SANS

Analyst Program

Custom Survey

2022 SANS Survey: Securing Infrastructure Operations

Written by **Matt Bromiley**

March 2022

Cadre information security

Introduction

Every day, organizations are migrating more and more of their infrastructure to cloud providers and cloud-based assets. For business operations, this transition makes sense. Cloud assets are easier to deploy and allow for rapid development cycles. Cloud resources enable an organization to quickly scale to meet operational and/or customer needs.

However, embracing a cloud infrastructure can pose a significant risk to an organization. As more and more cloud assets are spun up, an organization's risk profile grows—sometimes exponentially, depending on the risk profile of cloud assets. Consider, for example, an open storage bucket full of anonymous data versus an insecure web application tied directly into an organization's domain infrastructure. Which situation would you rather face as a security analyst?

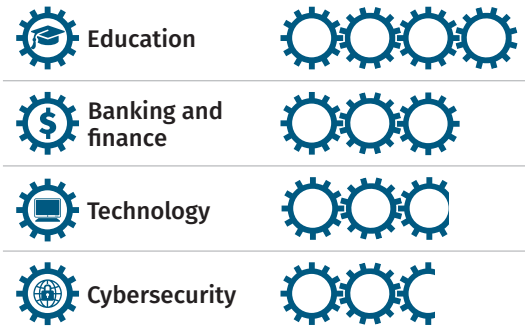
In this survey, our inaugural investigation into this topic, we wanted to tackle this exact issue: What does an enterprise cloud presence look like, and how are our respondents going about securing their assets? A cloud presence is an opportunity for both adversaries and administrators alike—and unfortunately the security team gets left pushing the advantage around the board.

As we read through our survey results, we identified the following notable takeaways for you to consider:

- Enterprise cloud footprints and infrastructure are growing—and security teams are often having trouble keeping up with these changes.
- Approximately 74% of security teams are trained about the differences between cloud and non-cloud security response.
- More than half of our survey respondents have more than 40% of their operations in the cloud.
- Approximately 85% of respondents will be moving even more assets to the cloud, on top of changes already made.
- Most DevOps teams (73%) are required to inform the security team of new risks upon deploying applications.

Finally, as you work your way through this paper, we encourage you to consider how your own organization compares to those of our respondents. Undoubtedly, our respondents included a broad range of cloud deployments and security capabilities, offering a unique viewpoint. The data and statistics from this survey provide a valuable barometer you can use to compare against your own environment and potentially identify where you might need to focus future efforts. Figure 1, on the next page, highlights some of the key demographics from this survey.

Top 4 Industries Represented

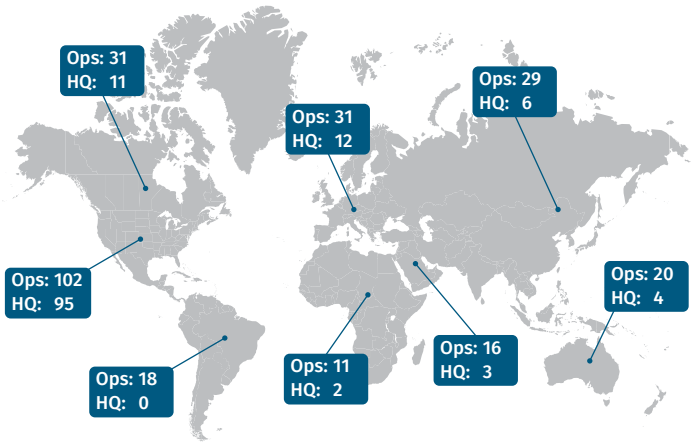


Each gear represents 5 respondents.

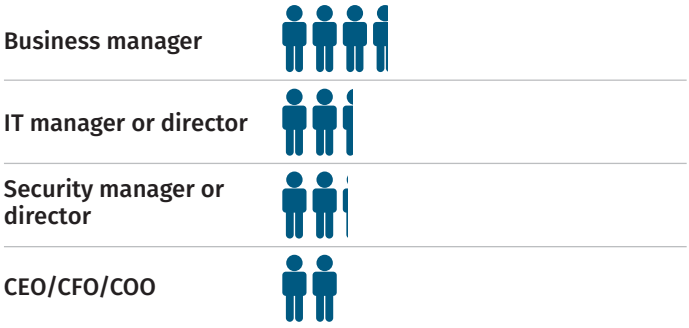
Organizational Size

Each building represents 5 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 5 respondents.

Figure 1. Demographics of Survey Respondents

Building in the Cloud

We began by examining the makeup of our respondents' presence in the cloud. Basic asset identification and visibility are perhaps among the most important starting points for any organization. After all, we cannot protect what we cannot see. We cannot expect administrators or security teams to know of every single asset once it is deployed without having a plan in place of achieving tomorrow.

Adversaries, however, may have the advantage of an asset that has been deployed and inadvertently left insecure—or worse yet, assets that have been deployed and intentionally left out of the visibility of a security team. These Shadow IT (or "Shadow Cloud") assets present a significant risk to an organization.

Visibility of cloud assets begins with an understanding of whether your organization utilizes cloud providers. Approximately 93% of our respondents indicated that any part of their environment is cloud-based. See Figure 2.

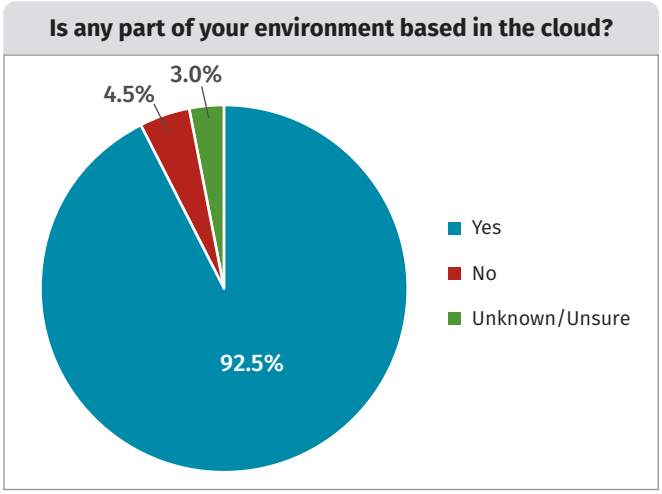


Figure 2. Overall Cloud Usage

Digging deeper, we also asked our respondents to identify which cloud provider(s) are in use within their environment. Figure 3 displays those responses.

Amazon Web Services (AWS) is the leading platform according to just over 56% of respondents. Microsoft Azure took a close second place at 50%, but Microsoft's overall reach may be greater than AWS given that Microsoft Office 365 (one of the most commanding and in-demand applications for businesses of any size) rounds out the top three platforms.

Finally, we drilled down one level deeper to understand what type of services and/or applications organizations are using or deploying in the cloud. Figure 4 provides a breakdown of the results.

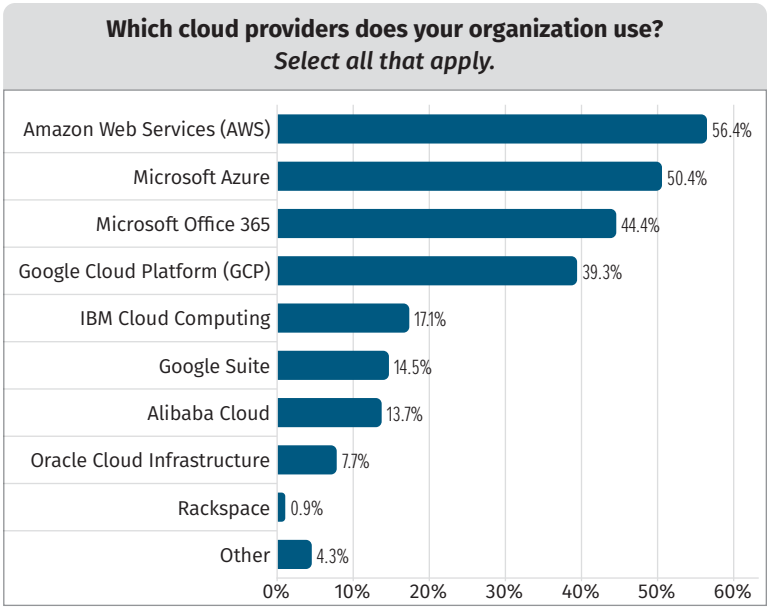


Figure 3. Preferred Cloud Providers

The statistics represented in Figures 2 through 4 do an excellent job of portraying what types of assets are hosted in the cloud and where organizations are hosting them. However, Figure 4 represents the knowledge that security teams need the most. The value of understanding what types of assets or services are deployed, and how teams are responsible for securing those assets, cannot be understated.

We weren't surprised by the top five cloud services/applications utilized by respondents' organizations. These are the types of assets or services that often take the top spots in any organization's cloud infrastructure—common SaaS applications used for purposes other than productivity. As seen in Figure 4, web applications are clearly the most popular type of asset or service, with 56% of respondents using external web apps and 51% using internal web apps. Office automation, file storage, and databases round out the leading categories.

What is more interesting are the less-utilized types: containerization, developer tools, machine learning, and Functions-as-a-Service. These provide a baseline for asset classes that may grow into the future. This may be due to lack of adoption by multiple organizations or the sheer amount of web apps and office automation products that consume most of our cloud deployments. As we continue this survey year after year, it will be interesting to see how these less-represented categories grow in utilization.

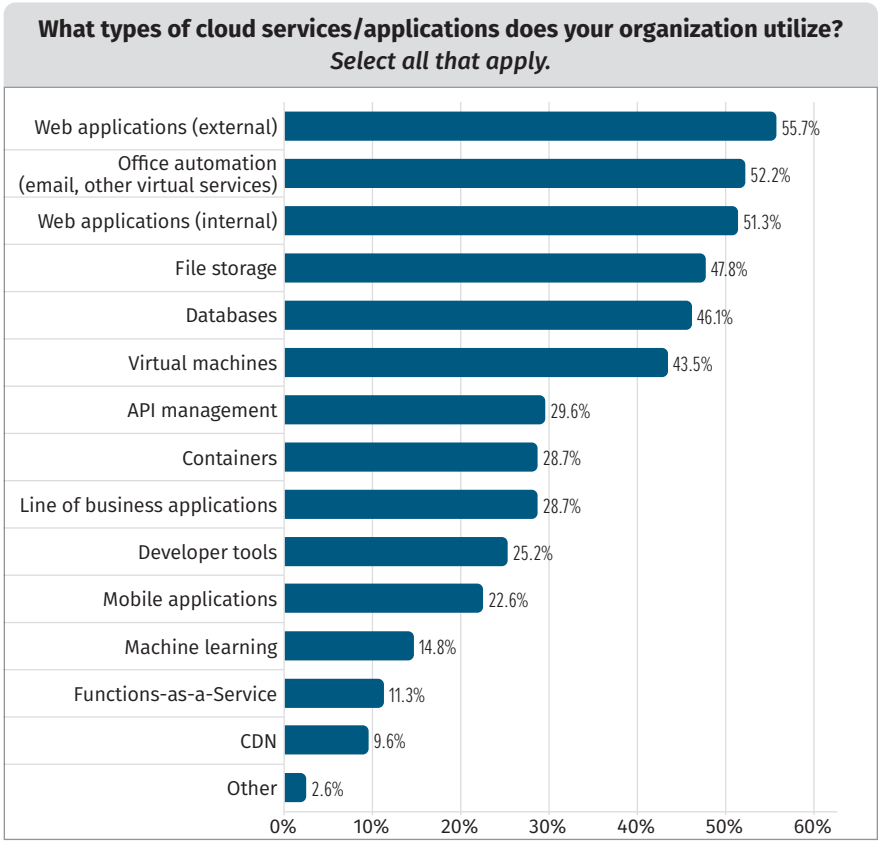


Figure 4. Cloud Services/Applications in Use

Third-Party vs. Custom-Developed Applications

Another critical area we wanted to explore from a security perspective is the use of third-party versus custom-developed applications in the cloud. Both approaches introduce different risks and require their own type of deployment and security controls. However, when an organization owns the development *and* deployment of an application, as with custom-developed apps, it can introduce new risks to an environment. This should be a top priority for security teams!

Survey results show that a little more than half (approximately 56%) of organizations have at least 40% of their cloud usage comprised of custom-developed applications. See Figure 5.

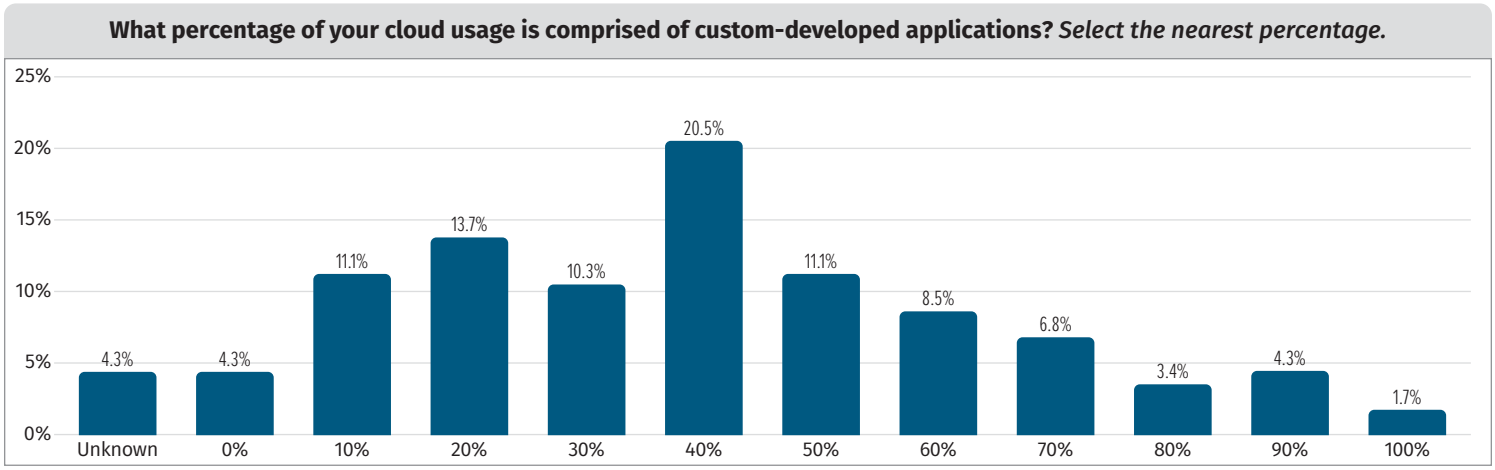


Figure 5. Cloud Usage Comprised of Custom-Developed Applications

This is an important result for two reasons:

- Organizations that secure and publish their own custom applications create a different risk profile for themselves than organizations relying on third-party applications. Think about code repositories, build processes, and other development processes needed to support custom-developed applications. Each item in the preceding list provides an opportunity for adversaries to gain a foothold into an organization's environment.
- Organizational security considerations or operational improvements must address this risk model. The percentage of custom-developed applications, in relation to cloud footprint, is a detail that the security team should know intimately because the use of custom-developed apps not only changes an organization's risk model, but also may create unique opportunities for adversaries.

The key takeaway from what we have observed so far is that many organizations have sizeable cloud footprints, and these footprints are likely growing. Even if current footprints never change, most are sizeable enough to represent a potential attack vector. This should expand the organization's threat model and should be considered in their defense mechanisms.

For cloud-based applications, organizations must also be cognizant of the development and deployment processes. Figure 6 shows the technologies our respondents are using to deploy their applications to the cloud. Exactly 50% of respondents indicated that they use a third-party application to help deploy applications to the cloud, while nearly the same (47%) use cloud provider portals. Rounding out the top four, at approximately 45% and 37%, is the use of custom scripts with APIs and custom scripts with third-party libraries, respectively.

What technologies does your team use to deploy applications to the cloud? *Select all that apply.*

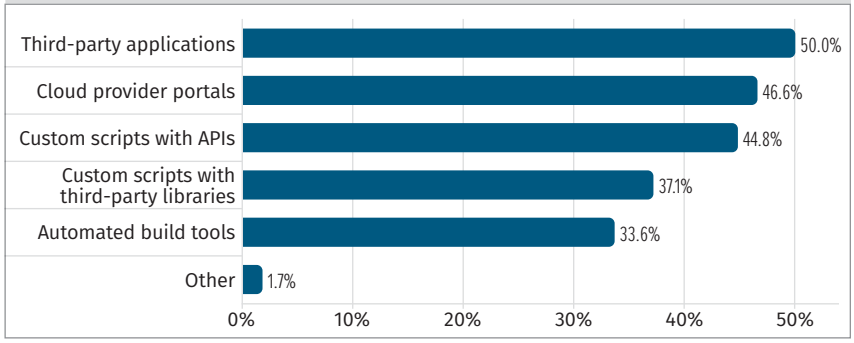


Figure 6. Cloud Technologies Deployed

For this question, we allowed respondents to select all technologies that apply. We are highly aware that teams likely use multiple deployment means. The results present a few interesting topics for discussion and threat assessments:

- Development teams may use a combination of third-party software and applications coupled with custom scripts. It is not uncommon to see a blend of administrators taking scripting work into their own hands.
- The use of custom scripts with third-party libraries represents some of the most interesting stats. As discussed earlier, custom-developed scripts and applications are potentially a sign of a good development team but, of course, carry certain security implications.
- Many teams think of third-party applications as including (by default) CI/CD automated build tools. However, we called that out separately and found that approximately 34% of our respondents utilize automated build tools. This can introduce complexities in the deployment process but may also introduce opportunities for automated security approaches.

It's a healthy sign when an organization can create, publish, maintain, and secure its own code. However, we would encourage that development processes and practices intimately involve the security team, from both an auditing and continuous monitoring perspective.

After a cloud-based application or service has been pushed to deployment, the *development* team should monitor and push changes to cloud-based applications (in a typical DevOps environment). Figure 7 indicates how our respondents approach this task.

How does your development team monitor and push changes to cloud applications? *Select all that apply.*

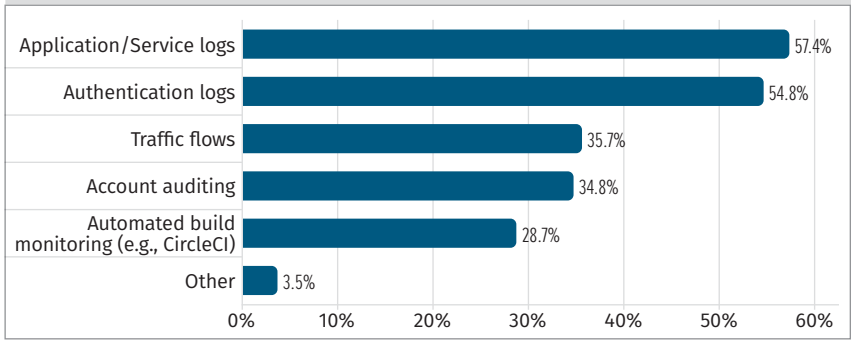


Figure 7. Methods for Monitoring/Pushing Changes to Cloud Applications

When an organization creates and deploys its own applications, it must be cognizant of the multiple third parties involved in software development and shipping. Whether it's DevOps providers, code repositories, or third-party libraries, each can open a unique attack vector for adversaries to abuse.

We were pleased to see that development teams look at the same types of data that security teams most value: application/service logs, authentication logs, and traffic logs as well as account auditing logs (35%). It was interesting to see the similarity of a reliance on log data.

Of course, this also presents an opportunity for unification of telemetry and environment visibility. This might be a question for our readers: **Your security teams are already looking at logs daily. Are they looking at (and for) the same data points that the development team may be after?** Is there a chance to condense or expand cloud asset monitoring capabilities? We think that there is a chance for unification here and explored this in our survey as well. See Figure 8.

