A SANS Survey

SANS 2021 Cloud Security Survey

Written by **Dave Shackleford**

April 2021

Sponsored by:

Sumo Logic

Executive Summary

Since 2019, we've seen more and more examples of vulnerabilities in cloud assets, sensitive data disclosure, and breaches involving the use of public cloud environments. In addition to the 2019 Capital One breach that occurred in Amazon Web Services (AWS),[1] other interesting and noteworthy examples include:

- Microsoft exposed a severe bug in its console in late 2019. This vulnerability, which researchers at CyberArk discovered, dealt with JavaScript and URL parsing in the Azure console and easily could have led to Azure account takeover. Microsoft patched the bug within two weeks of discovery, however.[2]
- In December 2019, Microsoft reported that it had inadvertently exposed a large database of customer support records within Azure, blaming the exposure on "misconfigured security rules" (likely meaning Network Security Group rules or perhaps an identity policy).[3]
- Earlier in 2019, Docker Hub discovered a breach of one of its account databases, exposing roughly 190,000 customer records. Only a small number had passwords and tokens included in the breach.[4]
- Several Microsoft outages during 2019 and 2020 were significant. The first was an Azure database outage in 2019 that was caused by DNS configuration changes and failure of some automation scripts. In 2020, numerous Office 365 outages caused many organizations to experience downtime and inability to access cloud applications and data.[5]

Even with these types of security issues, more organizations than ever are moving their data and workloads to the public cloud, building applications in the cloud, and subscribing to a wide range of SaaS and other cloud services. The goal of the SANS 2021 Cloud Security Survey is to provide additional insight into how organizations are using the cloud today, the threats security teams are facing in the cloud, and what they're doing to improve security posture in the cloud.

Key Takeaways Year over Year

In our 2019 cloud security survey, some of the top takeaways included the following:

- The 2019 survey reported a significant increase in unauthorized access by outsiders into cloud environments or to cloud assets: 28% of organizations in 2019 vs. only 12% in 2017.
- More than 55% of respondents stated that they were frustrated by trying to get low-level logs and system information for forensics in 2017, while only 30% said as much in 2019.
- ISO 27001 reports continued to be the most valuable audit reports made available by cloud providers, and more organizations were able to perform pen tests of their cloud provider environments than in the past.

What stands out in 2021? Here are some of the key findings from this year's survey:

- Serverless took the second spot in security automation technologies (behind infrastructure-as-code), beating security orchestration platforms.
- Respondents noted significantly more emphasis on 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.

[1] "Former AWS Engineer Arrested as Capital One Admits Massive Data Breach," https://threatpost.com/aws-arrest-data-breach-capital-one/146758/

[2] "I Know What Azure Did Last Summer," www.cyberark.com/threat-research-blog/i-know-what-azure-did-last-summer/

[3] "Microsoft discloses security breach of customer support database," www.zdnet.com/article/microsoft-discloses-security-breach-of-customer-support-database/

[4] "Docker Hub Breach Hits 190,000 Accounts," www.securityweek.com/docker-hub-breach-hits-190000-accounts

[5] "'Very Frustrating': Microsoft Office 365 Outage Hits U.S. Again," www.crn.com/news/cloud/-very-frustrating-microsoft-office-365-outage-hits-u-s-again

Figure 1 provides a snapshot of the demographics for the respondents to the 2021 survey.

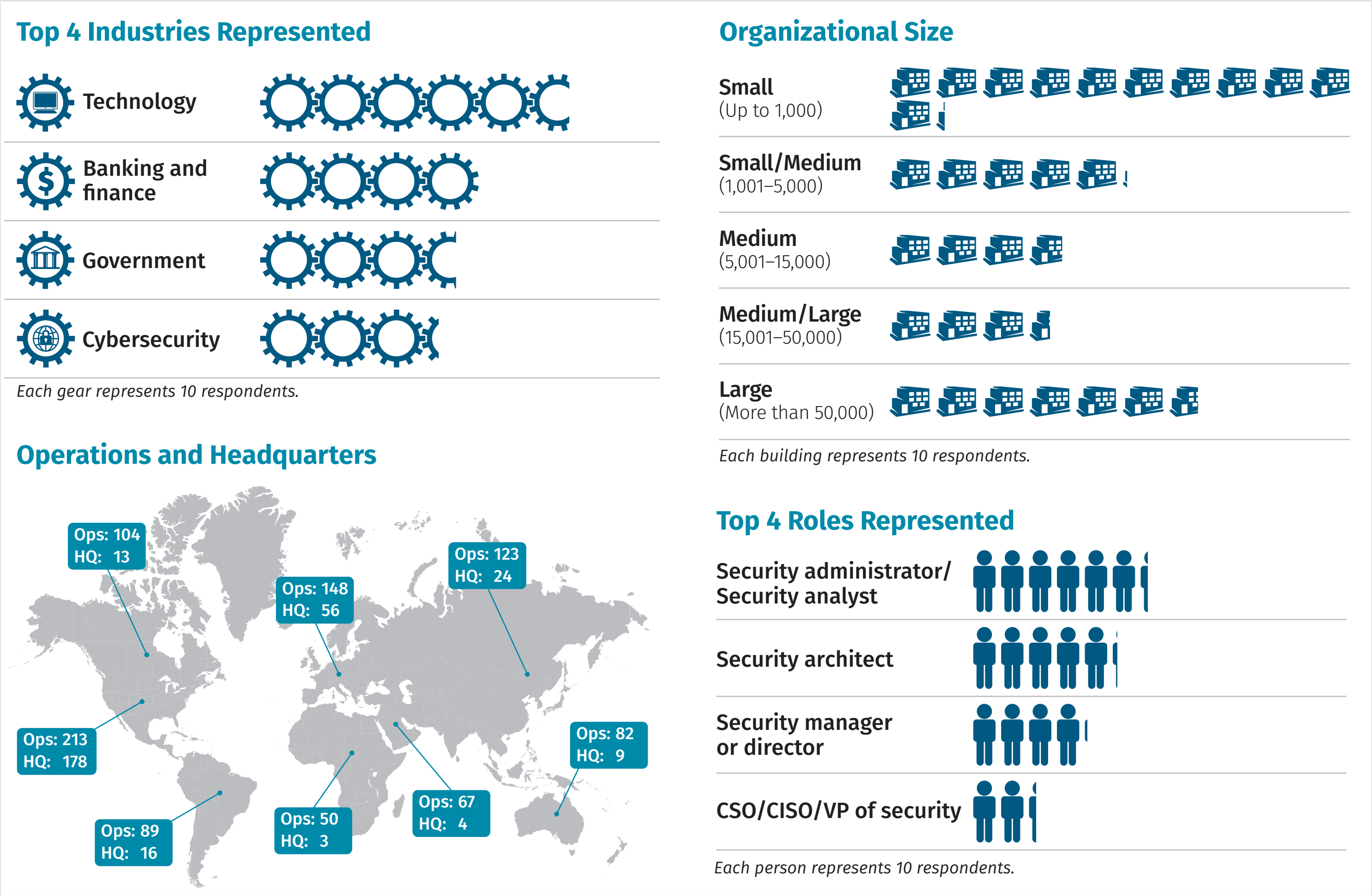

Figure 1. Demographics of Survey Respondents

What We're Doing in the Cloud

We asked respondents to identify the cloud applications they are using currently, and once again saw that business apps and data topped the list (72%). Our 2019 survey saw a big drop in the use of workforce apps such as Dropbox, which only 45% said they are using today, versus the 84% who affirmed this category in use in 2017. This number came back up slightly in 2021 to 49%. This could be a simple difference in the respondents, because SANS sees this as still being a very popular category, so it's one to note and track for the future. Security services rose by more than 10% from 2019, to 55%, with server (workload) virtualization in platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) and backups for disaster recovery also being fairly popular. See Figure 2 for the breakdown of responses.

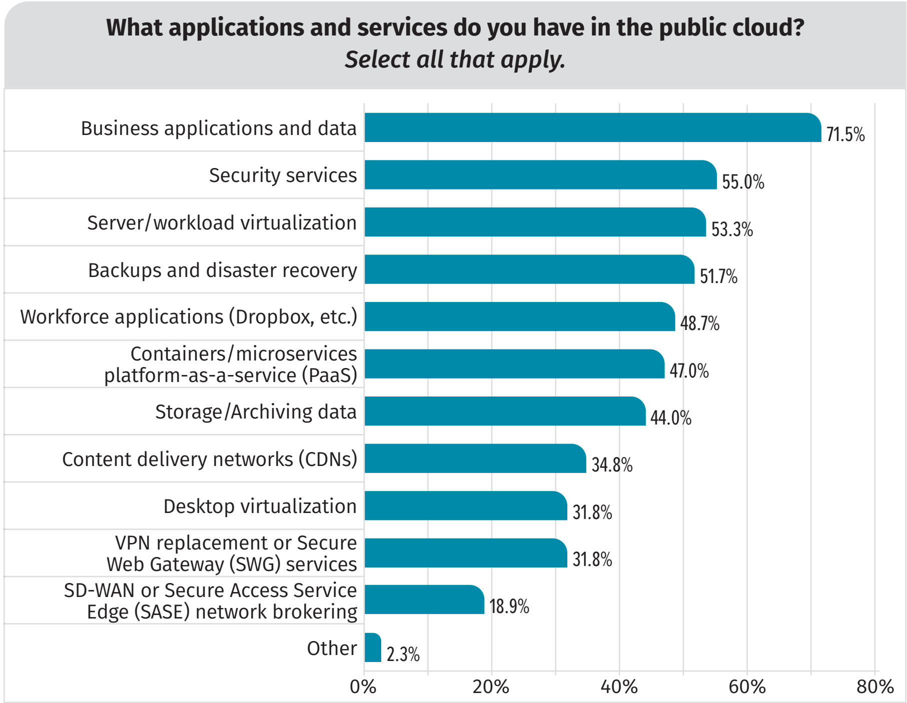

Figure 2. Cloud Applications in Use

This year's survey also saw a consistent response in the number of public cloud providers organizations are using. In 2019, the highest response category was two or three providers, and in 2021 that number is the same. A similar percentage of respondents were using only one provider several years ago (11%) versus today (12%), which may indicate that smaller organizations remain hesitant to move into multi-cloud deployments. Fewer organizations are using more than 20 cloud service providers, which is consistent with our last survey, as well. See Figure 3.

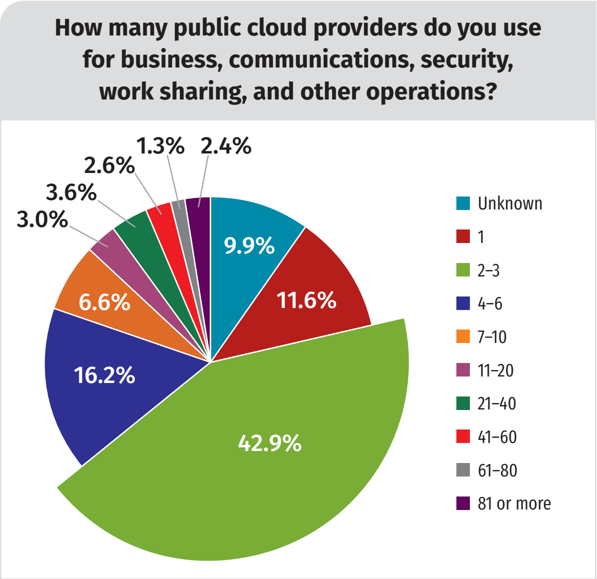

Figure 3. Number of Cloud Providers in Use

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 such as cloud access security brokers (CASBs) and identity federation platforms to help centralize control. More than half of respondents (56%) indicated that they are using federated identity services to help centralize user access and authorization into cloud applications (an increase over 2019's response of 48%). Many are also using cloud network access services (47%) and CASBs (43%), an increase over 2019's 35%. Not as many organizations (18%) had adopted a multi-cloud broker to centralize access to PaaS, IaaS, and other service provider environments. This number makes sense because security teams need new services that can help centralize user access and identity as well as implement user-oriented policies for monitoring activity and protecting data (CASBs) as cloud application use grows.

We also inquired about the use of cloud services related to the COVID-19 pandemic. Many organizations prioritized cloud service implementation to facilitate remote work. In the past year (2020–2021), 40% have started using more cloud services, while 49% have not (12% are unsure). For those using more cloud services, 29% are using business collaboration services, 22% are using more cloud storage, and 15% are using more remote VPN replacement services and brokering capabilities.

Are you currently storing any of the following sensitive or regulated (compliance-related) data in the public cloud? *Select all that apply.*

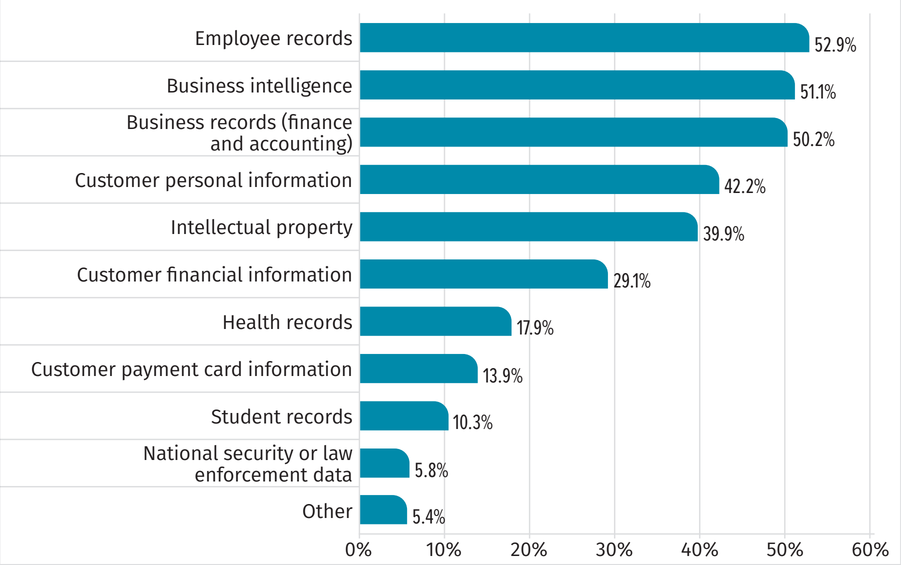

Figure 4. Sensitive Data Stored in the Cloud

As in our past several surveys focused on cloud security, we asked respondents to identify the kinds of sensitive data their organizations are hosting in the cloud today. Business intelligence, which topped the list at just over 48% in 2019, fell to second place with 51% in 2021. The top data type in 2021 is employee records at 53% (a huge increase from 2019 at 38%), with financial and accounting business records (50%) and customers' personal information (42%) close behind. See Figure 4.

We also asked if privacy regulations, such as the General Data Protection Regulation (GDPR), are impacting existing or planned cloud strategies. Just over half (55%) stated that they are, with 34% saying no and 11% remaining unsure. For some data types, especially consumer personal data, organizations would need to ensure cloud providers could adequately meet privacy compliance needs.

Overall, while the types of data changed a bit, the general trend here is very similar to what we have observed previously. Roughly one-half of respondents' organizations are willing to put a variety of sensitive data types in the cloud, with lower percentages of some types (customer payment card information at 14% and health records at 18%).

Concerns and Threats in the Cloud

We asked security professionals to identify their biggest concerns in the cloud and if any of those concerns were realized. As in 2019, unauthorized access to data by outsiders (56%) tops the list of concerns. Another major concern in 2019 was unauthorized access to data from other cloud tenants (50%). This concern dropped significantly to 40% in 2021, likely due to more trust in cloud provider security controls and capabilities. The other major concerns are poorly configured or insecure interfaces and APIs (54%) and a lack of cloud security skills/training (53%). Another change this year is a significant increase in misconfiguration issues with application components and APIs, from 46% in 2019 to 54% in 2021. See Figure 5 for the full breakdown of concerns and actual incidents.

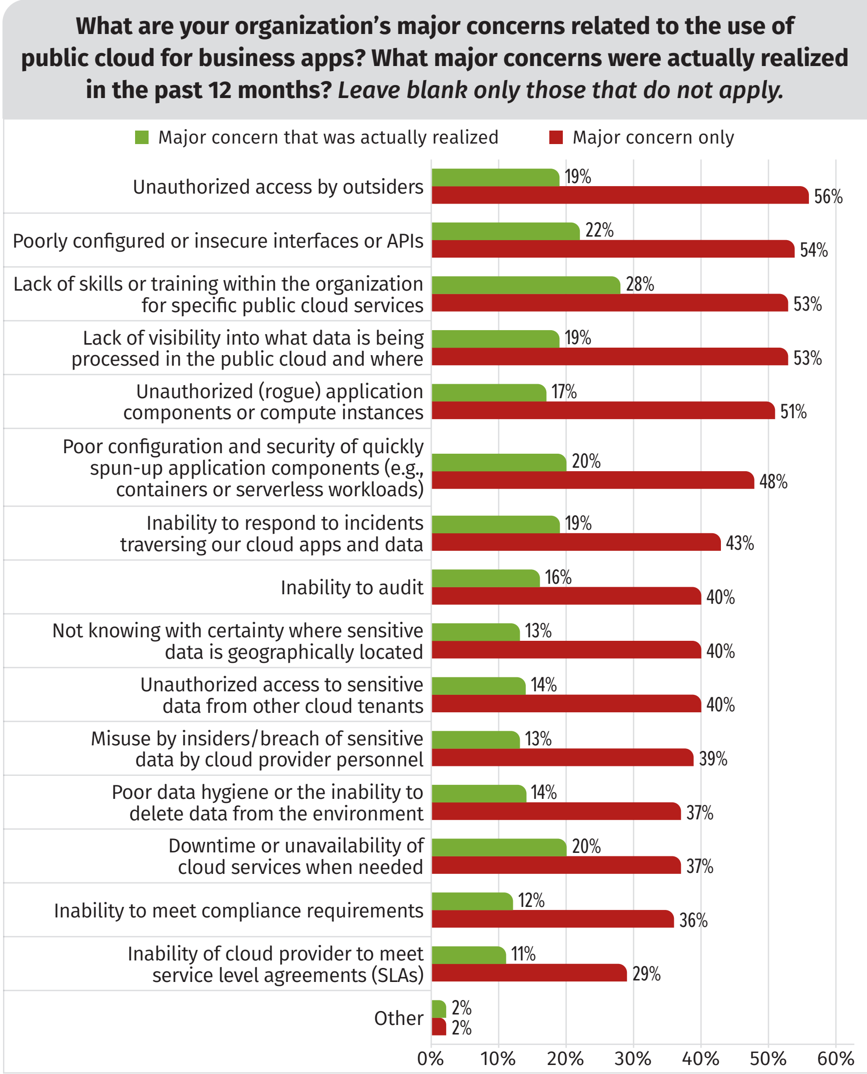
What are your organization's major concerns related to the use of public cloud for business apps? What major concerns were actually realized in the past 12 months? ***Leave blank only those that do not apply.***

Figure 5. Concerns and Incidents in Cloud

More than likely, some of these issues go hand in hand. By exposing poorly configured applications and API interfaces, organizations are inviting possible access by attackers who are constantly on the lookout for them using tools such as Shodan and network scans. In the past several years, the biggest issues were downtime, misconfiguration, and failure to meet service levels. While these are all still problems seen currently, they are overshadowed by attacks that seem to have surged in the past few years. With the rise of remote work during the COVID-19 pandemic, though, we wanted to find out if cloud risks or threats grew in priority or importance as a direct result of remote work scenarios related to the pandemic. Forty-three percent indicated that they have, with 41% stating that cloud risk had not increased or changed. Just over 15% remained unsure. For those respondents who experienced increased risk or security issues related to remote work, roughly two-thirds (65%) stated that account hijacking or remote user compromise was to blame, with 60% also indicating that configuration issues/errors and lack of monitoring contributed to a change in security profile.

Have these attacks and incidents actually led to cloud breaches in the past 12 months? Fortunately, the answer seems to be “no” for now. Most respondents (65%) said they aren’t aware of an actual breach. Another 17% just aren’t sure (compared with 7% in 2017). However, 19% said that they did experience a breach (a sizeable increase over 2019’s 11%). This is a fairly major change—almost double the number of respondents both experienced a breach and acknowledged they don’t know if they did.

In 2021, we again looked at what was involved in the successful attacks. The top responses were account/credential hijacking at 49% (identical to 2019) and misconfiguration of cloud services/resources at 49%. The third major issue was insecure interfaces or APIs (36%), followed by DoS attacks (30%).

These changes likely reflect the shifting nature of cloud, as well as maturity of providers and controls. Many control elements are completely managed by public cloud providers, so the surface area for attacks to this layer is greatly reduced. DDoS attacks are still happening, but don’t seem as prevalent in breach scenarios due to improvements in DDoS protection from public cloud providers as well as third-party services, which have grown in popularity over the past several years.

Organizations are still not protecting credentials as well as they should, and misconfiguration of cloud resources is a pervasive issue as evidenced by the plethora of exposed S3 buckets and APIs seen today. Privileged user abuse is likely symptomatic of the complexity of identity and access management (IAM) policies and settings that are tied to most cloud operations. The entire breakdown of factors involved in cloud attacks, as seen by respondents, is shown in Figure 6.

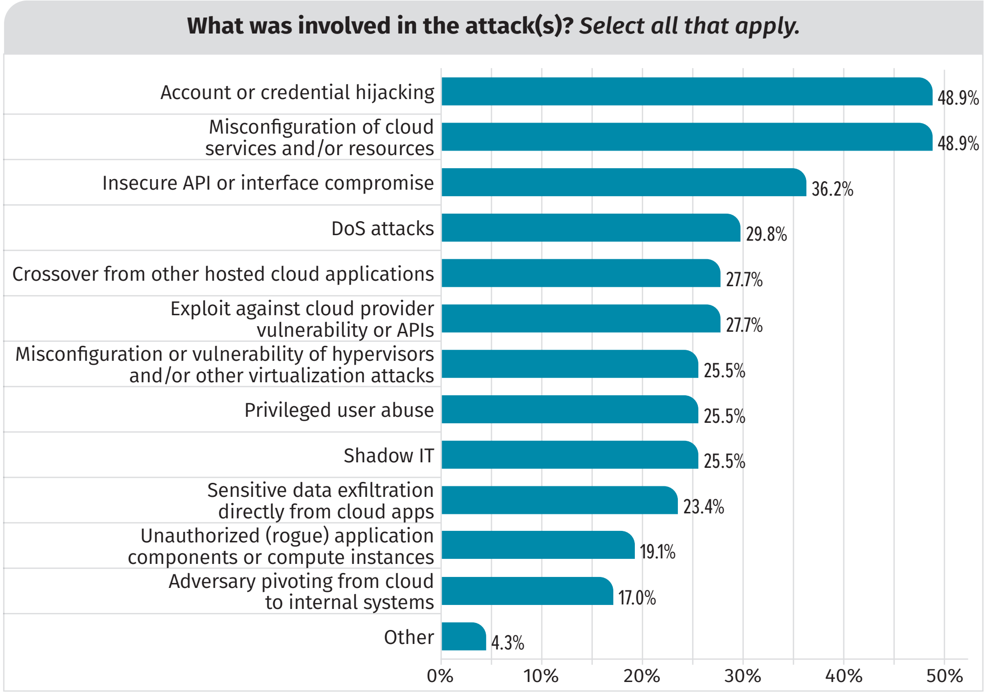

Figure 6. Breakdown of Cloud Attacks

Cloud Security Programs Today

As cloud use grows, organizations need to develop and enhance their processes and governance model to evolve as well. Today, 69% of organizations have cloud security and governance policies in place, which is up slightly from 68% in 2019. Twenty-three percent stated that they don't have policies in place, and 8% weren't sure. Gradually, we'll see more organizations evolve their governance and policy programs to incorporate cloud security and shared responsibility for controls and processes with cloud providers.

Over the years, we've already seen teams get better at implementing some of the most common security controls for cloud deployments, but many types of controls are now available as security-as-a-service (SecaaS) offerings versus standalone platforms. Cloud anti-malware (85%) is the most widely deployed security control, and for the right reasons—to protect the data repositories against theft/ransomware and workload/compute instances against compromise/disruption/abuse. At 59%, VPN is again the most successfully implemented internally managed tool, which is also the same result from 2019. Network access controls, vulnerability scanning, and anti-malware were also touted in our last survey as controls that organizations managed well internally, which again matches the results from this year. However, one notable change is the number of respondents who cited forensics and IR (44%) as a top in-house strength, as well. The top SecaaS services in this year's survey are multifactor authentication, identity management, and cloud encryption or CASBs. In 2019, the top services were network traffic analysis, vulnerability scanning, and multifactor authentication. The full breakdown of controls in the cloud for 2021 is shown in Figure 7 on the next page.

There's a lot of interesting data in here. First, the majority of controls across the board are still being managed internally. In some categories, however, there has been more growth in a hybrid or services model, including CASBs and encryption gateways (up to 18% for cloud native management) and identity management solutions. What stands out is the low numbers altogether. Many organizations may not feel wholly comfortable stating that these controls are capably implemented for the cloud yet.

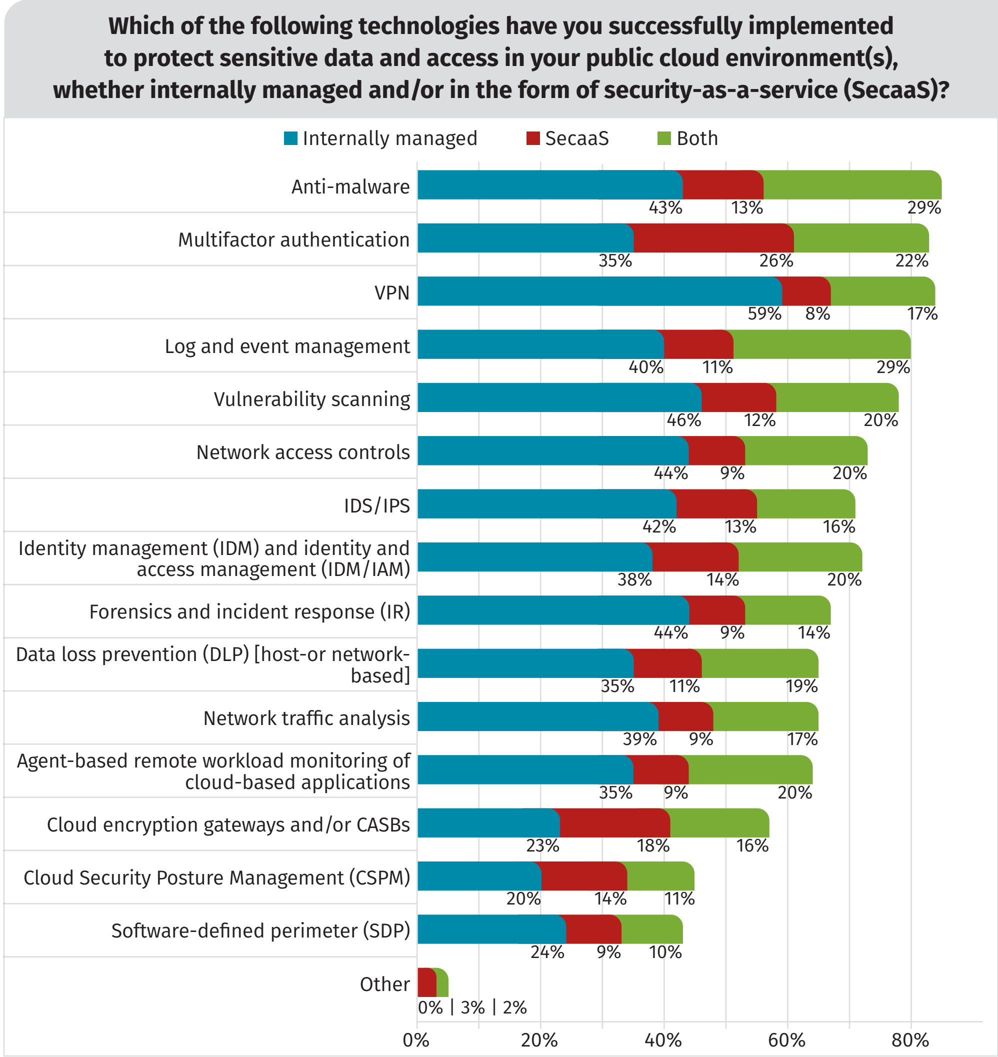
Which of the following technologies have you successfully implemented to protect sensitive data and access in your public cloud environment(s), whether internally managed and/or in the form of security-as-a-service (SecaaS)?

Figure 7. Security Controls for Cloud Adoption

This is somewhat corroborated by the fact that only 51% of respondents stated that they are leveraging cloud provider APIs in the cloud to implement security controls (a critical element of automation and cloud security maturity), which has improved since 2019 at 44%. For those leveraging these APIs, the most common control is logging and event management (64%), followed by IAM and configuration management (each at 58%). These top three categories match the results from 2019, but configuration management moved from the second spot to the third spot. These numbers suggest that these controls and functions are the easiest to tackle through cloud provider-enabled API capabilities, the most critical for organizations to implement, or both. Collectively, these numbers are similar to 2019 (a positive indication), but seeing only half of organizations make use of the APIs provided is concerning. This number should be higher by now. The full list of API-enabled security controls is shown in Figure 8.

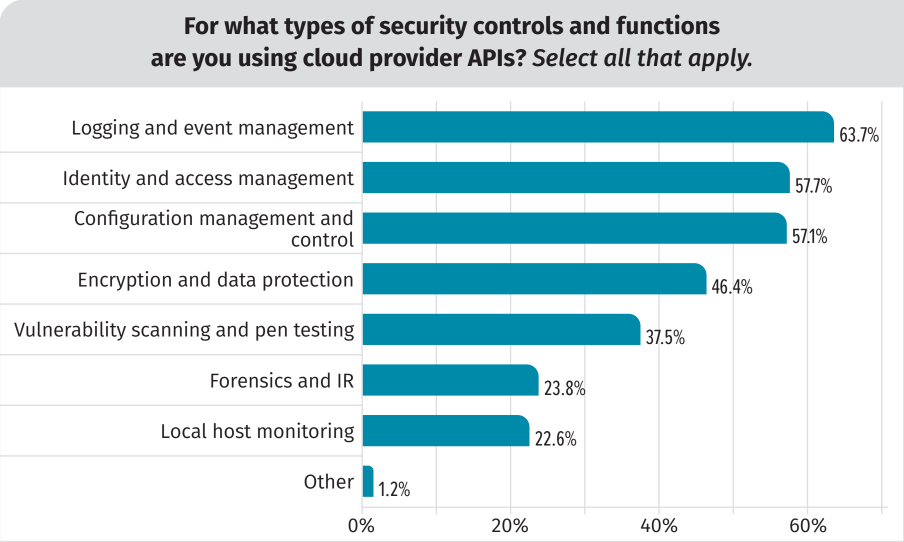
For what types of security controls and functions are you using cloud provider APIs? *Select all that apply.*

Figure 8. API-Integrated Cloud Security Controls

Given that most organizations are still managing many controls in-house, it's important to break down what controls organizations believe they've successfully integrated between traditional on-premises deployments and cloud environments, creating a true hybrid cloud security model. At present, 70% of respondents indicated that they've successfully integrated multifactor authentication (up from 65% in 2019), 54% feel that vulnerability scanning is well integrated in a hybrid model (down from 58% in 2019), and 64% have integrated anti-malware tools (up from 56% in 2019). These echo the top three technologies from our 2019 survey, as well. Forty-seven percent are confident that they've integrated network access controls, and another 46% are confident they've integrated SIEM and event management tools, too. The latter is especially important, because we saw previously that log and event management is one of the top three controls for cloud adoption (whether internally managed or through a SecaaS offering) and also a control area that involves high use of provider APIs. Because SIEM is a large, complex technology space, seeing this growth in a hybrid configuration is encouraging. The full breakdown of hybrid control integration is shown in Figure 9.

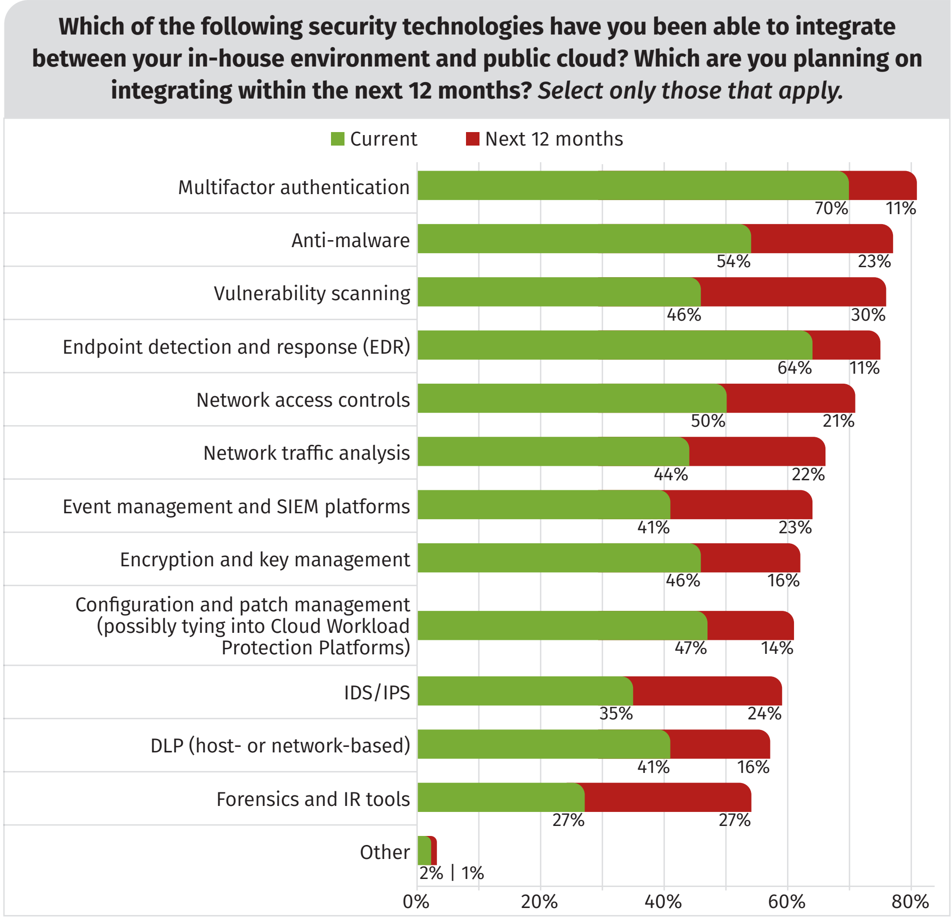
Which of the following security technologies have you been able to integrate between your in-house environment and public cloud? Which are you planning on integrating within the next 12 months? ***Select only those that apply.***

Figure 9. Hybrid Security Control Implementation

Note that we also asked respondents which controls they plan to integrate in the next 12 months. Nearly a third (30%) indicated that they plan on integrating event management, followed by forensics and IR tools (27%) and then DLP (24%). This indicates more focus on detection and incident response altogether, which has long been an immature control and process area for many teams.

In fact, we asked respondents to identify some of their biggest challenges in adapting forensics and IR to the cloud. Once again, the top result is a lack of real-time visibility into events and communications involved in incidents—a problem that event management/SIEM and forensics/IR tool integration may help with significantly. This is the same top challenge noted in 2019 and demonstrates that organizations are still struggling to get events and insight into cloud activity, which may support the number of organizations planning to focus on SIEM and cloud events in the near future. Other major challenges cited include difficulty 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 2017 more than 55% of respondents stated that they were frustrated by trying to get low-level logs and system information for forensics, only 30% said as much in 2019, and now only 18% stated this in 2021. This decrease is a strong indicator that providers are making this evidence more available than ever before, which bodes well for full integration of IR and forensics capabilities in a hybrid model in the near future. The full list of forensics and IR challenges respondents noted is shown in Figure 10.

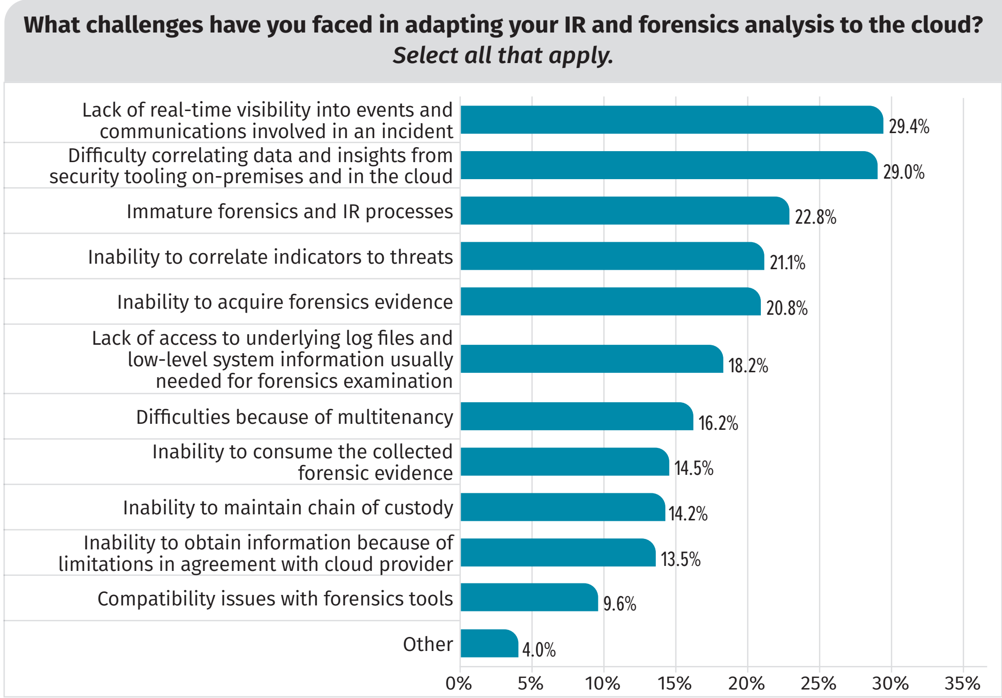

Figure 10. IR and Forensics Challenges in the Cloud

Returning to the concept of unifying and centralizing controls between on-premises and cloud environments, we wanted to find out if 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 altogether. Multifactor authentication and anti-malware are both relatively centralized, but SIEM and EDR are tied at 46%, and then followed by vulnerability scanning at 44%. This is a strong indicator that success in implementing hybrid controls is likely linked to vendor products that integrate well in both environments, also providing central management capabilities. The same top response (IR/forensics tools) was given for plans to implement in the next 12 months, too. However, vulnerability scanning is tied with configuration and patch management at 20%. See the full list of responses in Figure 11.

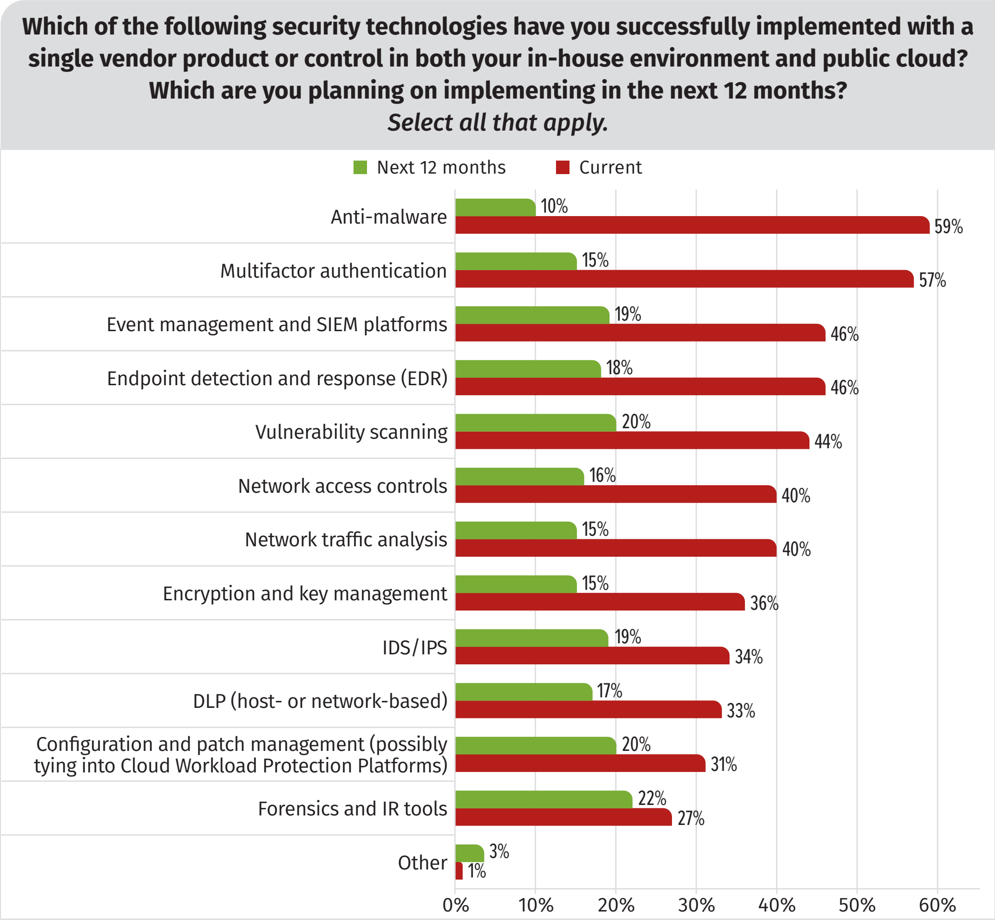

Figure 11. Single-Vendor Control Implementation for Cloud

As in past reviews, we looked at the use of IAM capabilities and tools for the cloud. IAM is rapidly becoming an essential element of most cloud implementations, so we asked respondents how they are using IAM for cloud today. As in 2019, the highest number of respondents (47%) are synchronizing their in-house user directories to a cloud-based directory, such as Azure AD. Use of identity-as-a-service (IDaaS) and IAM policy controls are tied at roughly 31% (similar to 2019), and this echoes similar percentages in 2019 as well (closer to 35% each). Slightly more respondents this year stated that they use an in-house IAM suite (27%) versus 2019 (23%), and 2019 saw more organizations mapping in-house identity to those in use by cloud providers (30%) versus this year (24%). The full breakdown of IAM use is shown in Figure 12.

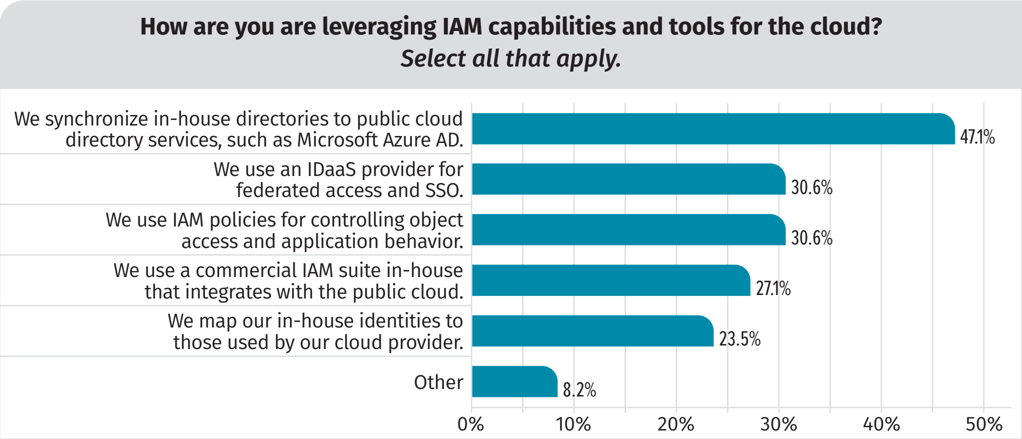
How are you are leveraging IAM capabilities and tools for the cloud? ***Select all that apply.***

Figure 12. IAM Use for Cloud Security

Finally, we asked respondents if they are using any automation and orchestration tools to improve their cloud security posture. With a gradual shift toward dynamic asset creation and changes, as well as more DevOps-style application pipelines, security teams are seeing a definite need to implement some automated controls and monitoring tactics. The most common tools in use today (more than half) are template technologies for implementing infrastructure-as-code (e.g., AWS CloudFormation, Azure Resource Manager templates, Terraform, and so on). These allow security teams to build in cloud-native controls and monitor them as file contents, which can prove valuable in tracking and keeping up with highly volatile cloud environments. In a change from 2019, more organizations are leveraging serverless technologies than in the past (50% versus 46% in 2019). Security orchestration, automation, and response (SOAR) tools are also in use by almost half of organizations, which presents a strong use case for central control and management of numerous security capabilities ranging from detection to response. One major change from 2019 is in the use of configuration orchestration tools such as Ansible, Puppet, and Chef—in 2019, these were used by close to half of respondents, and this fell to only 36% in 2021. This may indicate a move toward cloud provider native platforms (e.g., AWS Systems Manager) in lieu of third-party solutions. See Figure 13 for the full breakdown of automation/orchestration tools/methods in use today.

These are strong indicators that the use of automation and orchestration tools is growing, which is vital for security teams to keep pace with cloud operations and DevOps teams that want to move faster than ever before.

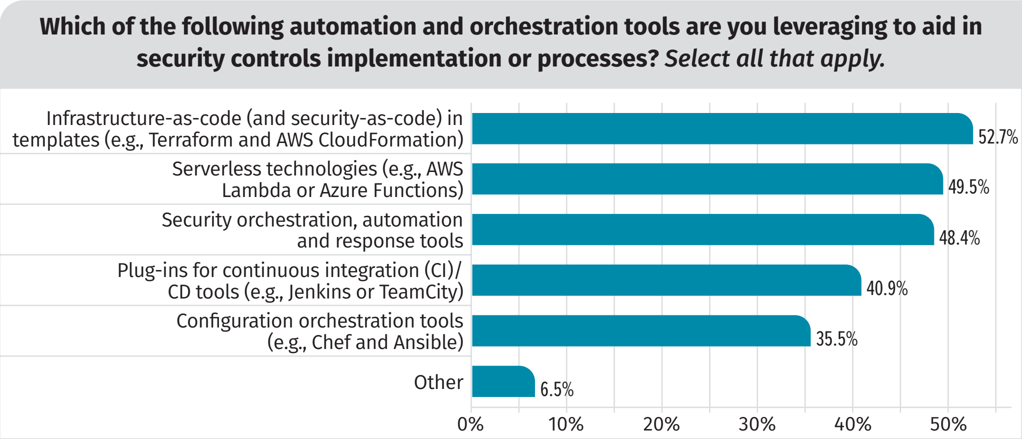
Which of the following automation and orchestration tools are you leveraging to aid in security controls implementation or processes? ***Select all that apply.***

Figure 13. Security Automation and Orchestration Tools and Techniques for Cloud

Auditing and Assessing Providers

A consistent push in the security community has been focused on getting cloud providers to document controls and provide more detail in the form of audit and attestation reports. We've consistently asked survey respondents to tell us which types of audit reports are most useful, because these are often some of the only ways to assess what a provider is actually doing behind the scenes. Here's what we found this year:

- ISO 27001: 52%
- NIST/FedRAMP: 44%
- SSAE 18 SOC 2: 36%
- CSA Cloud Controls Matrix and STAR program: 30%
- Others (CIS Top 20, HITRUST): 9%

ISO 27001 was also the most valuable audit report in 2019, and these numbers align closely with all the responses we received in 2019 overall. This may show that not much has changed in the world of cloud audits and controls reporting, but on the other hand, this may be perfectly OK.

Many organizations are also interested in performing penetration tests against their cloud applications and infrastructure. In fact, they may be required to do so for compliance reasons. Almost 56% of respondents stated that they are permitted to perform penetration tests against cloud assets (essentially the same as 2019), while another 25% can't perform their own tests but receive independent testing reports from the providers themselves. Only 10% are not permitted to test and do not get any reporting from the providers on pen test results (again the same as 2019). Some types of SaaS providers do not allow pen tests due to the application environment configuration, but many PaaS and IaaS providers do, and more providers overall are likely to facilitate pen tests in the future to help clients meet internal standards or compliance requirements.

Conclusion and Parting Thoughts

Every year, we conclude the survey by asking participants to provide general feedback on any other trends, concepts, experiences, and issues they're seeing in the cloud. Many respondents mentioned the need for better APIs and 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 with the shift toward multi-cloud deployments and geographically dispersed cloud environments, privacy issues are likely to become a greater concern, as noted by several respondents. 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 teams aren't getting many needed details about security controls and capabilities from the providers, too.

Overall, organizations seem to be improving the state of cloud security, albeit slowly. Cloud providers are becoming more open and accommodating of security data and controls, and more vendor solutions are bridging the gap between on-premises and cloud. There's progress and greater acceptance of in-cloud controls and services, but there's definitely room to grow.

About the Author

Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

sumo logic