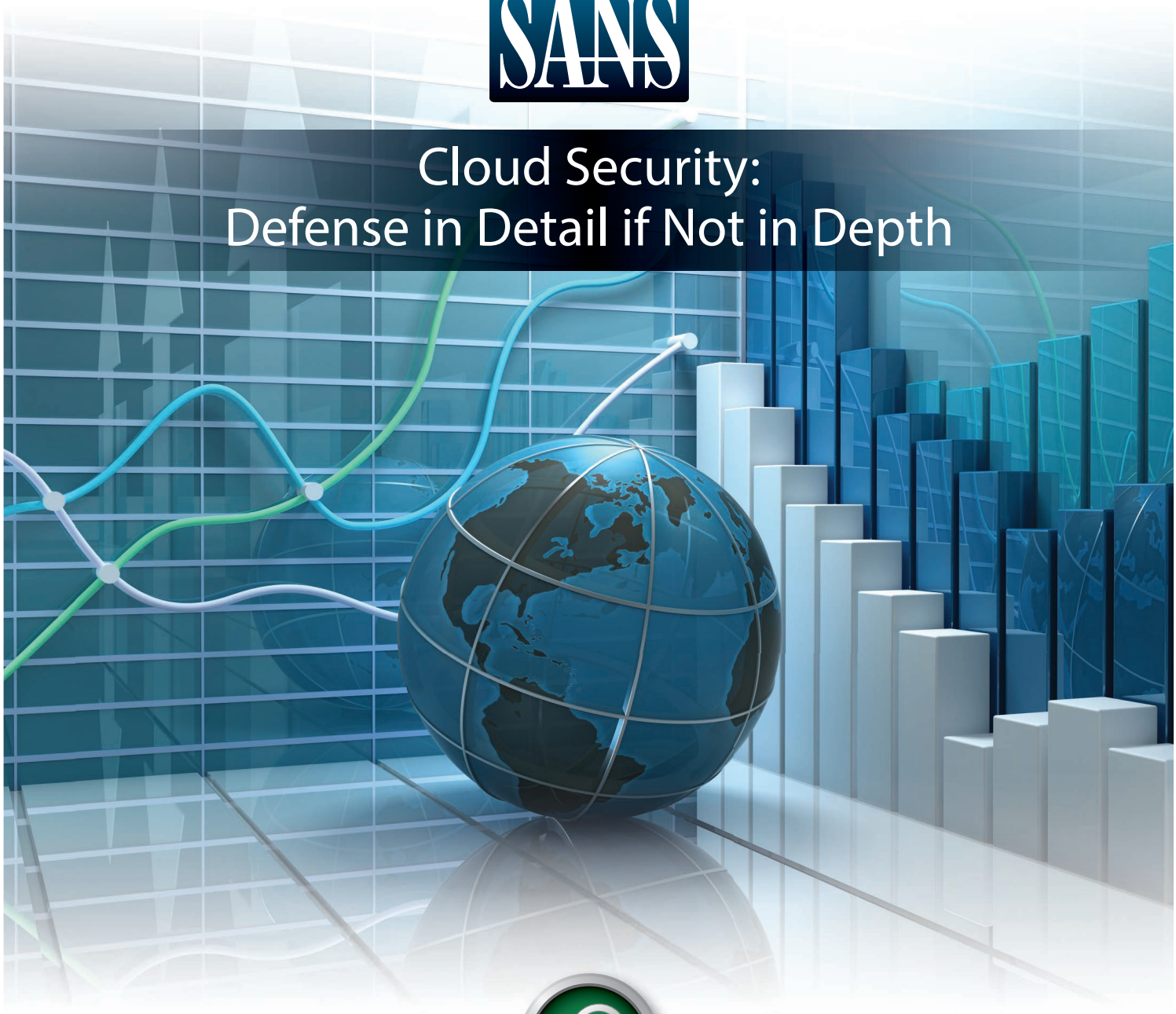
Interested in learning more about security?

SANS Institute InfoSec Reading Room

Cloud Security: Defense in Detail if Not in Depth

Survey respondents feel that they lack visibility, auditability and effective controls to monitor everything that goes on in their public clouds. We are, however, seeing increased use of security controls within cloud provider environments and wider use of security-as-a-service (SecaaS) solutions to achieve in-house and external security and compliance requirements. Related findings and best practices are discussed in the following report.



Cloud Security: Defense in Detail if Not in Depth

A SANS Survey

Written by Dave Shackleford

November 2017

Sponsored by
BMC, Forcepoint, McAfee, and Qualys

Executive Summary

Use of cloud computing services continues to grow rapidly as organizations migrate business applications and data to cloud-based software, platform and infrastructure services. Gartner estimates 2017 will see growth of 18% in spending on public cloud services and that cloud adoption will influence more than 50% of IT spending through 2020.[1]

Deloitte Global predicts that by the end of 2022 more than half of all IT spending will go to IT-as-a-service providers.[2] In the 2016 edition of this survey, 56% of the security professionals responding said limitations on access to collect incident response data and evidence for forensic analysis was a key challenge to securing the cloud. Sixty-two percent said they were concerned about unauthorized access by outsiders, and 59% said they worried about access by other cloud tenants. Of the 10% who reported being breached, half blamed stolen credentials or compromised accounts.[3]

Key Findings

of organizations store employee records in the cloud, and **40%** of organizations store customer PII in the cloud

use multifactor authentication, **46%** anti-malware technology and **41%** vulnerability scanning, topping the list of hybrid cloud controls that organizations have successfully configured today

still feel they are hindered from performing adequate forensic and incident response activities by a lack of access to logs and underlying system and application details in cloud environments

How are things different this year?

As use of the cloud becomes routine, organizations are putting more sensitive customer-related data, particularly customer personally identifiable information (PII) and healthcare records, in cloud environments. In our 2017 survey, 40% said they are storing customer PII in the cloud, as compared to 35% in 2016, while 21% are storing healthcare records in the cloud, as opposed to 19% in 2017.

Security teams cited major concerns this year with regard to their sensitive data. More than 60% worry about unauthorized access by outsiders, followed by insecure, unmanaged devices accessing sensitive info from the cloud, lack of ability to audit and breach of sensitive data by cloud personnel. This aligns with their top controls, in which more than 80% of respondents are utilizing VPN (to secure access), log management and vulnerability management as their top three controls that work for cloud environments. Just under 80% are utilizing encryption, as well.

[1] www.gartner.com/newsroom/id/3616417

[2] https://www.salesforce.com/assets/pdf/misc/IDC-salesforce-economy-study-2016.pdf

[3] "Security and Accountability in the Cloud Data Center: A SANS Survey," October 2016, www.sans.org/reading-room/whitepapers/analyst/security-accountability-cloud-data-center-survey-37327

And while these are their biggest concerns, the 20% who experienced breaches said their top incidents involve downtime/inaccessibility (such as might be expected from ransomware and DDoS), followed by poor configurations and account or credential hijacking.

Respondents also still feel as though they lack visibility, auditability and effective controls to actually monitor everything that goes on in their public clouds. We are, however, seeing increased use of security controls within cloud provider environments and wider use of security-as-a-service (SecaaS) solutions to achieve in-house and external security and compliance requirements.

These, along with other findings and best practices that work for survey takers, are discussed in the following report.

The perspectives presented here represent the experiences of a respondent pool that came from a mix of small organizations (50% employing 2,000 employees or fewer), mid-sized (31% employing 2,001–5,000 employees) and larger organizations (19% employing more than 15,000). Respondents came from a wide range of industries, including technology, cyber security, banking and finance, and government, among many others. The largest portion (22%) were security analysts, with 50% of the sample coming from cyber security roles and the remainder coming from predominately IT roles, with some business unit representation. Although respondents reported doing business in multiple global areas, they are largely based in the United States and Europe. For additional detail, please see Appendix A, "Respondents to This Year's Survey."

Adoption of cloud computing is becoming so pervasive we didn't want to ask respondents if they were following suit, as we had in the past. Instead we asked whether the number of business applications and mission-critical business applications they deploy in the cloud continues to grow.

Pervasive Usage

A small number (7%) said they expect to double the number of business applications they maintain in the cloud; an even smaller number (6%) predicted they would double the number of mission-critical applications. Most respondents said they expect growth of up to 10% in both mission-critical and non–mission-critical applications. But clearly the trend among respondents is to move more applications into the cloud. Table 1 offers more detail.

Table 1. Frequency of Cloud Usage for Applications

Type of Application	Increase by 100%	Increase by 70% to 90%	Increase by 40% to 60%	Increase by 30%	No Change	Decrease
Mission-Critical Applications	6.3%	1. 9%	15.2%	43.1%	32.3%	1.3%
Applications Overall	7.4%	4.3%	24.7%	44.5%	17.3%	1.9%

Business applications and data are most frequently hosted in the cloud, with 96% reporting their organizations are using business applications in private and public clouds. Workforce applications such as Dropbox, designed to help employees access an organization's systems more efficiently, came in second, with a nod from 84% of respondents. Cloud-based disaster recovery and backup services were big as well, showing up in 84% of responses, up from 80% in 2016.

Storage and archiving of data is hosted in the cloud by 80% of respondents. Other critical infrastructure functions are also popular: managed services (78%), server virtualization (77%), security services (77%) and hosted network services (74%). See Figure 1.

What applications do you have in the cloud? Are they hosted in public clouds (outsourced to third party like Amazon), in internally managed private clouds, or both?

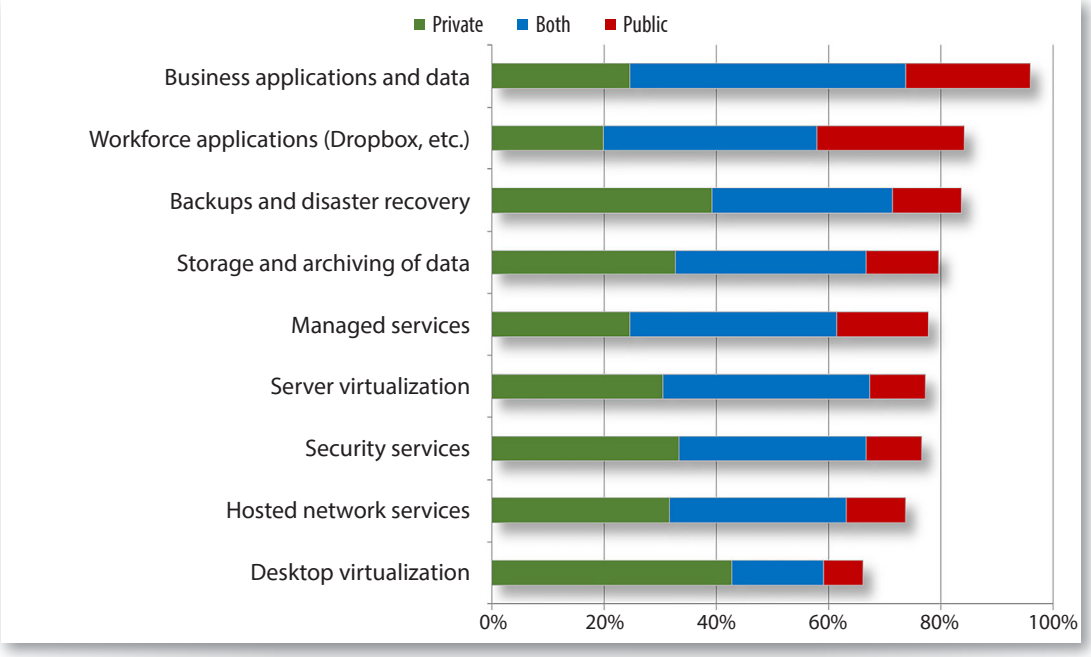


Figure 1. Workloads and Applications in the Cloud

Public, Private and Hybrid

One interesting trend of note is the significant use of private cloud services (or a mix of private and public) versus using only the public cloud for most applications and workloads. Workforce applications saw the highest public-only deployment scenario, with 26%, followed by general business applications, with 22%. The function housed most frequently in private clouds was desktop virtualization, at 43%, followed by backup and recovery at 39%.

Most organizations are using multiple public cloud providers these days, too. See Figure 2.

Please indicate how many public cloud providers you use for business, communications, security, work sharing and other operations.

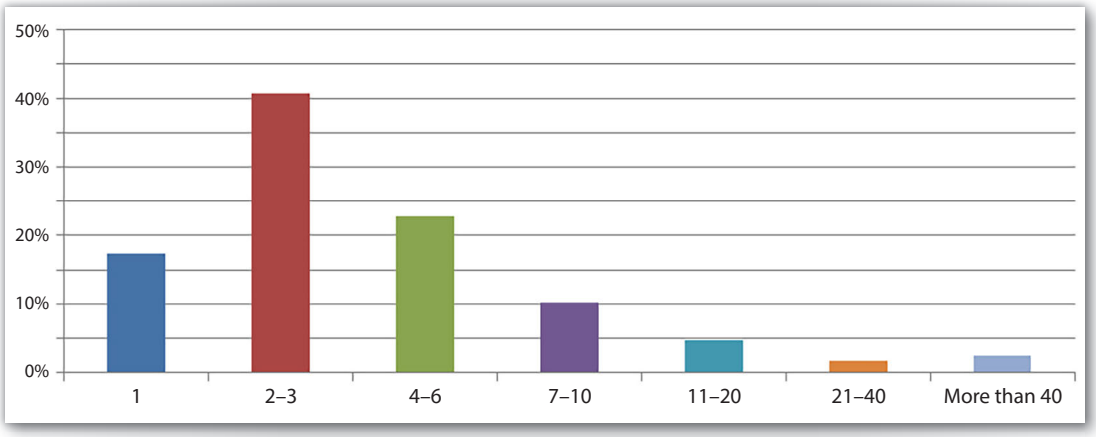


Figure 2. Number of Public Cloud Providers Used

While 17% stated they currently use only one cloud service/provider, almost 41% are using two or three, and another 23% use four to six. Nineteen percent are using seven or more.

Sensitive Data in the Cloud

The percentage who said their organizations store customer PII in the cloud rose from 35% in 2016 to 40% this year, but the percentage of customer financial records in the cloud has decreased slightly from 24% in 2016 to 22% in 2017. There was also a 2% jump in those storing medical records in the cloud. Other than that, there were minimal differences in data types utilized in the cloud from 2016. Table 2 presents the types of being data being stored in the cloud last year and today.

Table 2. Sensitive Data in the Cloud

Type of Data	2016	2017
Employee records	48.2%	47.5%
Business intelligence	40.9%	42.6%
Business records (finance and accounting)	37.8%	38.3%
Customer personally identifiable information	35.4%	40.4%
Intellectual property	35.4%	34.0%
Customer financial information	24.4%	22.0%
Health records	18.9%	21.3%
Customer payment card information	18.3%	19.2%
National security or law enforcement data	11.6%	6.4%
Student records	11.0%	10.6%
Other	6.7%	7.8%

The percentage of organizations storing sensitive data in the cloud remains high, however, despite concerns about skills, security, availability and data loss. Last year, 48% of respondents indicated they were storing employee records in the cloud, followed by business intelligence (41%) and business financial and accounting records (38%). This year, those numbers have stayed fairly consistent.

The news in 2017 has been full of cloud security and operational issues. In February, Amazon had a major outage in its S3 storage environment due to operator error.[4] Microsoft Azure also fell prey to a cooling systems outage that affected cloud services hosted in Japan.[5] And in a 2016 report, Gartner indicated that by 2020, 95% of cloud security failures will be the customer's fault.[6]

Top Concerns

As we did in 2016, we asked respondents to state their top concerns about using the cloud, as well as any concerns that actually "came to life" or were realized in the previous 12 months.

Unauthorized access to data by outsiders again took the No. 1 spot on the list of concerns in this year's survey, with mentions from 62% of respondents in 2017, though only 12% reported having it happen. In 2016, 84% cited this concern, with 28% experiencing an unauthorized access.

The possibility that an attacker could penetrate an organization's defenses and steal sensitive data is an obvious concern, but attackers aren't the only thing in the cloud causing information security professionals to worry. The No. 2 concern was that users would circumvent or bypass security controls by accessing secure data with insecure, unmanaged devices (60%). Other top concerns revolved around the potential for disaster created by the inability to investigate when you've been breached, poor data hygiene and dishonest staff at cloud service providers. See Figure 3.

[4] https://aws.amazon.com/message/41926

[5] www.datacenterknowledge.com/archives/2017/03/31/data-center-cooling-outage-disrupts-azure-cloud-in-japan

[6] www.scribd.com/doc/309877508/Market-Guide-for-Cloud-Access-Security-Brokers [Registration required for access.]

What are your organization's major concerns related to the use of the public cloud for business apps? Which reflect actual incidents during the past 12 months? *Leave blank those that don't apply.*

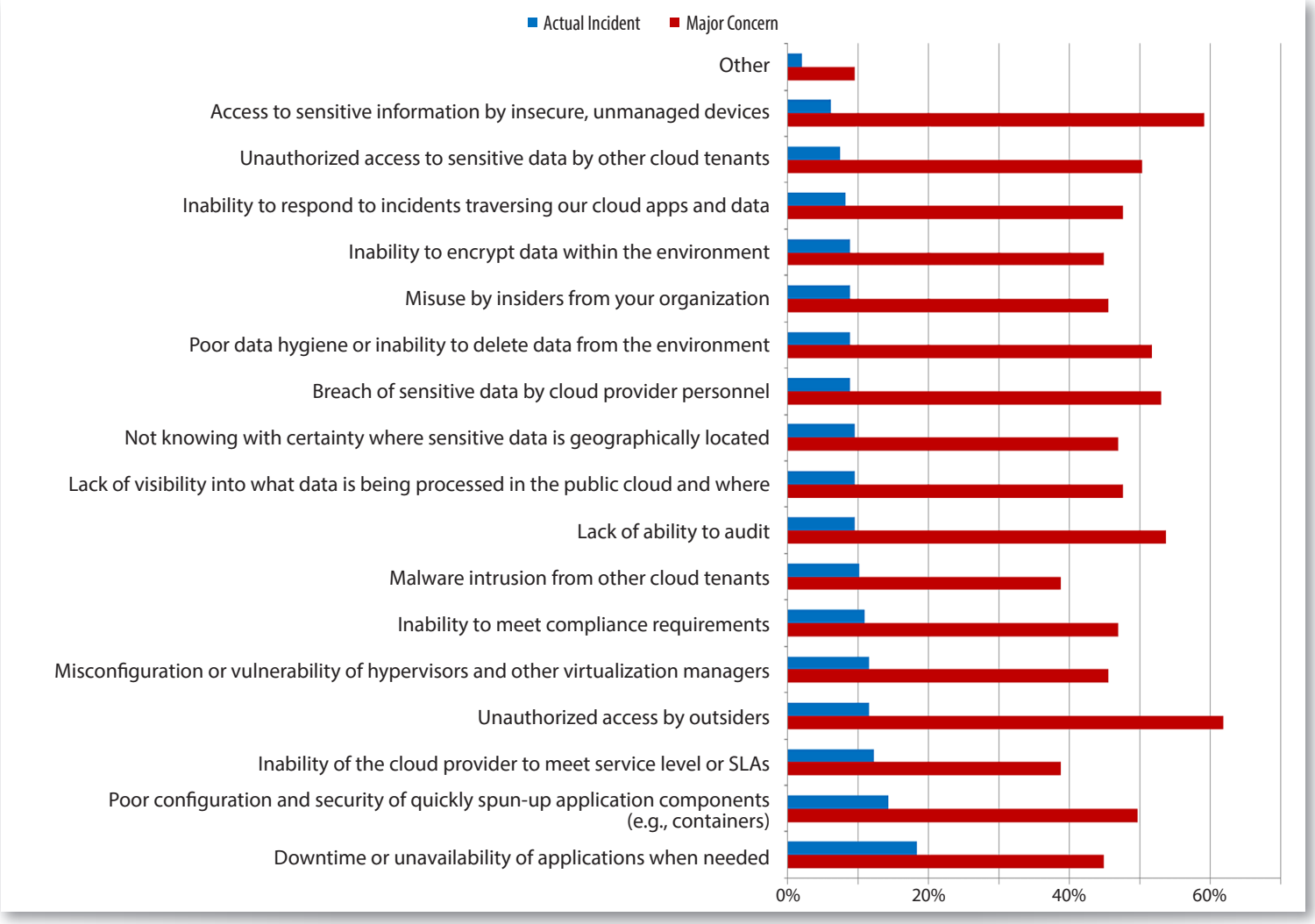


Figure 3. Top Cloud Concerns and Realized Issues

In 2016, 45% of respondents indicated that they experienced some downtime in the cloud, with this number hitting only 18% in 2017. In 2016, many also stated that they experienced a lack of visibility in the cloud (38%), and this number was way down in 2017 (10%). Could this indicate improved security controls and tools in the cloud today?

Attacks on Cloud Applications and Workloads

Respondents' concerns don't necessarily represent their biggest breach areas, however. For example, unauthorized access by outsiders is their No. 1 issue, followed by access to sensitive data by insecure, unmanaged devices and lack of ability to audit, as previously illustrated in Figure 3.

How Many Breaches?

Last year, slightly more than 10% of organizations claimed they had a breach involving cloud applications and data, which was a slight increase over 2015 (9%). The bad news is that this number went up significantly in 2017—in fact, it almost doubled (20%). This increase is likely due to more attackers focusing on the cloud, particularly on poorly configured cloud applications and management interfaces.

In 2016, 22% didn't know whether they had been breached, and 21% were unsure in 2017. While this represents a slight improvement in monitoring and detection capabilities in the cloud, as well as heightened awareness and more attention being paid to cloud environments by security teams, it is still concerning that almost one-quarter of respondents couldn't say with certainty whether they had been breached.

Cloud Attack Methods

Denial of service (DoS) attacks played a role in 55% of attacks involving the cloud. This was a significant increase from 2016, when DoS was involved in 29% of attacks. Respondents cited account and credential hijacking in 50% of attacks in 2016, and slightly fewer, 42%, experienced such attacks in 2017. Figure 4 illustrates the reported attack attributions.

What was involved in the attack(s)? *Select all that apply.*

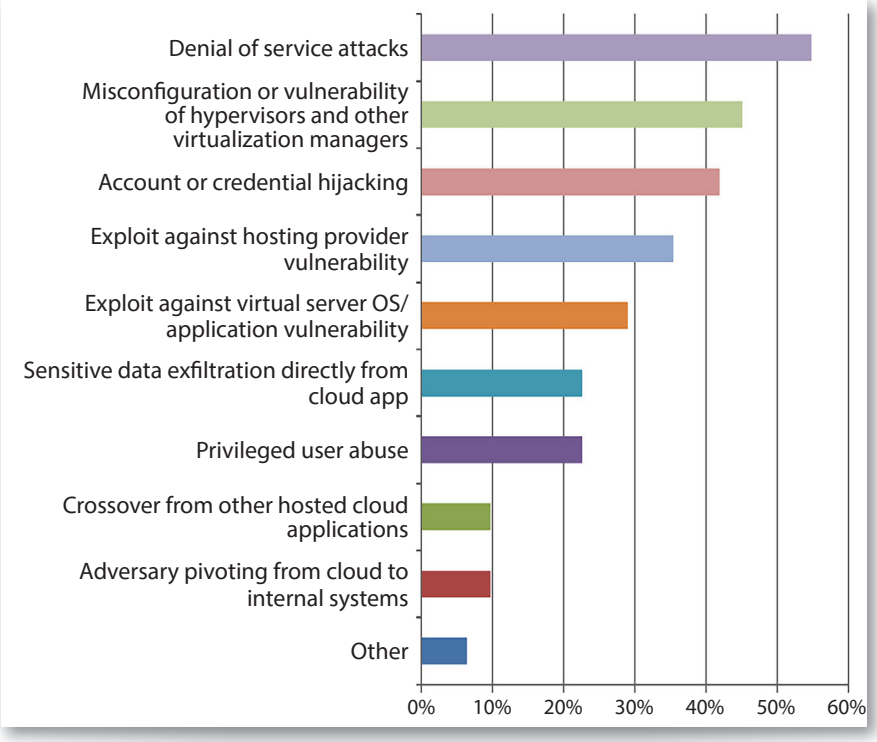


Figure 4. Causes of Cloud Attacks/Breaches

Hypervisors also proved to be surprisingly vulnerable during 2017, with misconfiguration or vulnerability showing up in 45% of attacks compared to just 25% in 2016.

One good example of this kind of issue was discovered in early 2017 within Microsoft Azure, where private keys for the cloud provider's orchestration tools were left embedded in provider-supplied images and discovered by a customer.[7]

[7] www.techcentral.ie/azure-customer-saves-microsoft-rhel-disaster

Lack of Confidence

Most respondents (58%) said they are not fully confident, but have some ability to mitigate risk. Only 16% felt they have full control over cloud risk; another 18% said they aren't sure where they stand, and 8% have absolutely no confidence in their ability to overcome cloud-based risk. Taken together, 26% either don't know or have no confidence!

This may indicate general frustration on the part of these organizations more so than true helplessness. Or it may be the result of a lack of understanding of the shared-responsibility model and the delineation of customer and service provider responsibilities common to most cloud providers. In any event, this lack of confidence is worrisome.

Confidence or Overconfidence?

The 16% who indicated they have full control over cloud risk may be overconfident or may come from organizations that have minimal deployment scenarios to tackle at the moment. It's unlikely that any organization has full control over all risks in the cloud for large deployment scenarios. Respondents from the cyber security and technology sectors, however, expressed more confidence in their abilities to overcome risks, possibly related to their involvement in providing security services.

Improving Governance

Most respondents appear better prepared to support their cloud environments with policy. In this year's survey, 62% said they have cloud security policies and governance in place (up from 48% in 2016). Yet 26% still don't have policies in place, based on results, which aligns with the 26% who don't know or have no confidence.

TAKEAWAY:
Most organizations are taking steps to implement policies and controls for the cloud, working diligently to mitigate risk and to integrate cloud risk and security into their existing programs.

In-house or Outsourced?

Regardless of policy, however, organizations are continuing to find success in managing or outsourcing cloud security controls in a number of areas.

Most security tools were predominantly managed in-house, as we saw last year; however, there was some movement toward security-as-a-service (SecaaS) offerings. Vulnerability scanning in the cloud (in the form of SecaaS) increased from 11% in 2016 to 18% this year. Cloud-based VPN and connectivity solutions, which likely include cloud proxies and connection gateways, increased from 8% to 10%, anti-malware increased from 12% to almost 16%, and identity and access management (IDM/IAM) tools went from 10% to 12%. Small increases, to be sure, but important nonetheless.

Overall, between in-house management and third-party SecaaS providers, most organizations are feeling reasonably comfortable with the majority of foundational security controls today. See Figure 5.

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

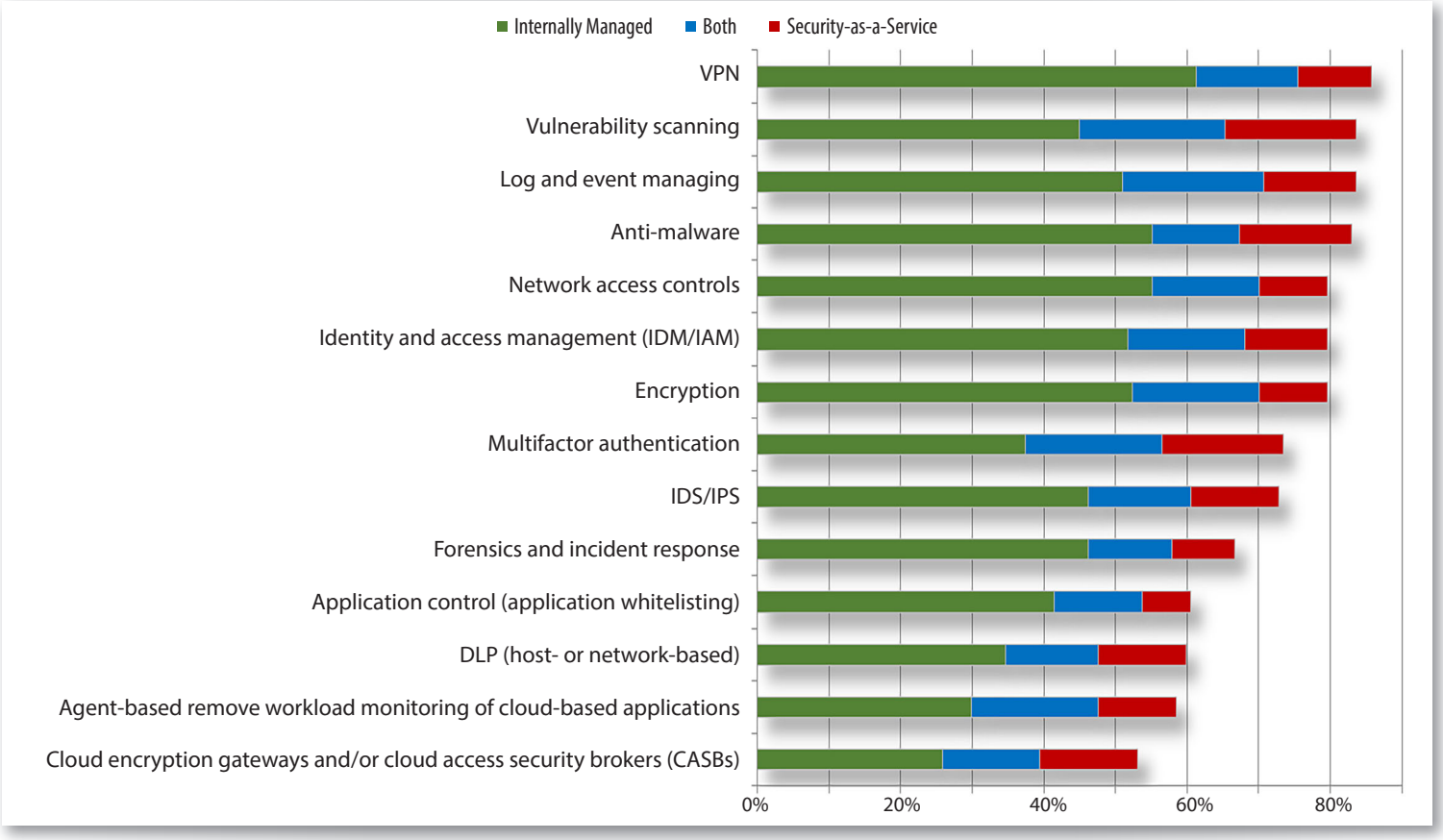


Figure 5. Security Controls in the Cloud

Log and event management seems to be steadily moving toward a hybrid model, as well. Given the expense and hassle of bringing log data back in-house from cloud providers, this makes a lot of sense.

Security-as-a-Service

For those leveraging SecaaS provider controls or integrating their own security solutions and capabilities, there is often a need to integrate with cloud provider APIs. In 2016, 32% of organizations were making use of these, and that number has risen significantly, to 43%, in 2017, which may indicate heavier use of CASB, identity-as-a-service (IDaaS) and other similar solutions. See Figure 6 for the full list of security controls and functions for which respondents use cloud provider APIs.

What types of security controls and functions are you using cloud provider APIs for?
Select all that apply.

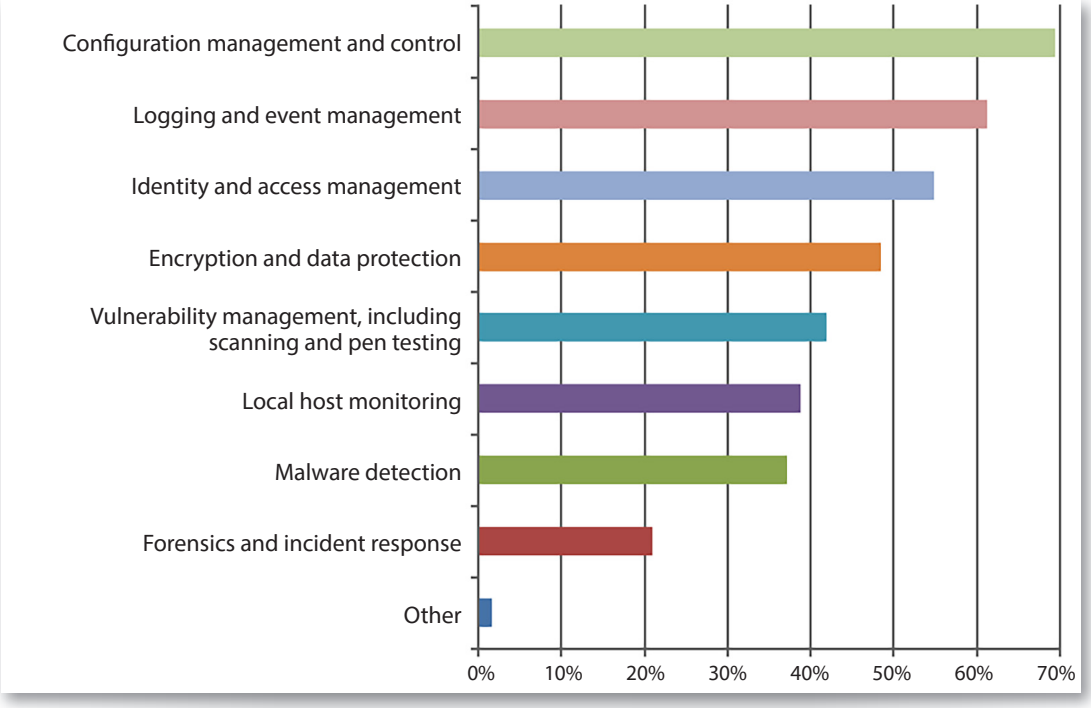


Figure 6. Cloud Security API Use

For those leveraging these APIs, the most common control is configuration management (69%), followed by logging and event management (61%). Identity and access management (55%) was a close third. Configuration management rose from just under 59% in 2016, indicating a strong need to gain control over cloud assets.

Of keen interest to security professionals is finding any controls they can easily integrate between on-premises and cloud environments, creating an effective hybrid controls model.

Unfortunately, not all tools and controls are easily translated into supporting the hybrid model, so this has been a challenge. Fortunately, some technologies are bridging the gap, notably multifactor authentication, anti-malware and vulnerability scanning. However, configuration management was selected by only 19% of respondents, indicating that this is an area where cloud/services providers can meet demand in both their customer's cloud environments as well as on premises. See Figure 7.

Which of the following security technologies have you been able to integrate between the private and public cloud? ***Check only those that apply.***

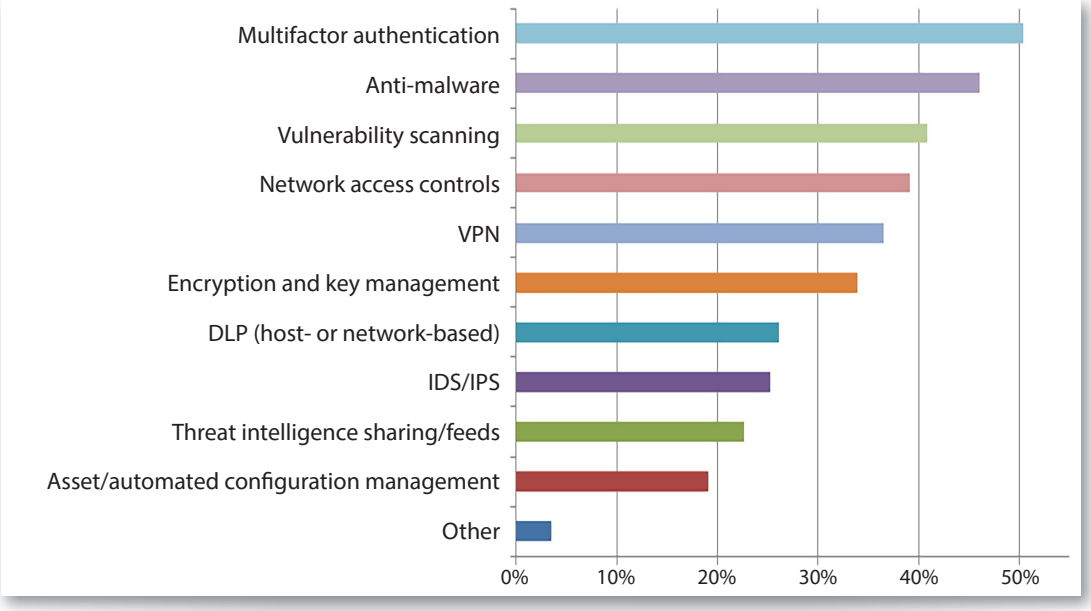


Figure 7. Hybrid Cloud Security Controls

This may explain why many organizations are pushing configuration management to API-integrated cloud models entirely, or it may simply mean that many organizations are struggling with configuration management in general (for both internal and cloud deployments). Sadly, almost none of the control areas we inquired about (other than multifactor authentication) are able to function in a hybrid model for more than 50% of respondents.

Managing the Users

Along with traditional controls listed in Figure 8, we asked how organizations are managing their user accounts for cloud access. Surprisingly, most seem to still be wholly leveraging on-premises directories and single sign-on (SSO). Nine percent say they are using these in-house tools for the public cloud, but 49% are using them for both—on premises and in the public cloud. See Figure 8.

How do you manage your users in private and public cloud applications?

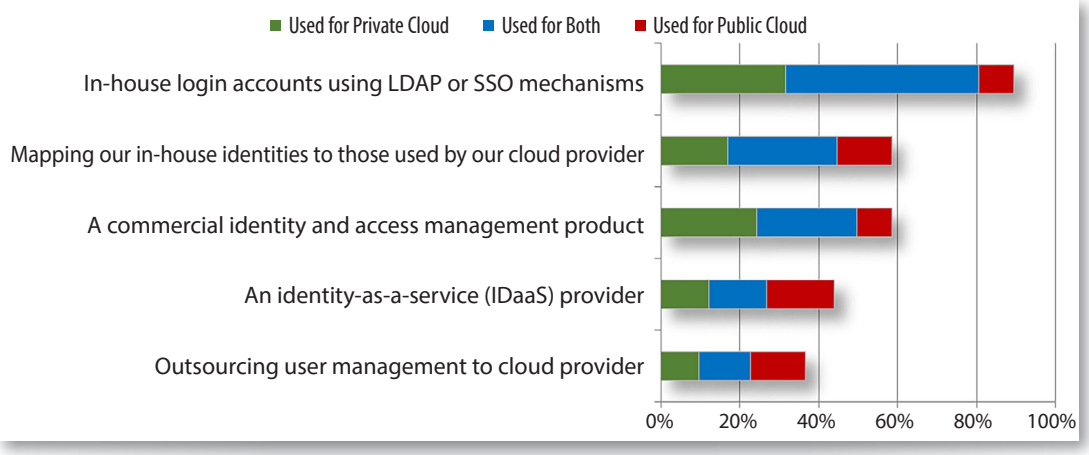


Figure 8. User Management for Cloud

TAKEAWAY:
Keeping identities in sync is important, but so is tracking and managing the life cycle of user accounts and access rights—especially considering the number of hijacked accounts implicated in security incidents and the concern about lack of visibility into cloud environments.

Given the huge growth in the market, we expected more organizations to be using IDaaS providers to manage IDM/IAM for end users needing access to both on-premises and cloud assets. Just 32% of respondents stated that IDaaS was in use in the private or public cloud, although this option had the highest percentage of public cloud adoption. The most popular option was to use LDAP or SSO to enable in-house login to cloud services. Mapping in-house IDs to cloud IDs and the use of commercial IDM/IAM products tied for No. 2 on the list of favorite options.

It's critical that security teams monitor and control user accounts and employee cloud usage, which can be difficult with large numbers of cloud users and many different cloud applications in use. Creating cloud accounts is easy—managing the life cycle of those accounts and deprovisioning them when they're no longer needed is trickier.

Keeping track of what employees do once they connect to the cloud is a tricky question as well. Most organizations in 2016 (30%) employed some form of real-time monitoring and alerting; that number fell sharply in 2017, to 14%. Another 28% were monitoring logs in an event management or SIEM platform in 2016; that number fell in 2017 as well, to 22%. See Figure 9.

How do you control and monitor employee cloud usage?
Select the most appropriate.

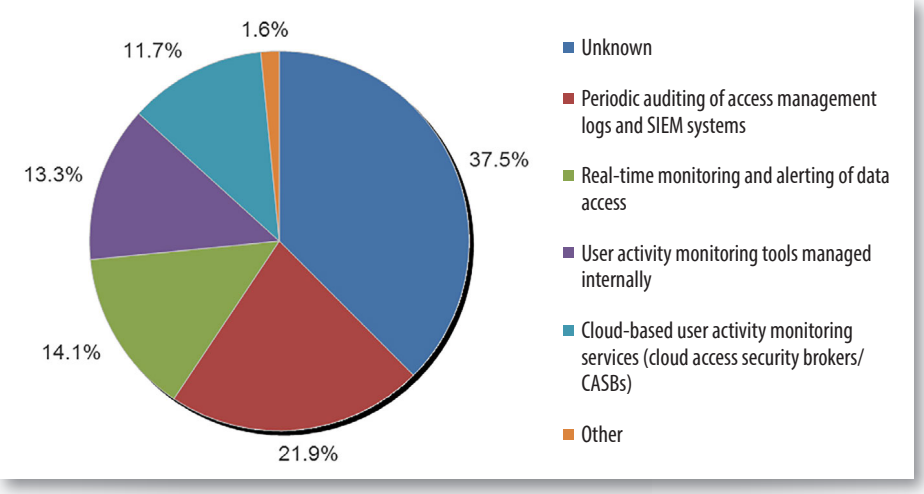


Figure 9. Control and Monitoring for Cloud Users

Surprisingly, CASB solutions were in use by only 12% of respondents. The biggest concern we saw this year was a huge increase in "We don't know" responses (38%). This doesn't bode well given the risks involved in losing control over and visibility into user accounts and data.

Getting to Best Practices

Results are inconclusive with respect to best practices for controlling and monitoring data sent from employee devices to the cloud. Currently, 47% of organizations are still requiring VPN or secured access to the cloud. Others are focusing more on data protection at rest and in transit (44%), and some are using DLP technologies (35%). Aside from these, though, the responses were all over the map. Some are using proxies; others are focusing on data segregation; and still others are using mobile protection tools. The full breakdown is shown in Table 3.

Table 3. Endpoint Control for Cloud Use

Approach to Control and Monitor Data Traversing the Cloud to and from Employee Devices	Percent
Requiring VPN or secure access to cloud-based apps and data	46.9%
Securing data at rest and during transport (encryption, DLP)	44.3%
Applying data loss prevention and protection technologies	34.5%
Separating corporate and personal data and apps	32.7%
Decrypting device traffic with a web proxy	31.0%
Centralizing management for mobile apps, content and devices (e.g., remote wipe)	30.1%
Restricting what applications can be downloaded and installed on a mobile device	26.6%
Using threat monitoring and reporting for network, device and applications/data	25.7%
Knowing, registering and controlling what sensitive data devices are able to access	22.1%
Enforcing data protection policy using an API integration to the cloud application	18.6%
Scanning traffic with an in-line cloud access security broker	18.6%
Using geolocation and tracking of mobile devices	17.7%
Registering and fingerprinting devices that access cloud apps and data (known device)	14.2%
Other	3.5%

Working with Providers

Given that one of the biggest concerns we heard about, and one the industry echoes, is lack of visibility into cloud provider operations, we asked respondents to tell us what types of audit reports they want to see from providers. Table 4 provides the breakdown.

Table 4. Desired Audit Report

Report Desired	Percentage of Respondents
ISO 27001	57.3%
CSA Cloud Controls Matrix and STAR Program	41.8%
SSAE 16 SOC 2	31.1%
FedRAMP	28.2%
Others (SOX, SIG, HIPAA)	3.9%

Audit and Compliance

Many organizations are also interested in performing penetration tests against their cloud applications and infrastructure. In fact, they are required to do so for compliance reasons. Almost 50% of respondents stated that they are permitted to perform penetration tests against cloud assets (up from 42% in 2016), while another 26% can't perform their own tests but receive independent testing reports from the providers themselves. Eighteen percent are not permitted to test and do not get any reporting from the providers on pen test results. Some types of software-as-a-service providers do not allow pen tests due to the application environment configuration, but many platform-as-a-service and infrastructure-as-a-service providers do. More providers overall are likely to facilitate pen tests in the future to help clients meet internal standards or compliance requirements.

Building Better Cloud Defenses

Given the concern about detecting and responding to cloud incidents, we asked security teams what their biggest challenges were in adapting incident detection and response to the cloud. The top challenge cited, which was the same in 2016, was gaining access to low-level forensic and event data normally involved in investigations (55%). In 2016, the second biggest challenge was multitenancy, but this came in third this year, with a lack of understanding of cloud provider data needed for analysis, at 43%, beating it. See Figure 10.

What challenges have you faced in adapting your incident response and forensic analysis to the cloud? ***Check only those that apply.***

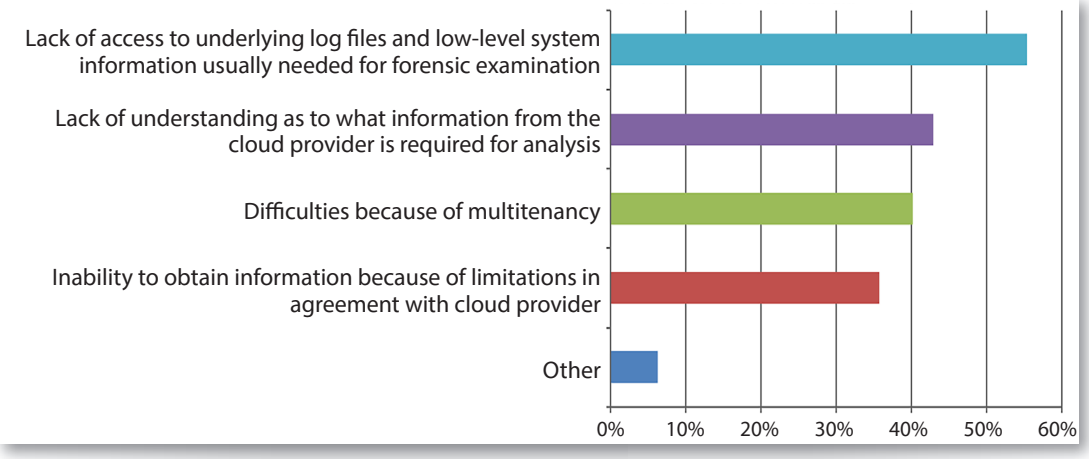


Figure 10. Incident Response and Forensics Limitations

This change in order could be a result of the growing complexity in cloud deployments, where the number and diversity of cloud services and assets is growing. Some teams also felt that they can't really gather the appropriate information from the cloud provider due to limitations in contractual agreements.

Shared Responsibility

In its 2016 "State of Cloud Security" report, the Cloud Security Alliance (CSA) acknowledges there are still many security shortcomings in cloud environments. First, cloud providers need to be more forthcoming with a variety of data, including threat intelligence and incident information, controls status and details, and support for open enterprise architectures. The CSA also acknowledges a significant skills gap in cloud security and a large shortage of qualified security analysts and operations staff to help design and maintain cloud security controls.[8] IT skills gaps are often difficult to confirm. Forbes reported that 49% of respondents to a recent 2017 state of cloud adoption and security report said their organizations are delaying cloud deployment due to a cyber security skills gap.[9]

TAKEAWAY:
Cloud service providers and organizations both have important roles to play in overcoming the cyber security skills gap and improving the state of cloud security.

Looking Forward

It's apparent that we still have a lot of work to do in designing and implementing our cloud security strategies. The open-ended feedback about cloud and security strategies provided by respondents indicate some major themes that must be addressed:

- Respondents would like to see more controls offered natively by providers if possible, which seems to be happening today.
- Security professionals are still looking for controls they can integrate between their on-premises and cloud environments.
- The use of "shadow cloud" was mentioned more than once, with a number of organizations struggling to control this in their environments.
- There is still a lack of balance between on-premises and cloud deployments, with organizations not fully understanding data ownership and the need to carefully define which data stays on premises. Not all applications and data are appropriate for use in the public cloud.
- Security does not have enough involvement in governance decisions, particularly with multicloud deployments.

[8] https://downloads.cloudsecurityalliance.org/assets/board/CSA-GEAB-State-of-Cloud-Security-2016.pdf

[9] www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security [Registration required to access the entire survey.]

Conclusion

This year's survey told us a few things. Organizations are still moving to the cloud—and quickly. Security teams are still uncomfortable with the lack of transparency from the cloud service providers. Monitoring and deprovisioning cloud user accounts is really tough, too.

However, we're seeing better controls in cloud and SecaaS offerings, and more organizations are using multifactor, anti-malware, vulnerability scanning and other mainstay controls in the cloud today. The use of APIs in cloud-based security is increasing. There's still a serious skills gap in cloud security, and that's not helping.

Overall, though, cloud security is improving, albeit slowly. However, until cloud providers become more open and accommodating of security data and controls, it's likely to be a slow process. This is fundamentally the same conclusion we reached in 2016.

The perimeter is changing dramatically, more and more data is now being stored in cloud environments, and we'll need to see changes that are highly data-centric, like Microsoft's Confidential Computing for Azure, or AWS Macie for data tagging and classification. Even these kinds of capabilities will need to be augmented with more cloud-native data security controls and updated processes.

As cloud service providers innovate, the benefits of cloud use continue to grow. But progress and acceptance of in-cloud controls and services continue to lag behind the pace of adoption.

Appendix A: Respondents to This Year's Survey

This year, as in years past, saw qualified responses from professionals in a variety of industries, led by technology, cyber security, and banking and finance. Government (a top three industry in 2015 and 2016) fell to the No. 4 spot. See Figure 11.

What is your organization's primary industry?

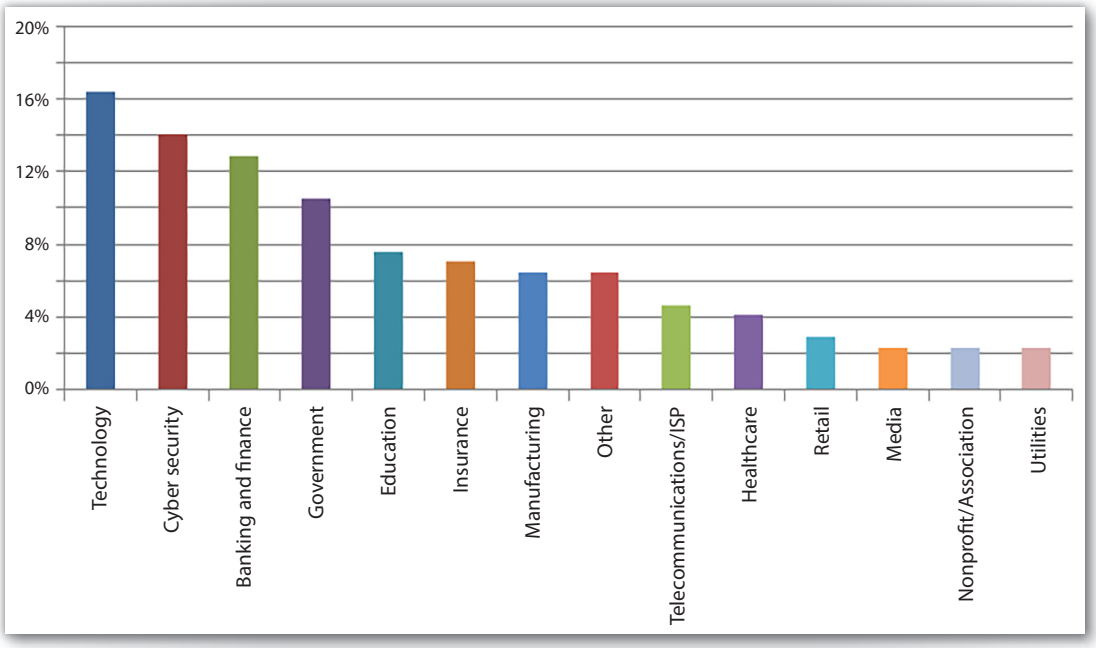


Figure 11. Respondent Industries

Responding organizations were about evenly split between those with up to 2,000 employees and those with more, though responses from larger organizations were relatively balanced among compiled ranges from 5,001–15,000 and more than 15,000 employees. Organizations with fewer than 100 employees made up 17% of responses; those with 100–1,000 responses made up 23%.

By far the most frequent title among respondents was security administrator/analyst, selected by 22%. But responses spread out across a wider range of titles than in previous years, including developers, business managers and compliance/risk managers, all of which are far more commonly involved in overall security operations than they might have been a few years ago. See Figure 12 on the next page.

What is your primary role in your organization, whether as an employee or contractor?

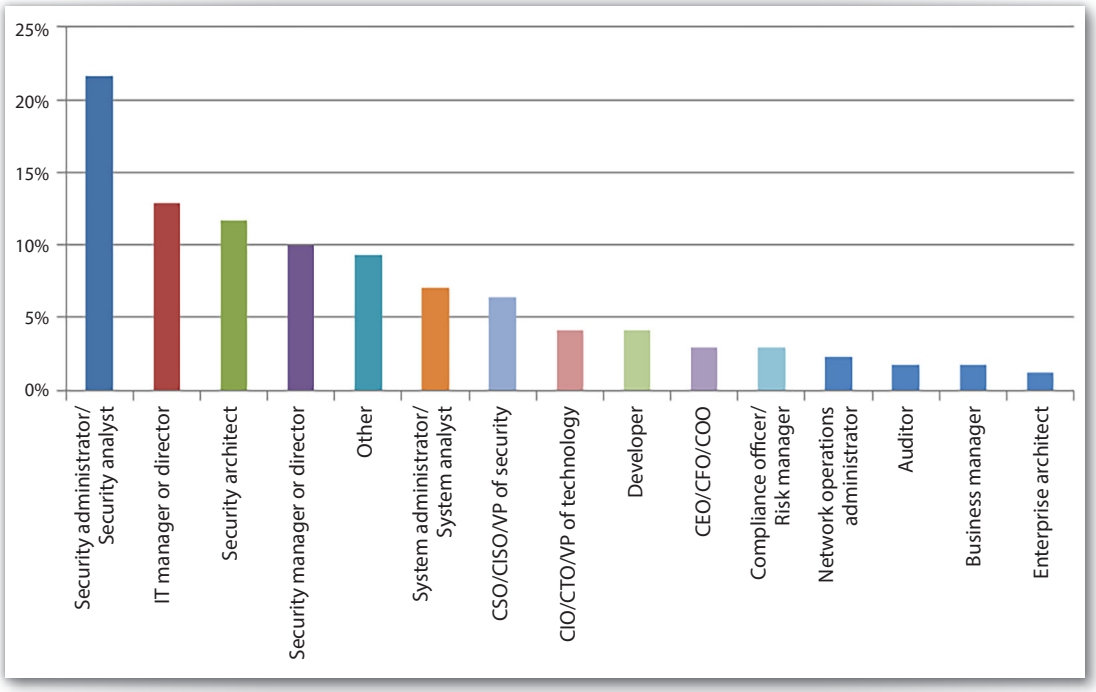


Figure 12. Respondent Roles

Most organizations (65%) are headquartered in the United States, with 14% in Europe, 8% in Canada and 4% in Asia. Respondents also represented organizations with a slightly more balanced international presence.

About the Author

Dave Shackleford, a SANS analyst, 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:

bmc

FORCEPOINT
POWERED BY Raytheon

McAfee™

Qualys®
Continuous Security

Last Updated: December 4th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS Frankfurt 2017	OnlineDE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced