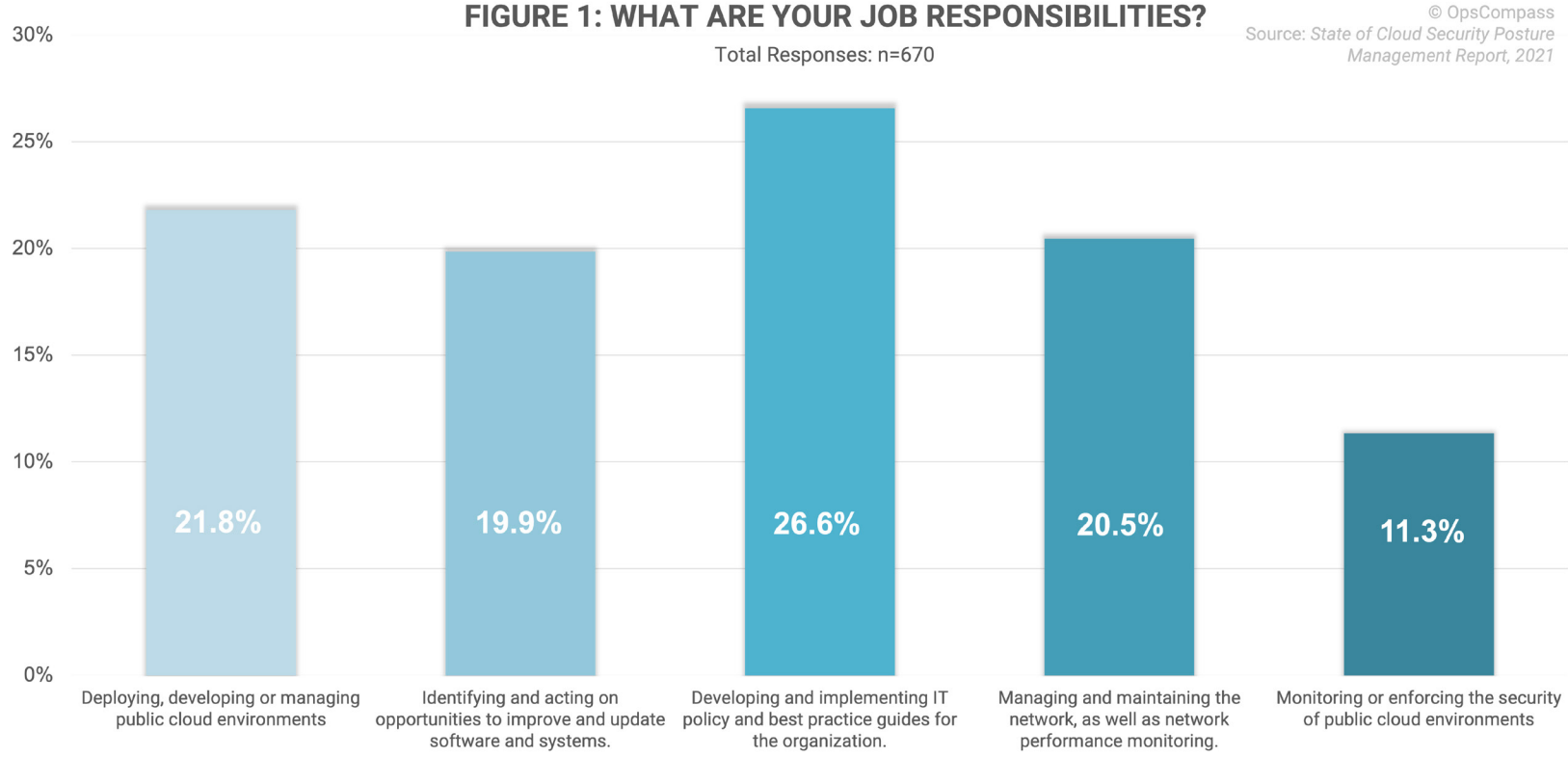
First, we wanted to know a little bit more about the job responsibilities of our respondents, knowing already that they're involved in cloud operations. We also asked for respondents to choose all that applied, so many have multiple responsibilities.

70.4% are responsible for "developing and implementing IT policy and best practice guides," the largest response. 57.7% are responsible for "deploying, developing, or managing public cloud environments." 54.2% are responsible for "managing and maintaining the network, as well as network performance monitoring." 52.6% have a hand in "identifying and acting on opportunities to improve and update software and systems." Finally, 30% help with "monitoring or enforcing the security of public cloud environments."

FIGURE 1: WHAT ARE YOUR JOB RESPONSIBILITIES?

Total Responses: n=670

Source: *State of Cloud Security Posture Management Report, 2021*



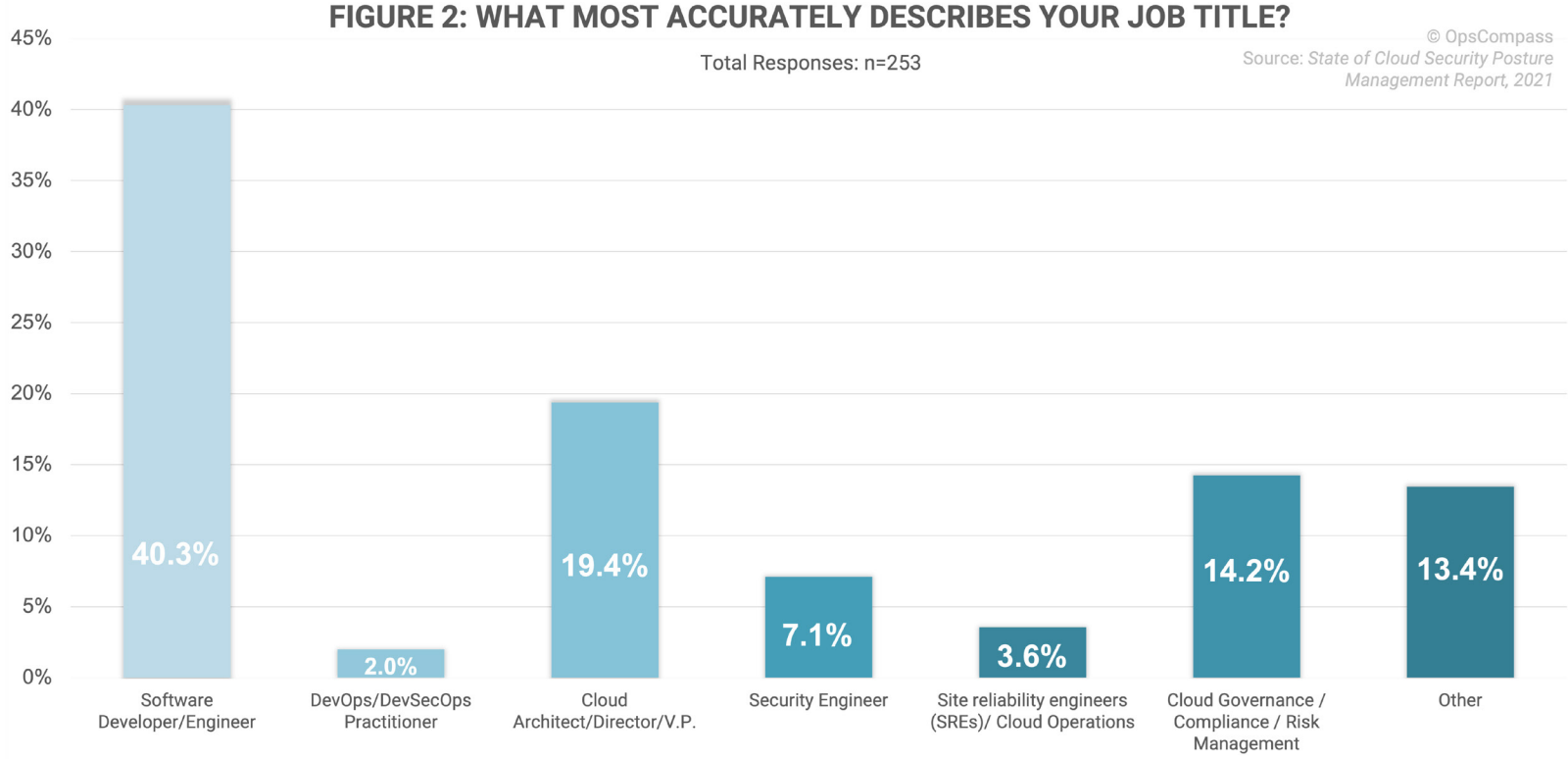
They're mostly Software Developers or Engineers.

Next, we were curious about their job title. The largest segment at 40.3% are Software Developers or Engineers. 19.4% are Cloud Architects, Directors, or VPs, and 14.2% are in Cloud Governance, Compliance, and Risk Management. A small number identified as Security Engineers (7.1%), Site Reliability Engineers or in Cloud Operations (3.6%), or as DevOps or DevOps Practitioners (2%). The 13.4% that replied "Other" mostly include Senior, MIS, IT, or Product Managers.

FIGURE 2: WHAT MOST ACCURATELY DESCRIBES YOUR JOB TITLE?

Source: *State of Cloud Security Posture Management Report, 2021*

Total Responses: n=253



Summary:

The population surveyed here has their hand in managing the cloud at their workplaces, yet they're involved in different ways. Most are involved in developing and implementing policies, and some are involved in deployments, network management, helping to improve software and systems, or monitoring security. Their jobs have different focuses as well, whether it be developing or designing for the cloud, overseeing compliance and risk, or monitoring security. Their various roles and responsibilities could affect their outlook on their security posture.

PART 2:

STATE OF CLOUD INFRASTRUCTURE

Our respondents are actively managing their cloud infrastructure, so we wanted to know what kind of cloud environment they were managing. Additionally, since they work so closely with their organizations' cloud environments, we wanted to know whether they had confidence in their cloud security, if they've ever suffered a breach, and what they're most concerned about on a daily basis.

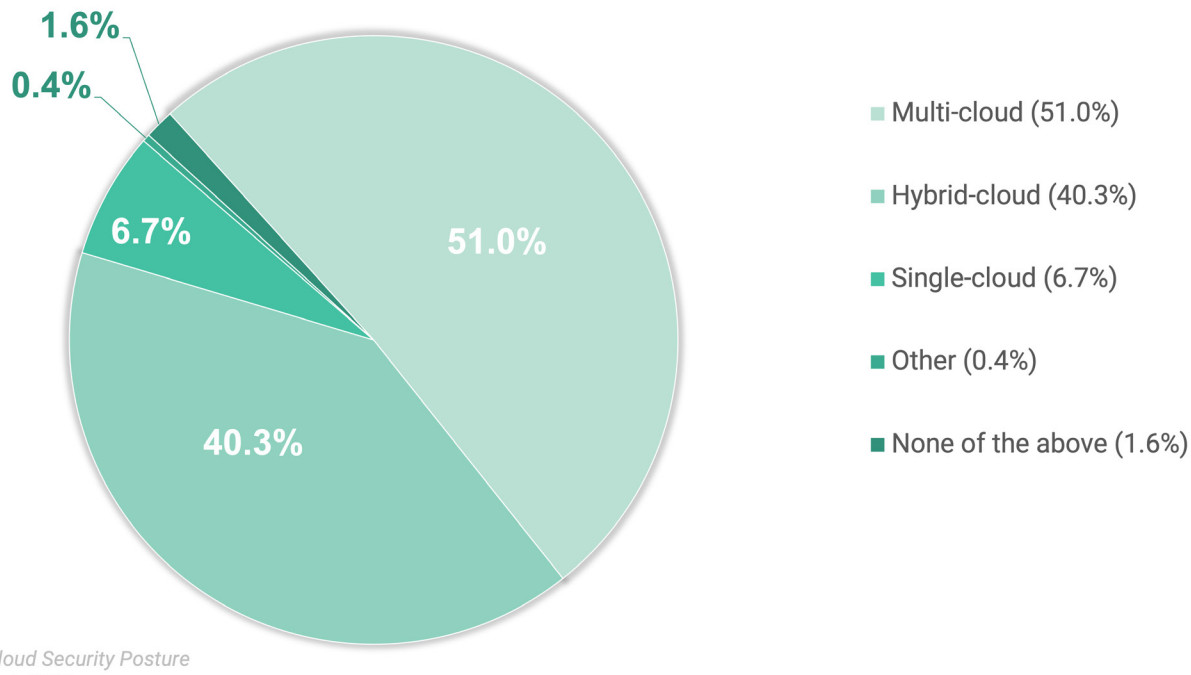
Multi- or hybrid-cloud environments are the standard.

91.3% of our respondents are in organizations that are handling different types of cloud environments simultaneously: 51% are working with a multi-cloud environment, and 40.3% have a hybrid-cloud environment in their organization. This means that the majority of organizations need security solutions to manage multiple environments, both public and private.

Only 6.7% are working with a single-cloud environment, at this point. 2% responded either "none of the above" or "other."

FIGURE 3: WHICH MOST ACCURATELY DESCRIBES YOUR CURRENT CLOUD ENVIRONMENT?

Total Responses: n=253



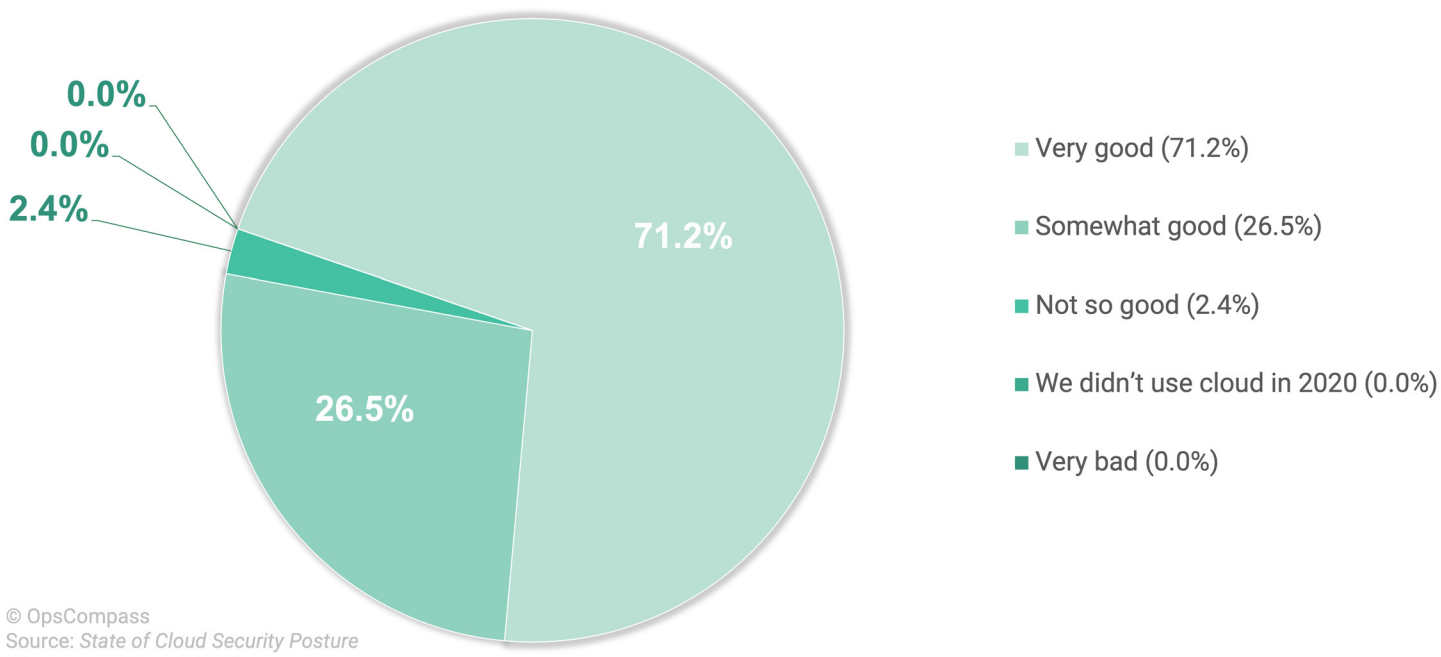
© OpsCompass
Source: *State of Cloud Security Posture Management Report, 2021*

71% felt their cloud adoption was very good.

In the past year, how did our respondents feel their organization performed in their cloud adoption? Nearly three-quarters (71.1%) felt their cloud adoption was very good, with 26.5% seeing it as somewhat good. Only 2.4% felt their cloud adoption was lacking.

FIGURE 4: OVERALL, HOW WAS YOUR ORGANIZATION'S CLOUD ADOPTION DURING 2020?

Total Responses: n=253



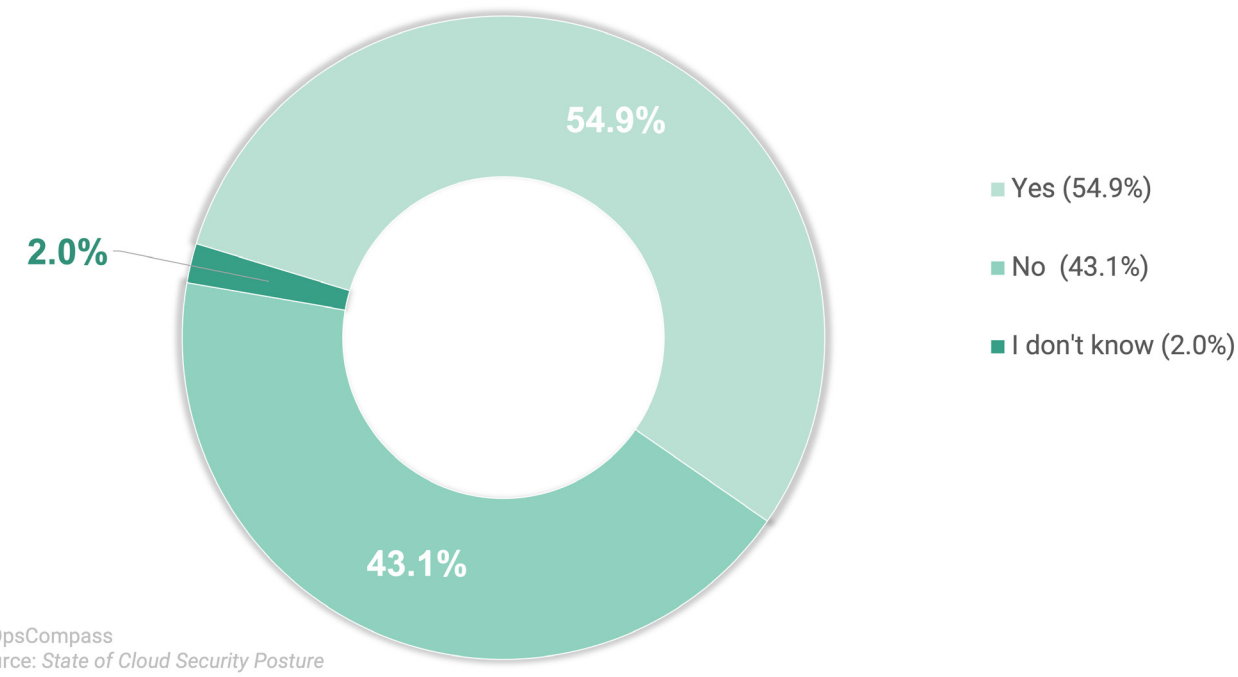
Source: *State of Cloud Security Posture Management Report, 2021*

55% have seen a cloud-related breach at their organization.

In their time working with cloud environments, had our respondents seen their organization have a cloud-related breach? 43.1% hadn't seen a cloud-related breach or issue. But over half had, with 55% saying they're organization had been breached — meaning there's something lacking in their security awareness or implementation, despite their confidence in their adoption.

FIGURE 5: HAVE YOU SUFFERED A CLOUD-RELATED BREACH BEFORE?

Total Responses: n=253



Source: *State of Cloud Security Posture Management Report, 2021*

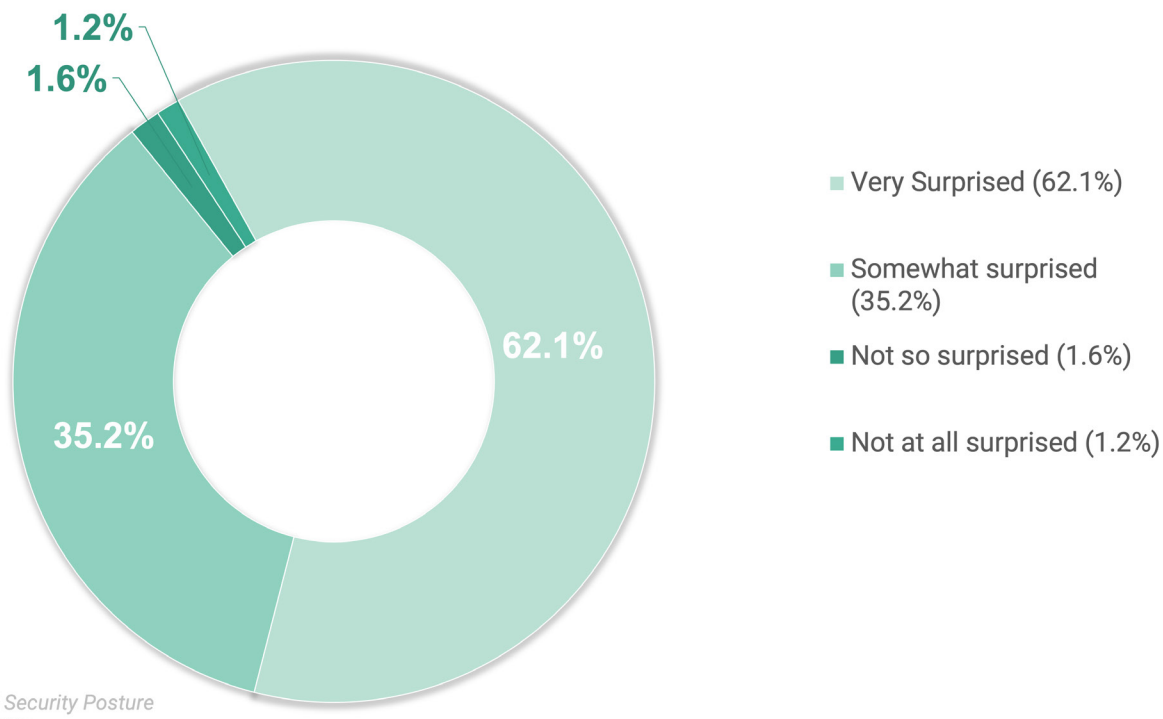
35% would only be somewhat surprised if their company made the news for a breach.

We wanted to know if our respondents would be surprised if their organization made the news for a cloud-related breach, considering they know the most about their organization's security practices. 62.1% said they'd be very surprised, meaning they believe they have enough insight into their cloud environments to know that a breach wouldn't happen. But 35.2% had some doubts, and replied that they would be somewhat surprised if their company made the news. In other words, they're confident to a certain extent in their cloud security, but not fully.

1.6% replied they'd not be so surprised, and 1.2% replied they wouldn't be surprised at all.

FIGURE 6: HOW SURPRISED WOULD YOU BE IF YOU SAW YOUR COMPANY ON THE NEWS WITH A CLOUD-RELATED BREACH?

Total Responses: n=253



Source: *State of Cloud Security Posture Management Report, 2021*

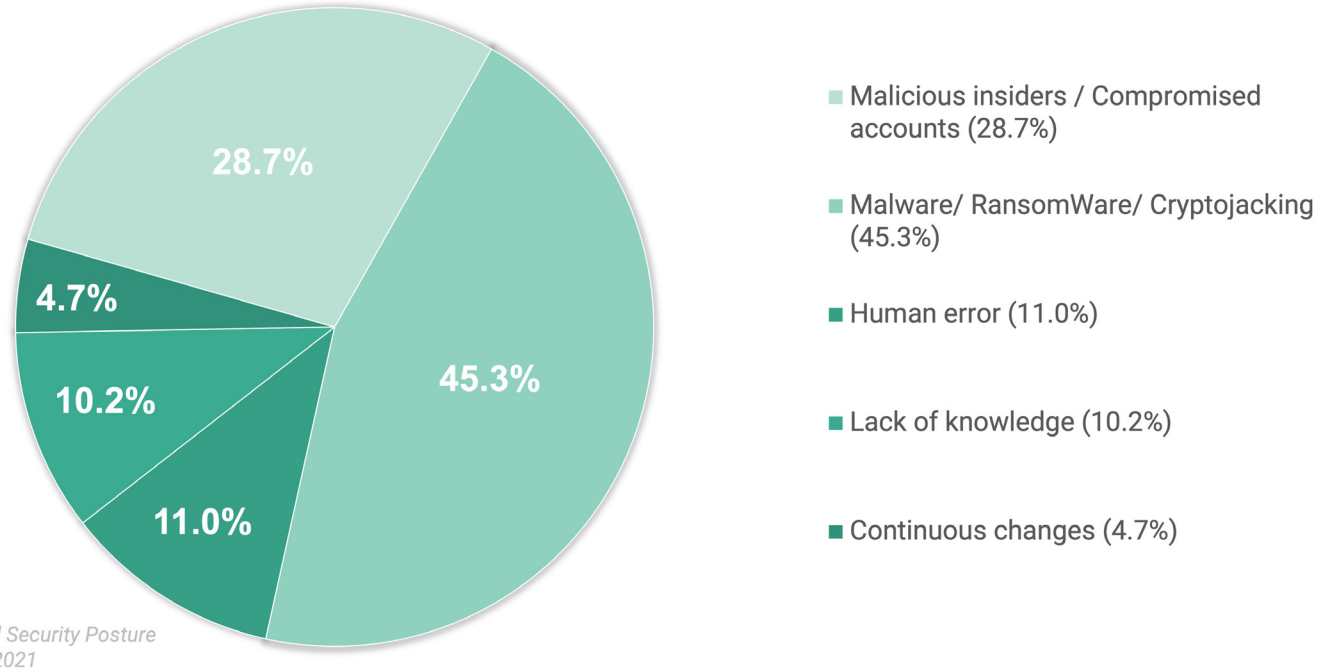
They're most worried about configuration errors, malicious insiders, and compromised accounts.

When it comes to a cloud-related breach that would put their company in the news, what kind of threat are they most worried about? The majority (54.6%) are worried about configuration errors, malicious insiders, and compromised accounts.

This includes human error creating an issue, a lack of knowledge about the cloud environment and it's configurations, continuous changes creating unnoticed gaps, and deliberate attacks from outside entities.

