SANS

Analyst Program

Survey

SANS 2022 Cloud Security Survey

Written by Dave Shackleford

March 2022

sysdig

Executive Summary

Over the past several years, we have seen more and more examples of vulnerabilities in cloud assets, cloud service provider outages, sensitive data disclosure, and breaches involving the use of public cloud environments. Some examples of security issues in the cloud in 2021 include:

- Amazon Web Services (AWS) experienced a number of significant outages that rendered many websites and online services unavailable. More than three critical outages occurred, leading to well-known sites like Roku, Delta Air Lines, Disney+, and others being unavailable for hours.
- Microsoft notified some of its Azure App Service customers that a serious security vulnerability (dubbed "NotLegit") had caused the exposure of hundreds of source code repositories. This vulnerability meant that customers could unintentionally configure the local `.git` folder to be created in the publicly accessible content root of the Azure App Service containers, which would put them at risk for information disclosure. Wiz, a cloud security firm, announced the issue in late December.

The 2021 Data Breach Investigations Report[1] from Verizon, released in the second quarter of 2021, noted that compromised external cloud assets were more common than on-premises assets in both incidents and breaches. Many attacks targeted credentials that were then used to access cloud-based collaboration and email services, as well.

Even with these types of security issues, we continue to see rapid growth in moving workloads to the cloud, building new applications in the cloud, and subscribing to a wide range of SaaS and other cloud services. The goal of the SANS 2022 Cloud Security Survey is to provide additional insight into how organizations are using cloud today, the threats security teams are facing in the cloud, and what we are doing to improve security posture in the cloud, as well. This year, we again had several hundred respondents, who represented a number of industries. Figure 1, seen on the next page, provides a snapshot of the demographics for the respondents to the 2022 survey.

[1] www.verizon.com/business/resources/reports/dbir/

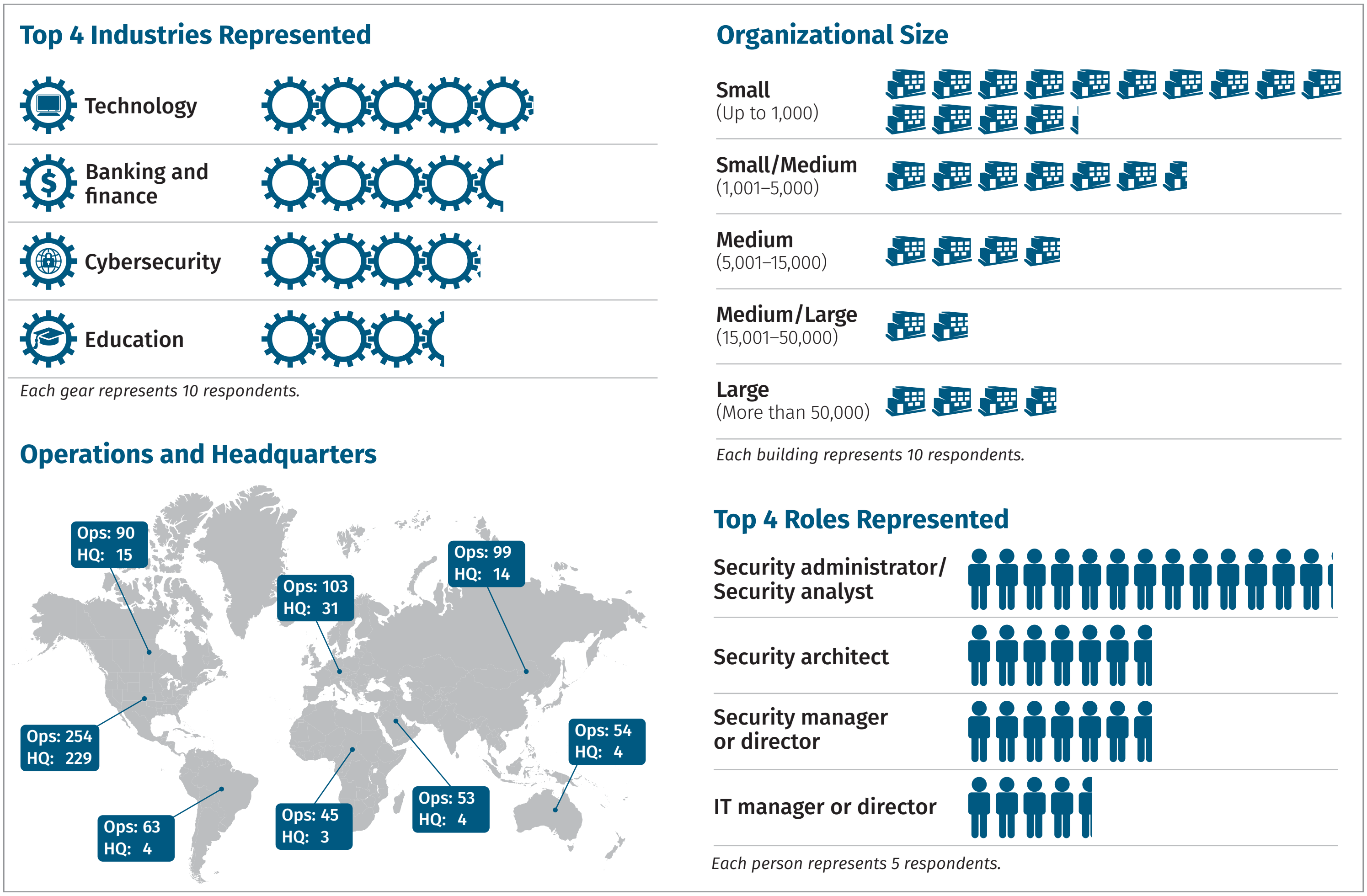


Figure 1. Demographics of Survey Respondents

In our 2021 survey,[2] some of the top takeaways included the following:

- In 2021, serverless took the second spot in security automation technologies (behind infrastructure as code [IaC]), beating security orchestration platforms.
- Our respondents in 2021 noted significantly more emphasis on the integration of cloud SIEM and event management, in addition to IR and forensics tools.
- Only 18% of 2021 respondents stated that they were frustrated by trying to get low-level logs and system information for forensics, a significant decrease that likely shows advancements from the cloud providers.

What stands out in 2022? Here are some of the key findings from this year:

- Serverless has overtaken IaC to become the first spot in security automation technologies, again beating security orchestration platforms.
- Over half of respondents are synchronizing in-house identity directories to cloud-based directory services for more capable cloud identity management and account control.
- In a surprising change from 2021, a greater number of respondents stated (once again) that they are frustrated by trying to get low-level logs and system information for forensics. This unusual increase could indicate higher log volume, issues with provider integration, or something else.

Let's explore what we heard from the community in 2022.

[2] "SANS 2021 Cloud Security Survey," April 2021, www.sans.org/white-papers/40225/ [Registration required.]

Cloud Usage Patterns

We asked the community what cloud applications they are using today and again see (for the third survey in a row) that business apps and data top the list, at 68%. After ranking fourth in the 2021 survey, backups and disaster recovery is now the second most popular category (57%), likely driven by ransomware attacks. Security services (54%) and storage and archiving of data (42%) are popular again this year, also potentially due to the growth in both cloud usage and ransomware attacks, as well (see Figure 2).

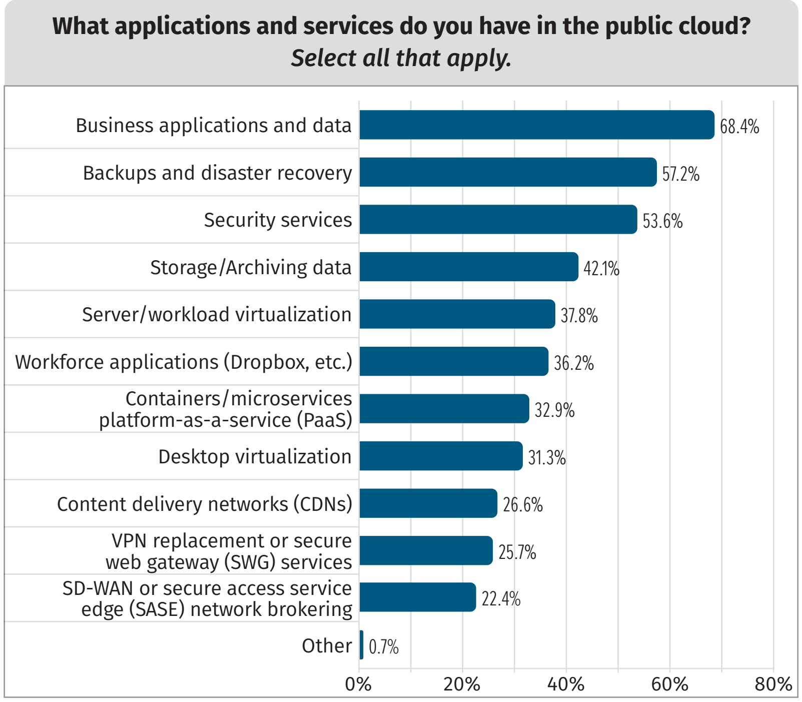


Figure 2. Cloud Applications in Use

This year's survey also shows a consistent response in the number of public cloud providers organizations are using. In 2019, the highest response category was 2–3 providers, and that number has stayed consistent. Smaller organizations are still hesitant to move into multi-cloud deployments, and only a small number of organizations are using more than 20 cloud service providers, consistent with our last survey, as well. It is interesting to note that in 2021, only 3% of organizations were using 11–20 providers, whereas that number has jumped up to 9% in 2022. Just over 16% were using 4–6 providers in 2021, and that number has increased to 23% in 2022 (see Figure 3).

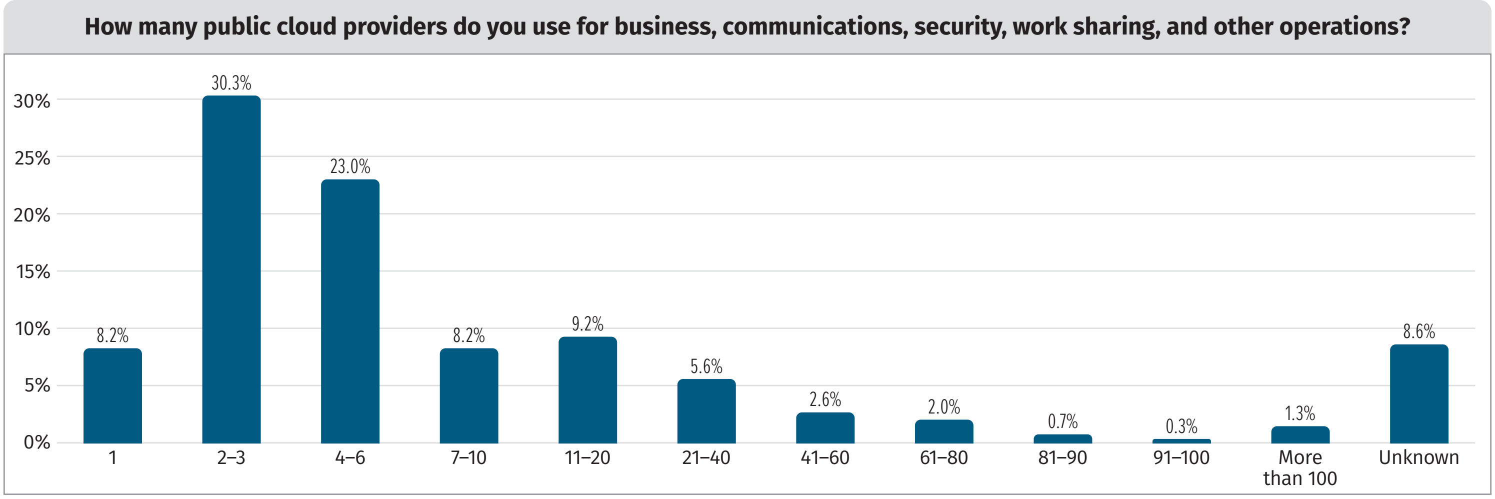


Figure 3. Number of Cloud Providers in Use

With the increase in the use of cloud applications and multi-cloud implementations, particularly those oriented toward end users, we wanted to find out if organizations are adopting new tools like cloud access security brokers (CASBs) and identity federation platforms to help centralize control. Many respondents indicated that they are using CASBs (53%), a significant increase over 43% in 2021). Quite a few of respondents' organizations are leveraging cloud network access services (49%), and many are also using federated identity services to help centralize user access and authorization into cloud applications (46%). Not as many organizations had adopted a multi-cloud broker to centralize access to platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), and other service provider environments, but the number grew from 18% in 2021 to 25% in 2022. The newer category of secure access service edge (SASE), which combines numerous security services into a central brokering model, is gaining traction with adoption by 18%. This makes sense. We need new services that can help centralize user access and identity, and also implement user-oriented policies for monitoring activity and protecting data (CASBs) as cloud application use grows.

Concerns, Risk, and Governance in the Cloud

As with past SANS surveys focused on cloud security, we asked what kinds of sensitive data organizations are hosting in the cloud today. Business intelligence (46%) has fallen to third place, down from second place last year. The top data type in 2022 is financial business records at 54%, compared to 2021's top result of employee records at 53% (now in second place at 49%). Overall, while the types of data changed a bit, the general trend here is highly similar to what we have observed previously. Roughly one-half of organizations are willing to put a variety of sensitive data types in the cloud, with lower percentages of some types of data that are more regulated (customer payment card information at 22% and healthcare records at 23%, for example). See Figure 4.

