PERMISO

2023

# CLOUD SECURITY SURVEY REPORT

## Summary

We surveyed more than 500 security, IT and engineering professionals to understand how they are tackling security in their cloud, understand the volume of identities and secrets they are managing, and assess their confidence with their existing team and tooling to manage security events in their environment.

We compared the results of this survey to other data such as industry benchmarks, other survey reports, in addition to data of actual practices and cloud behavior of thousands of customers by large cloud vendors. This survey highlights the current cognitive dissonance in the industry around the inherent feeling that enterprises are adequately protected in the cloud and the reality or actual state of cloud security. Even though many respondents reported having experienced a breach in their cloud environment, are utilizing insecure cloud management practices, and are concerned their teams don't have the tools or expertise needed to respond to a breach – an astonishing 80% believe their existing people, processes, and technology would prevent them from having a breach in the future.

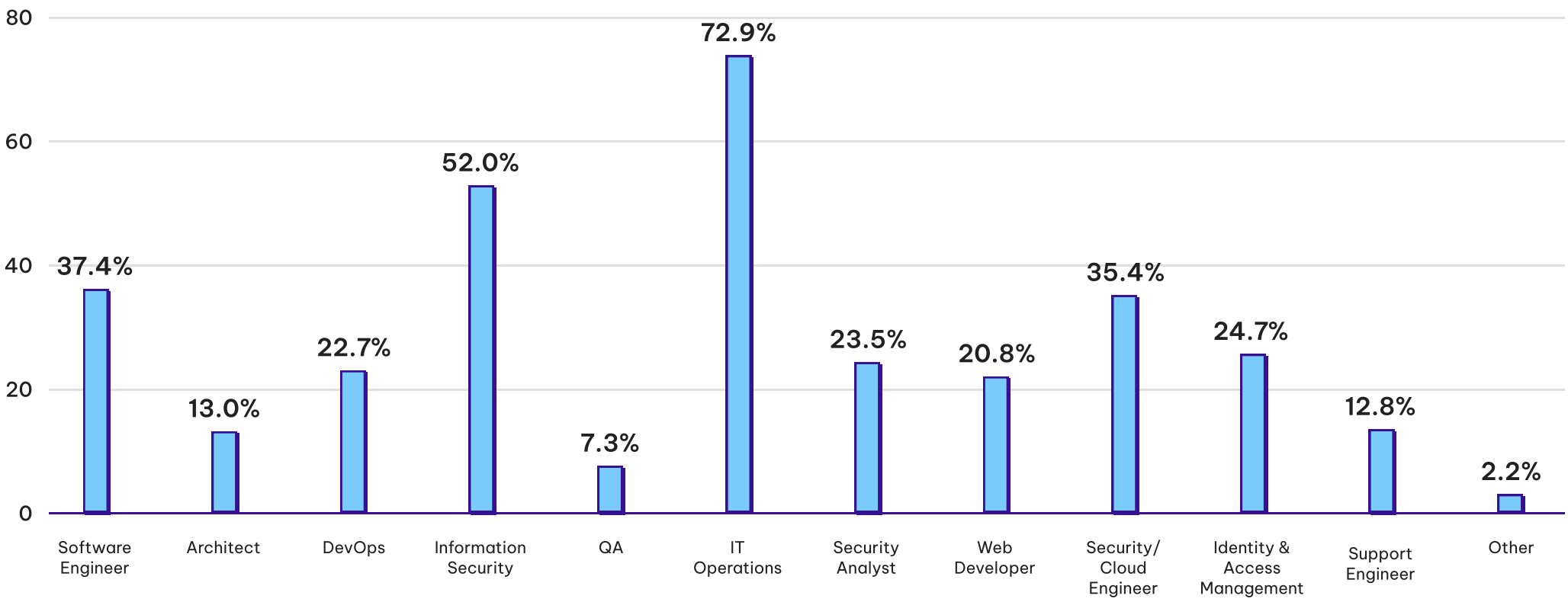
Cloud security practitioners seem to have confidence in both their security posture and the team that supports their cloud security programs, despite the fact that many respondents have experienced unauthorized access or a breach, and admitting to continuing to leverage high risk practices and behaviors in their cloud environment. Interestingly, respondents across the board, however, expressed a great deal of concern with their confidence in that same team and tooling's ability to detect and respond to a breach should a threat actor actually gain access into their environment. More than half of the respondents claimed they were 'very' to 'extremely' concerned about the ability for their teams and their tools to detect and respond to an environment.

## Key Findings

- 95% of the respondents expressed concern that their current tools and teams may not be able to detect and respond to a security event in their cloud environment. More than 55% described their level of concern as ‘extremely concerned’ and ‘very concerned’.
- 44% of respondents manage more than 5,000 identities across their cloud environment.
- When it comes to access in their cloud environments, nearly half of the respondents (46.2%) have local iam users with console access into their environment and 37% of respondents leverage long-lived access keys
- Despite high risk practices and widespread concern over a breach in their cloud environment, more than 80% of respondents feel that their existing tooling and configuration would sufficiently cover their organization from a well-orchestrated attack on their cloud environment

# Survey Results

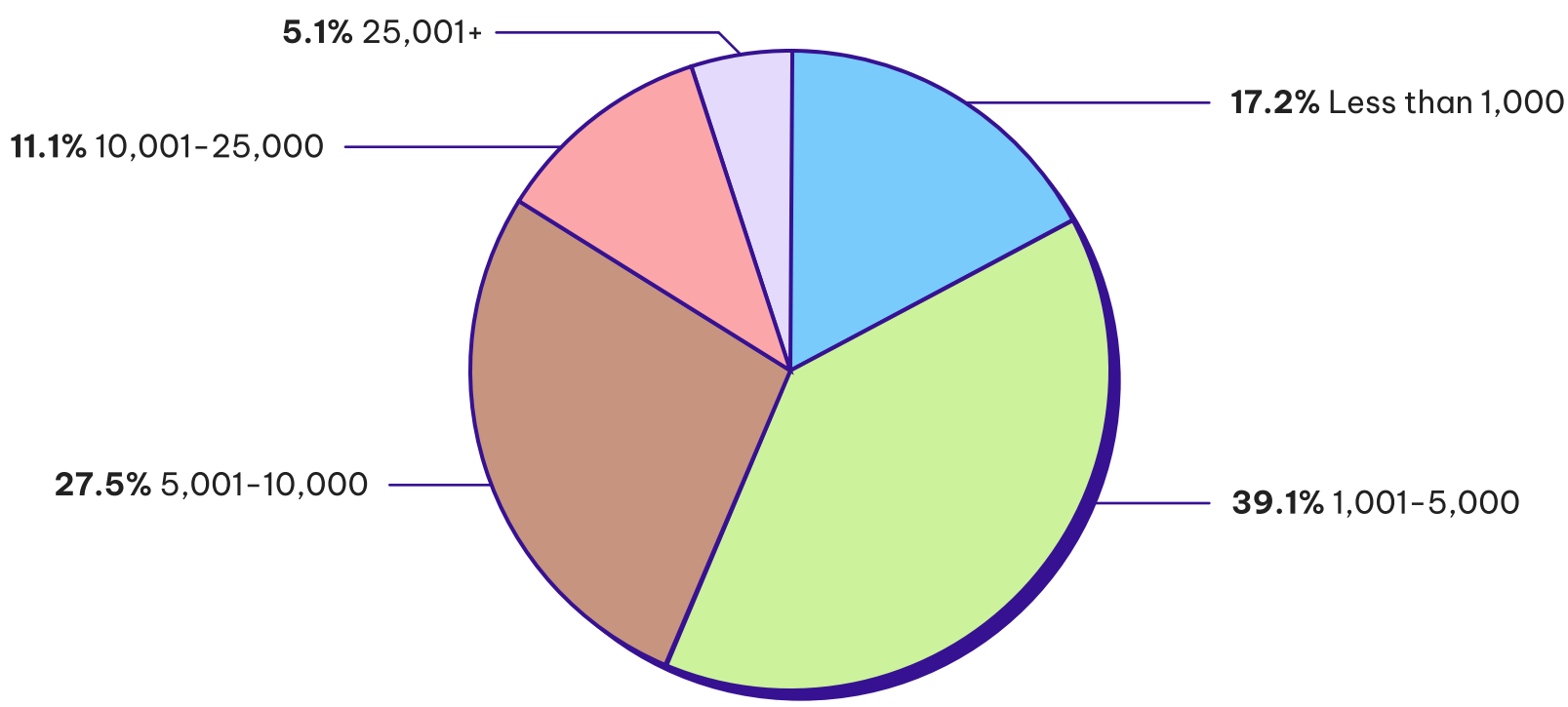
Which closely aligns with your responsibility(ies)/position(s) within the IT department at your company?




| ROLE | PERCENT | RESPONSES |
|---|---|---|
| Software Engineer | 37.4% | 189 |
| Architect | 13.0% | 66 |
| DevOps | 22.7% | 115 |
| Information Security | 52.0% | 263 |
| QA | 7.3% | 37 |
| IT Operations | 72.9% | 369 |
| Security Analyst | 23.5% | 119 |
| Web Developer | 20.8% | 105 |
| Security/Cloud Engineer | 35.4% | 179 |
| Identity & Access Management | 24.7% | 125 |
| Support Engineer | 12.8% | 65 |
| Other | 2.2% | 11 |

We asked those who took the survey to select all of the roles/responsibilities that encompassed their job within their respective engineering, security and IT team. The survey showed a pretty even representation across engineering, devops and security roles, with a slightly larger presence in IT Operations, Information Security and engineering. By pairing this data with the results, it becomes easier to understand where the concentration of responsibility for cloud security lies within most organizations.

How many identities do you manage across cloud and on-premise environments? (examples: human or machine users or identities for AWS, Okta, Azure, AD, GCP, Auth0, PingIdentity, etc)

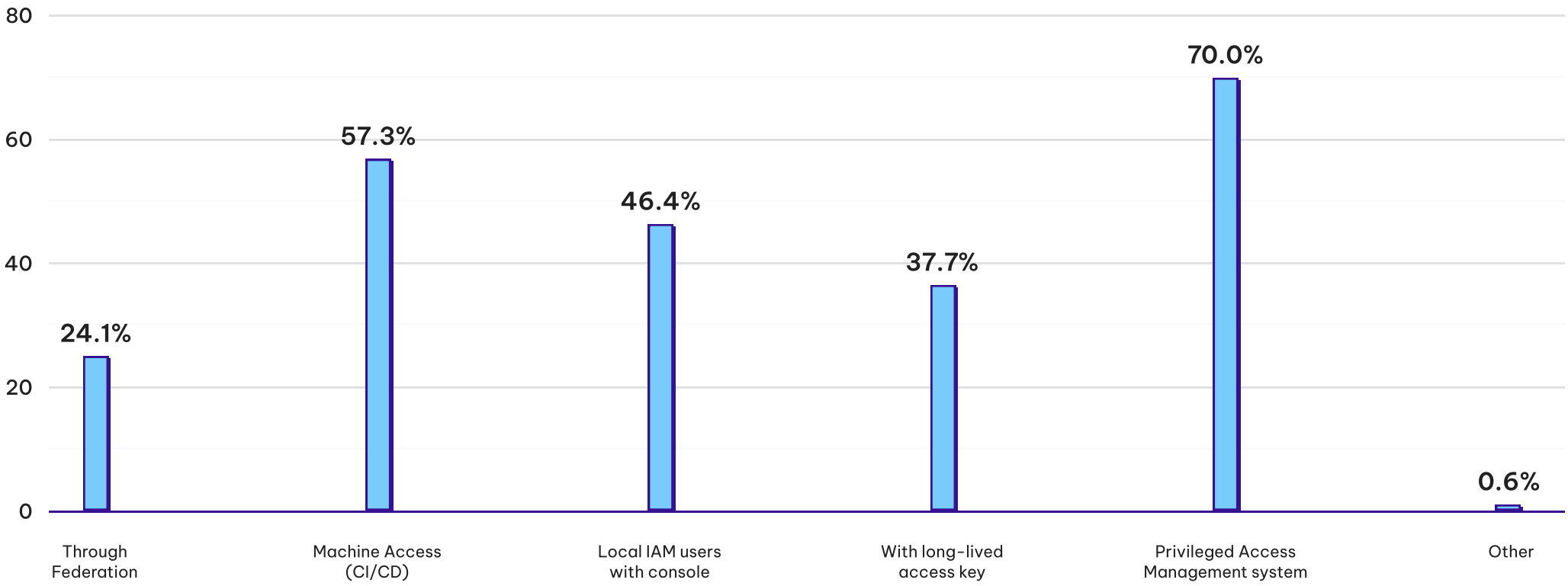



| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Less than 1,000 | 17.2% | 87 |
| 1,001-5,000 | 39.1% | 198 |
| 5,001-10,000 | 27.5% | 139 |
| 10,001-25,000 | 11.1% | 56 |
| 25,001+ | 5.1% | 26 |

As companies expand their adoption of the cloud and continue to embrace more cloud-native technologies, the number of identities that are being managed continues to grow rapidly. The Identity Defined Security Alliance (IDSA) reported that 98% — the vast majority of companies surveyed — confirmed that the number of identities has increased in their organization, with 52% saying it's because of the rapid adoption of cloud applications. Other factors increasing identities at organizations are an increase in third-party relationships (46%) and in new machine identities (43%). The growth in both human and non human users has made Identity and Access Management an ongoing challenge for many teams.

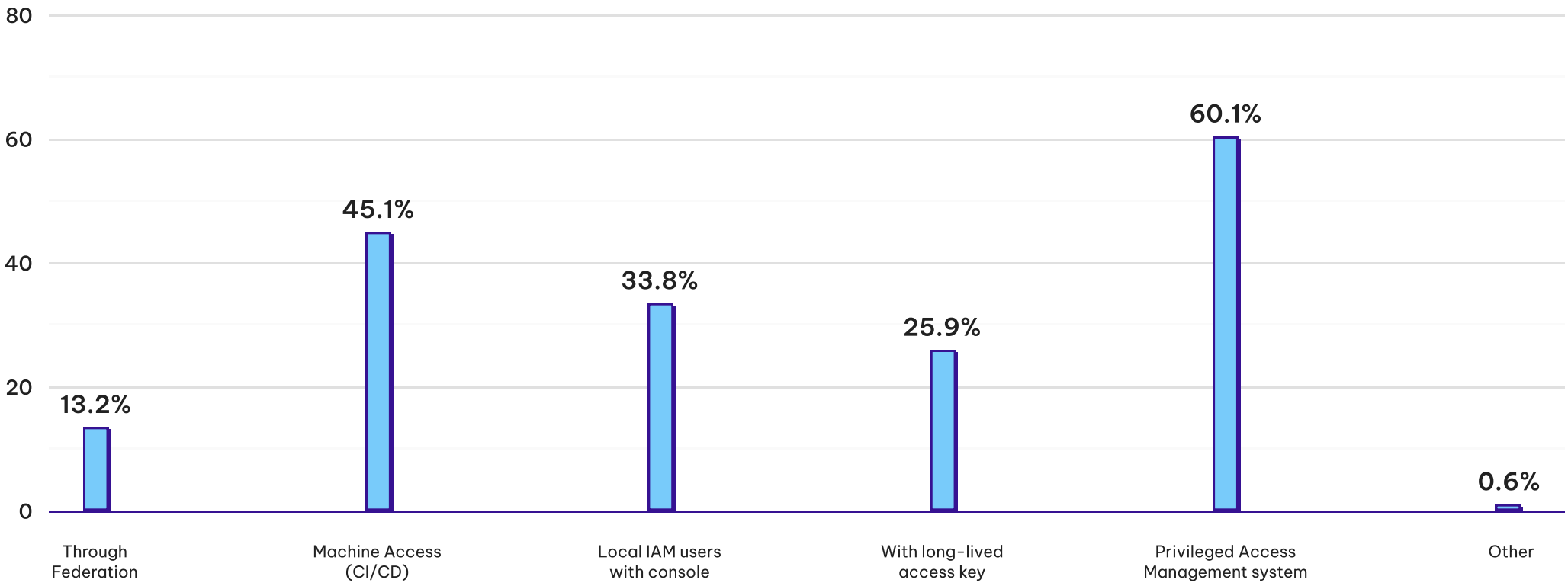
Our survey also found that managing identities across on-premise and cloud environments continues to be a challenge for many enterprises. Over 80% of the respondents manage at least 1,000 identities across their cloud environment. Roughly 44% of the respondents are managing at least 5,000 identities across both environments. The number of identities many organizations are managing across authentication boundaries in the cloud, in federated environments where actions are performed through shared credentials and roles makes identifying change attribution difficult.

Please select all the following ways those identities are accessing your environments: (Select all that apply)




| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Through Federation | 24.1% | 122 |
| Machine Access (CI/CD) | 57.3% | 290 |
| Local IAM users with console | 46.4% | 235 |
| With long-lived access key | 37.7% | 191 |
| Privileged Access Management system | 70.0% | 354 |
| Other | 0.6% | 3 |

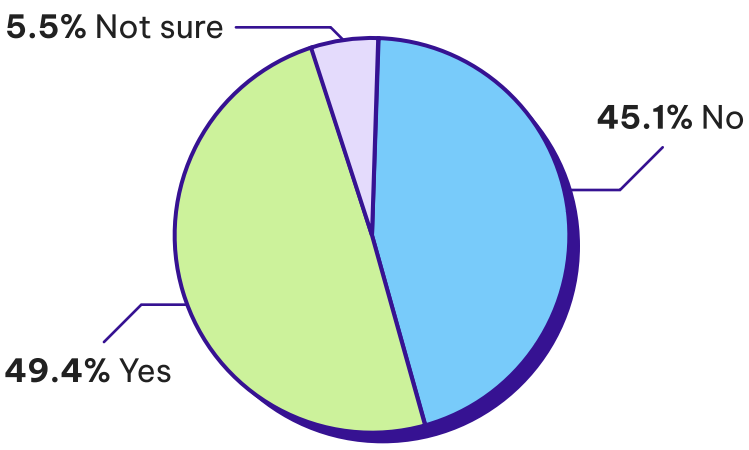
Of the access paths that were selected in the question above, select those that you have full visibility into access activity for (Select all that apply)




| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Through Federation | 13.2% | 67 |
| Machine Access (CI/CD) | 45.1% | 228 |
| Local IAM users with console | 33.8% | 171 |
| With long-lived access key | 25.9% | 131 |
| Privileged Access Management system | 60.1% | 304 |
| Other | 0.6% | 3 |

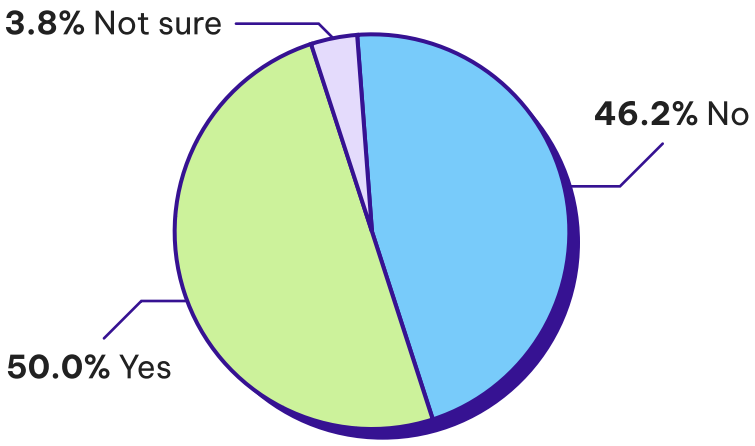
With the growth of the cloud has also come a variety of different access patterns with which users (both human and machine) are accessing those environments. While 25% of the respondents use federation to access their cloud environment, only a little more than half of them have full visibility into the access activity of those federated users. Our survey showed that nearly half (46.4%) of respondents allow console access via local iam users, which presents numerous security risks and violates some enterprise security policies. Of those respondents, more than 25% of them do not have full visibility into the activity of those users. Additionally, 38% of respondents also stated that they leverage long-lived keys to grant access into their environment, but almost a third of them (31.5%) do not have visibility into how those keys are being used for access into their environment. Long lived access keys can present a security risk to organizations and are more prone to being compromised the more they age. The 506 individuals that responded to the survey accounted for 1195 total types of access paths into their environment, meaning that on average, the respondents had 2.3 different ways users were access their environment. In 904 out of those 1195 total identified access paths, the respondents had full visibility into the access activity of those respective access channels, meaning almost 1 out of 4 have access paths which they have no visibility into.

Has there ever been unauthorized access into your cloud environment via a compromised credential?




| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Yes | 49.4% | 250 |
| No | 45.1% | 228 |
| Not sure | 5.5% | 28 |

Have you ever experienced a data breach as a result of unauthorized access to your cloud environment?