FIGURE 7: WHAT TYPE OF THREAT IS YOUR BIGGEST CONCERN TODAY WHEN IT COMES TO CLOUD SECURITY?

Total Responses: n=254



Source: *State of Cloud Security Posture Management Report, 2021*

Summary:

91% of our respondents are working with multi- or hybrid-cloud solutions — which will necessitate greater visibility and deeper awareness around how to implement an all-encompassing security posture. 71% felt their adoption was very good over the past year, yet many replied that it was somewhat good, meaning that there's room for improvement.

But while nearly three-quarters were confident in their adoption, only 43% haven't seen a breach or issue at their company. Additionally, over a third wouldn't be surprised if they saw their organization on the news for a cloud-related incident. This seems to imply overconfidence in their cloud security: We're doing a great job, but we still have problems.

What are they most worried about will cause that breach? Malware or ransomware, or malicious insiders and compromised accounts — deliberate outside attacks on their cloud.

PART 3:

CSPM AWARENESS

Keeping multi-cloud environments secure involves a robust approach to Cloud Security Posture Management (CSPM), which includes the governance, monitoring, and remediation necessary to ensure all assets in and deployments to the cloud are safe. Considering CSPM is a relatively new sector, what do our respondents know about it?

They're somewhat familiar with cloud security terms.

We wanted to know about our respondents' awareness when it comes to all the ways to protect their cloud environment, so we asked if they had heard of certain cloud security terms — and asked them to select all they had.

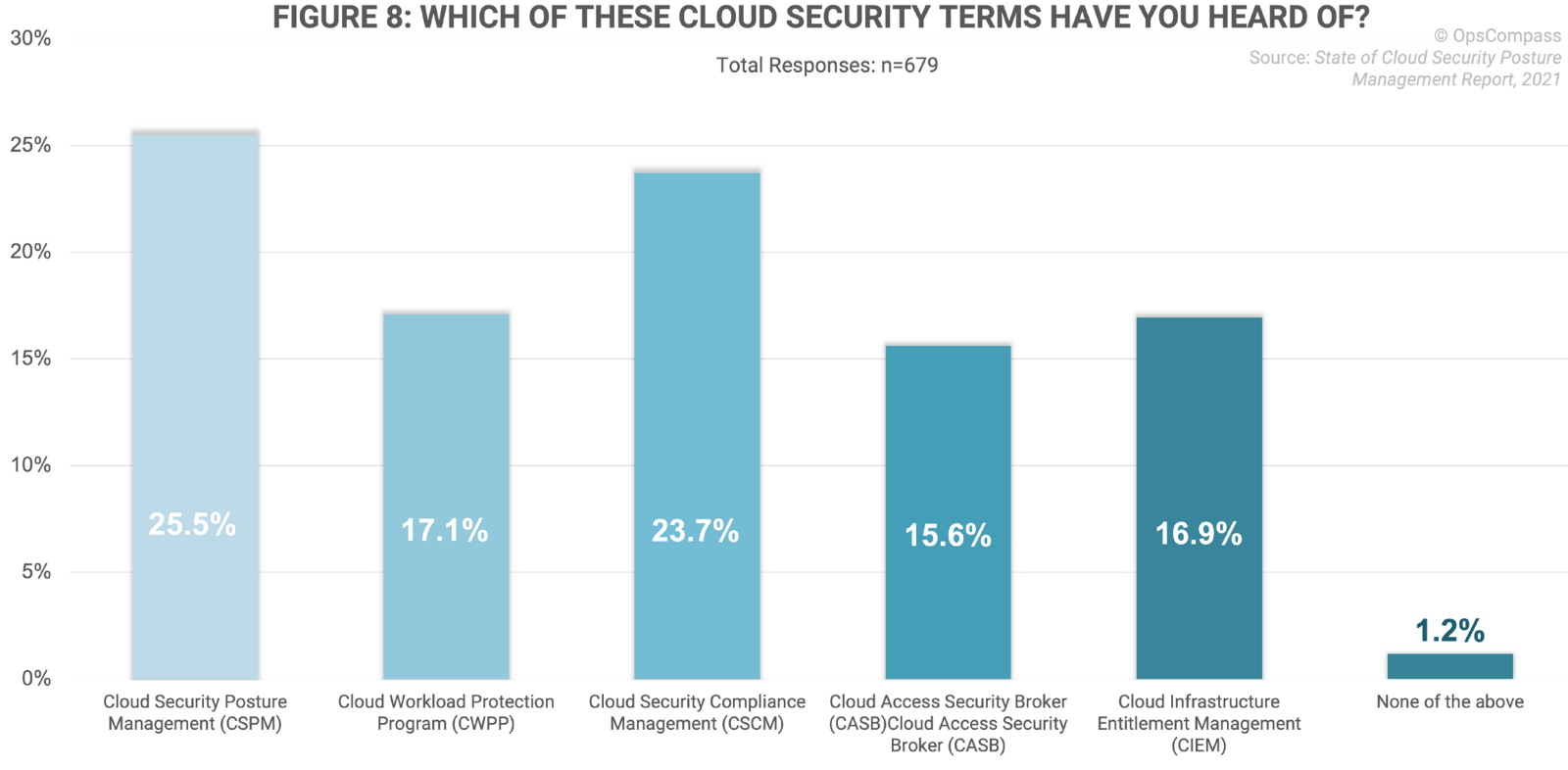
68.4% had heard the team "Cloud Security Posture Management (CSPM)," and 63.6% had heard of the term "Cloud Security Compliance Management (CSCM)."

Fewer were familiar with the terms "Cloud Workload Protection Platform (CWPP)" (45.9%), "Cloud Infrastructure Entitlement Management (CIEM)" (45.5%), and "Cloud Access Security Broker (CASB)" (41.9%). Only 3.2% report not having heard any of the terms.

FIGURE 8: WHICH OF THESE CLOUD SECURITY TERMS HAVE YOU HEARD OF?

Source: *State of Cloud Security Posture Management Report, 2021*

Total Responses: n=679



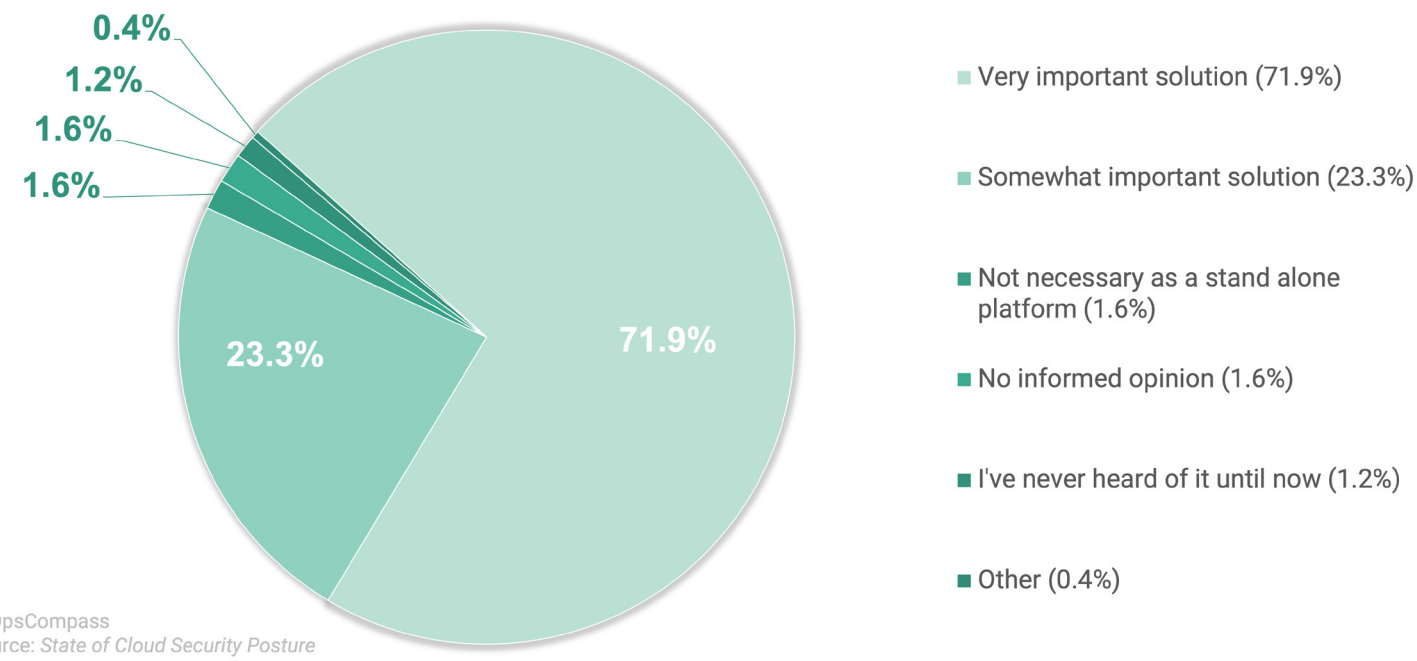
95% believe CSPM to be an important solution.

Next, with our respondents being cloud professionals, we wanted to know their thoughts about Cloud Security Posture Management (CSPM) overall. 71.9% called it a "very important solution," understanding not just what it is but what it can do. 23.3% called it a "somewhat important solution," meaning that 95.2% of respondents seem to be aware of its benefits.

Only 1.6% believed it's "not necessary as a standalone platform," 1.6% had no informed opinion, and 1.2% hadn't heard of it before the survey.

FIGURE 9: HOW WOULD YOU DESCRIBE YOUR OVERALL OPINION OF CLOUD SECURITY POSTURE MANAGEMENT (CSPM)?

Total Responses: n=253



Source: *State of Cloud Security Posture Management Report, 2021*

"Security," "protection," and "trustworthy" are associated with CSPM.

To make it a bit more personal and subjective, we asked our respondents what came to mind when they think of the term Cloud Security Posture Management?

Many replied with simply "security" as the first word they associated with CSPM. Some other words and phrases that came to mind were:

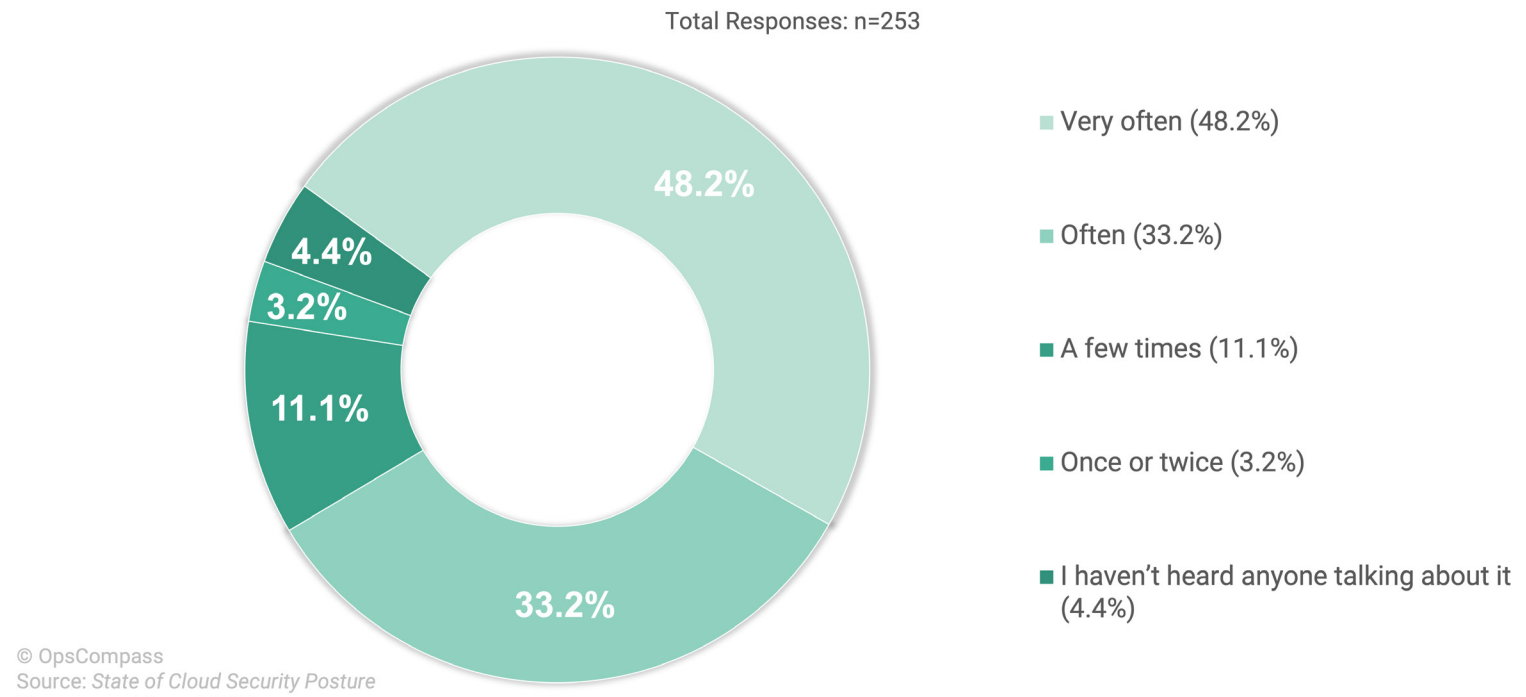
- "Protection," "trustworthy," "reliable," and "innovative"
- "Finding misconfigurations"
- "CSPM is the best way to work" and "the best solution"
- "Keeps bad people out"
- "It cleans the cloud environment"
- "Automation and remediation of security issues"
- "Keeping computer systems safe from hackers"
- Many cited Gartner's definition of "a continuous process of cloud security improvement and adaptation"

81% are actively hearing about CSPM from those around them.