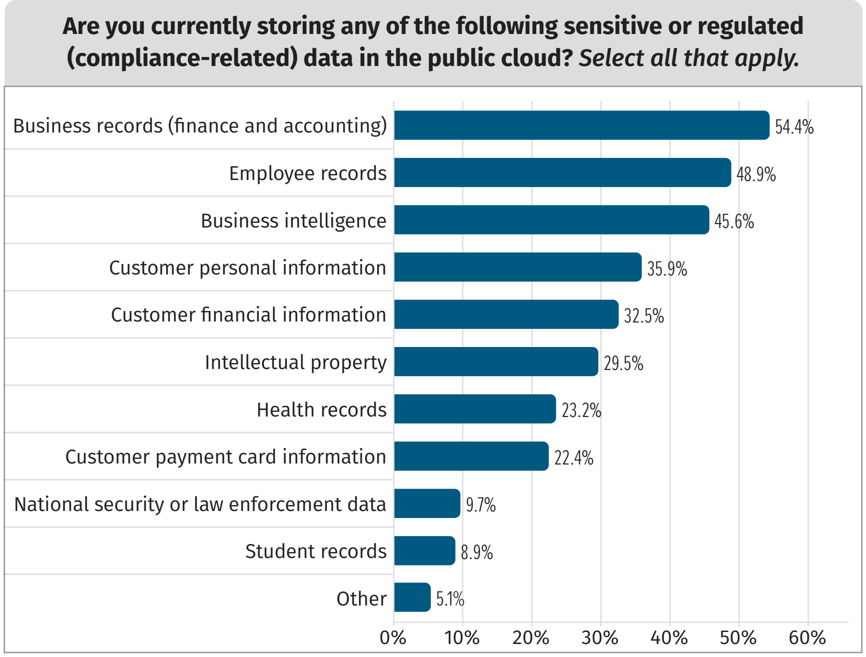


Figure 4. Sensitive Data in the Cloud

We asked whether privacy regulations like the GDPR are impacting existing or planned cloud strategies, and close to two-thirds (62%) stated that they are (up from 55% in 2021). For some data types, especially consumer personal data, organizations would need to ensure that their cloud providers could adequately meet privacy compliance needs. This increase from last year is likely to continue.

Every year, we ask security professionals to identify their biggest concerns in the cloud and whether any of those concerns had actually been realized in the previous year. In the last several years, unauthorized access to data by outsiders topped the list of concerns. This year, we see some significant shifts in responses, with unauthorized access coming in fourth (51%), behind unauthorized application components or compute instances (54%), poorly configured interfaces and APIs (52%), and inability to respond to incidents (51%). This shift shows that organizations are becoming more comfortable with locking down cloud environments, but now are more concerned with shadow IT and configuration errors/issues than in the past.

The biggest realized issues are downtime or unavailability of cloud services when needed (32%), lack of skills and training (31%), and unauthorized access by outsiders (28%). The realized issues are consistently seen across the industry and have been for some time. Why the disconnect on organizations' biggest concerns? We speculate that lack of familiarity with and visibility into cloud APIs and application components may be fueling more concern as cloud environments grow and become more complex, even if there's no clear relationship to intrusions. Intrusions are happening, however, and the heightened concern about respondents' inability to manage intrusion scenarios is likely to continue. See Figure 5 for the full breakdown of concerns and actual incidents.

Most respondents (62%) believed that remote work scenarios increase the risks and threats to cloud deployments, while 29% indicated they do not and roughly 10% are not sure. Among those respondents who felt the risk increased, the biggest risk reason they identified for the increase is a perceived lack of oversight and monitoring capability (35%), followed by remote user compromise (33%). In 2021, almost 43% of respondents felt that remote user compromise increases risk, leading SANS to believe that many organizations are more concerned about remote user compromise than ever. Other risk increases are attributed to configuration errors and issues (29%) and immature controls and processes (20%). Respondents also noted the critical nature of availability due to the negative impact to the remote workforce with provider outages as well as managed service providers trying to apply traditional on-prem security approaches to cloud environments.

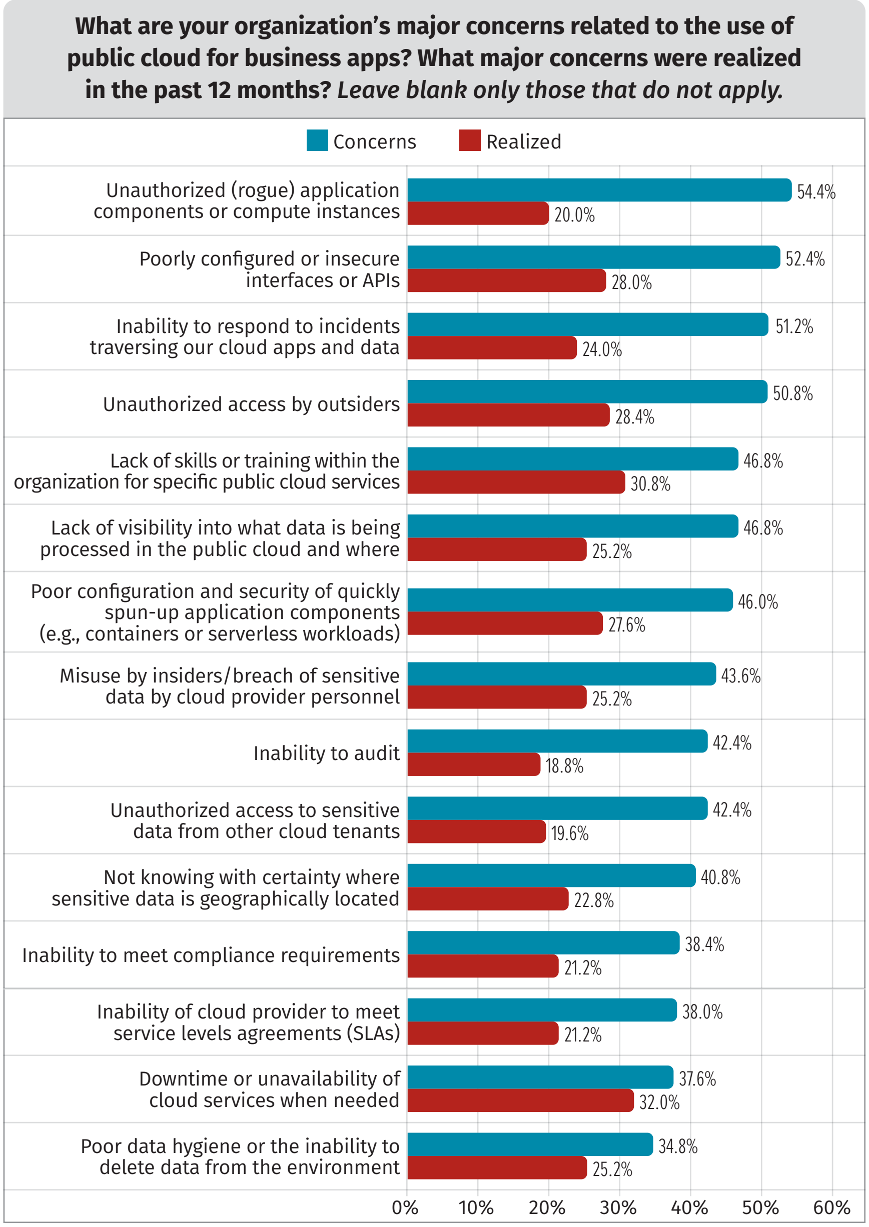


Figure 5. Concerns and Incidents in Cloud Today

The use of the cloud always raises concerns regarding breaches but, despite concerns, do results show an increase in cloud breaches over the past 12 months? Well, the percentage of known breaches remains largely unchanged. Approximately 19% of respondents indicated that they did experience a breach, almost identical to 2021 results. This percentage could be higher because more organizations are unsure now than in the past. In 2021, 65% of respondents said that they were unaware of an actual breach, but that number has decreased significantly to 53% in 2022, with another 21% suspecting they might have been breached but cannot prove it (as compared to 17% in 2021).

For several years, we've looked at what is involved in the successful attacks, and the top responses this year are account/credential hijacking (45%) and misconfiguration of cloud services/resources (43%), identical to our last two surveys. In 2021, the third major issue was insecure interfaces or APIs (36%), whereas this year *exploitation* of these APIs is the third biggest problem (34%). DoS attacks decreased in 2022 from 30% to 26% (a minor change, but notable). The entire breakdown of factors involved in cloud attacks is shown in Figure 6.

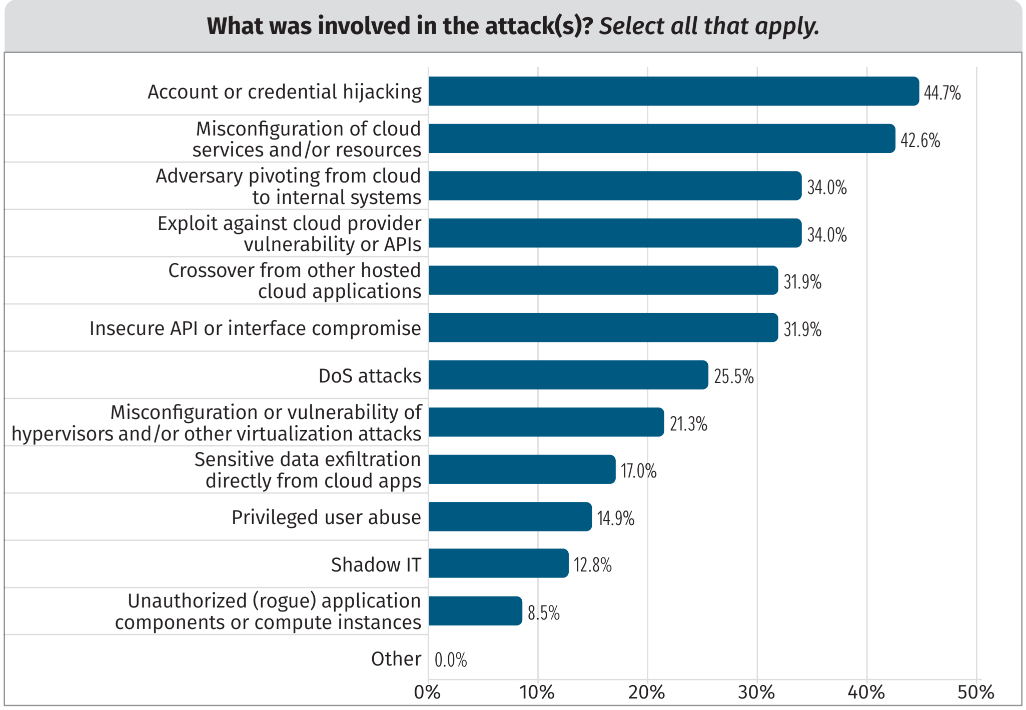


Figure 6. Cloud Attacks

These changes likely reflect the shifting nature of cloud, as well as maturity with the providers and controls available to us. Many control elements are completely managed by public cloud providers, and so the surface area for attacks to this layer is greatly reduced. DDoS attacks still occur, but they don't seem as prevalent in breach scenarios due to improvements in DDoS protection from both public cloud providers as well as third-party services that have grown in popularity over the past several years. We're still not protecting credentials as well as we should, and misconfiguration of cloud resources remains a major issue.

Security and Governance in the Cloud

As cloud use grows, organizations need to develop and enhance their processes and governance model. This year we see improvement: 77% of organizations have cloud security and governance policies in place today, as compared to 69% in 2021, and the number of respondents who stated that they don't have any policies has decreased from 23% in 2021 to 15% in this survey. This increase in governance shows that organizations are steadily improving and enhancing their governance and policy programs to incorporate cloud security and shared responsibility for controls and processes with cloud providers. Without proper oversight and governance, many cloud programs are consistently plagued with shadow IT, configuration issues, and lack of visibility into what is happening in cloud environments.

In the last several years, organizations have also been steadily implementing some of the most common security controls for cloud deployments, with many controls now also available as security-as-a-service (SecaaS) offerings versus standalone platforms managed in-house or directly in PaaS/IaaS environments. As in 2021, VPN is the most successfully implemented (45%) internally managed tool, but fewer organizations are managing traditional VPNs than previously. Network access controls, vulnerability scanning, and anti-malware were also touted in our last survey as controls that organizations managed well internally, but this year we see an increase in log and event management (also the top hybrid control) and multi-factor authentication, too. The top SecaaS services in this year's survey are multifactor authentication and anti-malware, and there is a dip in CASB implementation. The full breakdown of controls in the cloud is shown in Figure 7.

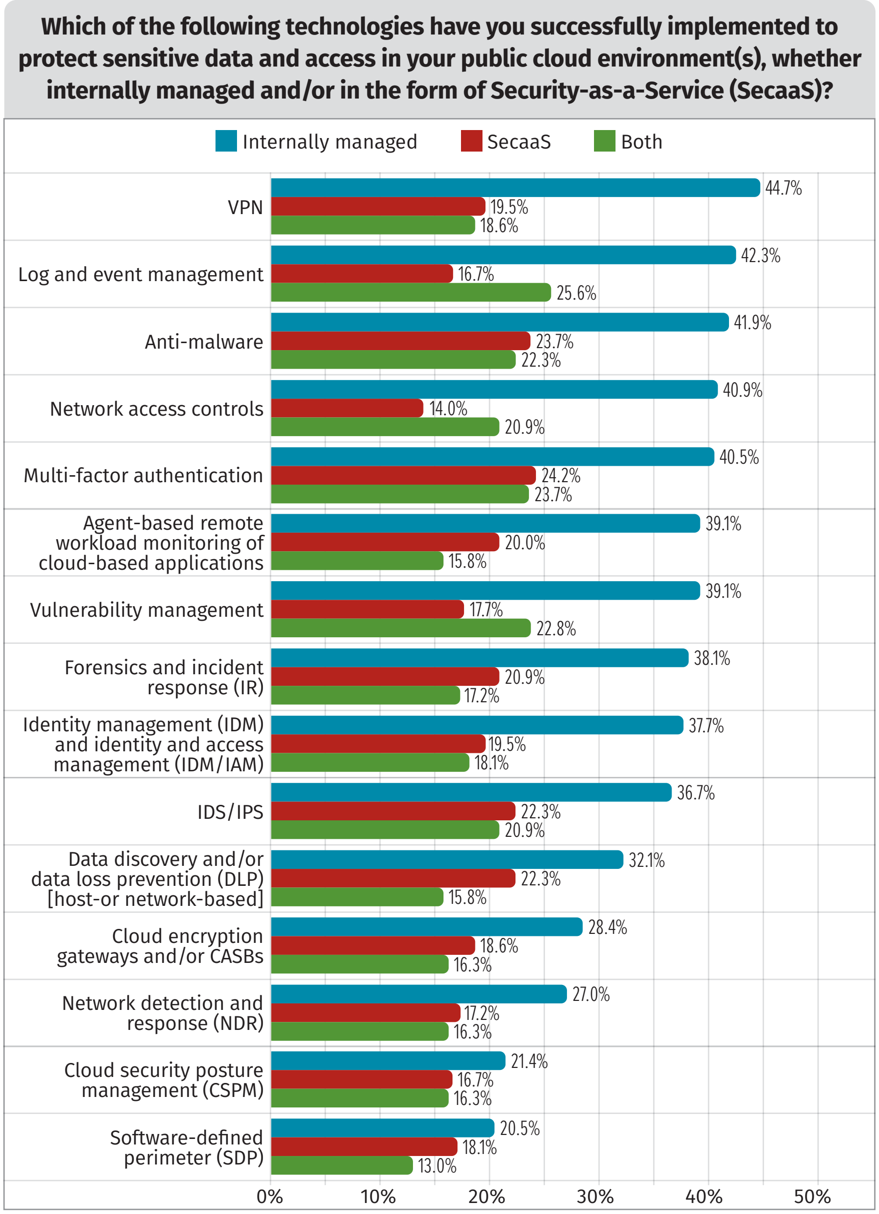
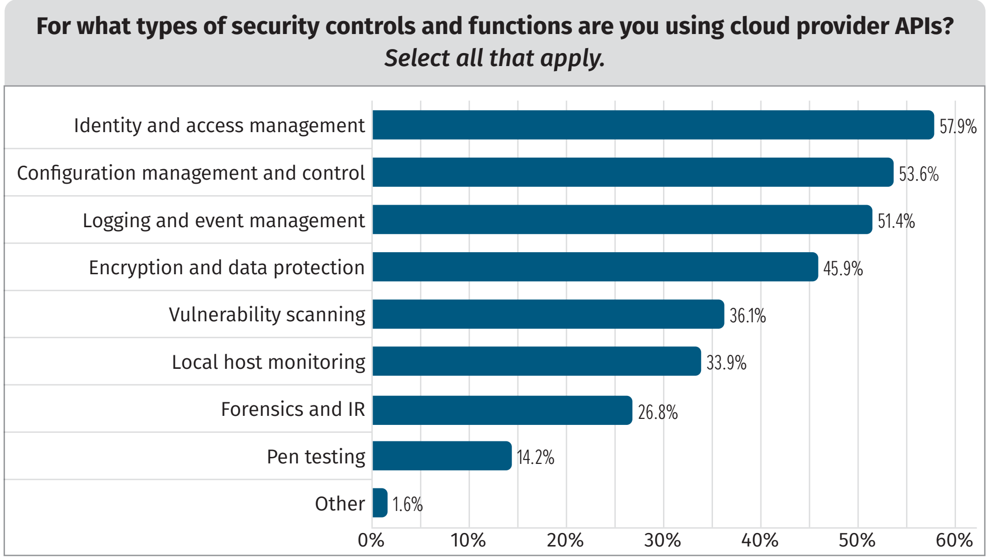

Which of the following technologies have you successfully implemented to protect sensitive data and access in your public cloud environment(s), whether internally managed and/or in the form of Security-as-a-Service (SecaaS)?

Figure 7. Security Controls for Cloud Sensitive Data Protection

These numbers are largely positive, showing an increase in the use of cloud-based SecaaS tooling (most of these services were at a range of 10–15% in 2021, and several are now above 20%) and hybrid options (again, with more than 20% in use). The use and integration of cloud APIs has grown, too. In 2021, 51% of respondents stated they were leveraging cloud provider APIs to implement security controls (a critical element of automation and cloud security maturity), whereas now that number is up to 61%. For those leveraging these APIs, the most common control is identity and access management, followed by configuration management and logging and event management. While these are the same top three categories that we saw in 2021, identity and access management has moved from second to first place. See the full list of API-enabled security controls and functions in Figure 8.

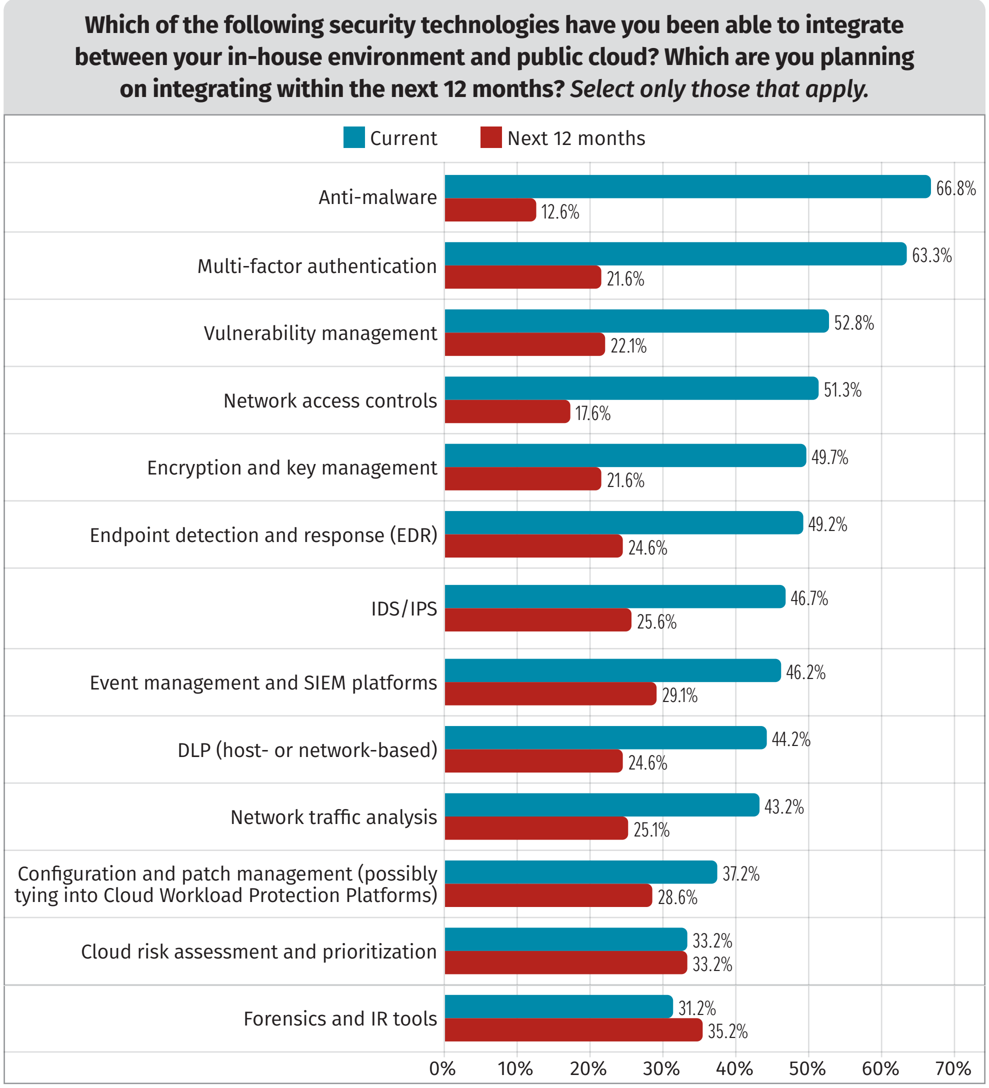


For what types of security controls and functions are you using cloud provider APIs? ***Select all that apply.***

Figure 8. API-Integrated Cloud Security Controls

These numbers suggest that these are the easiest controls and functions to tackle through cloud provider-enabled API capabilities, the most critical for organizations to implement, or both. Collectively, these numbers are similar to 2021, though, and while generally positive, it still shows that only half of organizations make use of the APIs provided. This has been somewhat stagnant for several years in a row.

For the most part, organizations are still managing many controls in-house, but this is slowly changing. Organizations have successfully integrated some controls between traditional on-premises deployments and cloud environments, however, creating a hybrid cloud security model. At present, almost 67% of respondents believe that their organizations have successfully integrated anti-malware tools (up from 64% in 2021), 63% have integrated multifactor authentication, and 53% feel that vulnerability management is well integrated in a hybrid model. These results echo the top three technologies from our 2021 survey, demonstrating some maturity in these control areas for the cloud. Approximately 51% of respondents are confident that they've integrated network access controls (up from 47% previously). Other technology areas showing strong hybrid integration include EDR, encryption, and IDS/IPS. The full breakdown of hybrid control integration is shown in Figure 9.



Which of the following security technologies have you been able to integrate between your in-house environment and public cloud? Which are you planning on integrating within the next 12 months? ***Select only those that apply.***

Figure 9. Hybrid Security Control Implementation

We also asked respondents which controls they plan to integrate in the next 12 months. Roughly a third indicated that they plan on integrating forensics and IR tools (35%) and cloud risk assessment tools (33%), a new category for 2022. Event management and SIEM platforms came in third. This indicates more focus on detection and incident response altogether, which has long been an immature control and process area for many teams, but a heightened focus on cloud risk indicates the need for more cloud-centric reporting and controls analysis, too.

Many security teams have struggled to deal with "tool sprawl" over the years, and this is no different when looking to adapt tools and services to cloud environments. We asked whether security teams are finding any success in using the same vendors and technology providers across in-house and cloud environments for various controls. Unsurprisingly, respondents provided some of the same answers categorically as mentioned earlier when expressing confidence in integrating these control areas. Multifactor authentication and anti-malware are both relatively centralized, but EDR lands in a strong third place, up significantly from 2021. This is an indicator that success in implementing hybrid controls is likely linked to vendor products that integrate well in both environments, also providing central management capabilities. One item of note in 2022 is continued commitment to implement centralized configuration and patch management in a hybrid single-vendor model (32% versus 31% in 2021), but no growth, which is surprising to see. See the full list in Figure 10.

Which of the following security technologies have you successfully implemented with a single vendor product or control in both your in-house environment and public cloud? Which are you planning on implementing in the next 12 months? ***Select only those that apply.***

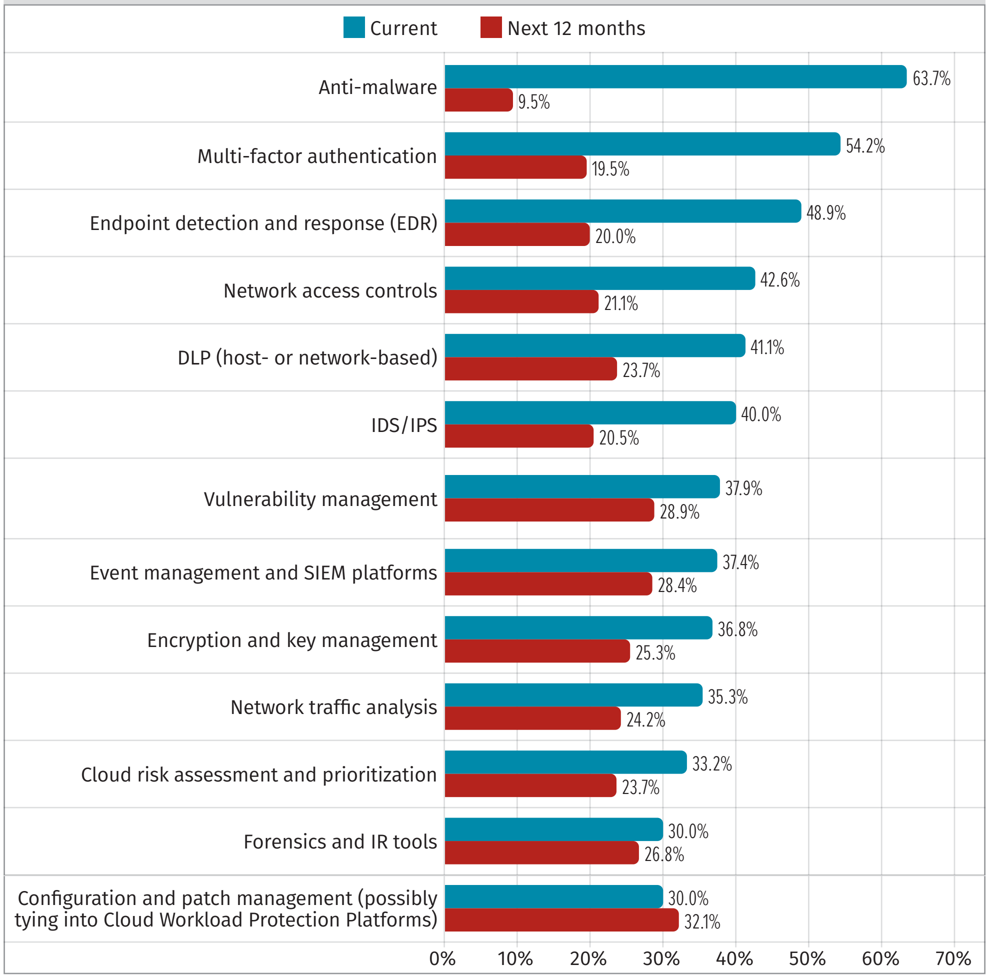


Figure 10. Single-Vendor Control Implementation for Cloud

As in past years, we asked organizations to identify some of their biggest challenges in adapting forensics and IR to the cloud. The top result is once again (for three consecutive surveys) a lack of real-time visibility into events and communications involved in incidents. This likely indicates that organizations are still struggling to get events and insight into cloud activity, a factor that may support the number of organizations planning to focus on SIEM and cloud events in the near future. Other major challenges cited include difficulty in correlating events between on-premises and cloud environments (likely tying into the strong emphasis on SIEM and event management integration) and immature forensics and IR processes. Getting sound forensics evidence is also challenging, but it's interesting to note that in 2021 only 18% stated they had difficulty getting access to log files and system artifacts in the cloud, while in 2022 this has increased to 38%. This number decreased for several years, which seemed to indicate that providers were simplifying log access and event management solutions were more integrated. With this 2022 update, clearly this needs more consideration. The full list of forensics and IR analysis challenges is shown in Figure 11.

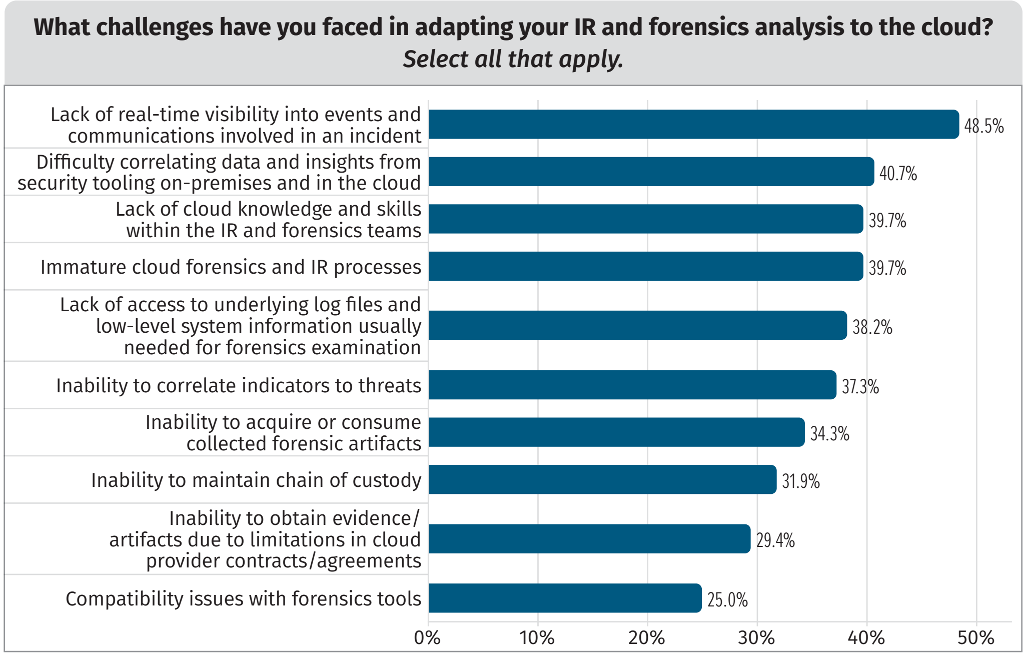


Figure 11. IR and Forensics Challenges in the Cloud

Finally, we asked respondents whether they are using any automation and orchestration tools to improve their cloud security posture. Security teams are increasing the use of automated controls and monitoring tactics, a trend that has been in progress for several years. The most common tools in use in last year's survey were template technologies for implementing IaC (AWS CloudFormation, Azure Resource Manager [ARM] templates, Terraform, and so on). In this year's survey, these IaC tools are still heavily used (54%), but are now superceded by serverless technologies (55%) and tied with security orchestration, automation, and response (SOAR) tools. Overall, the use of automation and orchestration tools has increased across the board, and we expect this trend to continue as organizations improve the speed and efficiency of cloud deployments. See Figure 12 for the full breakdown of automation/orchestration tools/methods in use today.

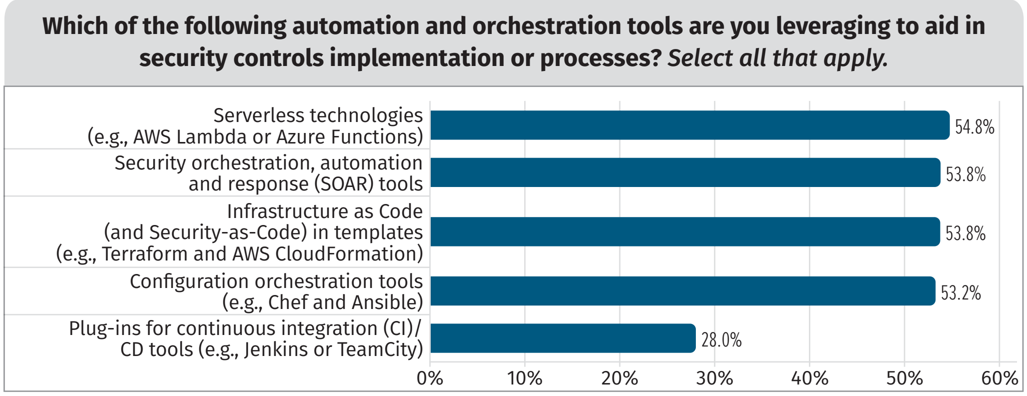


Figure 12. Security Automation and Orchestration Tools and Techniques for Cloud

Cloud IAM

In a new category for the year 2022, we asked the community about how they're addressing one of the most challenging areas of cloud security: identity and access management (IAM). The first area we focused on was responsibility for IAM controls and oversight, asking which team(s) manage this important function. Most indicated that this falls to the information security team (35%), which is not surprising given that a number of smaller organizations responded this year. Answers are fairly even between a dedicated IAM team and collaboration among several teams, with a smaller number handing off this responsibility to DevOps and cloud engineering teams (see Figure 13).

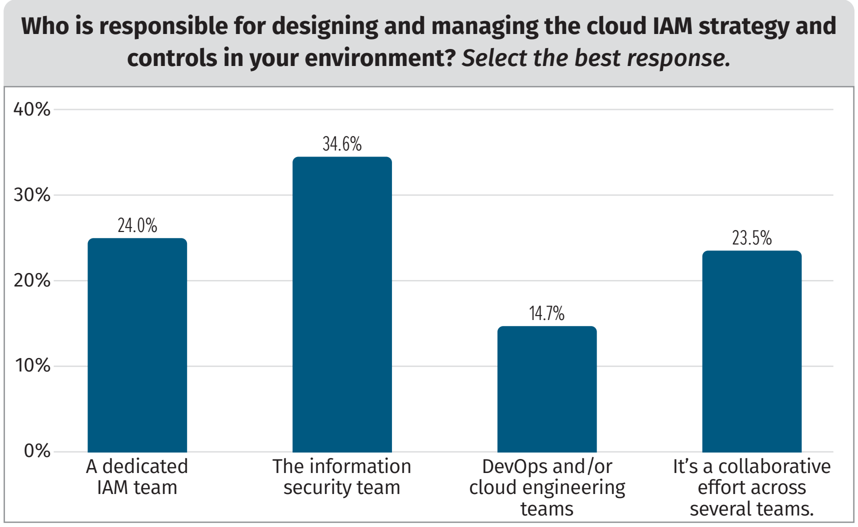

Who is responsible for designing and managing the cloud IAM strategy and controls in your environment? ***Select the best response.***

Figure 13. Cloud IAM Responsibility

Given the importance of identity to cloud implementation (for both end-user services and cloud infrastructure and application deployments), we asked how teams are leveraging identity capabilities and tools in the cloud. More than half (53%) are synchronizing identity stores like Active Directory to cloud directory services, enabling federation to other cloud services and more flexibility in controlling user access to cloud assets. From here, it's a broad mix in terms of IAM use cases. Approximately 38% of respondents are mapping identities to those available from cloud providers, and just over one-third are using identity-as-a-service (IDaaS) for federation and single sign-on (SSO). Others are leveraging in-house identity suites for hybrid cloud integration or making use of IAM policies to control object access and behavior in the cloud (see Figure 14).

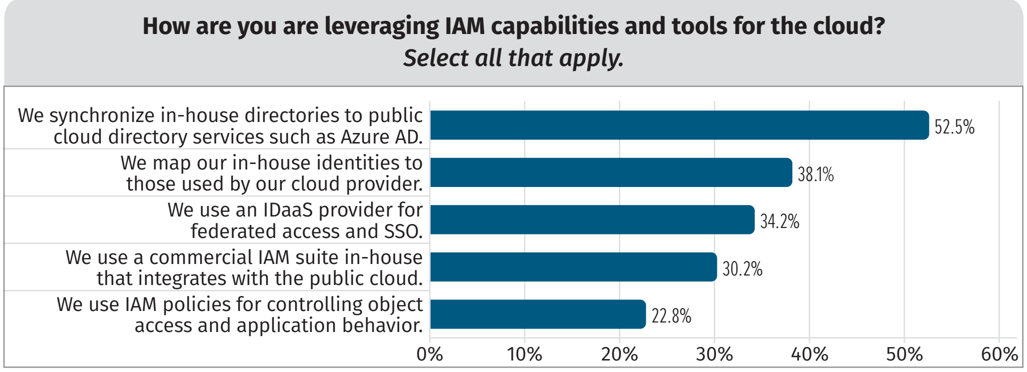

How are you are leveraging IAM capabilities and tools for the cloud? ***Select all that apply.***

Figure 14. Cloud IAM Usage

Based on what we see in the industry, it's surprising to see such low numbers of respondents employing IDaaS for federation, as well as a lack of using IAM policies to control object access and application behavior. For many organizations, these capabilities are mainstays of cloud security programs, and these results don't align with what we see in the community today. Because we don't have data from previous years for comparison, we'll have to track these going forward to determine why this year's statistics don't align with what's happening in the industry.

Finally, we asked respondents to tell us how they're controlling and managing IAM policies in their organization. Given the previous response on use of IAM policies, it's unsurprising that a lower number of respondents answered this question, but those who did primarily rely on native cloud services such as AWS IAM Access Analyzer, manual efforts, or IaC templates to implement and maintain IAM policies. Roughly 25% use third-party tools, and another 20% use open source linting tools, too (see Figure 15).

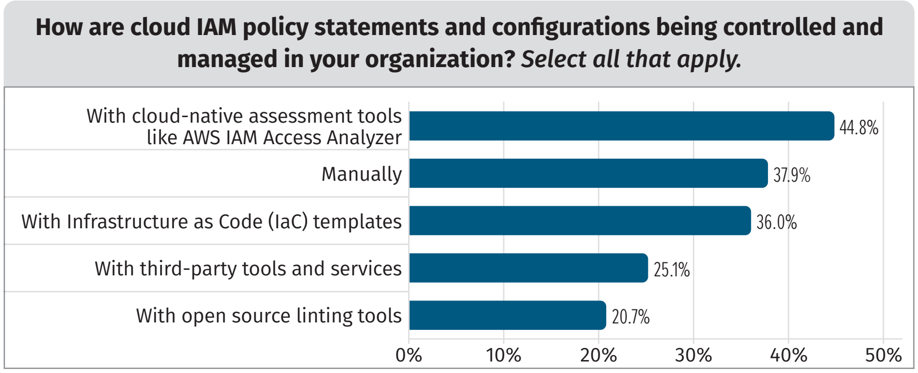


Figure 15. Cloud IAM Policy Management Tools

As we track IAM more specifically in future years, we'll be sure to compare results against this inaugural year.

Conclusion/Final Thoughts

Every year, we conclude the survey by asking participants to provide general feedback on any other trends, concepts, experiences, and issues they've observed in the cloud. This year, many respondents mentioned the need for better automation capabilities to keep pace with the rapidly changing services offered, as well as better centralized tools and services that can be used across more types of cloud service environments. Especially as we shift toward multi-cloud deployments and cloud environments that are geographically dispersed, privacy issues are likely to become a greater concern, as several respondents noted. Many security teams aren't well-versed in cloud concepts, both in design and operations as well as DevOps/automation tools and tactics. There's still the perception that we aren't getting many needed details about security controls and capabilities from the providers, too. A general theme we heard from respondents in this final question was "we need to bake security in earlier rather than later for cloud."

Things are improving in cloud security, both in knowledge level of the managing teams and the tools and services from both providers and vendors in the space. Overall, however, things are not moving quickly. This seems to be a marathon, not a sprint.

Sponsor

SANS would like to thank this survey's sponsor:

sysdig