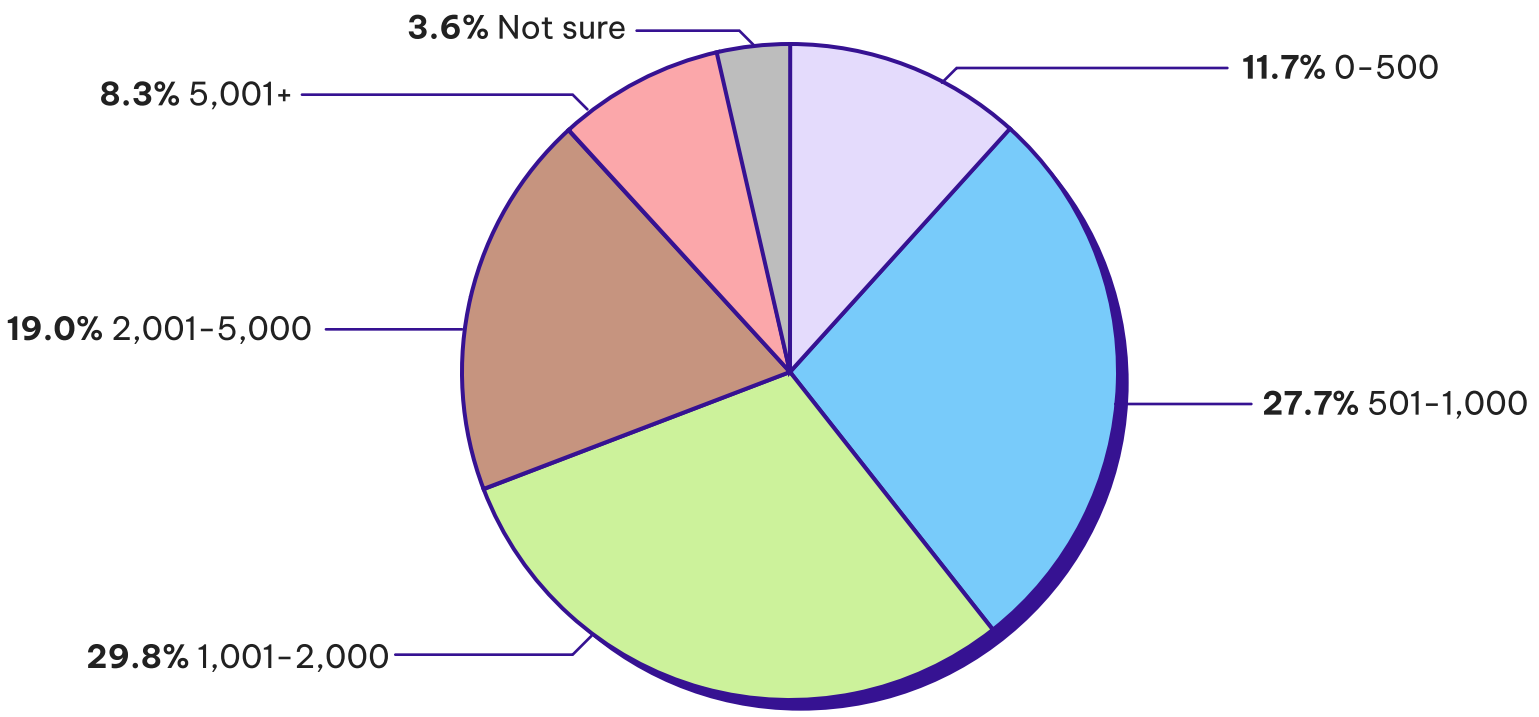

| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Yes | 50.0% | 253 |
| No | 46.2% | 234 |
| Not sure | 3.8% | 19 |

Cloud breaches continue to be both a concern and a reality for many organizations. According to the CyberSecurity Insiders 2022 Cloud Security report, 58% responders said that unauthorized access was one of their top three cloud security challenges. Similarly, The SANS 2022 Cloud Security survey, 50.8% of their respondents expressed concern about unauthorized access by outsiders and more than half (28.4%) realized that concern during the year.

Out of over 500 security and engineering practitioners who completed our survey, just about half (49.4%) said they have experienced unauthorized access in their cloud environment via a compromised credential. 5.5% unable to say confidently one way or the other. According to Verizon's recent 2022 Data Breach Investigations report, 61% of all breaches now involve compromised credentials. In our 2022 End of Year Observations Report, all of the incidents we detected and responded to were a result of a compromised credential.

Exactly half of the respondents said they had suffered a data breach as a result of unauthorized access to their cloud environment, with another 3.8% not sure.

How many keys/tokens do you manage across your cloud environment?

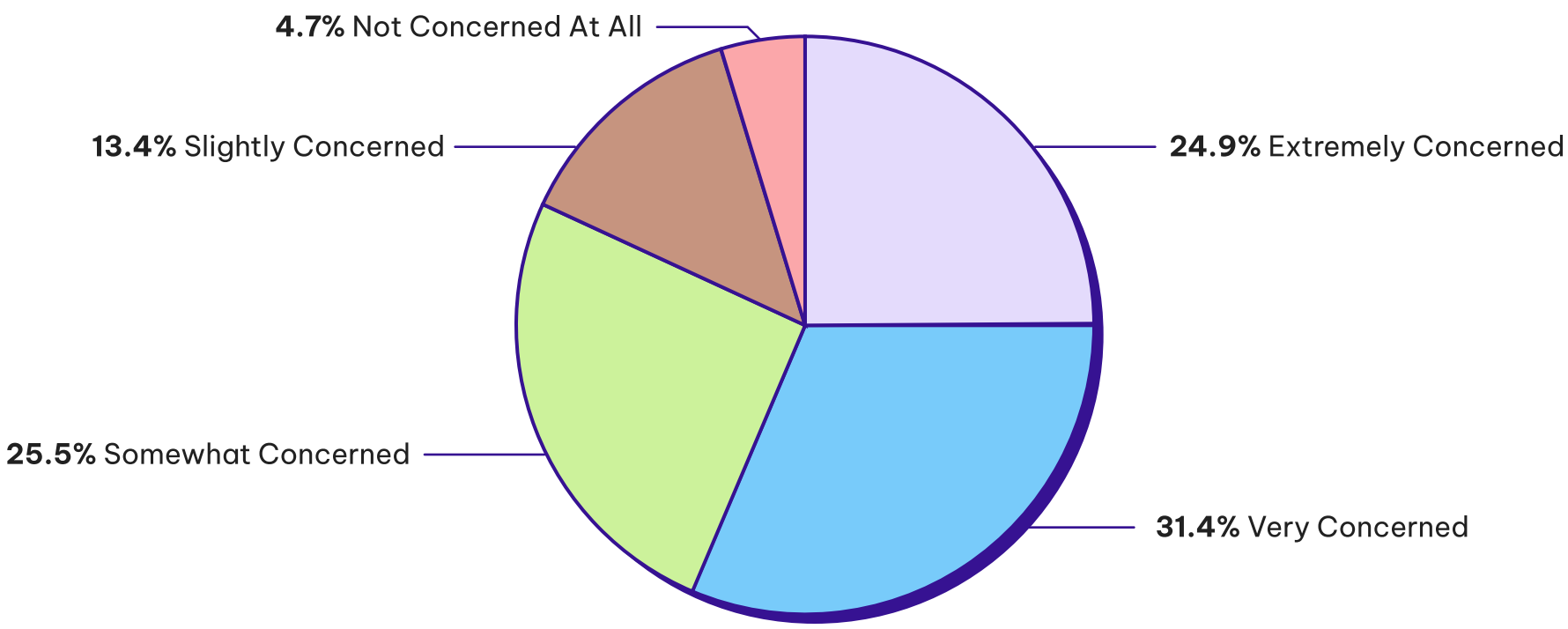



| VALUE | PERCENT | RESPONSES |
|---|---|---|
| 0-500 | 11.7% | 59 |
| 501-1,000 | 27.7% | 140 |
| 1,001-2,000 | 29.8% | 151 |
| 2,001-5,000 | 19.0% | 96 |
| 5,001+ | 8.3% | 42 |
| Not sure | 3.6% | 18 |

As the number of API driven ecosystems like CI/CD pipelines, data lakes and microservices grow, so do the number of secrets (keys/tokens/certificates) organizations need in order to secure the connections between applications and services. The explosive growth of APIs and corresponding secrets has meant that secrets are being leaked across development and deployment systems at an alarming rate. Over 60% of those we surveyed manage at least 1,000 API secrets across their cloud environment, and a little over 30% (30.9) manage at least 2,000 API secrets in their environment.

According to Apiiro's 2022 Secrets Insights, there are 3.28 secrets in each code repository on average, and .72% of repos have secrets that are public. The increase in the number of API secrets has attributed to the increase in the number of those API secrets that are getting leaked into the hands of threat actors. According to Corsha's State of API Secrets Management 2023, 53% of those surveyed said they had experienced a data breach to networks or apps due to compromised API tokens.

How concerned are you that your current tools and teams may not be able to detect and respond to a security event in your cloud environment?

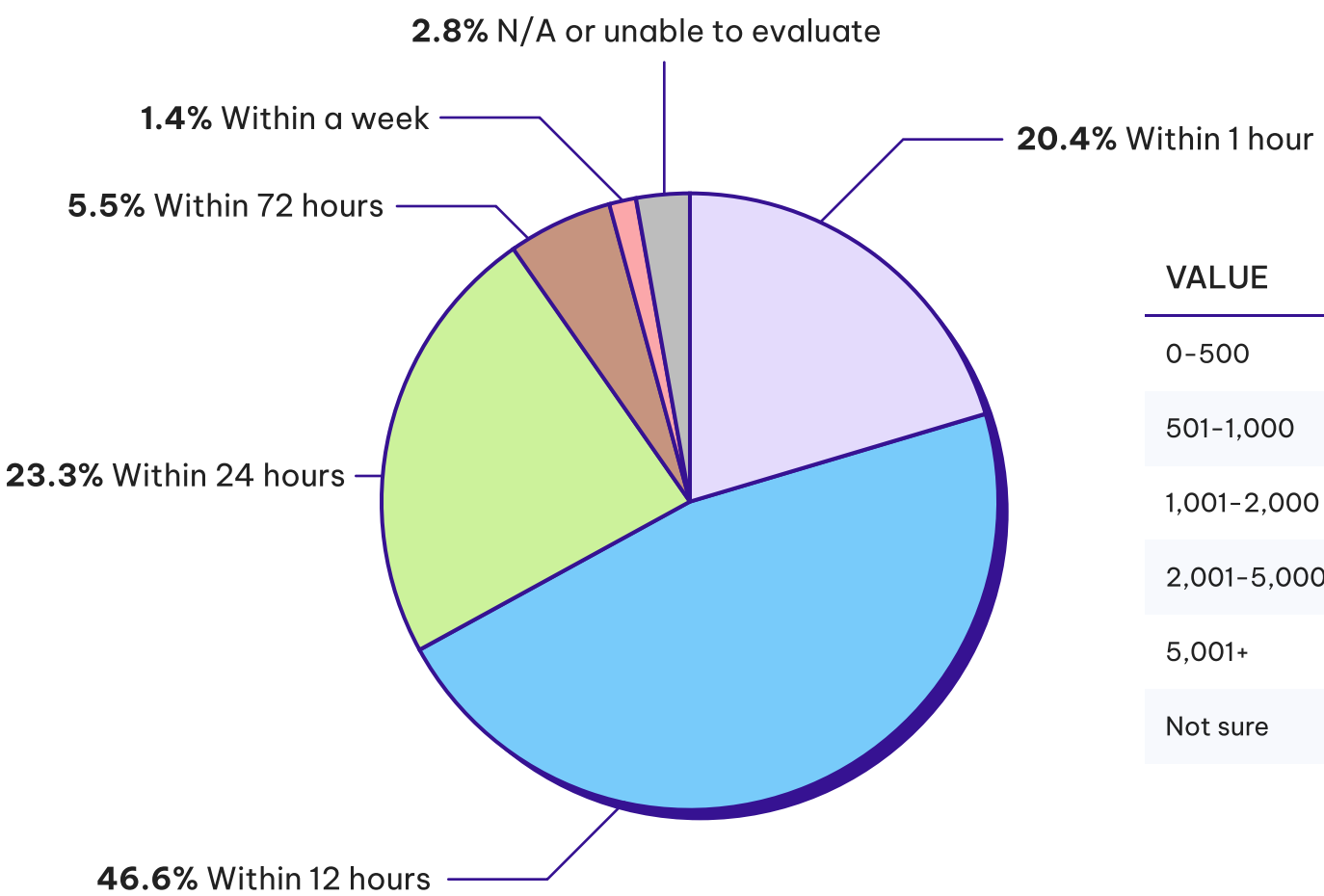



| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Extremely Concerned | 24.9% | 126 |
| Very Concerned | 31.4% | 159 |
| Somewhat Concerned | 25.5% | 129 |
| Slightly Concerned | 13.4% | 68 |
| Not Concerned At All | 4.7% | 24 |

Many organizations have come to realize that many of the security tools and techniques that served them well in the data center don't translate well to cloud and consequently, the concern they have secure the workloads in their cloud environments is rampant across many organizations globally. 95% of the respondents expressed concern that their current tools and teams may not be able to detect and respond to a security event in their cloud environment. More than 55% described their level of concern as 'extremely concerned' and 'very concerned'.

Similarly, ****99% of the respondents to the 2022 CyberInsider's Cloud Security Report expressed some degree of concern about the security of their public cloud environments.

What best describes how quickly would you be able to detect and replay the attack sequence if a threat actor were to gain access to your cloud environment?




| VALUE | PERCENT | RESPONSES |
|---|---|---|
| 0-500 | 11.7% | 59 |
| 501-1,000 | 27.7% | 140 |
| 1,001-2,000 | 29.8% | 151 |
| 2,001-5,000 | 19.0% | 96 |
| 5,001+ | 8.3% | 42 |
| Not sure | 3.6% | 18 |

Many respondents (>90%) claimed that their dwell time in a cloud based attack would be within the first 24 hours. Even the most mature security teams globally have constantly struggled to reduce this number below a few weeks and it continues to be one of the most important metrics teams use to measure the effectiveness of their team around detecting and resolving breaches.

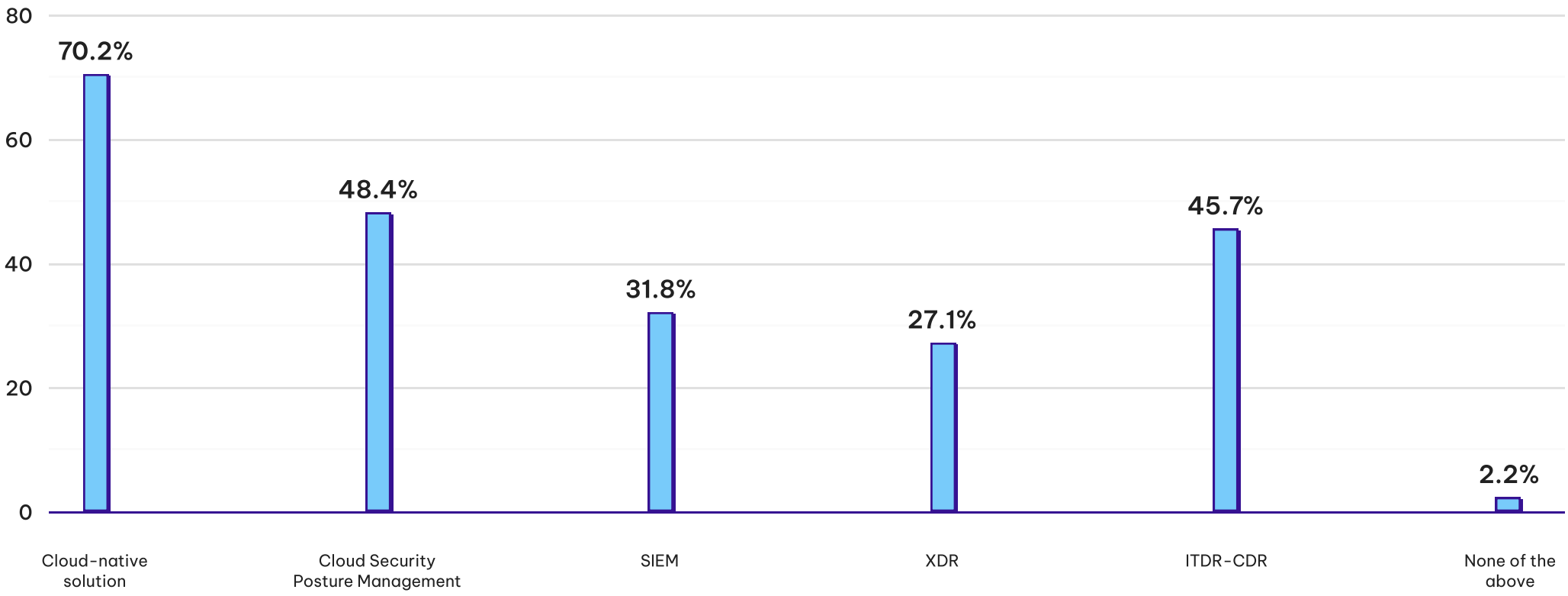
Actual data on attacks in cloud environments via Unit 42 and Google's Cybersecurity Action Team is showing something completely different. While much of the data in this report is based on anecdotal data, either through our survey or other industry partners, Unit 42 and Google provide the unique opportunity of publishing data based on their findings within customer environments across tens of thousands of customers.

According to a Unit 42 Cloud Threat Report (V7), on average, it takes 145 hours (approximately six days) for a security alert to be resolved. 60% of organizations take longer than four days to resolve a security alert. This data was derived from Palo Alto Networks observing the workloads in 210,000 cloud accounts, subscriptions, and projects over 1,300 organizations across all major CSPs.

According to Google's Cybersecurity Action Team, global median dwell time, which is calculated as the median number of days an attacker is present in a target's environment before being detected, was 16 days in 2022. This data is derived from more than 1,000 incidents that the Mandiant team responded to over the course of the last year.

At Permiso, this tells us there is a profound disconnect between an organization's perception on their ability to prevent, detect, and respond to threats versus the the reality of how long it takes to respond to those threats. While organizations have a perception that they are able to detect and replay an attack sequence in their environment within 24 hours, the actual data in real cloud environments is showing something very different. This false sense of confidence in an organization's security programs can be very dangerous and lower the vigilance required by security teams to properly protect their environment.

Please select all of the following tools your organization uses to help detect and respond to security incidents in your environment. (Select all that apply)

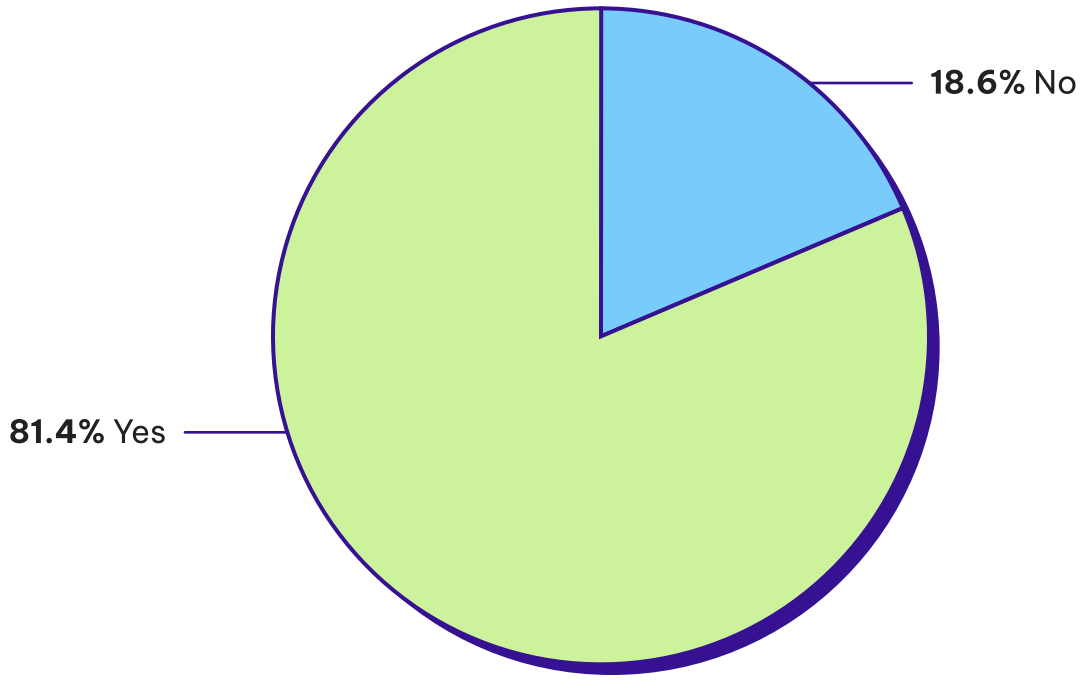



| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Cloud-native solution (AWS GuardDuty/GCP Chronicle/Azure ATP) | 70.2% | 355 |
| Cloud Security Posture Management (Wiz/Lacework/Orca/Prisma) | 48.4% | 245 |
| SIEM (Splunk/SumoLogic/Datadog/Snowflake) | 31.8% | 161 |
| XDR (Extended Detection and Response) | 27.1% | 137 |
| ITDR-CDR (Identity Threat Detection and Response or Cloud Detection Response) | 45.7% | 231 |
| None of the above | 2.2% | 11 |

While there has been more of a collaboration between developers and security professionals to secure cloud environments, so has the amount of tooling required to help secure the ever-expanding attack surface. But more collaboration and tooling hasn't necessarily equated to more secure environments or even increased visibility. According to Palo Alto Network's State of Cloud Native Security Report for 2022, 77% of organizations struggle to identify what security tools are necessary to achieve their objective and 76% of respondents say the number of cloud security tools they use create blind spots.

Additionally 75% of those that completed Google's Cybersecurity Action Team State of Cloud Threat Detection and Response Report said their security team's cloud-specific knowledge is limited and needs to grow. As our survey shows, the two biggest categories of tools adopted in the cloud are those that are offered by the cloud providers themselves and cloud security posture management solutions. Many organizations are leveraging a combination of these cloud-native tools, in addition to CSPMs and SIEMs as a set of solutions in order to help ensure their workloads they are deploying are secure and compliant, and are querying logs to help detect potential threat actors in their environment.

Do you feel like your current tooling is sufficiently covering your organization from a well-orchestrated attack on your cloud environment?




| VALUE | PERCENT | RESPONSES |
|---|---|---|
| Yes | 81.4% | 412 |
| No | 18.6% | 94 |

Despite a majority of respondents expressing concern over their current tools and teams ability to to detect and respond to a security event in your cloud environment, they do have a sense of confidence that their current tooling would sufficiently cover them from a well-orchestrated attack. Despite the fact that they may not have confidence in the tooling that might detect or help them respond to an attack, they feel their resources are configured in such a way to thwart most attacks from ever happening.

More than 80% of respondents claimed they feel their current tooling is sufficiently covering their organization from a well-orchestrated attack, but the rate at which organizations' cloud environments have been compromised (49.4%) would indicate the tooling is not sufficient against sometimes the most basic attacks.

Additionally, Google's Cybersecurity Action Team State of Cloud Threat Detection and Response Report found that 68% of total respondents, including 72% of practitioners, say their existing tool stack doesn't do enough to cut down on the time it takes to investigate threats