How often have our respondents heard about Cloud Security Posture Management from others, like colleagues, influences, vendors, and analysts? Nearly half (48.2%) replied that they hear about CSPM very often, with another 33.2% saying they hear about it often from others — meaning that 81.4% are actively hearing about CSPM.

11.1% have heard about it a few times, while 3.2% have heard about it one or twice. 4.4% haven't heard anyone talk about it.

FIGURE 10: IN THE PAST 12 MONTHS, HOW OFTEN DID YOU HEAR ABOUT CLOUD SECURITY POSTURE MANAGEMENT (CSPM) FROM COLLEAGUES, INFLUENCERS, VENDORS, ANALYSTS, ETC. ?



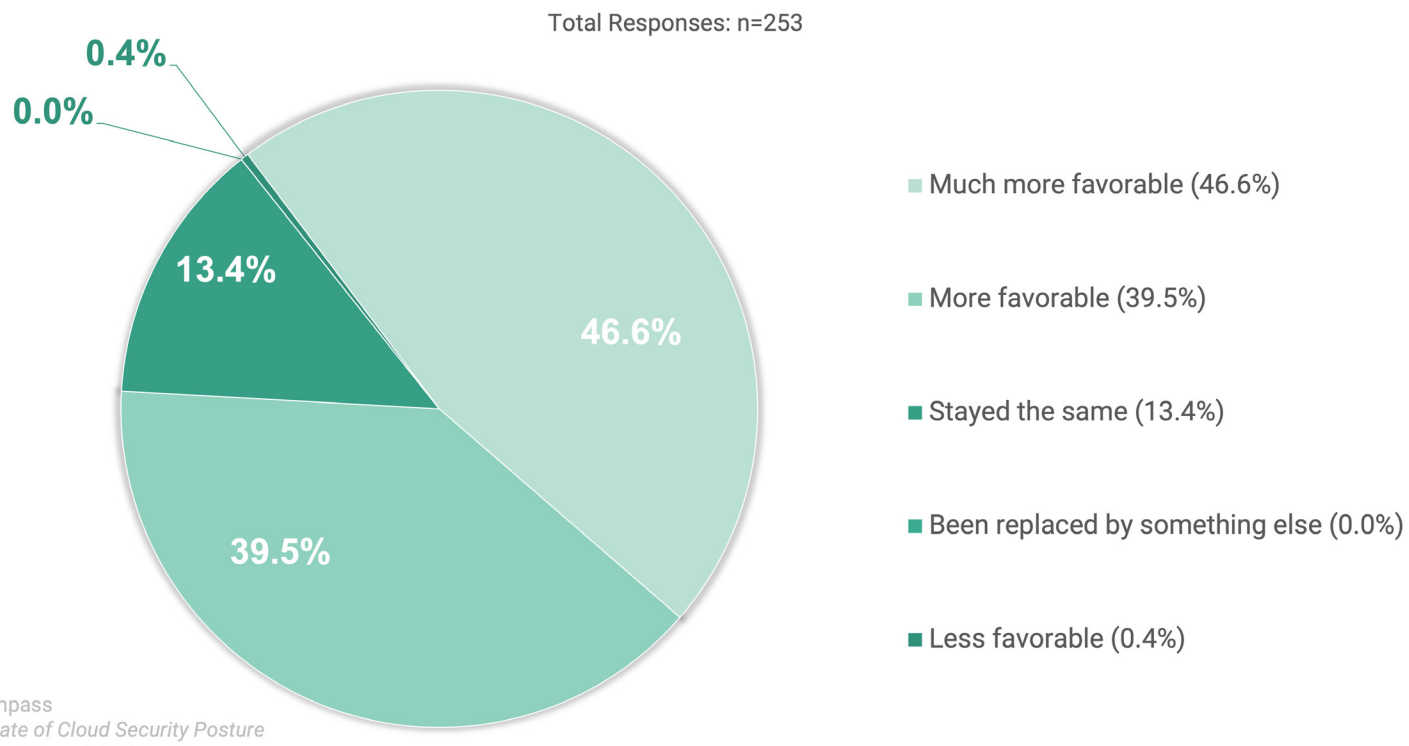
Source: *State of Cloud Security Posture Management Report, 2021*

86% have grown more favorable in their perception of CSPM since last year.

Seeing as how our respondents are at varying levels of awareness around CSPM, we wanted to know how their reception of it has changed over the past year. For 46.6% of respondents, their perception has grown much more favorable, with 39.5% saying it's gotten more favorable. This means that 86.1% feel more positive and confident about CSPM.

For 13.4%, their perception has remained the same. Only .4% said their perception became less favorable.

FIGURE 11: HOW HAS YOUR PERCEPTION OF CLOUD SECURITY POSTURE MANAGEMENT (CSPM) CHANGED OVER THE PAST 12 MONTHS?



Source: *State of Cloud Security Posture Management Report, 2021*

Summary:

As we learned from our respondents, awareness around the relatively new sector of CSPM is increasing. 86% of our respondents have grown more favorable in their perception of CSPM, and associate words like “security,” “protection,” and “trustworthy” with it, believing it to be an important solution for managing their cloud environment. They’re also hearing colleagues, vendors, and influencers talk about it as well. But how many are actively using CSPM solutions?

PART 4:

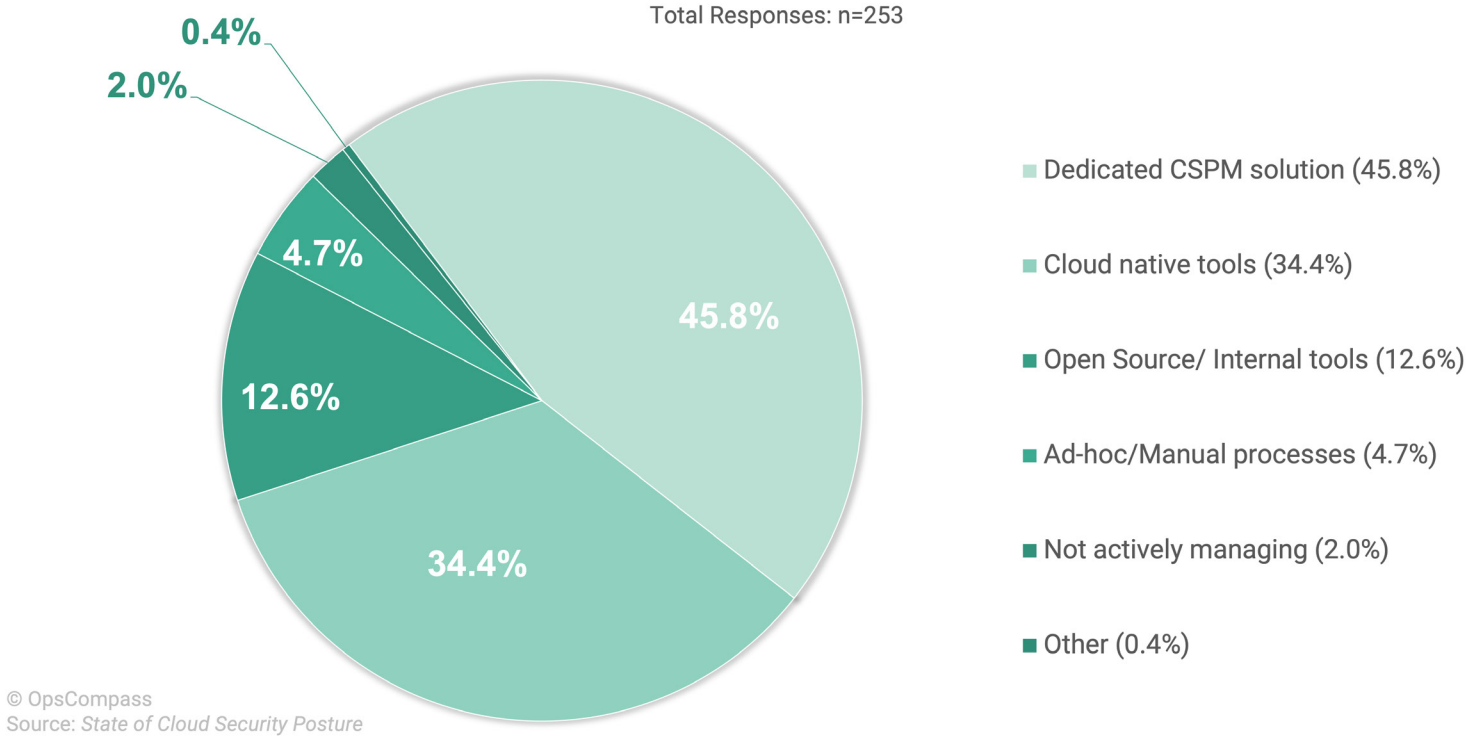
MANAGING CLOUD INFRASTRUCTURE

How well are our respondents managing their cloud? Are they using CSPM solutions effectively? Do they feel confident in their security posture, and if they do, why? Or do they have doubts about how well they're securing their cloud landscape? We had our respondents give us some insight into their daily management.

Less than half are using dedicated CSPM solutions to manage configurations.

We wanted to know in what ways our respondents and their organizations are currently managing the configurations across their cloud environments. Nearly half our respondents (45.8%) are managing their configurations using a dedicated CSPM solution. 34.4% report using a cloud native tool, and 12.7% are using an open source or internal tool. 4.7% are using an ad-hoc or manual process to manage configurations, and 2% admit to not actively managing their configurations at all.

FIGURE 12: HOW DO YOU CURRENTLY MANAGE YOUR CONFIGURATIONS IN YOUR CLOUD INFRASTRUCTURE?



Source: *State of Cloud Security Posture Management Report, 2021*

Cloud security is managed by different teams at different organizations.

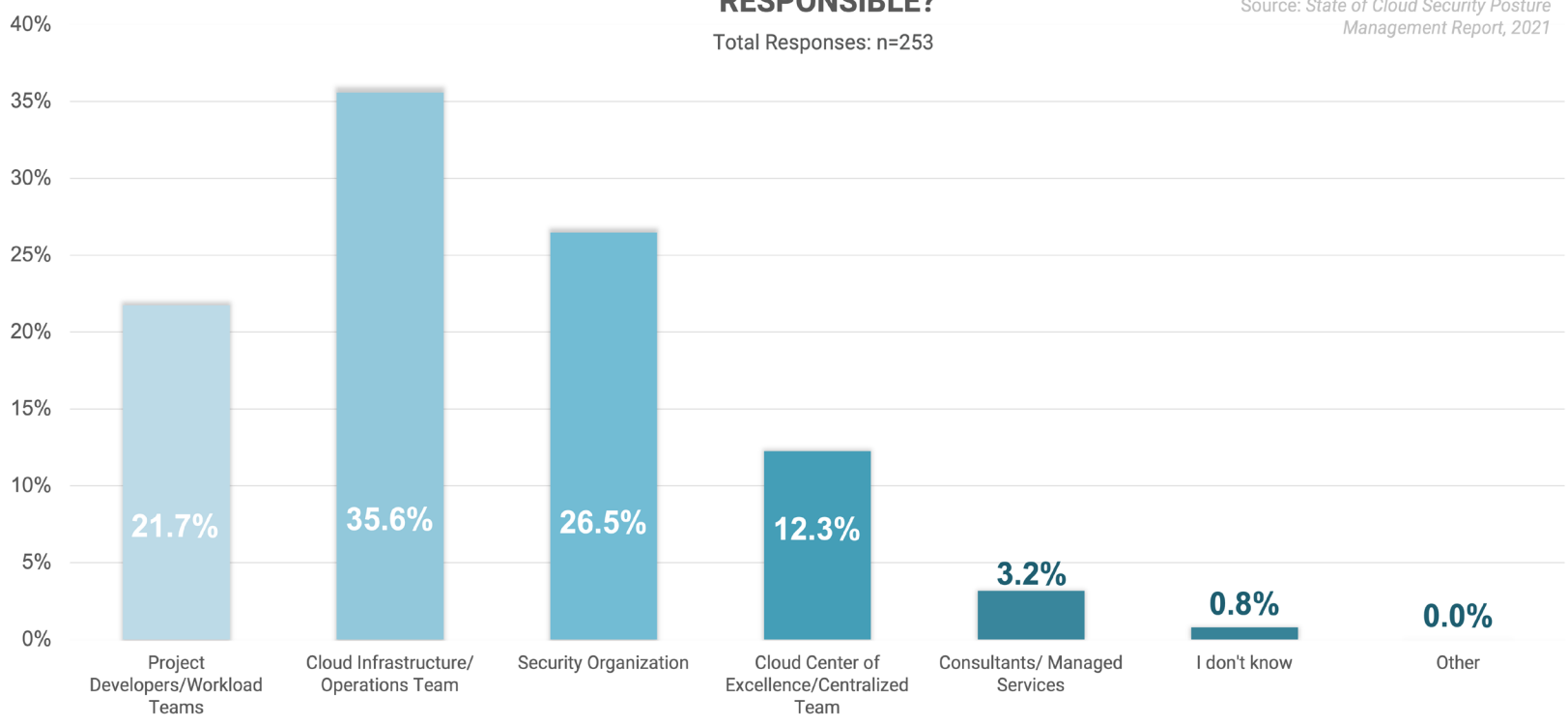
Knowing that many of our respondents are involved in creating and implementing policy and best practices at their organization, we wanted to know who was directly responsible for the overall cloud security there.

For 35.6%, it's a Cloud Instructure or Operations team. For 26.5%, it's a Security Organization, and for 21.7%, it's the Project Developers or Workload teams. 12.3% report that a Cloud Center of Excellence or Centralized team manages their security, while 3.2% have it as a managed service or assign the job to consultants.

This mix of responsible teams could indicate that organizations aren't sure where to "place" cloud security. It could also mean that organizations are aware that cloud security needs to be a priority for all teams, and are engaging everyone to contribute.

FIGURE 13: WHEN IT COMES TO OVERALL CLOUD SECURITY, WHO IS PRIMARILY RESPONSIBLE?

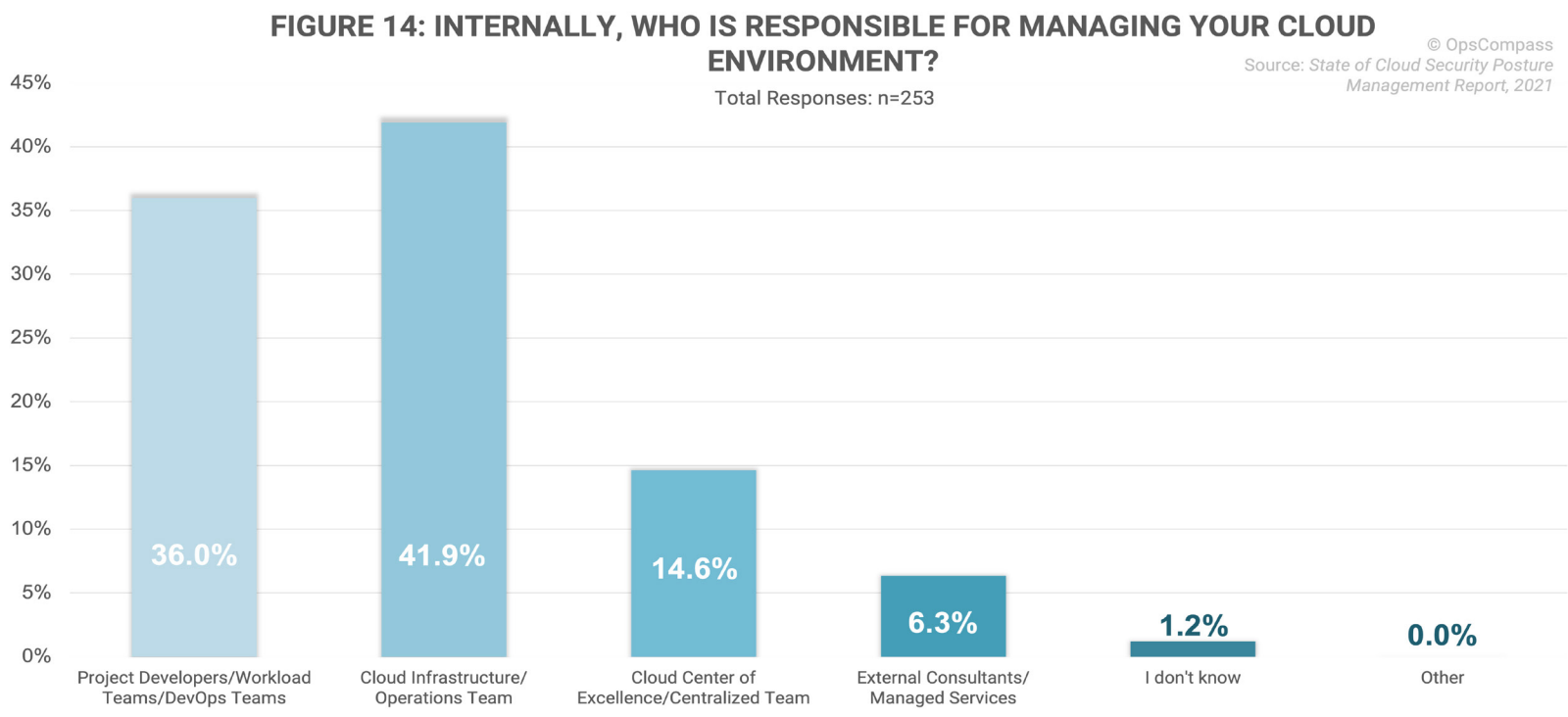
Source: *State of Cloud Security Posture Management Report, 2021*



Cloud Infrastructure or Operations teams are managing cloud environments.

Next, we wanted to know who was responsible for managing their cloud environments. 41.9% report that a Cloud Infrastructure or Operations team is responsible, and nearly as many (36%) say cloud management is with the Project Developers, Workload, or DevOps teams in their organization.

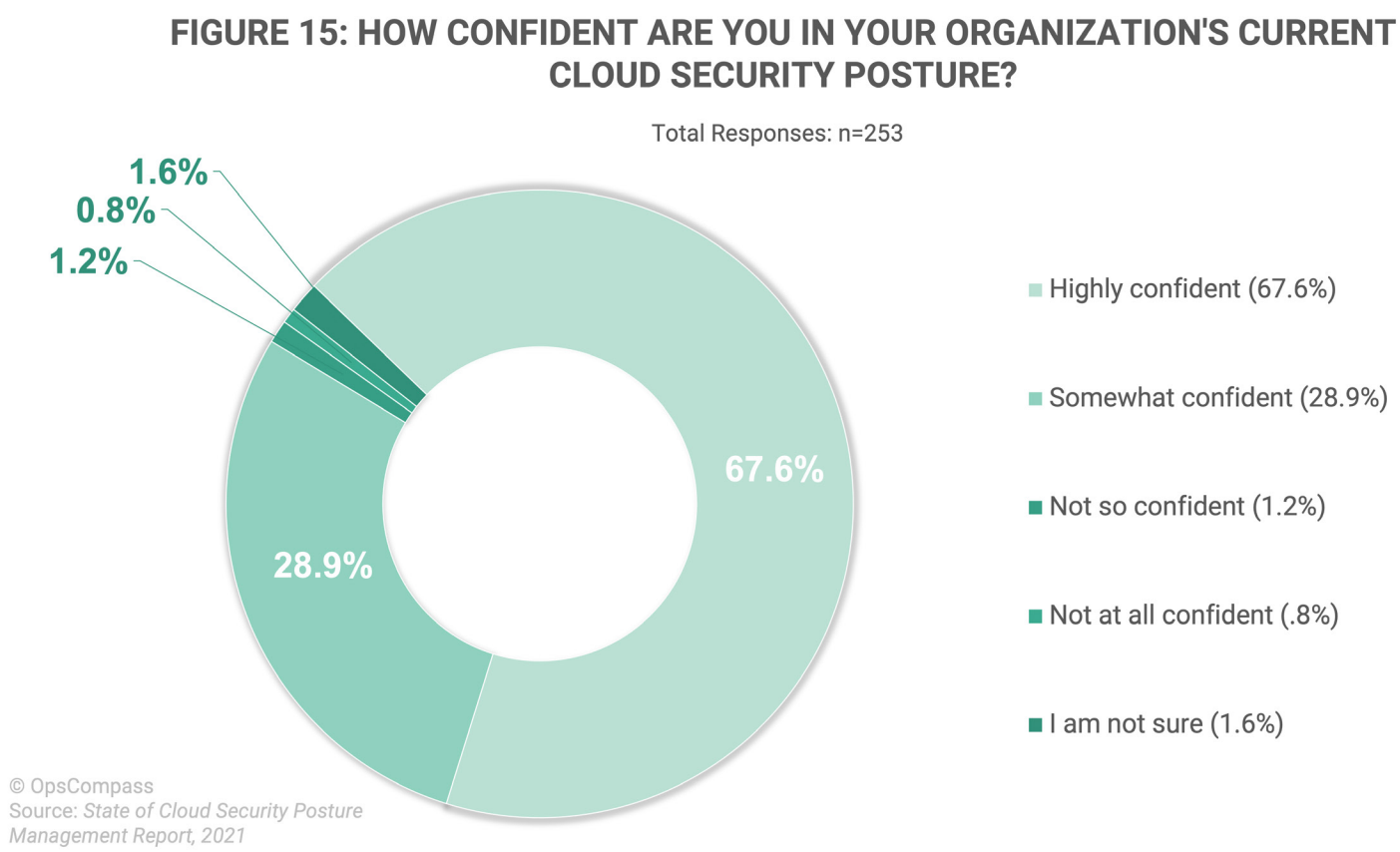
For 14.6%, a Cloud Center of Excellence or a Centralized team manages the cloud environment, and for 6.3%, it's a managed service with external consultants.



68% are highly confident in their security posture, while 29% are somewhat confident.

Are they confident in the current way their organization manages cloud security? 67.6% replied that they were highly confident in their security posture. 28.9% weren't as certain, though, replying that they were somewhat confident. While this means that 96.5% are confident overall, a portion still has doubts about the ability to keep their cloud environments secure. Only 1.2% were not so confident, and .8% were not confident at all.

The Software Developers and Engineers had higher confidence in their organization's security posture, with 75.5% highly confident, and 77.8% of SREs had high confidence. Yet only 61.1% of Security Engineers were highly confident.



They feel confident because they monitor their cloud in real-time.

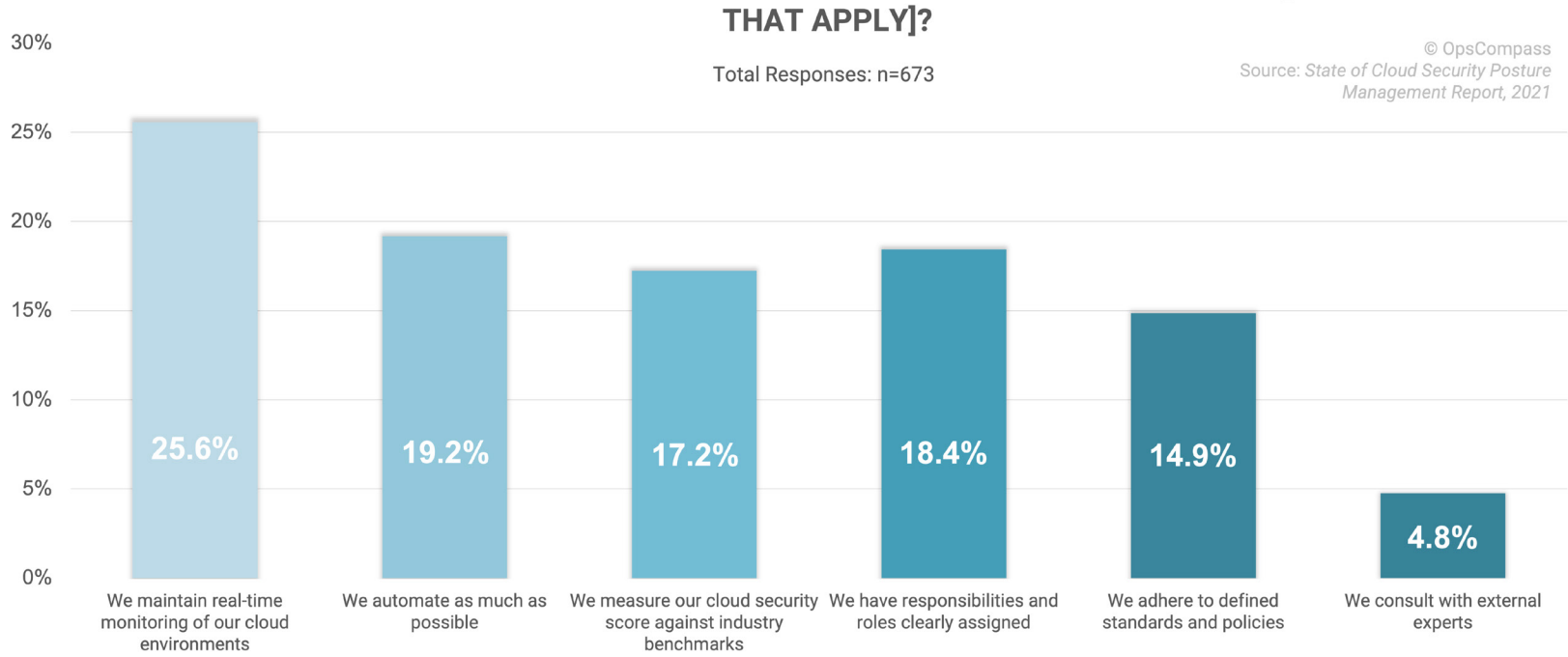
Of those who said they were confident in their current security posture, what was their organization doing to ensure that confidence? Here's what they replied, and they chose all that were applicable:

- We maintain real-time monitoring of our cloud environment (70.5%)
- We automate as much as possible (52.9%)
- We have responsibilities and roles clearly assigned (50.8%)
- We measure our cloud security score against industry benchmarks (47.5%)
- We adhere to defined standards and policies (41%)
- We consult with external experts (13.1%)

FIGURE 16: [IF HIGHLY/SOMEWHAT CONFIDENT] WHAT BEST PRACTICES DO YOU APPLY THAT MAKE YOU CONFIDENT IN YOUR CLOUD SECURITY POSTURE? [CHECK ALL THAT APPLY]?

Source: *State of Cloud Security Posture Management Report, 2021*

Total Responses: n=673

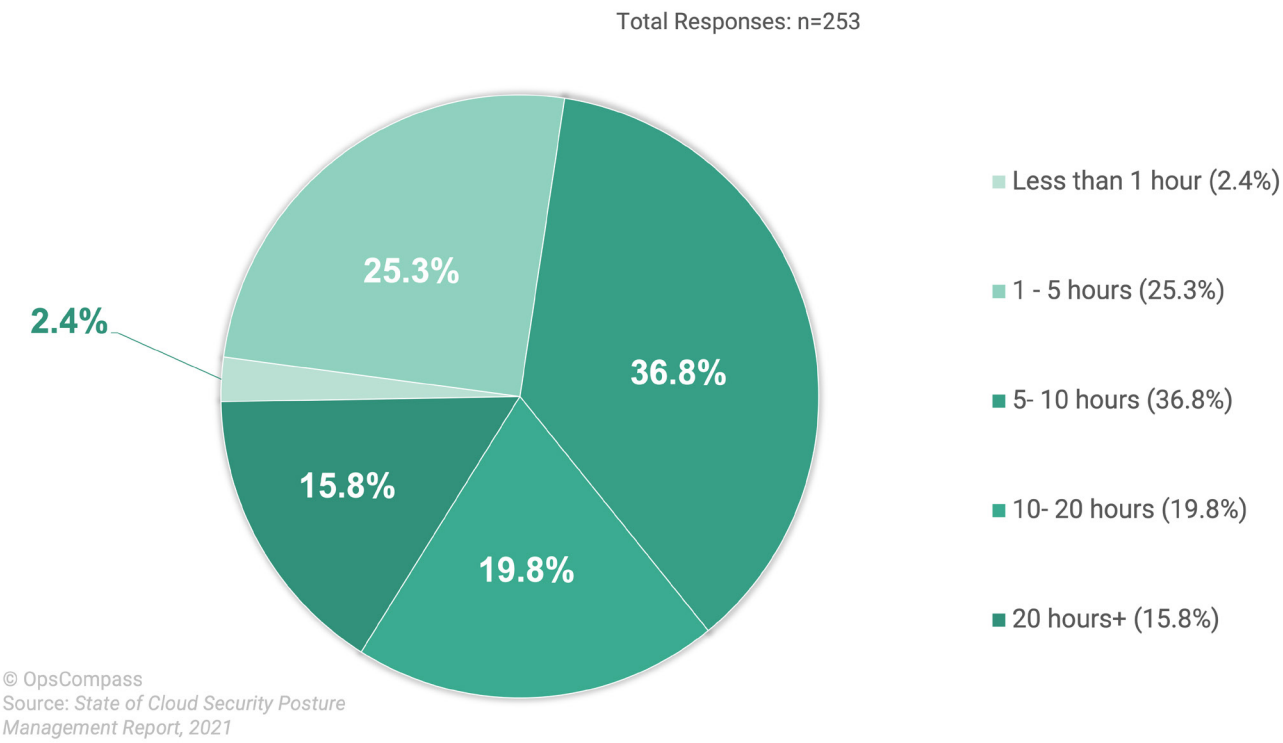


The majority spend 5-10 hours a week on managing their cloud.

When asked about how much time they dedicate to managing their cloud, the answers were split. The majority (36.8%) spend between five and ten hours a week. 25.3% spend between one and five hours, and 2.4% spend less than one hour.

For 19.8%, they're dedicating between 10 to 20 hours per week, and for 15.8%, they're devoting 20 or more hours.

FIGURE 17: HOW MUCH OF YOUR TIME PER WEEK IS DEDICATED TO MANAGING YOUR CLOUD ENVIRONMENT?

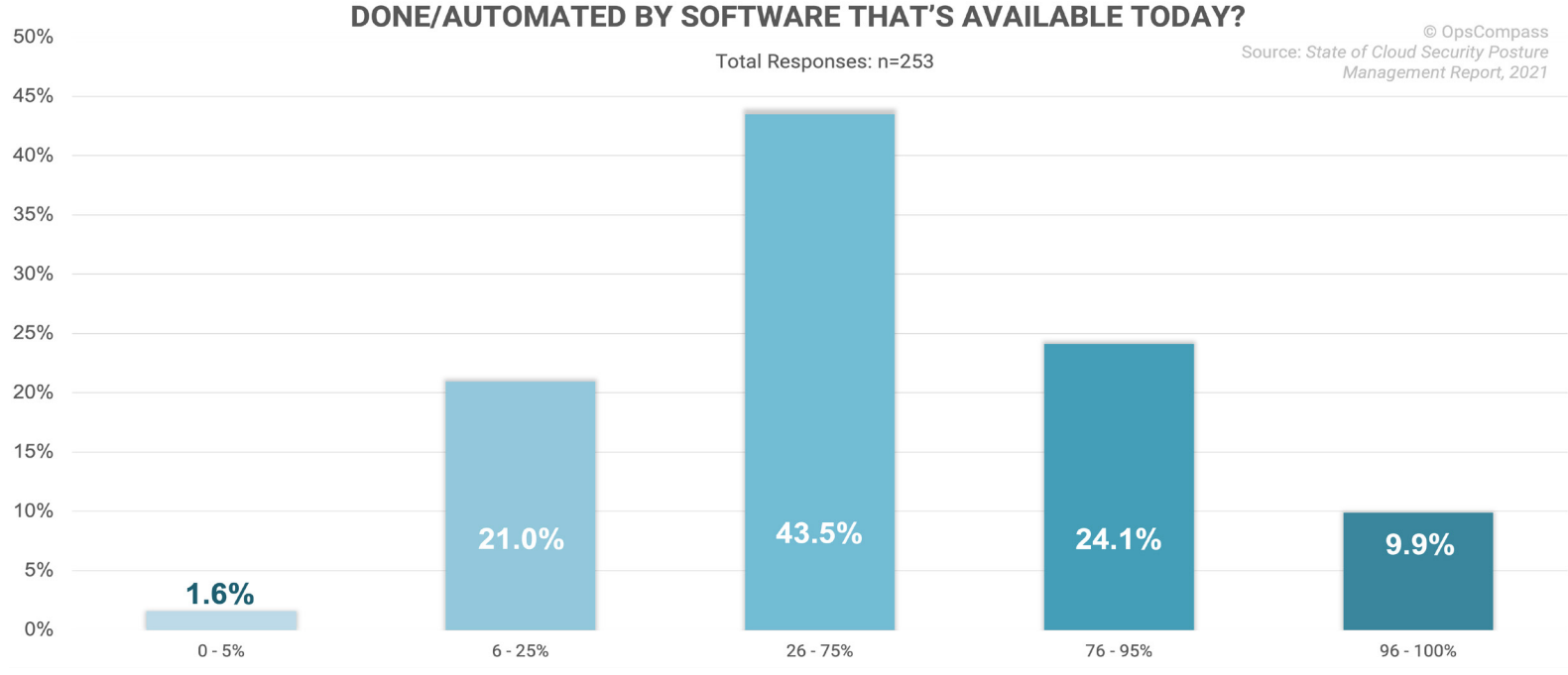


Many believe automation can help with a number of tasks.

Now that we know how much time they're devoting to managing their cloud, we wanted to know what percentage of their work could be supported by automation, if any. The majority (43.5%) reported that they believed 26% to 75% could be supported by automation. 21% believed about 6% to 25% of their duties could be supported by automation, and 1.6% believed that only up to 5% of their duties could be supported by automation.

24.1% felt that 76% to 95% of their duties could be completed using software options, with 9.9% feeling that most if not all of their work could be supported by automation. When it came to those believing that 76% to 100% of their work could be supported by automation, the largest respondent group were Software Developers or Engineers (56%).

FIGURE 18: WHAT PERCENTAGE OF YOUR WORK, IF ANY, DO YOU BELIEVE COULD BE DONE/AUTOMATED BY SOFTWARE THAT'S AVAILABLE TODAY?



Summary:

Despite growing positivity around CSPM solutions in the last section, we found that only 46% are using a dedicated CSPM solution to manage their cloud. Still, 97% are feeling confident — either highly or somewhat — in their security posture, and they feel so because of the way they maintain real-time monitoring, the way they've automated their processes, and the way they've assigned their roles.

Additionally, we found that cloud security and the cloud environment are mostly being managed by Cloud Infrastructure or Operations teams, followed by Project Developers, Workload, or DevOps teams, with other teams responsible as well. And many believed there was room for further automation in their job duties.

As we next look at challenges they're facing, today and beyond, we'll see if that confidence remains high.

PART 5:

CHALLENGES

Ensuring a secure cloud isn't just confined to managing one or two aspects of it. Cloud managers need to ensure that they're watching for a number of issues that can compromise their environments, including data leaks and configuration drift from the inside, and malicious threats from the outside. We wanted to know the biggest challenges facing our respondents when it comes to security.

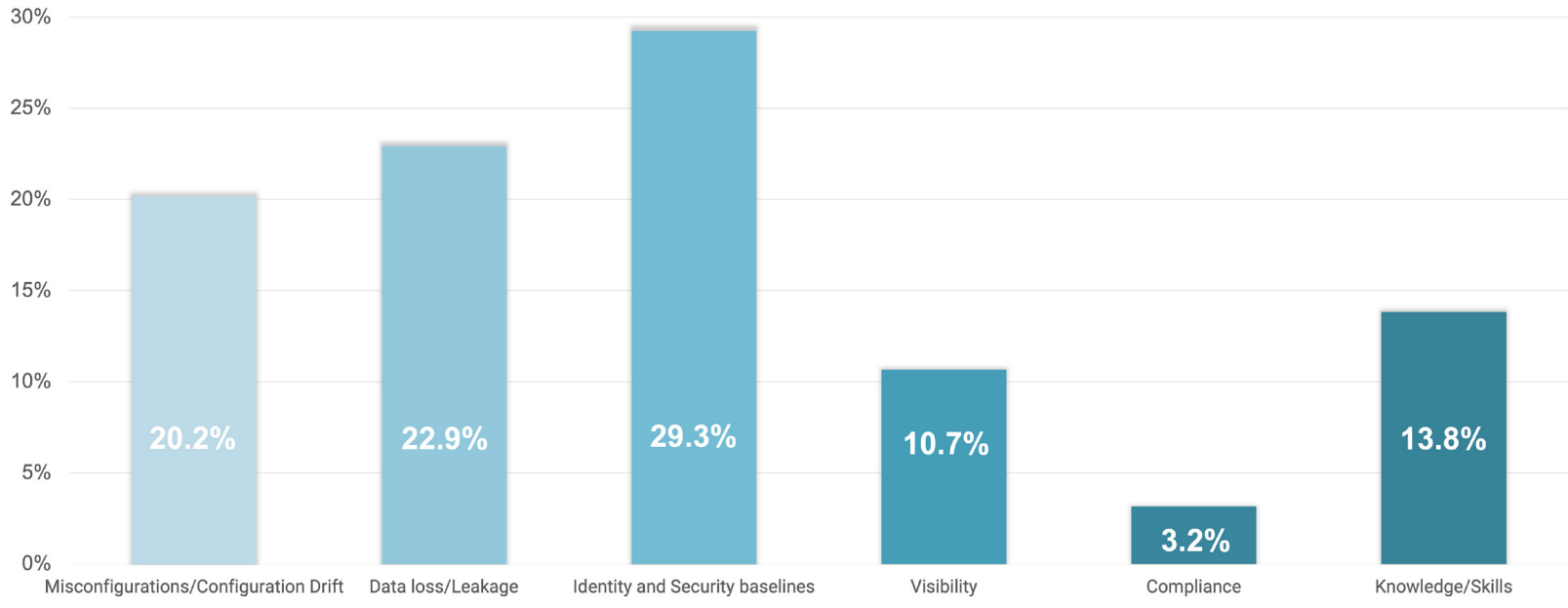
Visibility, the skills-gap, misconfiguration and drift detection are major concerns.

Our respondents are split on what their biggest challenge is today when managing their cloud infrastructure. When combined, 44.7% are concerned with visibility across their cloud environment and related issues including the skills-gap, misconfigurations and configuration drift. 29.3% believe it's managing identity and security baselines. 22.9% say their biggest challenge is data loss or leakage. 3.2% are worried about compliance.

FIGURE 19: OTHER THAN CLOUD COSTS, WHAT IS THE BIGGEST CHALLENGE YOU FACE WHEN IT COMES TO MANAGING YOUR CLOUD INFRASTRUCTURE?

Total Responses: n=253

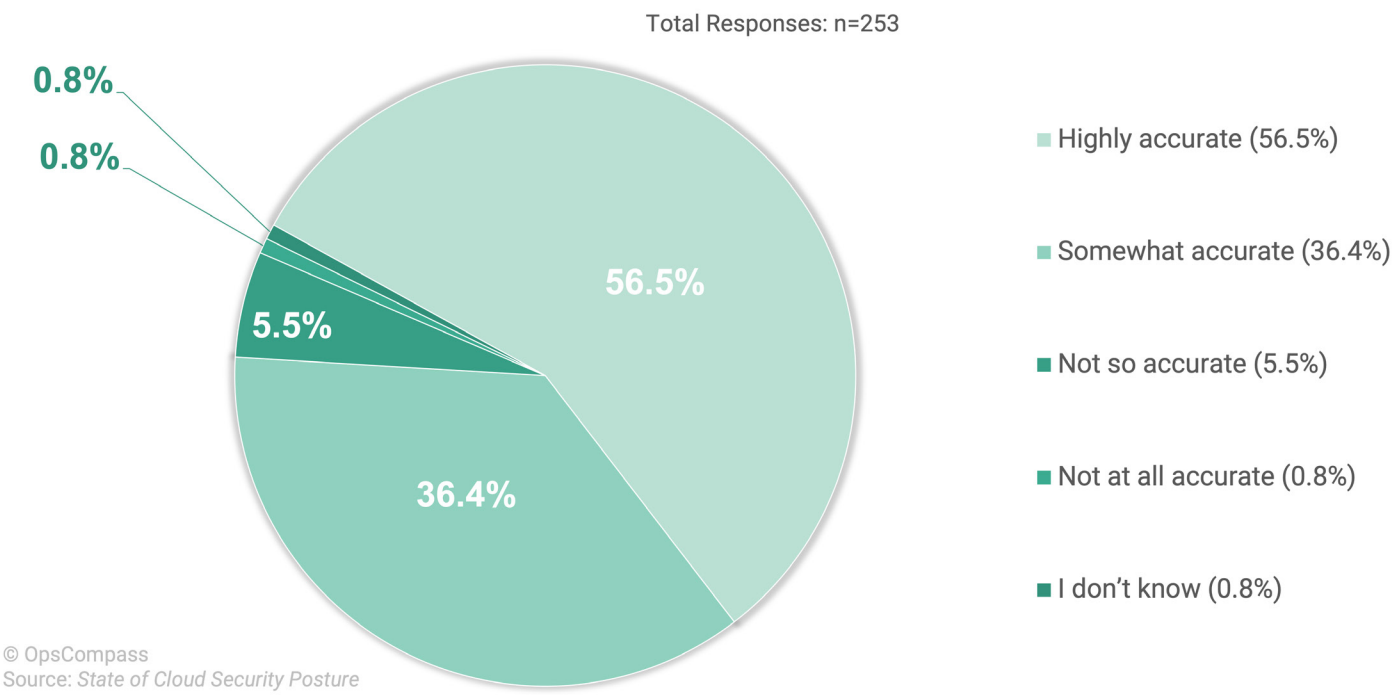
Source: *State of Cloud Security Posture Management Report, 2021*



93% believe their organization has a high level of visibility into their cloud environment.

When it came to their understanding around visibility into their cloud environment, 56.5% highly agreed that their organization has a high level of visibility. 36.4% somewhat agreed that their organization has a high level of visibility. This means that 92.9% of respondents are confident in their organization's ability to see into all aspects of their cloud environment. Only 5.5% replied they were not so confident, and .8% weren't confident at all.

FIGURE 20: HOW DO YOU FEEL ABOUT THE FOLLOWING STATEMENT: MY ORGANIZATION HAS A HIGH-LEVEL OF VISIBILITY IN OUR CLOUD ENVIRONMENT?

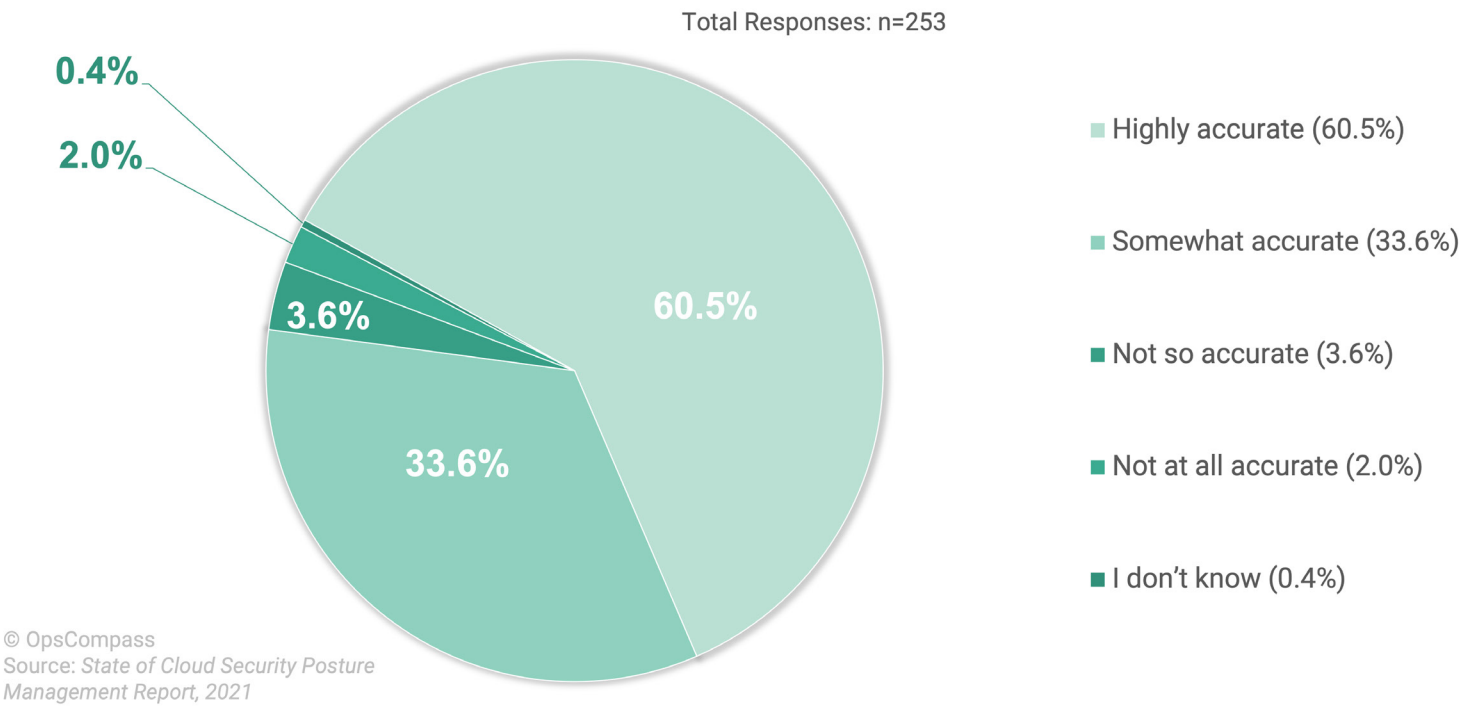


Source: *State of Cloud Security Posture Management Report, 2021*

94% believe their organization is adhering to clear compliance policies.

Finally, we wanted to know their thoughts about how clear they believe their organization's cloud policies are, and how well they're adhering to them. 60.5% highly agree that their organization has clear policies and that they're following them well, while 33.6% only somewhat agreed. Only 3.6% weren't so confident in their organization having clear policies they execute, and 2% weren't confident at all.

FIGURE 21: HOW DO YOU FEEL ABOUT THE FOLLOWING STATEMENT: MY ORGANIZATION HAS VERY CLEAR CLOUD COMPLIANCE POLICIES AND WE DO AN EXCELLENT JOB OF ADHERING TO THEM?



Source: *State of Cloud Security Posture Management Report, 2021*

Summary:

We were able to gain some insight into what our respondents see as their biggest challenges in managing their cloud security today, outside of costs. The biggest were managing and adhering to identity and security baselines, data loss or leakage, and misconfigurations or configuration drift — all items that fall under the scope of continuous monitoring and real-time visibility, and items that, if left unaddressed, significantly increase security risks, especially misconfiguration or drift, as they potentially open doors for hackers. Additionally, 94% see data loss or leakage specifically as a problem needing to be solved.

When it comes to confidence — or possibly overconfidence — in visibility, 93% of our respondents believe that their organization has a high level of visibility into their cloud environment, which means being able to continuously track and monitor all assets, configuration, deployments, and more. But is their visibility high-fidelity, and are they receiving trustworthy, actionable information? Or are they receiving a number of low-fidelity alerts that they think are helpful, but are merely just distracting? Additionally, 94% believe their organization is in compliance.

Yet, again, the numbers we saw earlier around the amount of cloud-related breaches, and the uncertainty around their organization's cloud security, seem to suggest either an overconfidence, or an unawareness of what the real posture is. But fortunately they have plans for future improvements.

PART 6:

CSPM PLANS FOR 2021

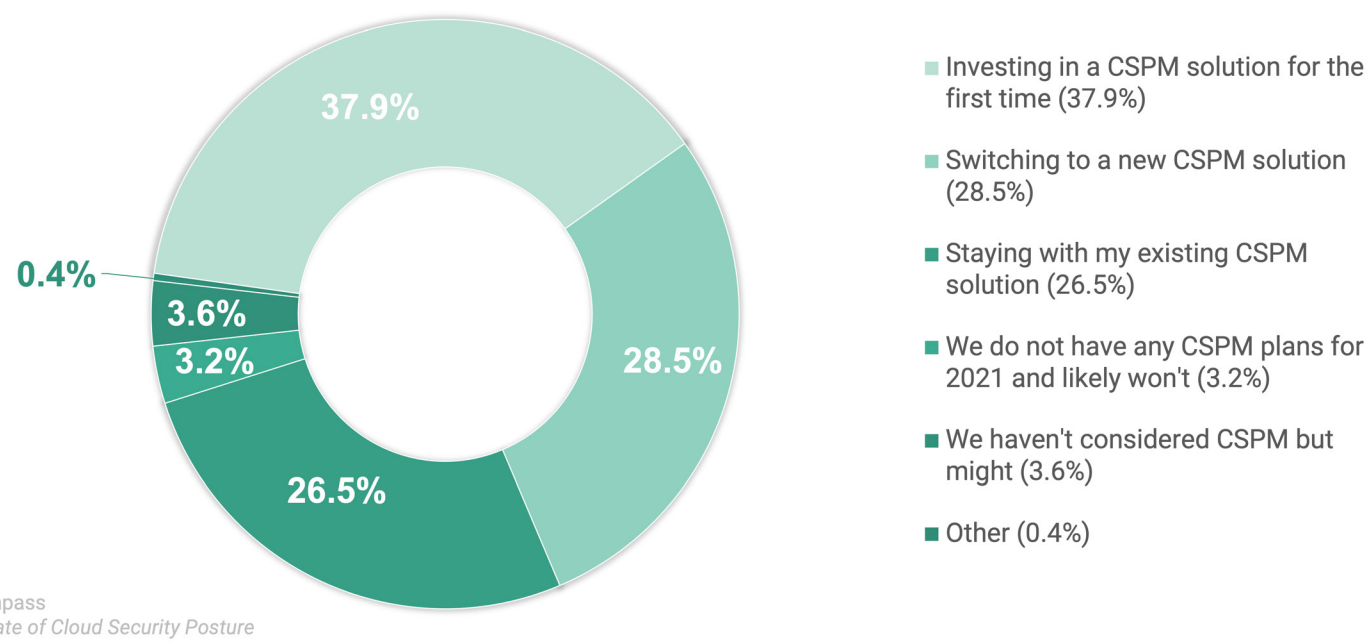
Finally, we wanted to know their plans for the future in regards to their CSPM solutions. Are they happy with their current CSPM, or have they never adopted one before? What are their biggest priorities for cloud security over the coming year? Here's what they're looking towards in 2021.

38% are looking for CSPM solutions for the first time, and 29% want to switch.

Looking forward, what are the plans for our respondents' organizations when it comes to implementing CSPM solutions? The majority (38%) are looking to invest in a CSPM solution for the first time this coming year. 28.5% replied that they're looking to switch to a new CSPM solution from the current one they have. 26.5% report being satisfied with the current CSPM solution, and will stay with it. Only 3.2% say they don't have any CSPM plans for 2021, and 3.6% report that they haven't considered CSPM, but might.

FIGURE 22: WHAT ARE YOUR CLOUD SECURITY POSTURE MANAGEMENT (CSPM) SOLUTIONS PLANS, IF ANY, FOR 2021?

Total Responses: n=253



Source: *State of Cloud Security Posture Management Report, 2021*

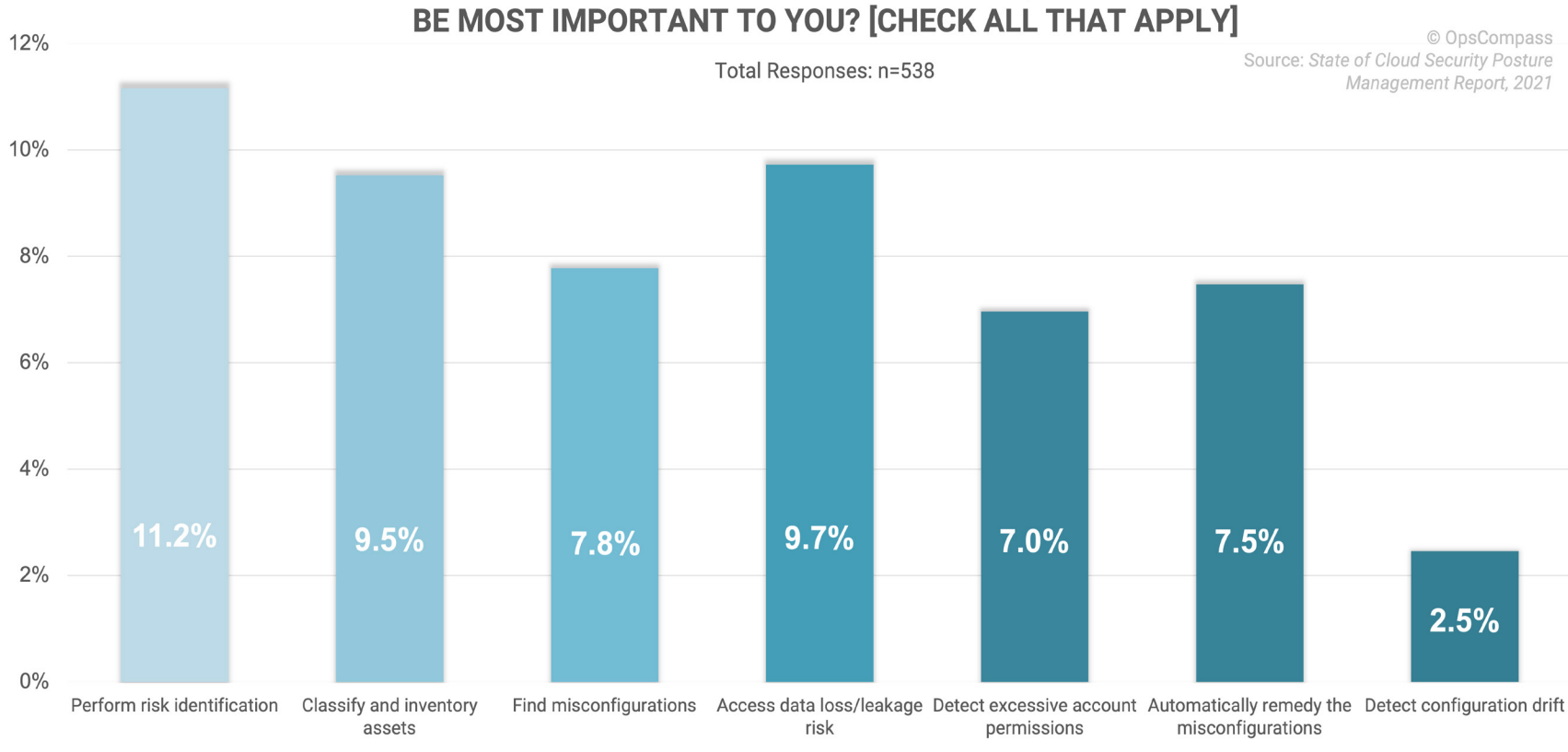
Having full visibility is a priority in a CSPM solution.

Since we know that many want to invest in a CSPM solution for the first time, or switch, we wanted to know what capabilities in a CSPM were most important to them. Here's what they wanted:

- Have full visibility across our entire cloud environment (71.5%): Considering the majority use multi- or hybrid-cloud environments, this is key in seeing the full picture and context.

- Continuously monitor and assess compliance policy violations (49.4%): Keeping assets not just safe but compliant to various policies and frameworks is also a necessity.
- Perform risk identification (43.1%): They're looking for a tool that can alert to risky configurations or assets.
- Classify and inventory assets (36.8%): In order to manage their cloud, organizations need to know what's in it.
- Find misconfigurations (30%): Misconfigurations can happen anytime, and often occur outside of the pipeline.
- Detect excessive account permissions (26.9%): They're looking for a solution that can help manage identity and access into the cloud.
- Automatically remedy the misconfigurations (28.9%): They want a solution that can automate response to ensure swift remediation.
- Detect configuration drift (9.5%): They want a tool that can help track configurations outside the pipeline.

FIGURE 23: IF YOU WERE TO INVEST IN A CSPM SOLUTION, WHAT CAPABILITIES WOULD BE MOST IMPORTANT TO YOU? [CHECK ALL THAT APPLY]



They want to improve real-time monitoring, become more proactive, and increase automation.

Finally, what were their top priorities for cloud security in general over the coming year? Here's how they responded:

Improving our real-time monitoring (67.2%): Our respondents reported earlier that they felt confidence in their security posture because of their real-time monitoring, so it seems they want to improve upon one of their best practices.

Becoming more proactive and less reactive (52.2%): Since many have seen a breach in their organization, they want to become more proactive around their security posture, instead of reacting after an issue happens.

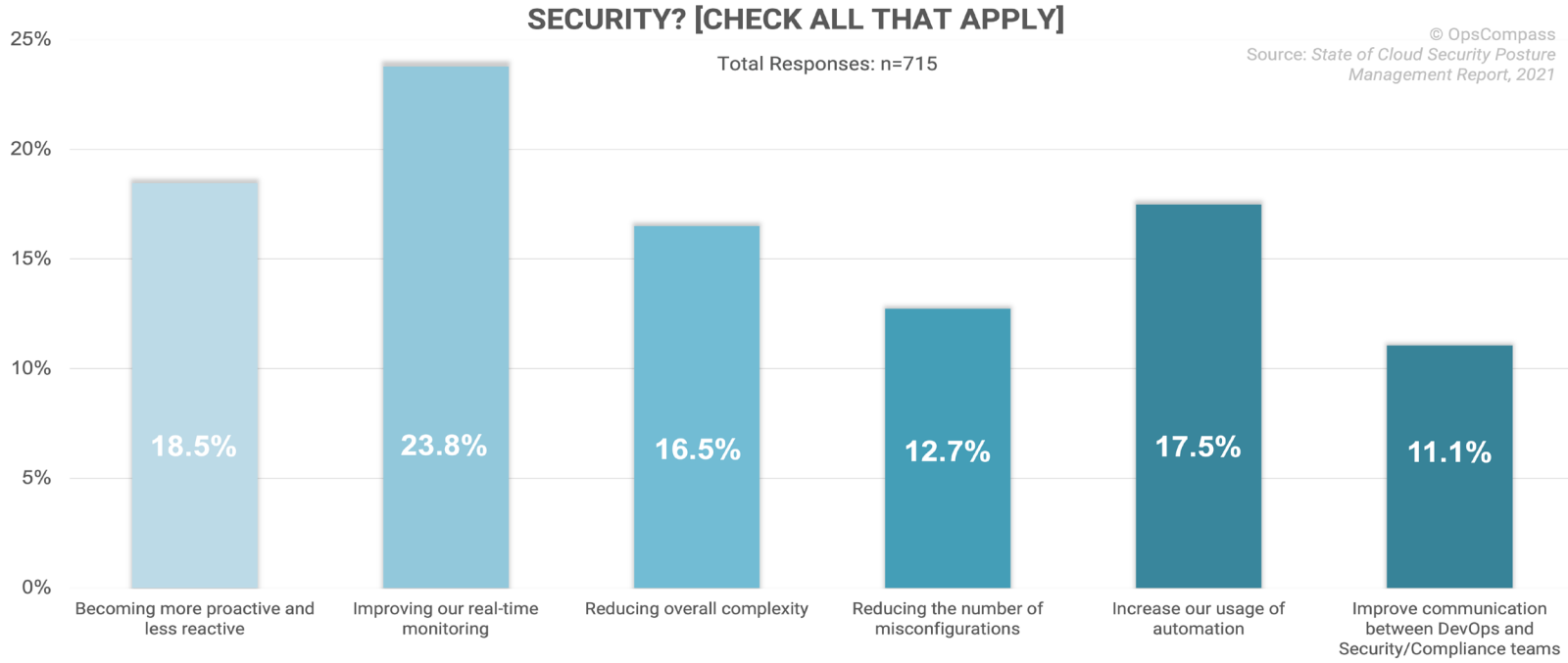
Increase our usage of automation (49.4%): Our respondents believe that many parts of their job can be supported by automation, and they want to make it happen.

Reducing overall complexity (46.6%): Since nearly all are dealing with multi- or hybrid-cloud environments, they want to reduce complexity and streamline their security approach.

Reducing the number of misconfigurations (36%): Misconfigurations can go undetected, and can cause increased risk, so organizations want better tracking of where they happen.

Improve communication between DevOps and Security and Compliance teams (31.2%): Since managing an effective security posture falls to everyone in an organization, they want to increase communication to have better governance and a more holistic approach.

FIGURE 24: WHAT ARE YOUR TOP PRIORITIES FOR 2021 WHEN IT COMES TO CLOUD SECURITY? [CHECK ALL THAT APPLY]



Summary:

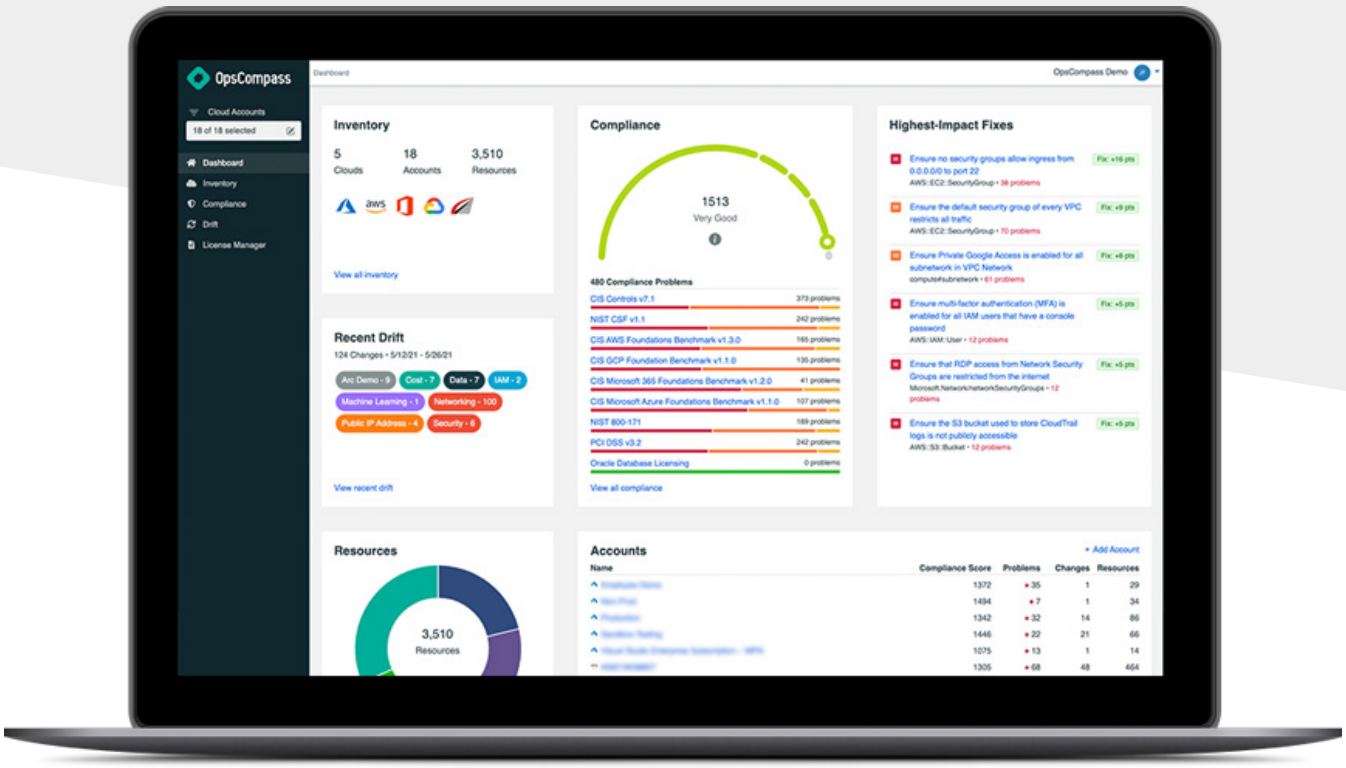
Over a third of our respondents want to adopt a CSPM solution for the first time this coming year, and over a quarter want to switch to a better solution. They're going to be looking for tools and approaches that are going to give them full visibility across the cloud environment, manage incident responses, and continuously monitor and assess their compliance.

CONCLUSION

The majority of our respondents are confident in the state of their cloud: they believe their posture management is strong, they have visibility into multi- or hybrid-cloud environments, and they're in compliance. Yet many have seen cloud breaches, and many have big concerns around issues like data loss, identity management, and configuration drift — meaning that there's still work to be done.

Fortunately, many are looking to embrace new CSPM solutions this year, and recognize the value in having a holistic approach to cloud security. They want to become more proactive in putting policies and procedures in place before an issue occurs, improve monitoring and visibility, and use the tools available to them to ensure a safe cloud that will allow their organizations to grow easier and quicker in the future.

Their priorities for security in 2021 signal a dedication to making what they already have in place more efficient and effective: improving real-time monitoring, being more proactive, and increasing automation.



ABOUT OPSCOMPASS

OpsCompass is the cloud security, operations, and management solution for the multi-cloud world. Our technology, products, and services provide real-time visibility, intelligence, and control so that operations teams proactively know what's in their cloud and what to fix.

With OpsCompass, businesses eliminate costly compliance and misconfiguration issues and achieve greater security and performance.

To learn more about OpsCompass visit opscompass.com/get-started