SANS

A SANS Survey

SANS 2019 Cloud Security Survey

Written by **Dave Shackleford**

May 2019

Sponsored by:

ExtraHop

Sophos

Sysdig

Analyst Program

Executive Summary

Since our last Cloud Security Survey in 2017, we've seen a growing number of sensitive data disclosure scenarios and breaches involving the use of public cloud environments. One all-too-common scenario is sensitive data exposure in misconfigured and publicly available Amazon Simple Storage Service (S3) buckets. There are too many to name, but some of note include:[1]

- A Verizon partner leaked personal records for more than 14 million Verizon customers, including names, addresses, account details and even account PINs in several cases.
- An Amazon S3 bucket leaked the personal details of more than 198 million American voters. The database contained information from three data mining companies known to be associated with the Republican Party.
- An ISP left 73GB of incredibly sensitive data in an exposed S3 bucket in late 2018 that included cleartext passwords, AWS keys, network diagrams and more.[2]

The Los Angeles Times exposed its website source code in S3, and in February of 2018, an attacker edited the code to include cryptocurrency mining functions.[3] If the numbers are to be believed, 7% of S3 buckets are wide open to the world, and another 35% are not using encryption (which is built into the service).[4] In June 2018, more than 22,000 container orchestration administration and API management consoles were discovered publicly, and some of them didn't have any authentication in place (and many had weak or default authentication in use).[5] These primarily consisted of exposed Kubernetes platforms that security teams might not have had knowledge of or visibility into. Are these isolated incidents or common occurrences? What are security professionals doing to implement more effective controls within cloud environments?

The goal of the SANS 2019 Cloud Security Survey is to provide additional insight into how organizations are using the cloud today, what threats security teams are facing in the cloud, and what can be done to improve security posture in the cloud.

About Our Respondents

This year, we had several hundred respondents who represent a number of industries. More than 21% are in the technology industry, and more than 11% each are in finance/banking and cybersecurity. Close to 10% are from government organizations, and many other verticals are represented in smaller numbers. Almost 40% work in smaller organizations (1,000 employees or fewer), more than 22% are in midsize organizations with between 2,000 and 10,000 employees, and close to 17% work in large organizations with 50,000 or more employees. Twenty-six percent of respondents are security analysts or admins, 12% are security architects, and 11% are IT managers or directors. Other roles represented include CSOs and CISOs, security managers and directors, and systems admins and compliance analysts. Organizations have operations in most countries, with the United States having the greatest presence (71%), followed by Europe (43%) and Asia (36%). Respondent organizations' headquarters are mostly in the US as well (62%), with Europe (18%) and Canada (6%) rounding out the top three.

---

[1] "Leaky Buckets: 10 Worst Amazon S3 Breaches," https://businessinsights.bitdefender.com/worst-amazon-breaches

[2] "Another S3 Bucket Leak—PocketiNet's Data Exposed!," https://divvycloud.com/blog/s3-bucket-leak-pocketinets-data-exposed/

[3] "Guys, you're killing us! LA Times homicide site hacked to mine crypto-coins on netizens' PCs," www.theregister.co.uk/2018/02/22/la_times_amazon_aws_s3/

[4] "7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks," www.bleepingcomputer.com/news/security/7-percent-of-all-amazon-s3-servers-are-exposed-explaining-recent-surge-of-data-leaks/

[5] "22K Open, Vulnerable Containers Found Exposed on the Net," https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-the-net/132898/

What stands out in 2019? Here are some of the key findings from this year:

- We saw a significant increase in unauthorized access by outsiders into cloud environments or to cloud assets; this occurred at 19% of organizations in the 2019 survey, whereas in 2017 this was experienced by only 12% of organizations.
- More than 55% of respondents in 2017 stated that they were frustrated trying to get low-level logs and system information for forensics, but only 30% said as much in 2019.
- ISO 27001 reports continue to be the most valuable audit reports made available by cloud providers, and more organizations are able to perform pen tests of their cloud provided environments than in the past.

What We're Doing in the Cloud

We asked the community what applications they have in the public cloud, and once again business apps and data top the list (76%). One big change we noted from our last survey was a significant decline in the use of workforce apps such as Dropbox. Only 45% said they were using such apps today versus the 84% who affirmed using such apps in 2017. This could be a simple difference in the respondents, given that SANS sees workforce apps as being a very popular category, so it's one to note and track for the future. Storage and archiving of data, as well as server (workload) virtualization in platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offerings, were also fairly popular. See Figure 1 for the breakdown.

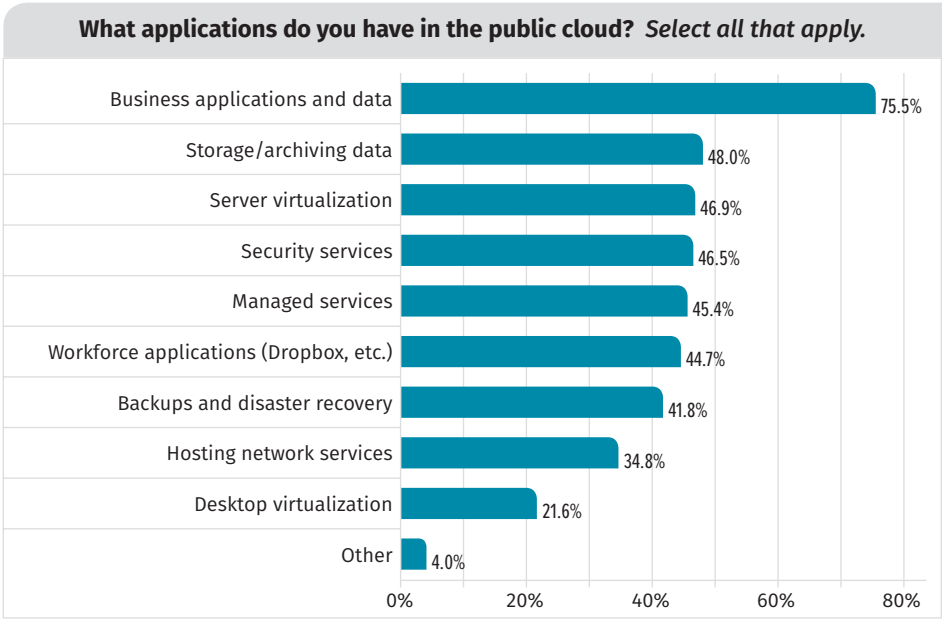

Figure 1. Cloud Applications in Use

This year's survey also saw a consistent response in the number of public cloud providers that organizations are using. In both 2017 and 2019, the highest response category was "two to three providers." A higher percentage of respondents were using only one provider in 2017 (17%) versus today (16%). This slight change may indicate the beginning of a gradual shift toward multicloud. More organizations are using more than 20 cloud service providers in 2019 (7.5% total), versus our last survey, when just 4% used more than 20. See Figure 2 on the next page.

The use of workforce apps, such as Dropbox, declined sharply since our last survey—with only 45% using such apps today versus 84% in 2017.

With the increase in use of cloud applications and multicloud implementations, particularly those that are oriented toward end users, we wanted to find out whether organizations are adopting new tools, such as cloud access security brokers (CASBs) and identity federation platforms, to help centralize control. Almost half of the respondents

(48%) indicated they are using federated identity services to help centralize user access and authorization into cloud applications. Many are also using cloud network access services (43%) and CASBs (35%). Not as many organizations (19%) have adopted a multicloud broker to centralize access to PaaS, IaaS and other service provider environments. 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.

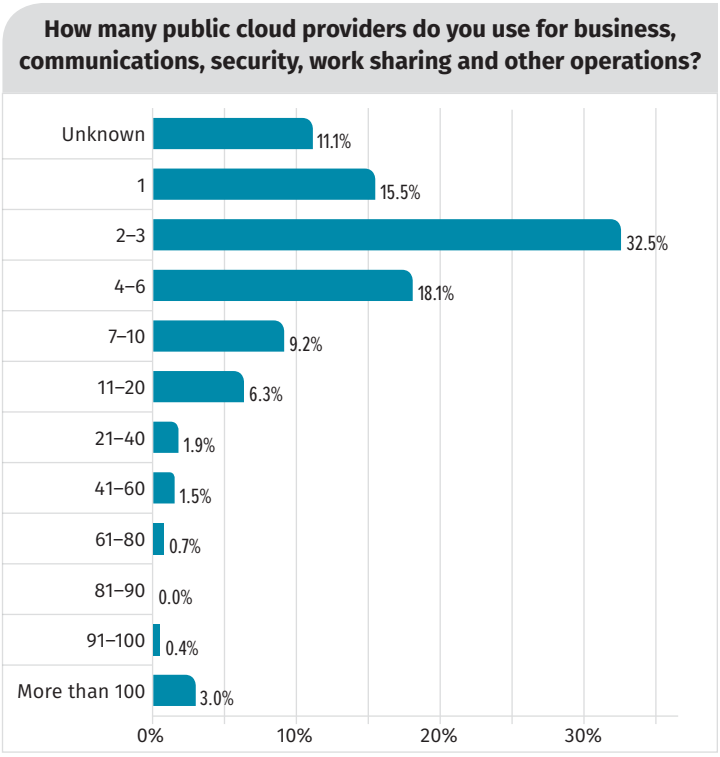

Figure 2. Number of Cloud Providers in Use

As in past cloud security surveys, we looked at the kinds of sensitive data organizations are hosting in the cloud today. Business intelligence topped the list at slightly more than 48%, in a virtual tie with intellectual property (48%), and with customer personal information (43%) close behind. In 2017, business intelligence had come in second, behind employee records. This year, however, that former chart-topper had fallen to fifth place, with only 38% indicating that employee records are being stored in the cloud. Overall, the general trend is very similar to what we saw previously: Roughly one-half to one-third of organizations are willing to put a variety of sensitive data types in the cloud, with lower percentages of some types (customer payment card information was less than 20% in both years, and health records were still lower than some other categories), as seen in Figure 3.

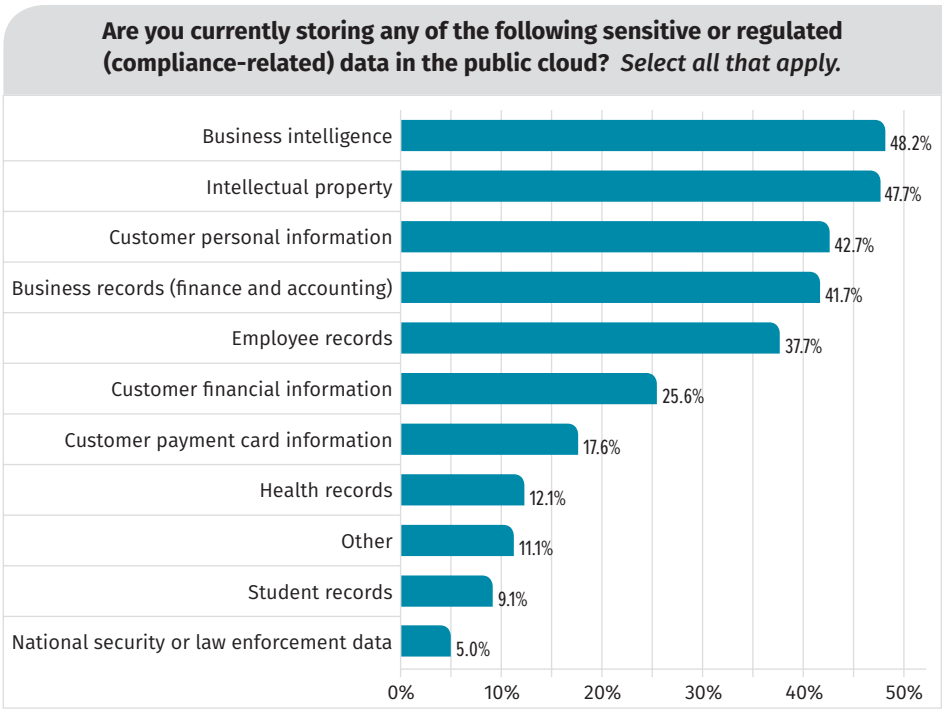

Figure 3. Sensitive Data in the Cloud

More than half of respondents (54%) indicated that privacy regulations such as the General Data Protection Regulation (GDPR) are impacting existing or planned cloud strategies, while 34% disagreed and 12% were unsure. Because of the GDPR requirements, organizations need to ensure cloud providers can adequately meet privacy compliance needs for some data types, especially consumer personal data. We cross-correlated those who answered yes to this question with the location of respondents' headquarters, and those who expressed the greatest concern were based in Africa, Europe and Latin/South America. This is not surprising, given that the European Union is directly affected by GDPR, and surrounding countries and business partners may be under pressure to provide the same protections.

Concerns and Threats in the Cloud

As in 2017, unauthorized access to data by outsiders topped the list of concerns, at 56% (slightly lower than in 2017 but still the highest category). In second position, inability to respond to incidents (52%) moved up from seventh position in 2017, when 48% chose this concern. Other major concerns were lack of visibility into what data is being processed and where (51%, up from 48% in 2017) and unauthorized access to data from other cloud tenants, at 50% (very similar to our responses in 2017). The concern for data breaches by cloud provider personnel dropped from 53% in 2017 to 44% this year, which may indicate some growth in trust in the providers.

TAKEAWAY

The biggest change overall this year was a significant increase in unauthorized access by outsiders at 19%—in 2017 only 12% of respondents' organizations reported this problem.

For the issues that were actually realized, downtime occurrences were fairly consistent from the last survey (up slightly from 18% to 21%). We also saw an increase in misconfiguration issues with application components and APIs. See Figure 4 for the full breakdown of concerns and actual incidents.

More than likely, some of these issues go hand-in-hand. By exposing poorly configured applications and API interfaces (such as the Kubernetes APIs mentioned earlier), organizations are inviting access by attackers who are constantly using tools such as Shodan and network scans to look for targets. In 2017, the biggest issues that actually happened were downtime, misconfiguration and failure to meet service levels. While these are all still problems seen currently, they are overshadowed by actual attacks, which seem to have surged in the past few years.

Have these attacks and incidents actually led to cloud breaches in the past 12 months? Fortunately, the answer seems to be no for now—72% of respondents said they weren't aware of an actual breach, compared with 59% in 2017. This is good news, assuming that lack of awareness isn't an issue in itself. While 7% just aren't sure at all (compared with 21% in 2017), 11% said they did experience a breach, and another 11%

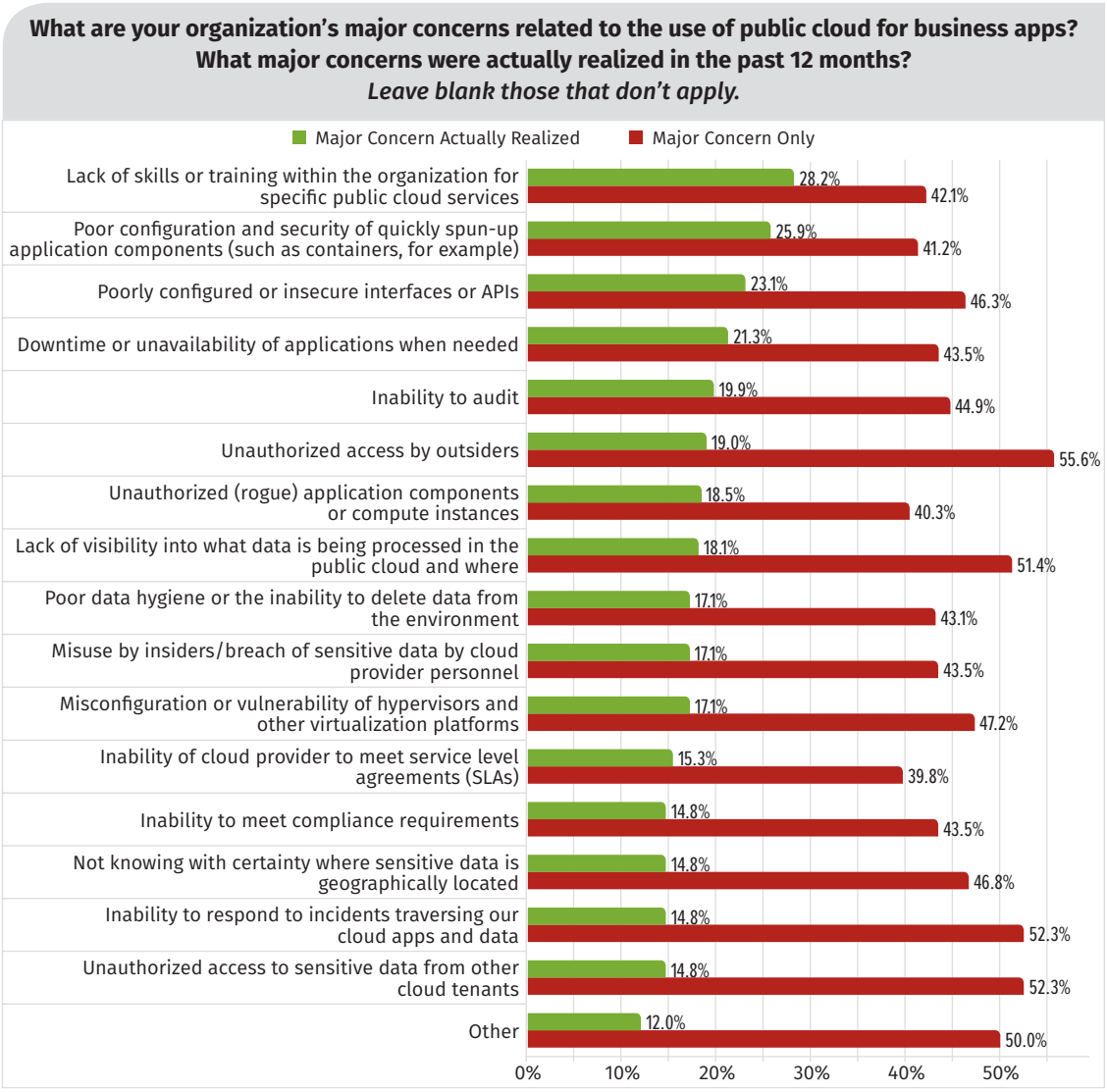

Figure 4. Concerns and Incidents in Cloud Today

think they've had one but can't prove it. The percentage of those who have (or believe they have) experienced a breach is roughly the same percentage as in 2017, which could be good or bad news, depending on how you want to see it: On one hand, things haven't gotten worse (superficially). On the other hand, why haven't we cut this number down in the past few years?

In 2017, we looked at what was involved in the successful attacks, and the top response was DDoS, followed by misconfiguration or other issues with hypervisors and virtualization management. The third major issue was the compromise or hijacking of credentials, but this was the No. 1 issue in 2019, with 49% experiencing this attack vector. Next in order was misconfiguration of cloud services or resources (42%), and then privileged user abuse (38%). These changes likely reflect the shifting nature of cloud, as well as maturity with providers and controls we have available to us. Virtualization elements are completely managed by public cloud providers, and so the surface area for attacks to this layer is greatly reduced.

DDoS attacks are still happening, but they don't seem as prevalent in breach scenarios due to improvements in DDoS protection from both the public cloud providers and the third-party services that have grown in popularity in the past several years. We're still not protecting credentials as well as we should, and misconfiguration of cloud resources is a pervasive issue, as evidenced by the plethora of exposed S3 buckets and APIs we see 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 things involved in the cloud attacks our respondents experienced is shown in Figure 5.

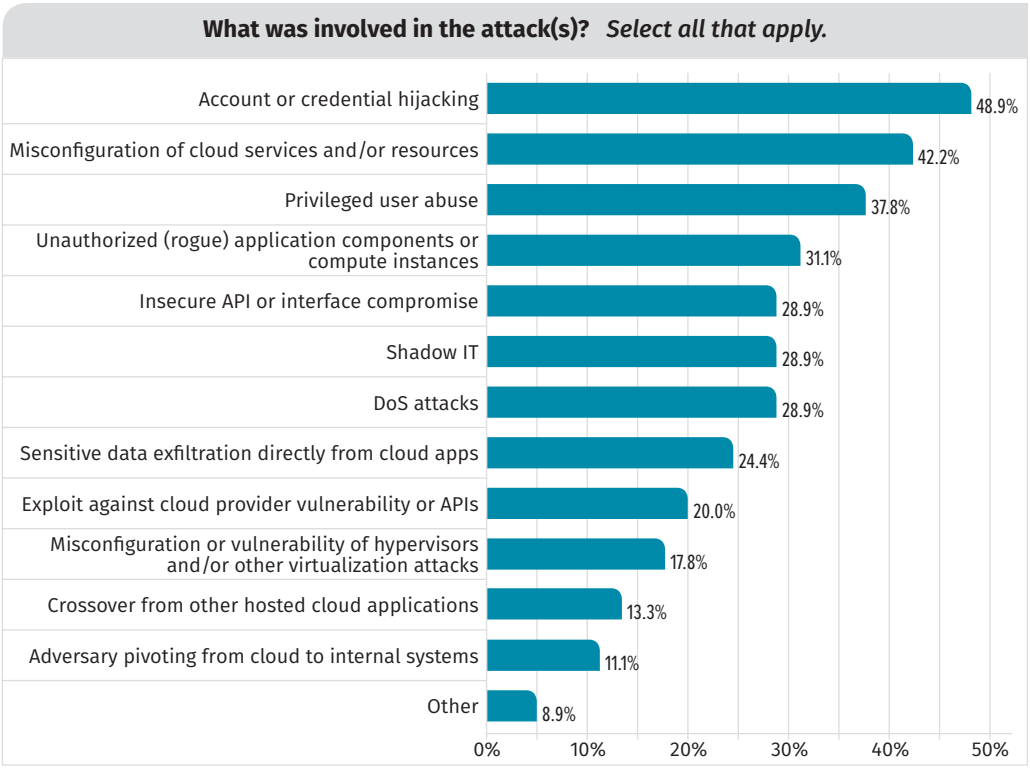

Figure 5. Cloud Attacks

While it sounds as if most organizations haven't yet experienced breaches in the cloud, it may be too soon to know, given that many are unsure. This could also indicate a need for improved visibility into cloud and container environments overall. For those that did experience attacks or exposures, most of them related to credential hijacking and misconfiguration of cloud resources, which are both familiar issues to security teams.

Cloud Security Programs Today

As cloud use grows, organizations must develop and enhance their processes and governance models, so they evolve congruently. Today, 68% of organizations have cloud security and governance policies in place, which is up from 62% in 2017; 24% stated that they didn't, and 8% weren't sure. Gradually, we'll see more and more organizations evolve their governance and policy programs to incorporate cloud security and shared responsibility for

controls and processes with cloud providers. In the types of attacks noted, only two would be wholly the responsibility of the provider: cloud provider vulnerabilities or API issues (20%) and hypervisor vulnerabilities or configuration issues (18%).

Security Controls for Cloud Deployments

Through the years, we've 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 rather than standalone platforms. VPN was the most successfully implemented internally managed tool (59%), as it was in 2017. Network access controls and anti-malware were also touted in the 2017 survey as controls that organizations managed well internally, which again matches the results from this year (48% for network access controls and 50% for anti-malware).

TAKEAWAY

The top SecaaS services in this year's survey were cloud encryption gateways and CASBs, network traffic analysis, vulnerability scanning and multifactor authentication.

In 2017, the top SecaaS controls in use were mostly the same, but anti-malware was used more frequently than network traffic analysis. Finally, the top controls managed between internal systems and SecaaS offerings in 2017 were vulnerability scanning and log/event management, where in 2019 the top results were log/event management and multifactor authentication. The full breakdown of controls in the cloud is shown in Figure 6.

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)?

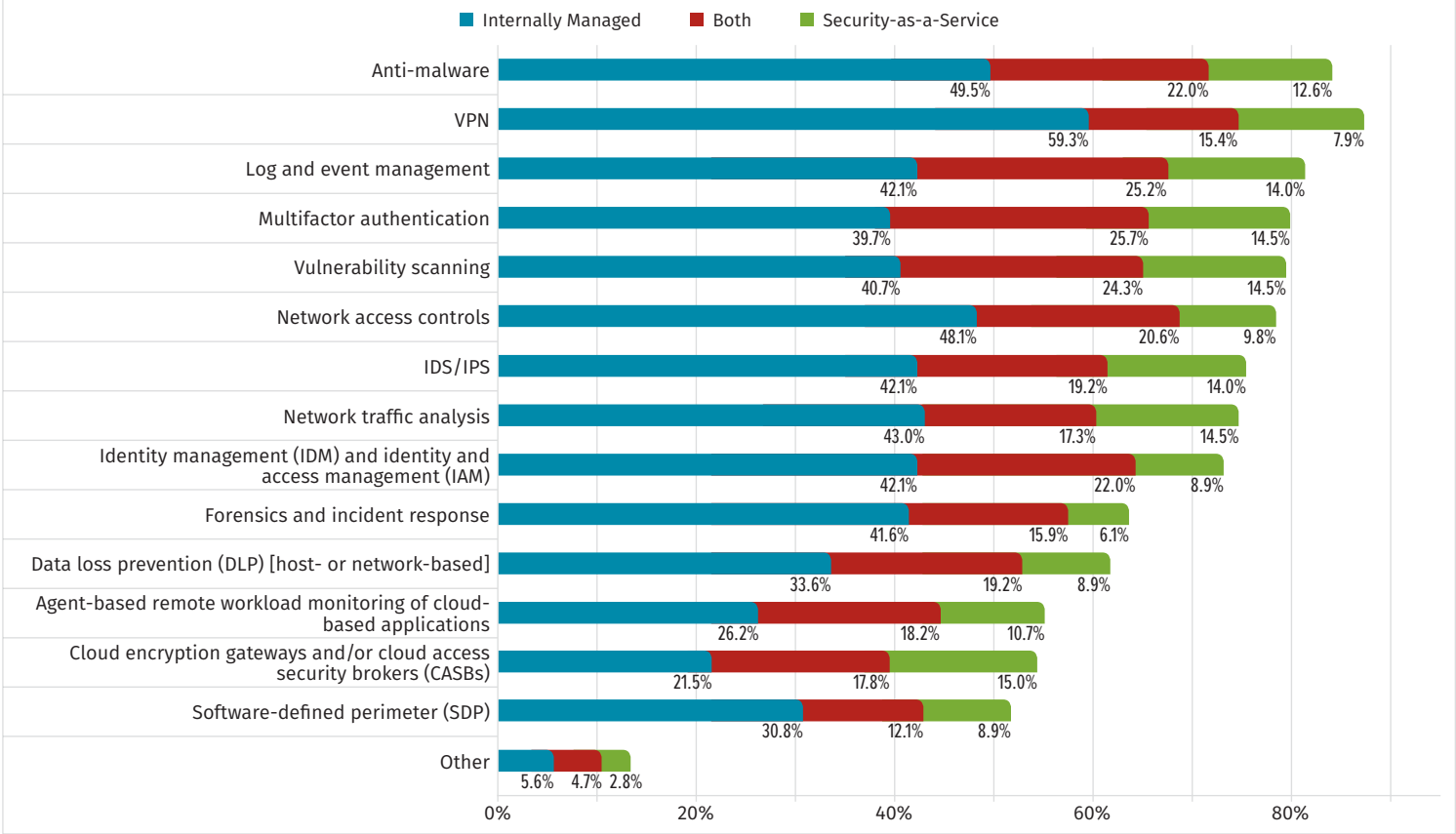

Figure 6. Security Controls for Cloud Adoption

There was a lot of interesting data with regard to controls. 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 (18% for hybrid management) and identity management solutions (22% in hybrid management from slightly more than 16% in 2017). 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.

This concern is somewhat substantiated by the fact that only 44% of respondents stated they are leveraging cloud provider APIs in the cloud to implement security controls (a critical element of automation and cloud security maturity)—almost unchanged from 2017 (43%). For those leveraging these APIs, the most common control is configuration management (75%), followed by logging and event management (72%), and then by identity and access management in third place (59%). These top three categories match what we saw in 2017, which suggests that these are the easiest to tackle through cloud provider-enabled API capabilities, the most critical for organizations to implement, or both. Collectively, though, all of these numbers are higher than they were in 2017, which is a positive trend; nonetheless, it is concerning to see fewer than half of organizations make use of the APIs provided. APIs offered by the cloud provider can afford security teams much more automated and capable access to and control over cloud environments, and hopefully we'll see increased use of these APIs in the future. See the full list of API-enabled security controls and functions in Figure 7.

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

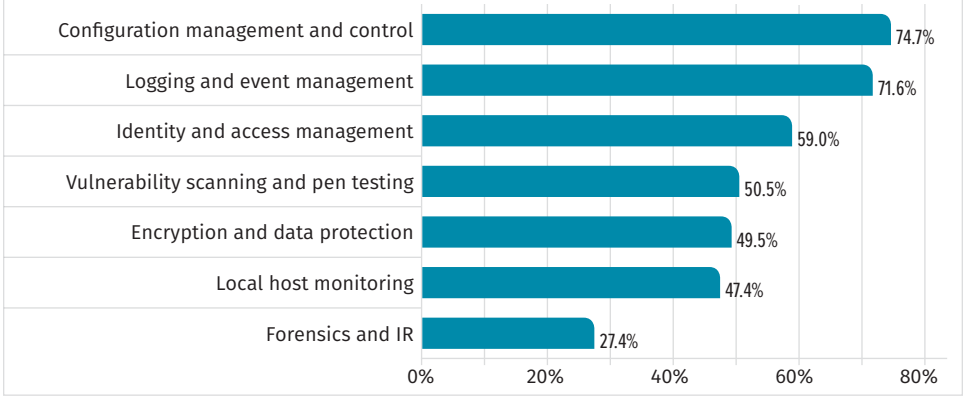

Figure 7. API-Integrated Cloud Security Controls

Integration of Controls

Given that most organizations continue to manage many controls in-house, it's important to break down which controls organizations feel they've successfully integrated between traditional on-premises deployments and cloud environments, creating a true hybrid cloud security model. At present, 65% of organizations feel they've successfully integrated multifactor authentication, 58% feel that vulnerability scanning is well-integrated in a hybrid model, and 57% have anti-malware tools integrated. These findings are similar to the top three technologies from our 2017 survey, though vulnerability scanning and anti-malware are reversed in order.

More than half have integrated network access controls (52%), and 47% have integrated network traffic analysis, which has been notoriously difficult in cloud provider environments in the past. Given many security teams' focus on capturing and analyzing network traffic for signs of intrusion and malicious activity, these are both critical to advance security maturity in the cloud.

Another 45% have integrated SIEM and event management tools, too. This is especially important, given that log and event management is one of the top three controls for cloud adoption (whether internally managed or through a SecaaS offering) and is a control area that involves high use of provider APIs. Because SIEM is a large, complex technology space, seeing its integration growing in a hybrid configuration is encouraging. The full breakdown of hybrid control integration is shown in Figure 8.

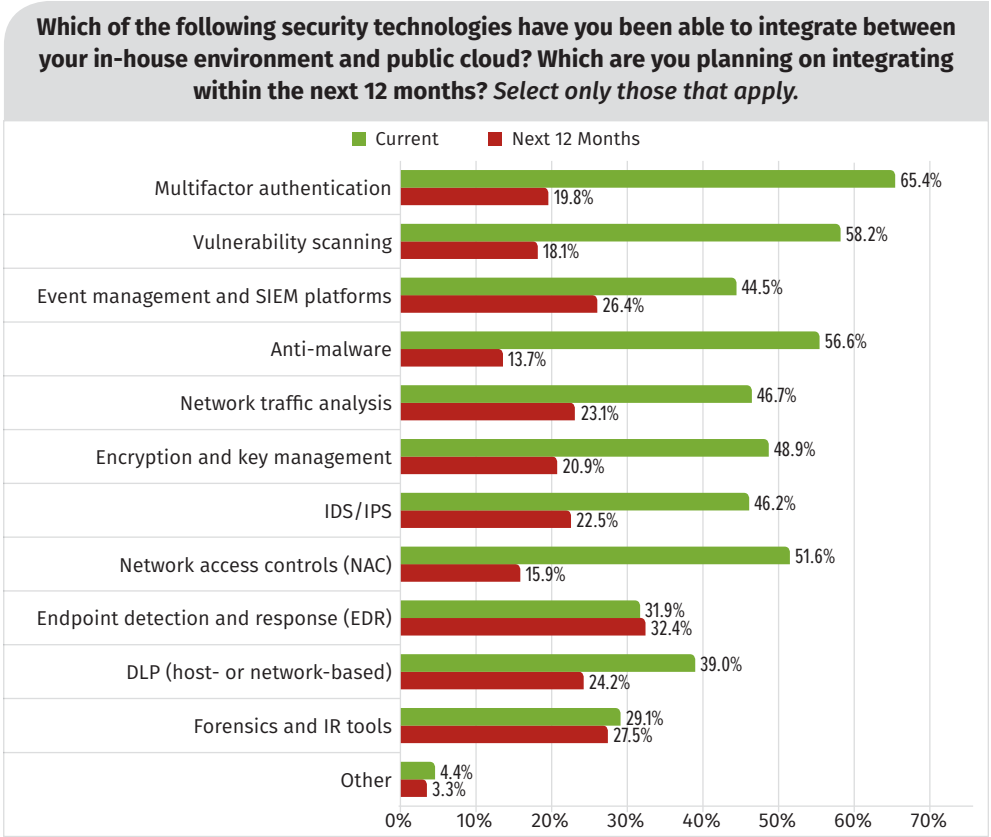

Figure 8. Hybrid Security Control Implementation

Note in Figure 8 that we also asked respondents which controls they planned to integrate in the next 12 months. Nearly a third indicated that they planned on integrating endpoint detection and response (EDR) tools (32%), followed by forensics and IR tools (28%), and then by event management at 26%. 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 organizations what some of their biggest challenges were in adapting forensics and IR to the cloud. The top result was a lack of real-time visibility into events and communications involved in incidents—a problem that EDR and forensics/IR tool integration may help with significantly. Other major challenges cited include the 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 2017, more than 55% of respondents stated that they were frustrated trying to get low-level logs and system information for forensics, and only 30% said as much in 2019. This is a strong indicator that providers are making this evidence more available than before, which bodes well for full integration of IR and forensics capabilities in a hybrid model in the near future. At its heart, this is a data security challenge as much as a visibility issue. The full list of forensics and IR challenges noted is shown in Figure 9 on the next page.

Returning to the concept of unifying and centralizing controls between on-premises and cloud environments, we looked to see 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 the same types

of answers mentioned earlier when expressing confidence in integrating control areas: multifactor authentication, network traffic analysis, vulnerability scanning and anti-malware. 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 answers were given for plans to implement in the next 12 months, too (EDR tools and IR/forensics tools). See the full list in Figure 10.

What challenges have you faced in adapting your IR and forensics analysis to the cloud? *Select all that apply.*

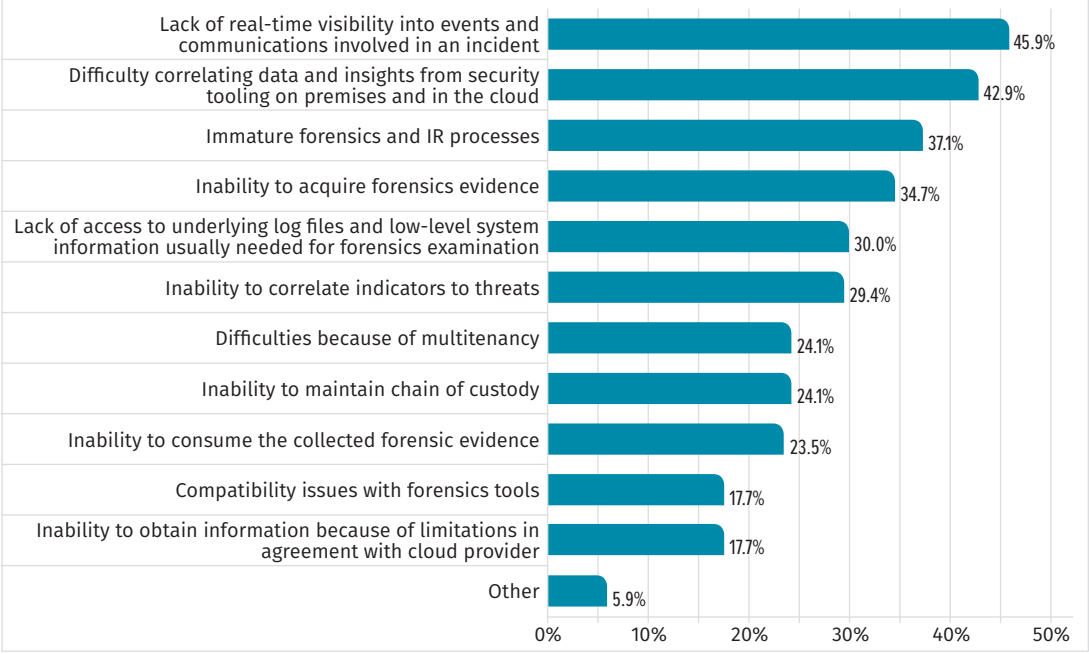

Figure 9. IR and Forensics Challenges in the Cloud

Identity and Access Management

One of the most critical and growing areas of security controls for cloud environments today is identity and access management (IAM). IAM is rapidly becoming an essential element of most cloud implementations. More than half of respondents (52%) stated they were synchronizing in-house user directories to cloud-based directory services such as Azure Active Directory (Azure AD) and others, which is not surprising given cloud services' increasing reliance on access to user entities and attributes. On a related note, many organizations (35%) are also using identity-as-a-service (IDaaS) providers for SSO and federation activity to

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.*

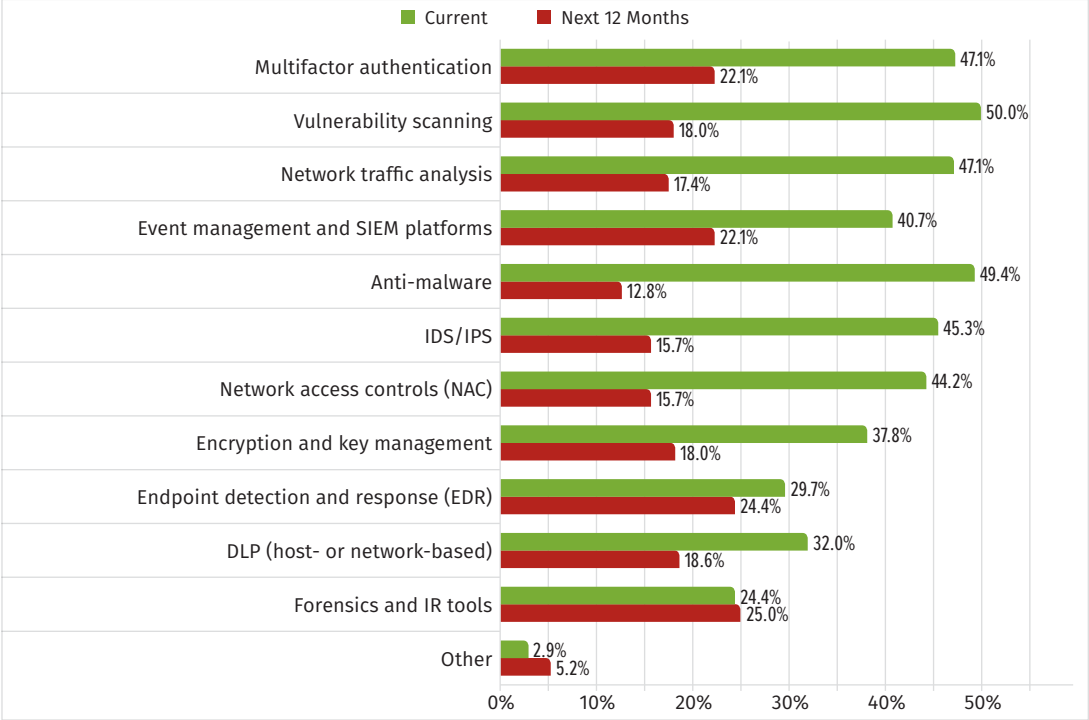

Figure 10. Single-Vendor Control Implementation for Cloud

provision user accounts and attributes to numerous cloud services from a single source. More than a third of respondents (34%) use IAM policies to control object and application access and behavior, too—primarily in PaaS and IaaS clouds. Some are also mapping internal identities to their cloud providers and integrating traditional on-premises IAM suites to the cloud, as well, as seen in Figure 11.

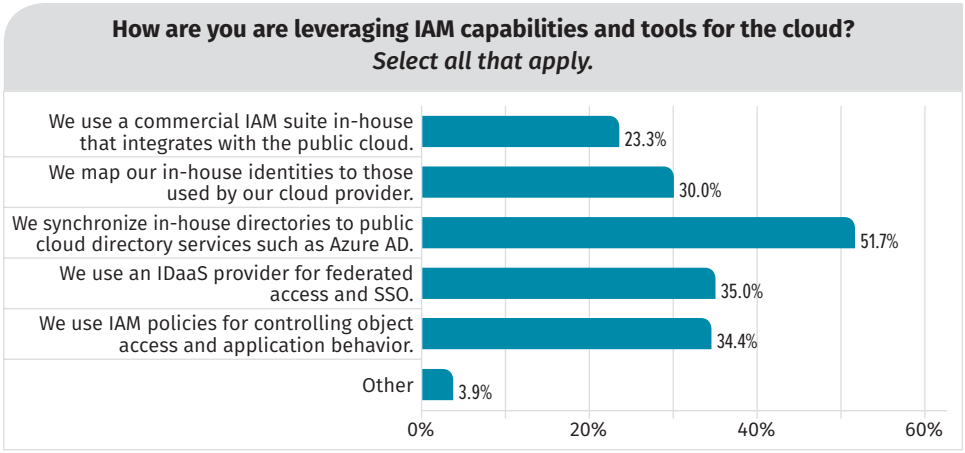

Figure 11. Use of IAM in Cloud

Automation and Orchestration

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. A smaller subset of respondents (55%) voiced their thoughts on automation and integration tools and methodologies. Within that group, the most common tools in use today, selected by more the half of respondents, are template technologies for implementing infrastructure-as-code (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. 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. Configuration orchestration tools such as Ansible, Puppet and Chef are used by close to half of respondents as well, as are serverless technologies for execution of security functions. Not as many organizations have adopted security-specific plugins to build and deployment tools for DevOps pipelines (Continuous Integration [CI]/Continuous Delivery [CD]). See Figure 12 for the full breakdown of automation/orchestration tools/methods in use today.

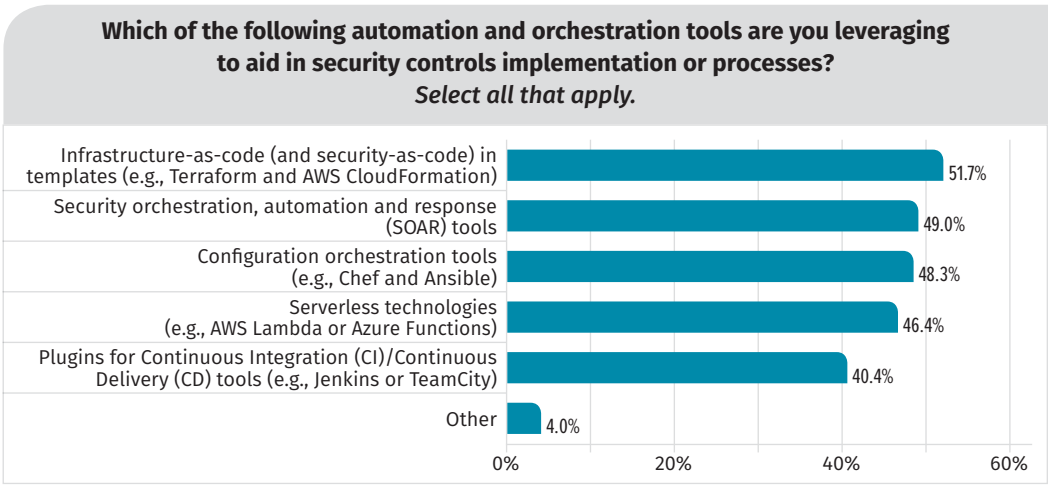

Figure 12. Security Automation and Orchestration Tools and Techniques for Cloud

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.

Auditing and Assessing Providers

A consistent push in the security community has been to get 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 among the few ways to assess what a provider is actually doing behind the scenes. Table 1 shows this year's results.

ISO 27001 was also the most valuable in 2017, but the CSA and SSAE reports were considered the second and third most valuable—the biggest change here is reporting reliance on the NIST Cyber Security Framework (CSF) and other controls, as well as FedRAMP for US government agencies and others to use a brokered, central auditing model in assessing and reviewing cloud provider controls. FedRAMP was considered valuable by only 28% of organizations in 2017, and has obviously grown significantly in maturity and adoption, likely due to increased adoption of the NIST standards in both public and private sector organizations.

Table 1. Audit Report Types

Audit and Security Reports	Percentage
ISO 27001	54.6%
NIST/FedRAMP	48.5%
SSAE 18 SOC 2	42.4%
CSA Cloud Controls Matrix and STAR program	31.5%
Others (CIS, PCI DSS, SIG, HIPAA)	6.7%

Many organizations are also interested in performing penetration tests against their cloud applications and infrastructure. In fact, they might be required to do so for compliance reasons. Almost 55% of respondents stated that they are permitted to perform penetration tests against cloud assets (up from slightly less than 50% in 2017), while another 24% are not permitted to 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 (down from 18% in 2017, which is an improvement). Some types of SaaS providers do not allow pen tests because of the application environment configuration, but many PaaS and IaaS providers do. More providers overall are likely to facilitate pen tests in the future, to help clients meet internal standards or compliance requirements.

This year, nearly 55% of respondents stated that they are permitted to perform penetration tests against cloud assets, while just less than 50% of respondents had permission to do so in 2017.

Conclusion

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 today. This year, we also got feedback from the Cloud Security Alliance (CSA) as to what it is seeing in public cloud adoption and trends. Many organizations are continually evolving in their use of cloud services, looking to the cloud for procurement, management and other functions. The cloud provides capabilities for implementing new technology strategies in IoT and cryptocurrency, too, but many respondents mentioned the need for better APIs and automation capabilities to keep pace with the rapidly changing services offered. Especially as we shift toward multicloud deployments and cloud environments that are geographically dispersed, privacy issues are likely to become more of a concern. Many security teams aren't well versed in cloud concepts, both in design and operations areas and in DevOps/automation tools and tactics; this can be the case with container tools and technology, even more than with traditional server-oriented workloads. The perception remains that we aren't getting many needed details about security controls and capabilities from the providers, too, which limits our comfort level with the providers overall; conversely, some expressed the opinion that cloud may afford significant improvements in security over traditional on-premises data center environments.

Overall, the state of cloud security seems to be improving, albeit slowly. Cloud providers are becoming more open and accommodating of security data and controls, and more vendor solutions are able to bridge the gap between implementations on premises and in the cloud. There's progress, and more acceptance of in-cloud controls and services—but that progress is still slow.

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.

Sponsors

SANS would like to thank this survey's sponsors:

ExtraHop

SOPHOS

Sysdig