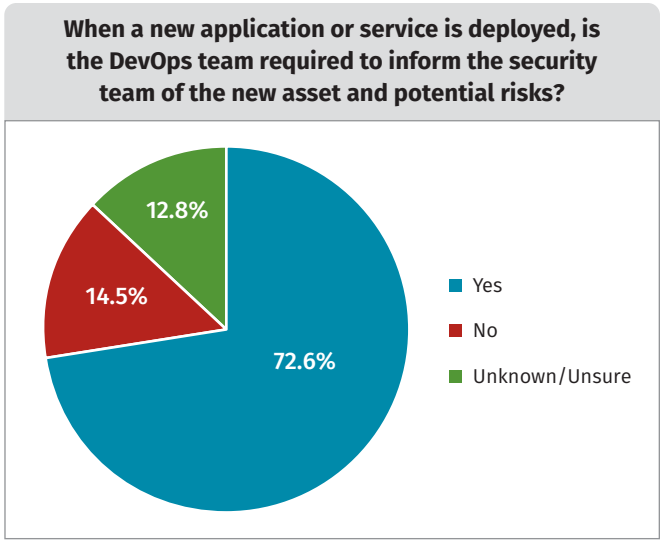


Figure 8. DevOps Communication with Security Team

A whopping 73% of our respondents indicated that the deployment of a new application or service requires the notification of the security team of the new asset and potential risks. We loved seeing this statistic! Looking at the previous figures, we see ample evidence that a development team can quickly get ahead of a security team with asset creation and deployment. However, as we've highlighted already, when development and security teams can work together it creates an opportunity for holistic environment visibility *at the time of deployment*, rather than *at the time of attack*.

Securing the Cloud

While development and security teams should be encouraged to work together, it creates a challenge because it's easy for each to try and find flaws in the other. Having development teams moving at a speed faster than the security team can keep up with is a constant challenge for many organizations. However, as we saw in Figure 8, with procedures in place, the development team is more than happy to notify the security team of new asset(s) and potential risks.

With this information in hand, we look to the security team to determine how it will go about securing various assets. Our survey explores these concepts, first beginning with a differentiation between cloud-native and on-premises assets. Approximately 74% of respondents indicated that the security team is trained on the differences between these two assets. See Figure 9.

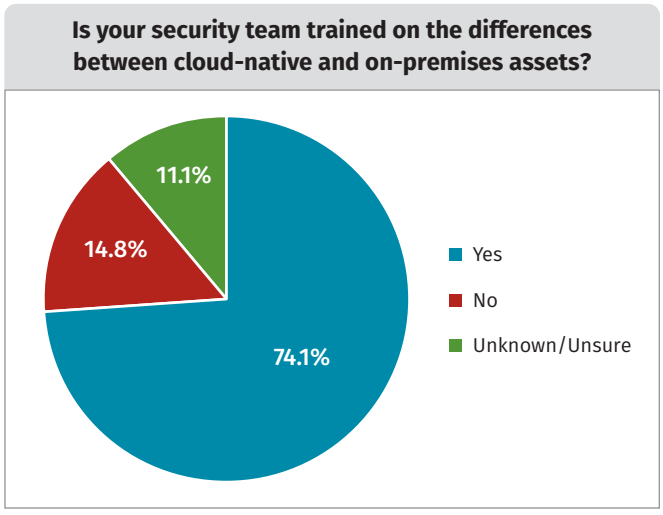


Figure 9. Current Security Team Training on Cloud-Native vs. On-Premises Assets

Perhaps more concerning is that nearly 26% of respondents admitted that their security teams are either not trained on the differences or (worse yet) they simply don't know. Unfortunately, these types of gaps create:

- **Difficulties** for teams to determine how to secure asset classes
- **Opportunities** for adversaries who look for unmonitored, unpatched, or insecure assets among the midst of a confused security team
- **A false sense of security** because the security team doesn't even know what it doesn't know, which can create a larger risk if security is assumed of a cloud asset when, in fact, nothing is there!

Having little insight into your organization's cloud-native versus on-premises assets can create confusing detection and response scenarios for your security teams. Should the IR processes be different for each, or can you define a plan generic enough to cover both? Is it still effective, and does the place handle any changes a cloud-native asset may experience?

In the face of these results, we also asked our respondents if they have any intention to offer training to increase their security team's knowledge of cloud-native and on-premises assets. Approximately 58% of respondents hinted at future training, while the remainder indicated they either have no intention of providing training (15%) or do not know (27%). See Figure 10.

Our key point remains the same: Security teams must be trained on how to handle these various asset classes, and organizations must ensure that their detection and response capabilities match their assets and capabilities. When deploying cloud assets, the security team must be ready to assist in secure deployments and should also be performing their own assessments of the chosen cloud environments. This includes how your current tooling may or may not fit as a detection and response tool. If new tooling must be brought in or capabilities built, the team must identify and prioritize those.

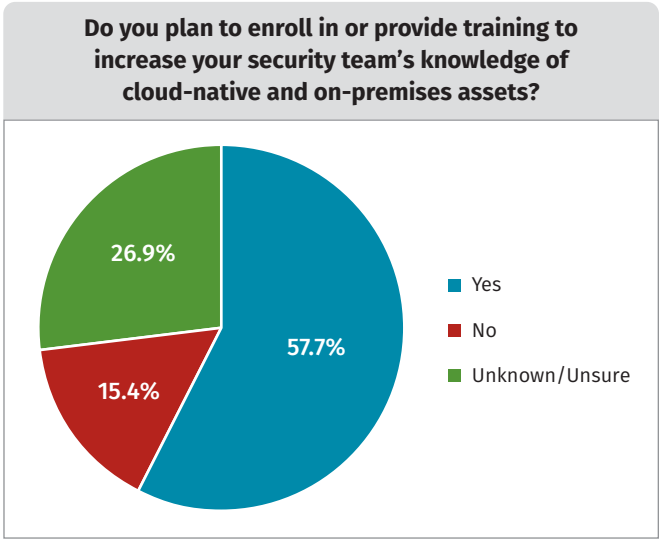


Figure 10. Planned Security Team Training on Cloud-Native vs. On-Premises Assets

Cloud Monitoring

For organizations that discern or expect their security team(s) to discern between cloud-native and on-premises apps, we believe that a portion of monitoring, detection, and response capabilities are likely either cloud-specific or cloud-leaning. Approximately 86% of our respondents collect telemetry from their cloud platforms or applications, which gives us a healthy representation of *how* that telemetry could be best used. See Figure 11.

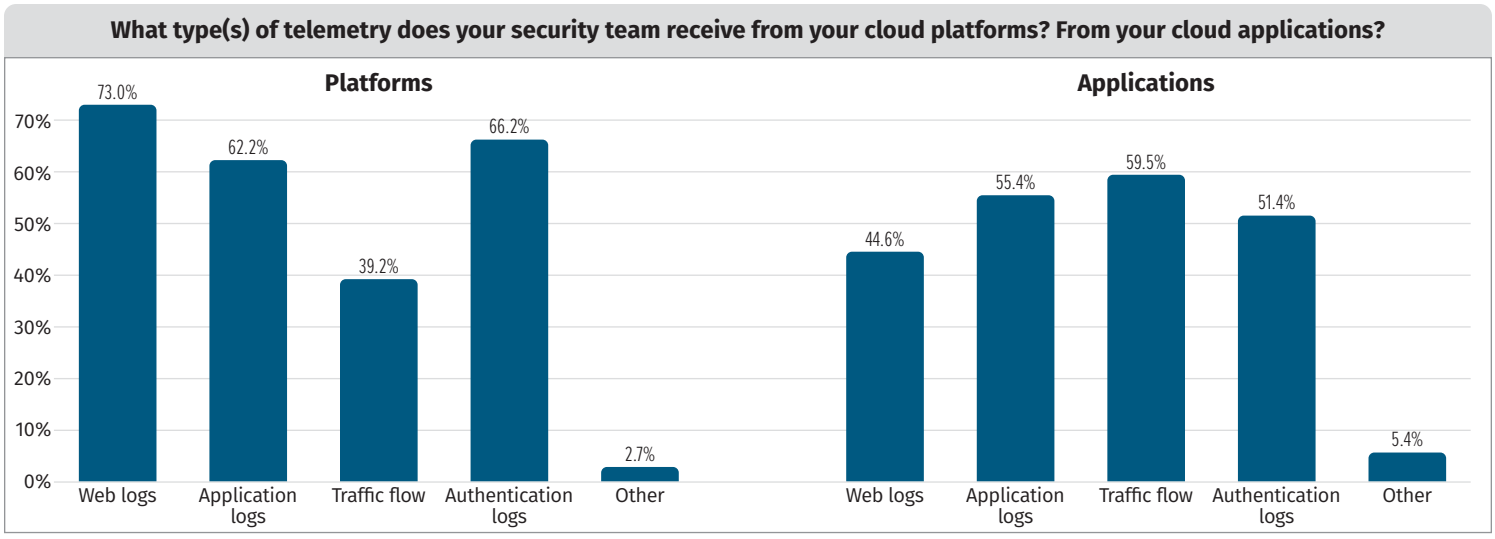


Figure 11. Cloud Platform Telemetry

Distinguishing between platforms and applications to identify valuable telemetry types, we see some interesting differences, which are likely due to the type of assets that they include. Examining both, we can see:

- **Platform telemetry** heavily favors web logs (73%) and authentication and application logs (66% and 62%, respectively). Traffic flows have a weaker representation, at only 39%. This weighting makes sense from our perspective. After all, traffic flows may be quite voluminous, especially with a large cloud footprint.
- **Application telemetry**, on the other hand, heavily favors traffic flow (60%), followed by application and authentication logs (55% and 51%, respectively). The interesting takeaway is the switch between reliance on web logs between platforms and applications.

The difference in telemetry types may also speak to their effectiveness, something that security teams have hopefully had time to assess and make a proper decision on. Another difference we can think of is the ease (or difficulty) with which teams can get telemetry out of cloud providers, which may skew the results in a specific direction.

There is also a chance for security teams to spend time analyzing their monitoring and telemetry needs and ensure that they are receiving what's necessary from their cloud providers or cloud-hosted assets. While our survey limited results to only a few high-level categories, it is possible that an organization could find benefits in a hybrid approach, such as flow logs coupled with application-specific logs to help combine various data points.

Cloud Incident Response

Based on telemetry available, we would expect that security teams hone and build their cloud-native detection processes and capabilities. We brought this question to light, asking our respondents how confident they are in their ability to *detect and respond* to an incident involving a cloud-native asset. Figure 12 provides those results.

Approximately 66% of respondents indicated that they are either highly or moderately confident in their abilities—a solid representation in this survey. The more concerning side of this question lies with the organizations that expressed no confidence (27%), no insight (4%), or simply don't know (3%). As always, a lack of knowledge, capabilities, or visibility will introduce issues and weaknesses into an environment that adversaries are all too quick to take advantage of.

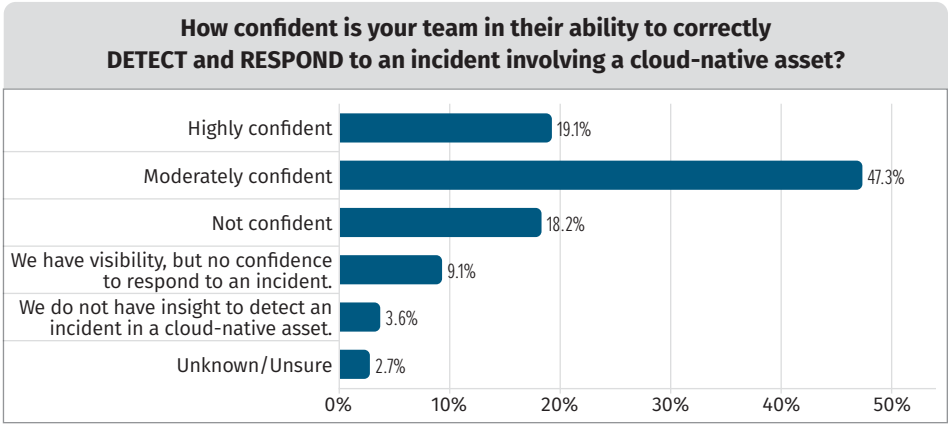


Figure 12. Detection and Response Confidence

Because we expect cloud to become more integral within an organization's security posture, we would equally expect to see overall confidence increase from moderate to high. This will likely be a gradual shift of confidence, rather than a spot change, as organizations implement more visibility and tooling to be able to successfully detect and respond to an incident within their cloud environments. Furthermore, we would also expect that the number of unknowns or lack of insight decreases as these organizations achieve insight and begin to build their own confidence.

Looking Ahead

Finally, just as important as determining where and how cloud assets are currently being secured, we also look to our survey to determine where spend and cloud deployments will be in the future. Because cloud spend and deployment is an ever-growing area, we expect most organizations to be moving or considering moving operations. Figure 13 supports this expectation with a significant amount of our respondents (82%) having indicated that they will be shifting more assets to the cloud.

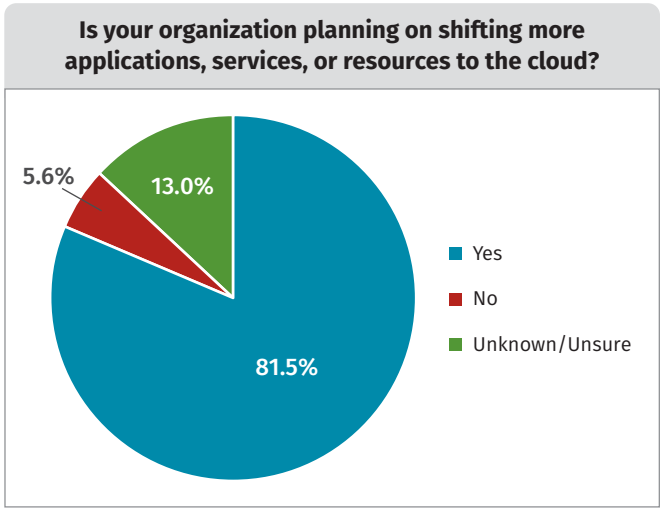


Figure 13. Planned Shift of Applications, Services, or Resources to the Cloud

Interestingly, 13% or respondents do not know or are unsure of their organization's plan for moving to the cloud. While we often attribute "Unknown" responses to a lack of visibility or environment knowledge, it is highly likely that, in this case, organizations are unsure of how or when applications, services, or resources can be moved to the cloud rather than *when* they might be moved.

To help understand this point better, we also asked about the time frame organizations are considering for moving their operations to the cloud. Figure 14 provides insight into this question.

A majority of respondents (85%) will be moving assets to the cloud within the next 24 months, with the bulk of that occurring in the next year. This data should not come as a surprise. We expect a trend of moving assets to the cloud to continue for months and years to come. Furthermore, we would also expect organizations to move myriad assets to the cloud.

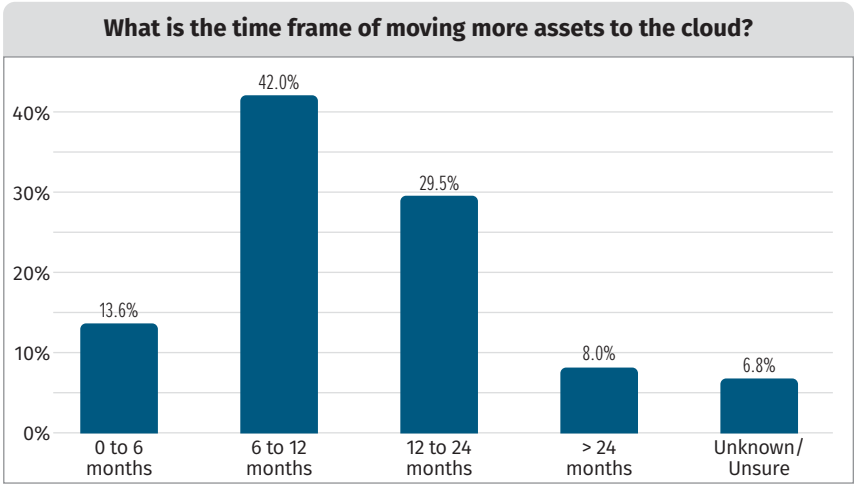


Figure 14. Time Frame for Moving Assets to the Cloud

Most organizations are planning on moving assets to the cloud over the next one to two years. We encourage you to ensure that the security team is included in planning and deployment discussions, so that they can also account for and protect assets as they are deployed.

Thinking on this topic, we also asked what type of services and/or applications respondents' organizations would be shifting to the cloud, most likely away from on-premises requirements. Figure 15 shows the the prioritization of upcoming cloud deployments.

This information is perhaps some of the most informative data every security team should have—not only a time frame of cloud asset deployment, but also the type(s) of assets being deployed. Internal web applications represent the highest move (50%), followed closely by virtual machines, databases, and external-facing web applications. File storage rounds out the top five, with a healthy representation at approximately 36%.

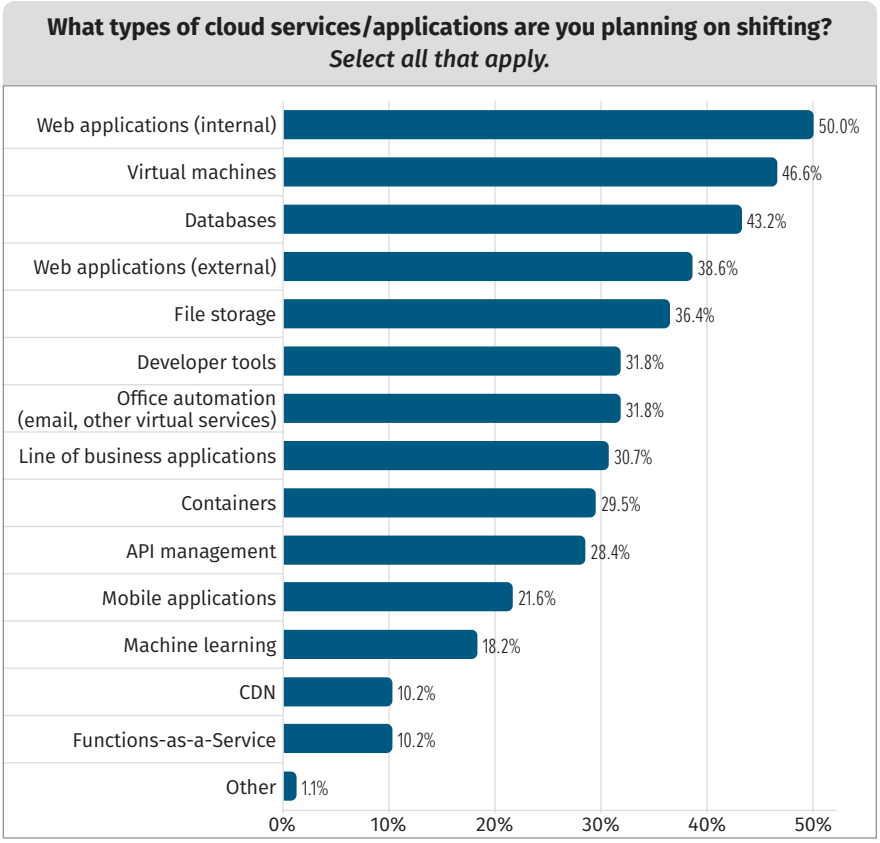


Figure 15. Asset Types Moving to the Cloud

Knowing this information represents a gold mine and opportunity for security teams. Knowledge of assets to be deployed enables teams to gain an advantage on securing those assets ahead of time, whether via ACLs or other cloud-based defense mechanisms. Furthermore, organizations can also utilize their threat intelligence capabilities to identify what and how adversaries are targeting and align those concerns with asset deployment.

Knowledge of an organization's cloud assets and how to secure them, as discussed earlier, is an important sign of maturity for security teams charged with protecting cloud infrastructures. Only with visibility, training, and threat intelligence will organizations be able to effectively defend their clouds from a wide range of adversaries.

Conclusion

This survey provided a wealth of insight into how organizations are deploying and securing their cloud assets. We asked our respondents to provide us insight into their current and future cloud footprints, the differences in third-party versus custom applications, and how their security teams can secure this ever-growing footprint. As we continue to see growth in these areas, we hope to see an embrace of secure development and deployment practices.

This survey also gave us insight into how security teams are handling these changes. Far too many teams are rooted in legacy, on-premises-based security programs. Organizations that give security a seat at the table when it comes to managing risk and deploying cloud assets—whether third-party or custom-developed—currently lead the best practices. Adversaries are too crafty these days. They can find holes and weaknesses in the least expected places. Therefore, we hope that, as time goes on, security teams take a cloud-first or cloud-centric approach when building their detection and response programs.

Finally, this survey also served as an excellent barometer for organizations that might find themselves somewhere in the middle. Deploying in the cloud and unsure of best practices? Perhaps a security team is just getting familiar with cloud assets or attempting to understand their footprint. Tucked within these results are good insights into how others are approaching the problem and what may be the next best steps for your organization.

Sponsor

SANS would like to thank this paper's sponsor: