



Interested in learning  
more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Orchestrating Security in the Cloud

Survey results indicate a strong need to keep security close to the data as it traverses cloud systems. Findings also indicate a need to integrate monitoring capabilities across hybrid environments and partnership with public cloud providers for full-spectrum visibility and response. Learn more by in this survey report focusing on cloud security.

Copyright SANS Institute  
Author Retains Full Rights



# Orchestrating Security in the Cloud



## **A SANS Survey**

*Written by Dave Shackleford*

September 2015

*Sponsored by  
CloudPassage, Evident.io, HP, and Intel Security*

# Executive Summary

Collaboration services, email, managed services, and backups and disaster recovery are the most common current use cases for cloud services, according to the results of a new SANS survey on cloud security. The 485 IT professionals who participated in the survey reported using a variety of cloud providers and service models, including software-as-a-service (SaaS) cloud offerings, along with a fairly even mix of infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) implementations. Most respondents said they are investing in both public and private clouds as needs dictate.

## Key Findings

40%

of survey respondents store or process sensitive data in the cloud

40%

cited unauthorized access to sensitive data from other tenants as the most pressing concern with public cloud deployments

33%

do not currently have enough visibility into their public cloud providers' operations

33%

of those organizations that have experienced breaches in the cloud cited malware as the top private cloud attack vector, while 36% said DoS is the top attack vector in the public cloud

However, while cloud services provide the functionality businesses need, they also come with increased security risks, particularly given that 40% of respondents said they process sensitive data in the cloud. Concerns include lack of control over access to data, geographic location of sensitive data, compliance, and visibility and security controls built into organizations' public and hybrid cloud environments.

Along with these issues, more than 27% of respondents said they have little or no incident response support within their public cloud implementations, citing a litany of problems, including an inability to determine who is responsible for security and compliance in the cloud and how to implement and assess security controls.

Overall, survey results indicate a strong need to keep security close to the data as it traverses through cloud systems—not only through encryption, but also by controlling permissions and access. Findings also indicate the need for organizations to integrate monitoring

capabilities across their hybrid environments and partnerships with public cloud providers for full-spectrum visibility and response.

These and other survey highlights are covered in the following report.



# State of Cloud Computing

## HYBRID CLOUD

An infrastructure that links private (enterprise-run) and public cloud implementations to gain business advantages, but the segments remain separate entities

## PUBLIC CLOUD

An infrastructure typically managed by a third party in which space is available to multiple tenants that share resources

## PRIVATE CLOUD

An implementation, available on-premises or as a segment of the public cloud, that provides separate resources and computing environments for different tenants

Because of its flexibility and cost savings, more organizations are moving workloads to the cloud than ever before. According to Forrester Research, "In 2015, cloud adoption will accelerate and technology management groups must adapt to this reality by learning how to add value to their company's use of these services through facilitation, adaptation and evangelism."<sup>1</sup>

## Architectures

Clouds are being developed to support many types of business services using a variety of architectures. Hybrid cloud architectures are the most commonly used among survey respondents, with 40% currently deploying them and 43% planning to move in that direction in the next 12 months. Private cloud implementations are close behind at 38%, while 12% use public cloud implementations. See Figure 1.

**Would you classify your organization's current cloud computing model as primarily public, private or hybrid? Do you foresee this being the case in the next 12 months?**  
*Select the most appropriate response.*

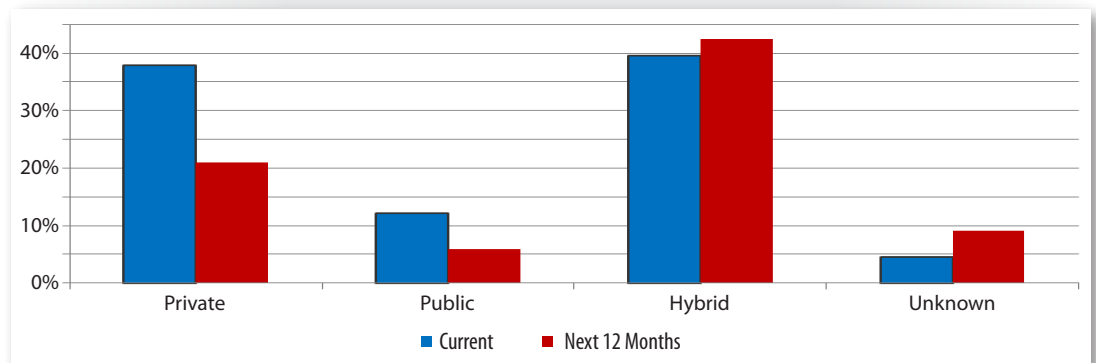


Figure 1. Primary Cloud Architecture Models in Use

Some private and public cloud strategies are planned for the next 12 months, but the vast majority of respondents seem to be balancing internal and public cloud resources.

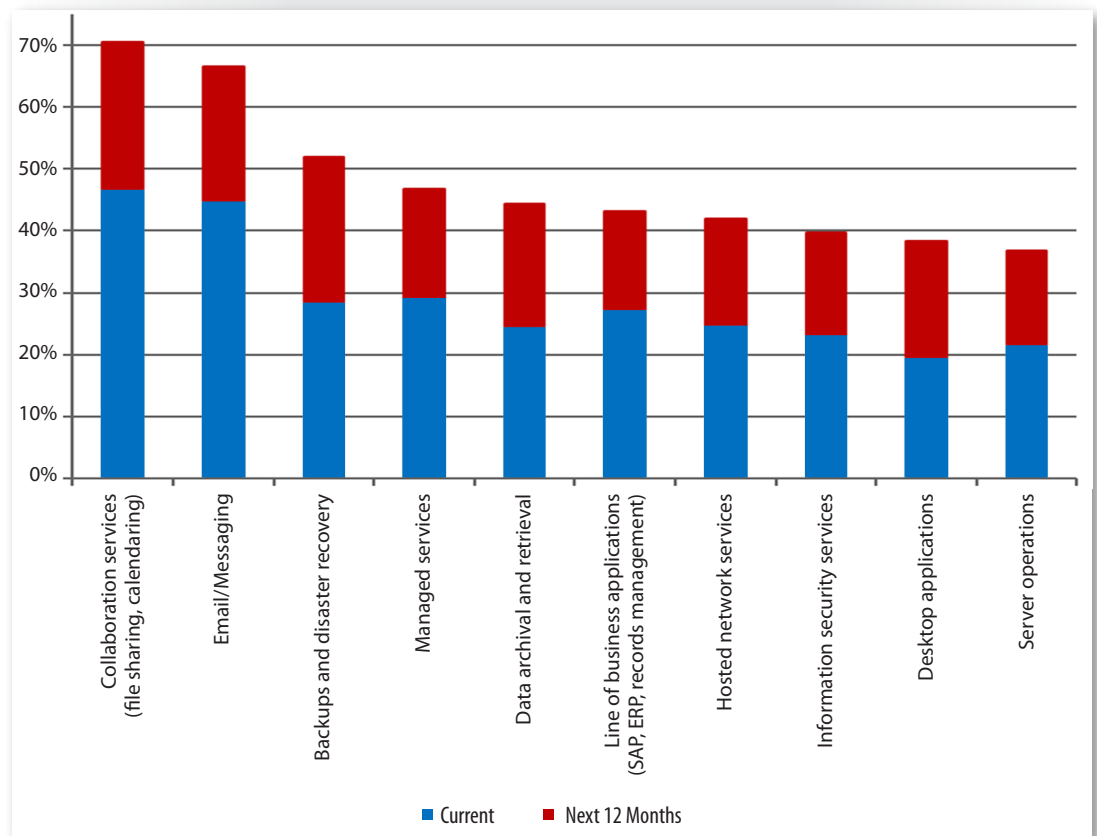
<sup>1</sup> <http://whatsthebigdata.com/2014/12/02/top-2015-it-predictions-from-forrester-research>



## Business Workloads in the Cloud

Respondents are moving a variety of workloads into cloud service provider environments: 47% currently use collaboration services such as file sharing and calendaring, 45% use email and messaging services, and 29% use cloud-based managed services. In the coming 12 months, 24% plan to use cloud collaboration services, 23% will use cloud-based backup and disaster recovery services, and 22% are looking at implementing messaging and email services. The full breakdown of current and planned workload deployments is illustrated in Figure 2.

**What applications have you moved to the cloud or are you planning to move?**



*Figure 2. Current and Planned Cloud Workload Deployments*

As results show, SANS survey respondents are using an incredibly broad mix of services, particularly collaboration and messaging tools, with well over 60% indicating that they either have or will have these services in the cloud in the next 12 months. Cloud workloads planned for implementation in the next 12 months are more evenly distributed but still vary widely. Other key applications respondents plan to move to the cloud include data archival and retrieval applications, cited by 20%, followed by desktop applications, managed services, hosted network services and information security services, at 19%, 18%, 17% and 16%, respectively.



Percentage of respondents who expect to have collaboration services in the cloud within the next 12 months



Percentage of respondents who plan to have email and messaging tools in the cloud within the next 12 months



## State of Cloud Computing (CONTINUED)

Each of these applications involves processing or storing sensitive information within the cloud provider environment, including security and network data that can be used to break into the physical network. Preventing exploitation across these applications and their associated attack surfaces is now a key support goal for security groups with any type of dynamic cloud-based operation.

### Business Drivers

There are a variety of business drivers for adoption of cloud services today, but those differ depending on the organization. KPMG research found that business executives are focused primarily on business transformation and performance, followed by agility and then cost savings.<sup>2</sup>

SANS survey respondents echoed those priorities, with 61% citing faster time to deployment as their main driver and 54% saying they use cloud services because they can't scale their own solutions. In addition, 48% said they need a central way of managing compliance. See Figure 3.

#### What are your top three motivators for moving applications and workloads into the cloud?

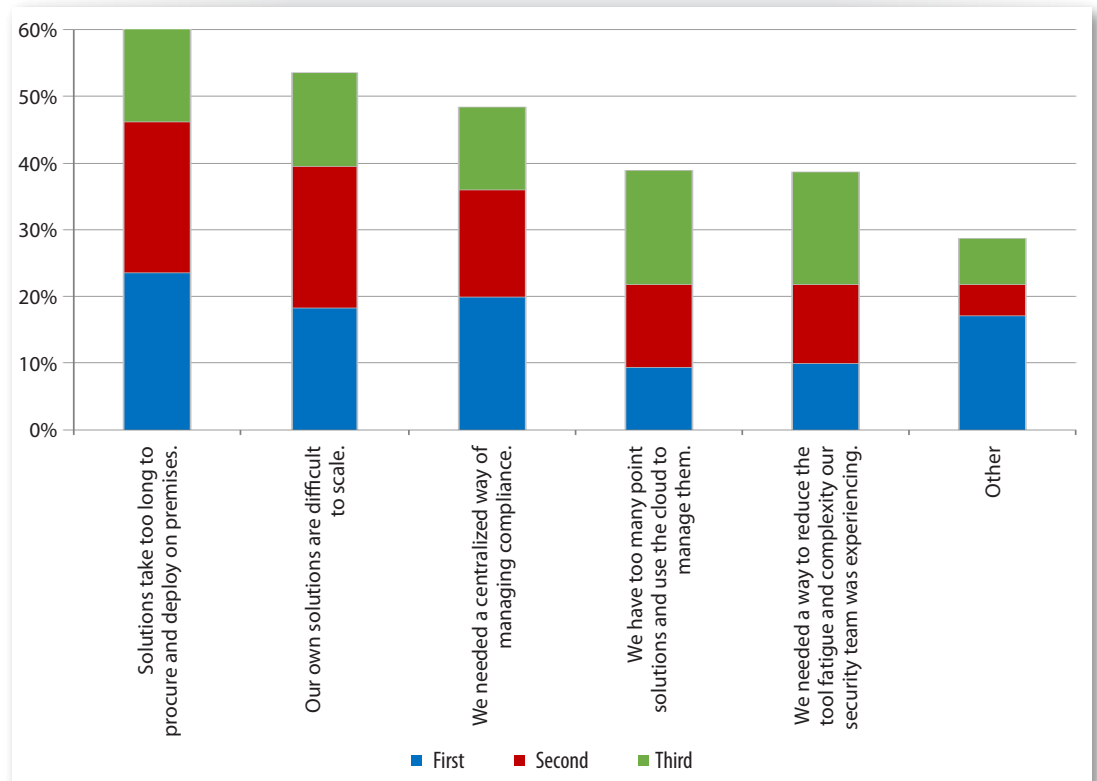


Figure 3. Reasons for Cloud Deployment

<sup>2</sup> [www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014 KPMG Cloud Survey Report - Final 12-10-14.pdf](http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014%20KPMG%20Cloud%20Survey%20Report%20-%20Final%2012-10-14.pdf)





Write-in additions to the list of motivators for cloud deployments include cost savings, availability and ease of use. Taken together, results indicate that the hybrid cloud model, driven by the demands of business, is here to stay. This trend further marks a strong growth area for IT security professionals who want to specialize in the cloud and vendors developing tools for integrating access, data protection, monitoring and visibility—as well as protective intelligence across these systems, platforms and providers.

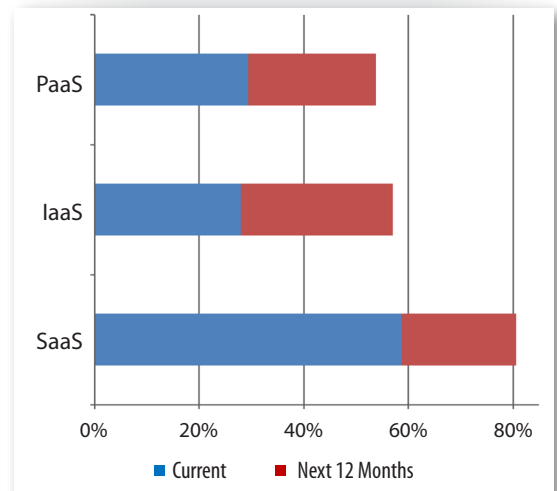
### Usage Models

Currently, 59% of enterprises are using software-as-a-service (SaaS) offerings, most likely for collaboration and messaging tools, as highlighted earlier. Virtual machine (VM) systems and application workloads are being deployed in infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) environments today as well. See Figure 4.

In the next 12 months, 29% of respondents said they plan to deploy an IaaS environment, making it the largest area of predicted growth. The reasons for moving to PaaS and IaaS are no different than those for SaaS deployments: speed and scalability, along with additional services cloud providers can offer. Many organizations are looking to reduce the overall size and footprint of their in-house data centers, so migrating system instances into the cloud makes sense.

In the KPMG survey cited earlier,<sup>3</sup> CIOs and business executives alike indicated that they are highly focused on data security and privacy as well as the risks of intellectual property theft when evaluating cloud providers today—and for good reason. Some 40% of SANS survey respondents indicated that they are storing or processing sensitive data in their public cloud environments today, while another 13% said they don't know whether they have sensitive data in the cloud.

**What cloud usage model(s) are you either using now or planning to deploy in the next 12 months?**



*Figure 4. Current and Planned Cloud Models*



Percentage of respondents who expect to deploy a SaaS environment within the next 12 months

<sup>3</sup> [www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014 KPMG Cloud Survey Report - Final 12-10-14.pdf](http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/2014%20KPMG%20Cloud%20Survey%20Report%20-%20Final%2012-10-14.pdf)



## State of Cloud Computing (CONTINUED)

Business intelligence and financial and accounting information are the most common types of data respondents are storing or processing in the cloud, each reported by 52% of respondents. Another 48% store or process employee records, and 40% store customers' personal information. See Figure 5.

### What type of sensitive information are you storing or processing in the public cloud? *Select all that apply.*

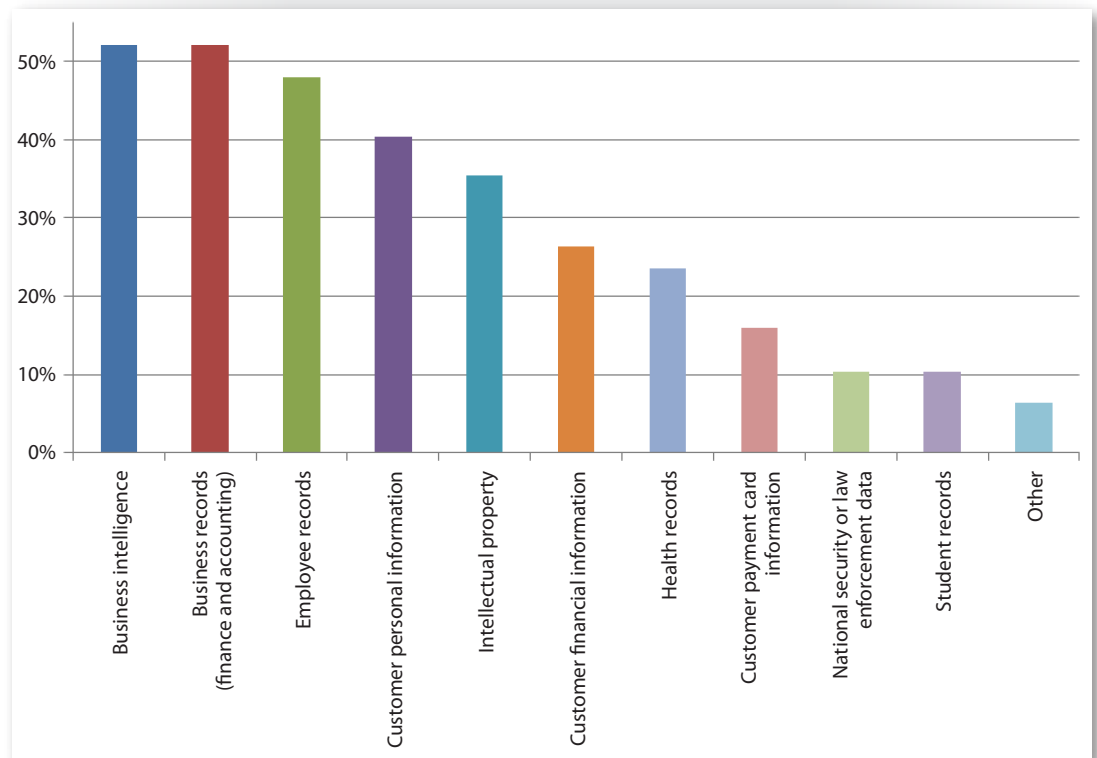


Figure 5. Sensitive Data Stored or Processed in the Cloud

#### TAKEAWAY:

Take steps whenever possible to secure the data that is sent into the cloud environment—in transit, at rest and in use.

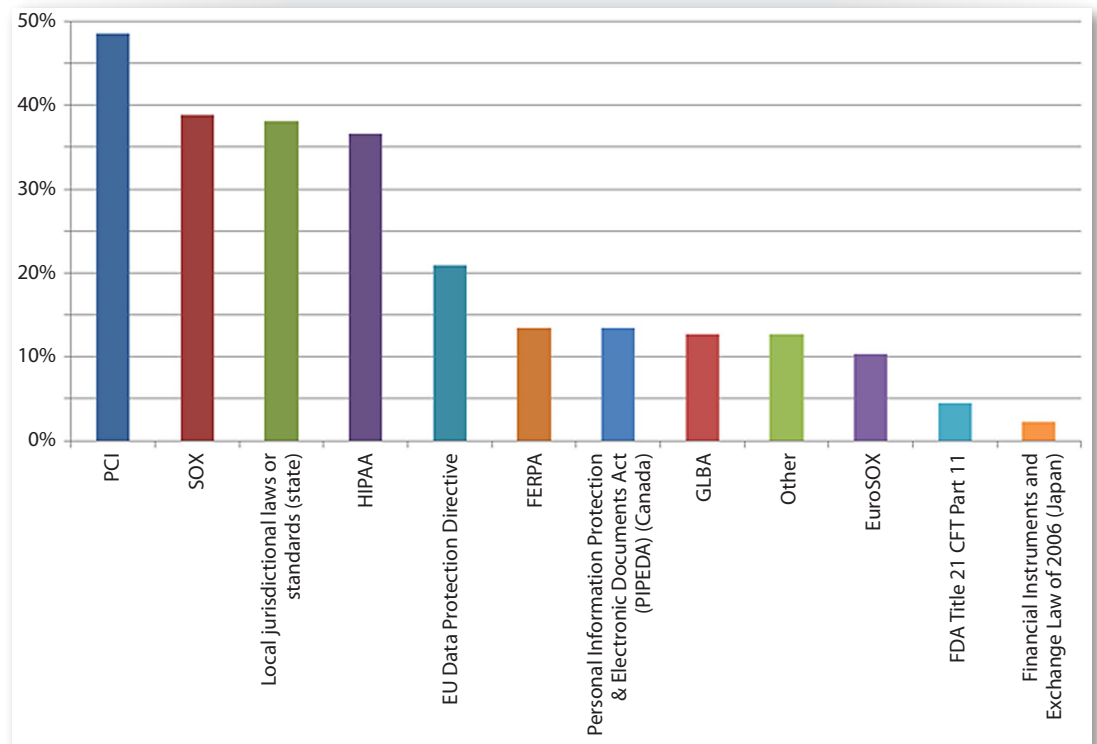




## State of Cloud Computing (CONTINUED)

At least 20% of respondents said they are also using the cloud to store or process intellectual property, customer financial information and health records. With all these different types of sensitive data represented in today's cloud environments, organizations need to comply with various regulatory and industry compliance mandates: 49% of respondents said they must meet Payment Card Industry Data Security Standard (PCI DSS) requirements, 39% cited Sarbanes-Oxley (SOX) compliance, and 37% must comply with Health Insurance Portability and Accountability Act (HIPAA) mandates. The full breakdown of compliance mandates respondents must adhere to is shown in Figure 6.

**What are the applicable regulations or standards with which you must comply?**  
*Select all that apply.*



*Figure 6. Enterprise Compliance Requirements*

Complying with various data protection rules in the cloud is quite different from using the cloud to achieve compliance with these mandates. It's reasonable that the organizations surveyed would use the cloud to do both, as shown previously in Figure 2 (on page 3), with nearly 30% using cloud-based managed services and just under 25% using cloud-based information security services. Given that CIOs and their businesses are dealing with more and more compliance requirements, trying to offload some of this work to cloud providers actually starts to make sense.

### TAKEAWAY:

Organizations should carefully assess the types of sensitive data they are storing in the cloud and whether they can meet related compliance requirements in SaaS, PaaS and IaaS provider environments.



## State of Cloud Computing (CONTINUED)

### Who Is Using Cloud

European Union data protection requirements also apply to just over 21% of respondents. Given that adherence to regulations, particularly privacy laws, in Europe were cited by one-fifth of respondents, it's not surprising that roughly 36% of respondents said they have some sort of operations in that region. See Table 1 for a full breakdown of respondents' enterprise operations.

Table 1. Regions/Countries Represented	
Region/Country	% Respondents
United States	77.3%
Europe	36.1%
Asia-Pacific	27.4%
Canada	22.9%
South and Central America	18.1%
Australia and New Zealand	17.5%
Middle East	16.5%
Africa	12.0%

Survey respondents represent a variety of industries, with information technology (17%), government (14% total), and banking and finance (11%) being the top three. See Figure 7.

### What is your organization's primary industry?

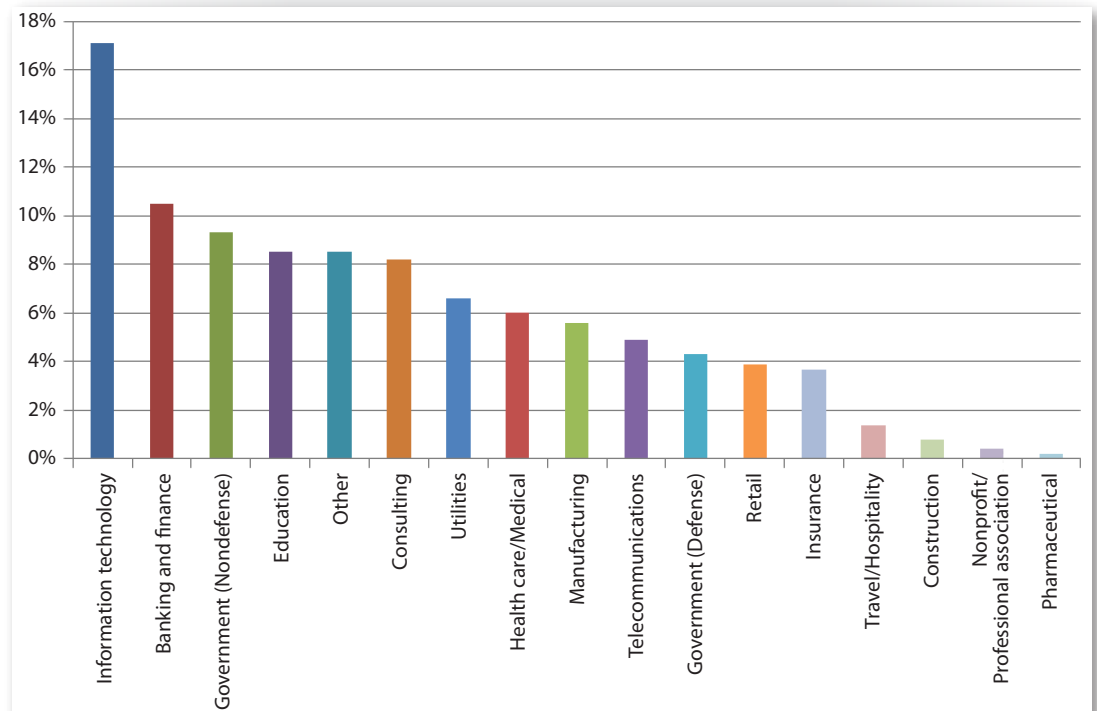


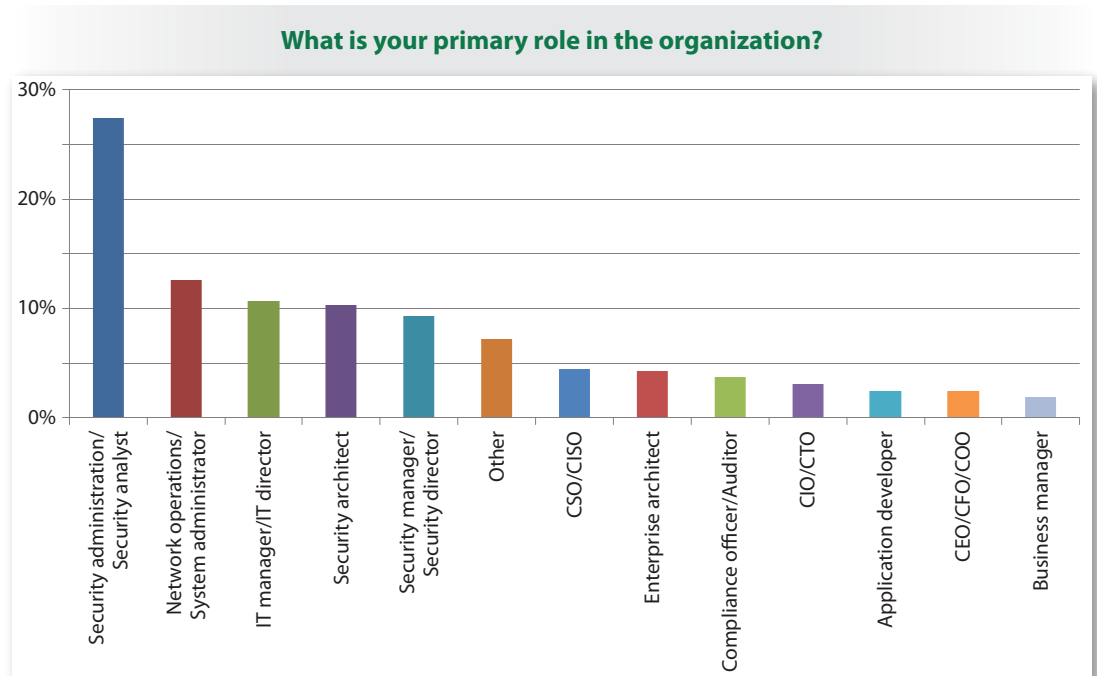
Figure 7. Industries Represented



## State of Cloud Computing (CONTINUED)

Survey respondents also represented a mix of small and larger organizations, with 38% having 1,000 or fewer employees, 24% with over 15,000 employees, and the remainder having between 1,000 and 10,000.

Most responses came from security operations (administrators and analysts), followed by network operations, systems administration and IT management. A good mix of responses came from other roles in IT, as well as internal audit, application development and senior executives, as shown in Figure 8.



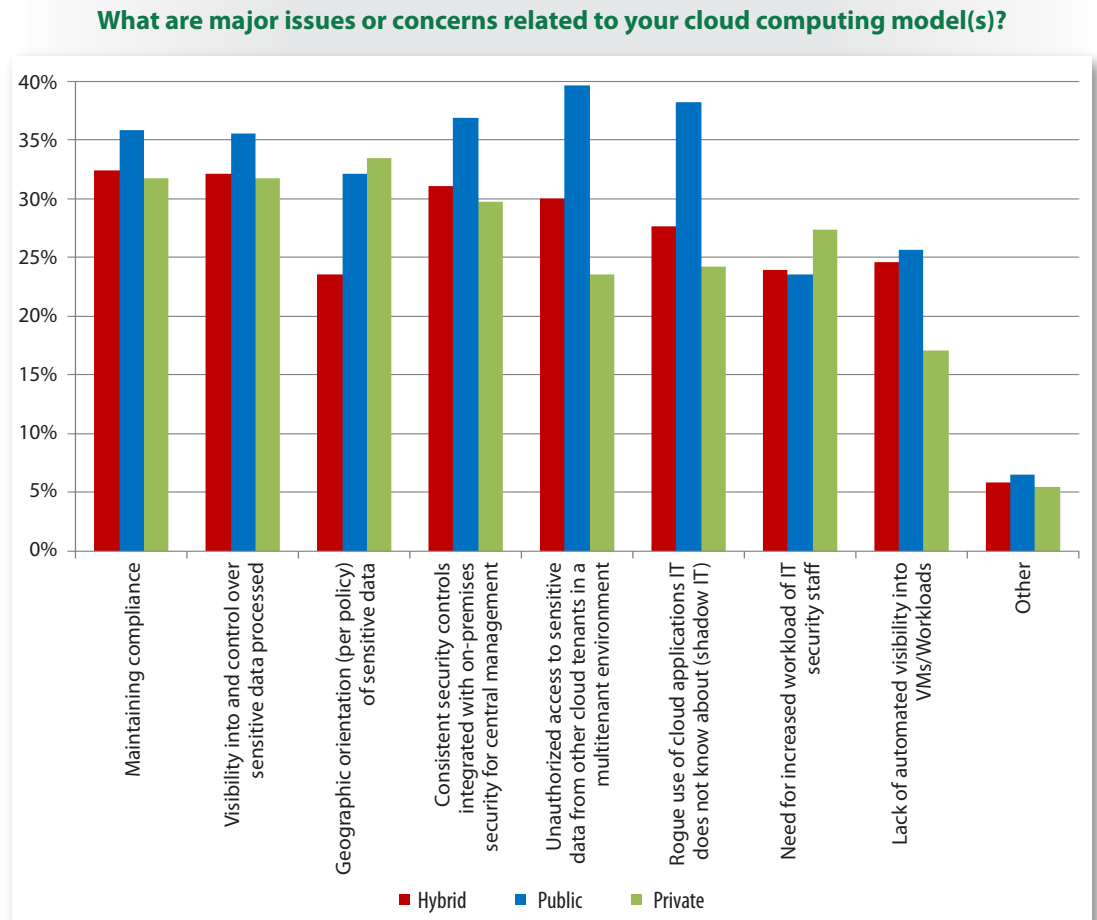
*Figure 8. Respondent Roles*

Overall, most survey respondents represent larger organizations that are global or operate in several regions and hold a wide range of different and overlapping security, business, compliance and IT positions within their respective industries and organizations.



# Cloud Security Concerns

With so many different environments and applications, the top concern with data processing in clouds is maintaining compliance. In fact, when averaged across all models (public, private and hybrid), it was cited by 72% of respondents. See Figure 9.



*Figure 9. Major Security Concerns in Cloud Deployments*

The biggest concern with public cloud computing is the risk of exposing sensitive data, with 40% saying they are primarily concerned with unauthorized access to data by other tenants, while 38% are concerned about potential misuse of cloud resources (shadow IT in the cloud). Another 37% said a top overall concern with having their data in the public cloud is a lack of consistent security controls that integrate with on-premises tools and security management.

For organizations using private cloud services, 33% rated geographic location of their data as a key concern, which likely coincides with the multitude of regions they operate in and the regulations they need to comply with. Maintaining compliance and ensuring visibility into controls in place, both cited by 32% of respondents, are key for both private and hybrid cloud users.



## Cloud Security Concerns (CONTINUED)

### Lack of Control

Other issues with public cloud providers include dependency on providers and intermediary services, third-party library vulnerabilities and an overall lack of visibility into the practices of cloud providers in general.

The various cloud models allow different levels of control:

- **SaaS:** Users have control over their own data but not over the applications or data protection controls within the provider's environment.
- **PaaS:** Platform services allow users to manage applications, and vendors can provide some simple infrastructure controls, but the majority of user-managed controls are related to data protection, such as encryption and monitoring.
- **IaaS:** Users can create network-based controls and have full security visibility and management of systems running on IaaS platforms.

### Lack of Visibility

Regardless of the model used, the issues are the same: Lack of visibility, steep fees for vendor-provided security and lack of compliance support are respondents' top three concerns with their public cloud services. See Figure 10.

**Has your organization had any of the following issues with your cloud provider(s), whether supporting your private, public and/or hybrid cloud? Select all that apply.**

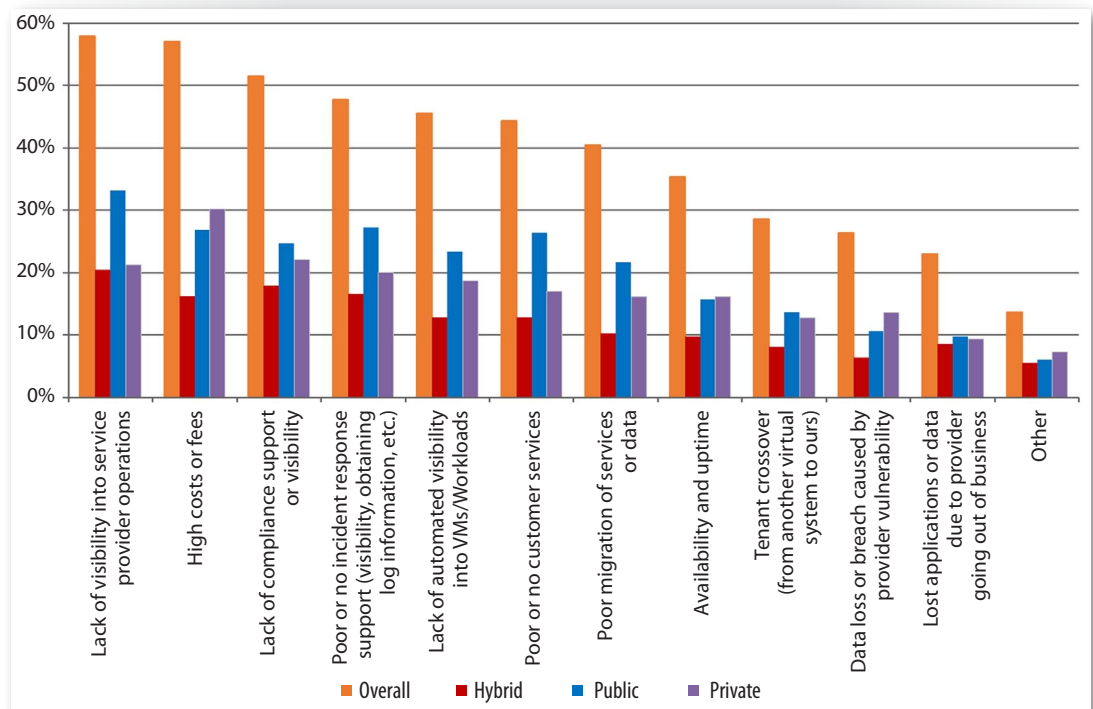


Figure 10. Issues with Cloud Providers



## Cloud Security Concerns (CONTINUED)

### TAKEAWAY:

Regardless of the cloud model you implement, liability and risk management issues with your cloud provider are inevitable. Determine ahead of time what issues can and cannot be addressed and how you will handle them.

Overall, lack of visibility into cloud provider operations and controls, cited by 58%, stands as the biggest problem respondents have with their vendors. In fact, among all the concerns related to the cloud, respondents said lack of visibility and control plays a leading role in other issues, such as:

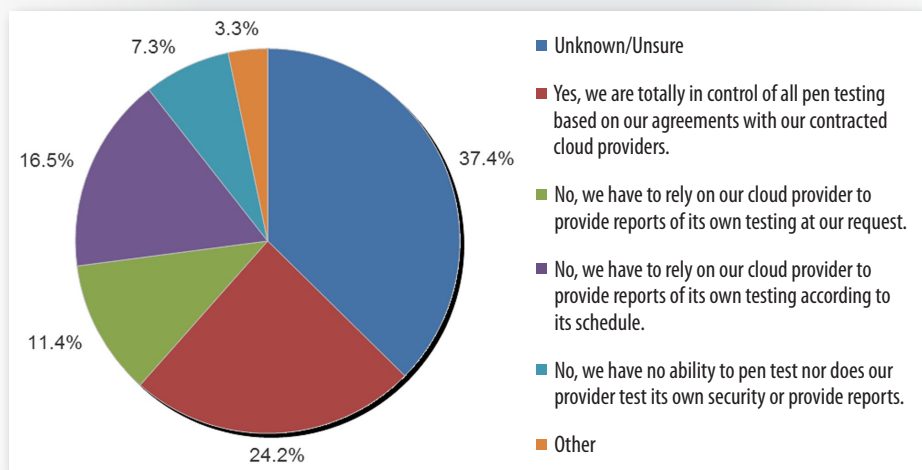
- Lack of incident response support, with lack of visibility cited (48%)
- Lack of VM and workload visibility (46%)
- Provider-introduced vulnerabilities resulting in a breach or incident (26%)

Surprisingly, 57% of respondents said high costs and provider fees are a major issue, which seems to contradict the widely held perception that a big driver of moves to the cloud is cost savings. As such, survey findings indicate there likely are hidden costs associated with audit and discovery of cloud provider security controls and compliance.

### Inability to Test

Another big issue facing many organizations' cloud projects is a lack of support for penetration testing. Only 24% of respondents stated that they are able to perform penetration testing of their cloud assets with no restrictions, as shown in Figure 11.

**Are you able to perform regular penetration tests of your public cloud assets and data according to your agreement with your cloud provider?**



*Figure 11. Penetration Testing Challenges with Cloud Providers*





The remainder of respondents must either request that their cloud providers perform network and application penetration tests or rely on providers' schedule, or they receive no reports at all. Under the "other" response, one respondent said testing depends upon which provider the organization is using (uses more than one), one indicated penetration testing was scheduled upon approval, and another said the organization can test but not to the degree it desires.

Organizations, however, should not be forced to take the word of their providers when it comes to penetration testing. They should have a viable way to test the security of their hosted and processed applications and data to ensure:

- Secure zones between tenants cannot be breached
- Operating system and application flaws cannot be exploited
- Sensitive data is not exposed to cloud provider personnel or external attackers

### Ripe for Breach

From what we currently know, cloud-based computing systems have not been massively breached in a way that impacts respondents' sensitive data. In this survey, only 9% of respondents experienced an actual breach in either the public cloud or their SaaS or private cloud applications. However, 25% weren't sure, which circles back to the lack of visibility and control survey respondents said they are experiencing.

That doesn't mean breaches in public and private clouds aren't occurring. In 2014, the Amazon Web Services environment of private company Code Spaces was compromised, leading to the destruction of sensitive data and ultimately to the closure of the company.<sup>4</sup> Google Drive, Dropbox, Box and iCloud made it onto the list of top 2014 cloud hacks as well.<sup>5</sup>

<sup>4</sup> <http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan>

<sup>5</sup> <http://psg.hitachi-solutions.com/credeon/blog/google-drive-dropbox-box-and-icloud-reach-the-top-5-cloud-storage-security-breaches-list>





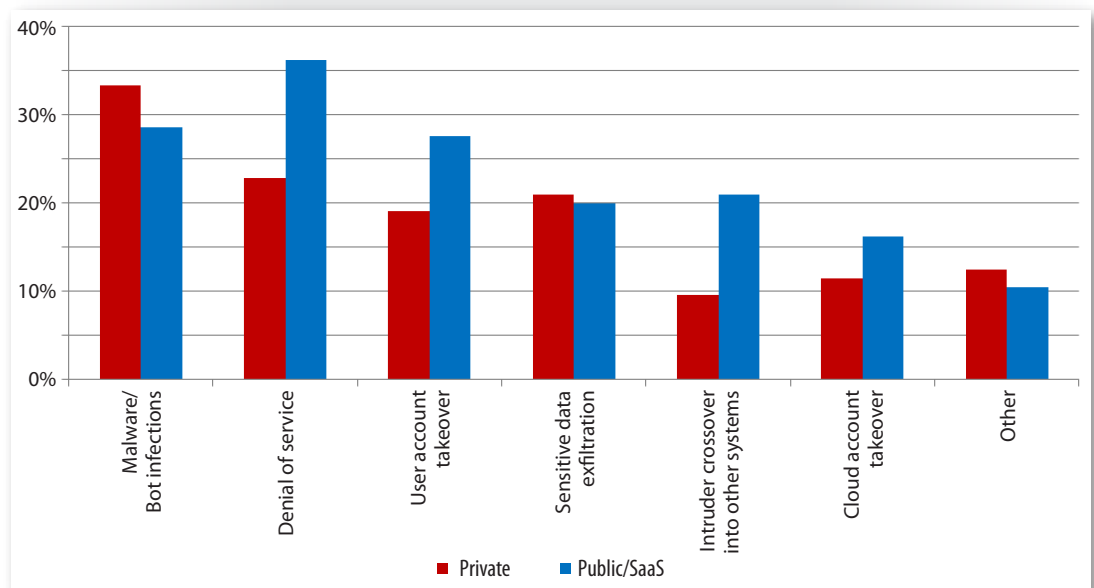
## Cloud Security Concerns (CONTINUED)

For the 9% of respondents that did experience breaches or attacks, 55% were hit by a malware or botnet infection and 54% experienced a denial of service (DoS) attack. Broken down between public and private cloud breaches, the attack vectors look like this:

- In their private clouds, 33% of respondents identified malware or botnets as the nature of the attack, with only 23% citing DoS.
- In the public cloud, 36% said DoS was their leading breach experience, with 29% citing malware and 28% identifying user account takeover as the nature of their breaches.
- In public and private clouds, answers align around sensitive data exfiltration: 20% of public cloud users and 21% of private cloud users experienced sensitive data exfiltration from their breaches.

See Figure 12 for a full breakdown of respondents' breach experiences.

**What was the nature of the actual breaches experienced by your organization in either the public cloud or SaaS or private cloud applications?**  
*Select all that apply.*



*Figure 12. Attacks and Breaches in the Cloud*

The Cloud Security Alliance "Top Threats to Cloud" report indicates that DoS attacks can occur on any hosting environment, regardless of cloud architecture model, so it stands to reason that DoS attacks are common for both public and private cloud providers.<sup>6</sup> In 2014, Kelly Jackson Higgins of Dark Reading predicted a rise in DDoS attacks on cloud-based services as a result of a sustained DoS on the Feedly news and information aggregation site. The motivation is often ransom for restoring the service, according to the article.<sup>7</sup>

<sup>6</sup> [https://downloads.cloudsecurityalliance.org/initiatives/top\\_threats/The\\_Notorious\\_Nine\\_Cloud\\_Computing\\_Top\\_Threats\\_in\\_2013.pdf](https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf)

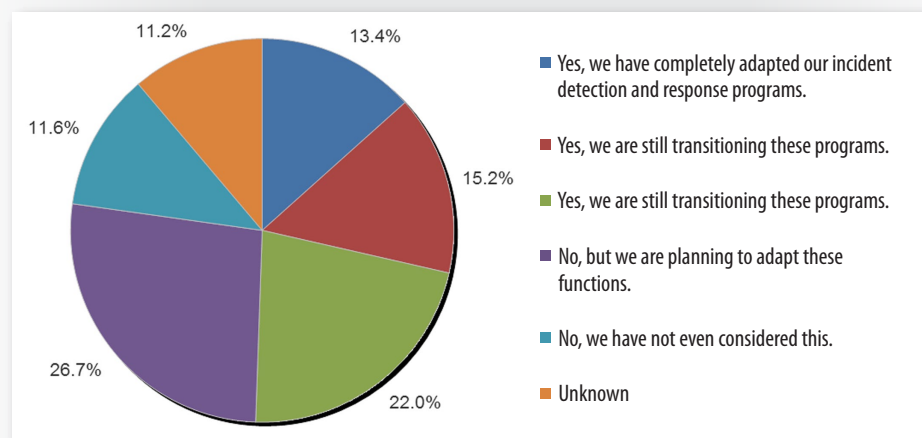
<sup>7</sup> [www.darkreading.com/attacks-breaches/wave-of-ddos-attacks-down-cloud-based-services/d/d-id/1269614](http://www.darkreading.com/attacks-breaches/wave-of-ddos-attacks-down-cloud-based-services/d/d-id/1269614)



### Response Preparedness

Even though cloud incidents don't yet seem altogether common, organizations still need to adapt their incident response processes to better accommodate cloud assets and services. Unfortunately, only 13% of respondents said they have completely updated their incident response processes and tools to fit their cloud models, while another 15% have partially updated processes and tools and 22% are in the process of transitioning now. See Figure 13.

**Have you adapted your incident detection and response programs to the cloud computing model(s) you use?**



*Figure 13. Adapting Incident Response in the Cloud*

For those organizations that have started to adapt their incident response functions for cloud computing, there have been challenges. The biggest issue, which goes back to the problem of visibility into internal cloud provider operations, is the lack of access to log files and other forensic artifacts, experienced by 53% of respondents. Another 46% said they are confused as to what information cloud providers should make available for proper incident response capabilities (see Figure 14).



## Cloud Security Concerns (CONTINUED)

### TAKEAWAY:

Focus on reviewing all cloud service account access and determine whether your in-house security vendors also offer cloud-compatible products and services. Start working with your providers to coordinate penetration testing and incident response processes, if you haven't already.

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

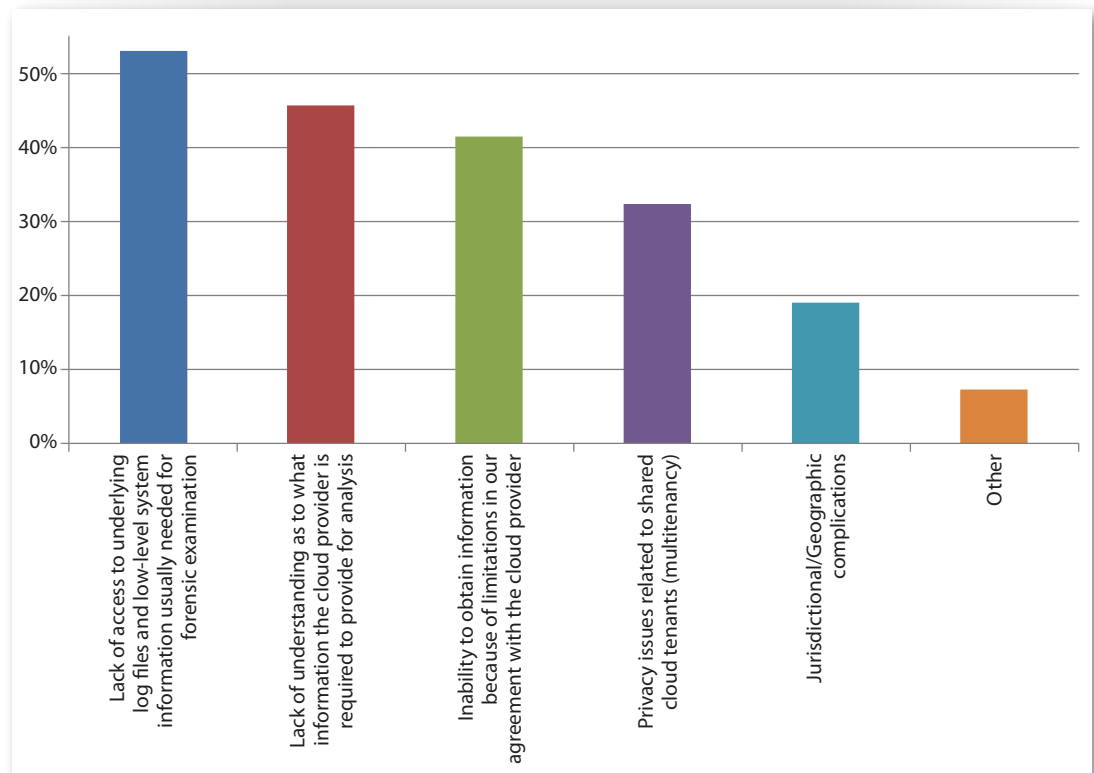


Figure 14. Incident Response Challenges in the Cloud

Survey participants provided numerous open-ended responses to this question that indicate many security teams are struggling not only in dealing with cloud providers, but with internal teams in their efforts to detect and respond to cloud-based incidents effectively. Some said they have challenges training internal security staff to work with cloud provider APIs to extract data, while others cited political roadblocks with IT not handing over data or relevant information from the cloud provider on a timely basis. Some responses went so far as to say that cloud-based incident response is impossible or very nearly so.

Although most organizations have not experienced a breach in the cloud, security teams are concerned about illicit account and data access, maintaining compliance and integrating with on-premises security controls. In addition, visibility into cloud environments remains a challenge, as does implementing cloud-focused incident response and penetration testing processes.



# How to Build Better Cloud Defenses

## SECURITY-AS-A-SERVICE

Security-oriented cloud services that consumers subscribe to, much like traditional cloud services

There are many different types of security controls available for the cloud today. Gartner's "Hype Cycle for Cloud Security, 2015"<sup>8</sup> lays out a number of technologies and standards that are currently in use or evolving in cloud computing. Given the attention and focus on security and compliance seen in survey responses and third-party research, new and innovative offerings are rapidly evolving for securing systems, applications and data in the cloud.

### Cloud Security Adaptation

Many traditional security vendors are adapting their offerings for some cloud environments, and cloud providers are rapidly adding more native security options for cloud consumers. Amazon Web Services offers network access controls, numerous encryption and key management models, and access to its CloudTrail service. Microsoft Azure offers built-in anti-malware, as well as encryption and network access controls.

Cloud providers increasingly are offering more services, but in the Hype Cycle report, Gartner spells out some of the commercial offerings and trends that are shaping cloud security today.<sup>9</sup> Many of the new technologies it discusses fall into the category of security-as-a-service (SecaaS), security-oriented cloud services that consumers subscribe to, much like traditional cloud services. Such services usually integrate with cloud provider environments or protect data in hybrid cloud architectures.

Some of the rapidly evolving and successful controls that are helping advance cloud security include the following:

- **Identity and access management (IAM).** Usually in the form of federated identity management, IAM services can help organizations integrate Active Directory and other user IDs into numerous cloud application and infrastructure environments without complicated and messy on-premises IAM solutions.
- **Cloud access security brokers (CASBs).** CASBs can monitor and control traffic bound for the Internet and cloud services specifically, applying data monitoring and control policies to prevent shadow IT and data leakage, as well as malware infections. Many CASB tools can also implement encryption and other data protection techniques.
- **Disaster Recovery-as-a-service (DRaaS).** Cloud services providing disaster recovery (DR) and business continuity planning (BCP) in the form of VM and data backup, messaging and coordination services, and planning dashboards and applications for DR are growing steadily. Maintaining full DR and BCP capabilities in-house or in standby sites is declining in favor of much more affordable cloud storage and planning options.

<sup>8</sup> "Hype Cycle for Cloud Security, 2015," [www.gartner.com/doc/3096419/hype-cycle-cloud-security-](http://www.gartner.com/doc/3096419/hype-cycle-cloud-security-) (Gartner account required.)

<sup>9</sup> "Hype Cycle for Cloud Security, 2015"



## How to Build Better Cloud Defenses (CONTINUED)

- **Host-based IDS/IPS (HIDS/HIPS).** HIDS/HIPS solutions for IaaS (and potentially PaaS) can offer firewalling, file integrity, application whitelisting, configuration and patch management, and more standard intrusion detection and prevention capabilities. With less control over network resources, many are turning to services that work within each VM and can be managed from a central cloud console.

Survey respondents have had some success implementing security and data protection technologies and processes in their cloud environments. However, the vast majority of security controls are still internally managed by respondents' organizations.

Traditional security controls such as application security controls and firewalls are most prevalent, used by 76% of survey respondents overall, which is likely due to the basic offerings from IaaS providers and the built-in controls with most SaaS offerings, the predominant cloud services in use right now. Anti-malware and vulnerability scanning follow, used by 74% overall. Lower in the list, however, we see the use of IAM solutions and CASBs, cited by 50% and 43% of respondents, respectively. See Figure 15.

### Which of the following security and data protection technologies and processes have you successfully implemented in your cloud environment(s)?

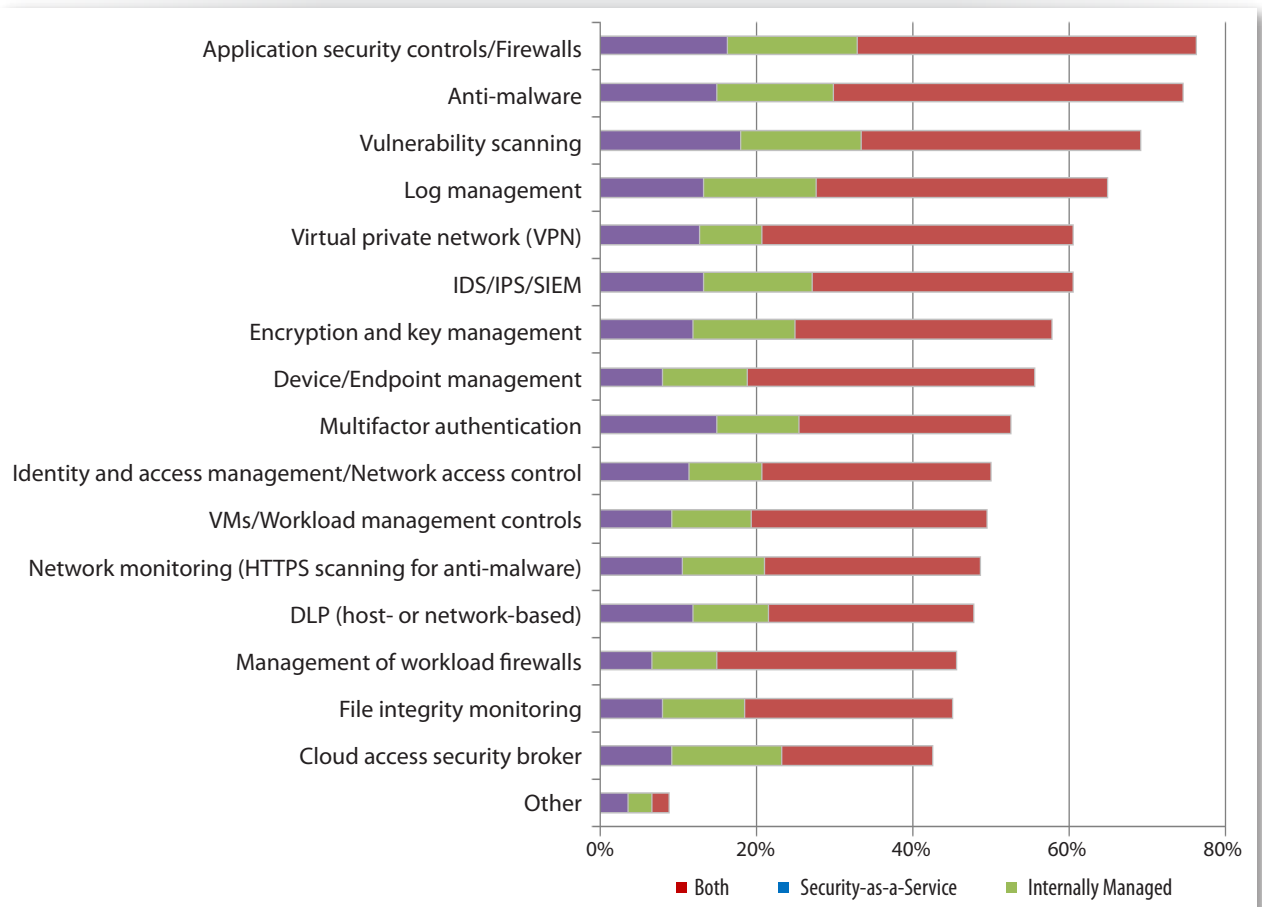


Figure 15. Cloud Security Controls in Use



## How to Build Better Cloud Defenses (CONTINUED)

### TAKEAWAY:

Although many controls are still managed internally, SecaaS is emerging as a viable means to enhance security in the cloud environment. Security teams should start considering the use of SecaaS options when designing and architecting cloud security models.

Most of the controls that are in use by over 50% of organizations (those controls between “Application security controls/Firewalls” and “Multifactor authentication” in Figure 15) are common baseline controls that many are likely required to have to meet compliance mandates. Other controls, such as IAM, data loss prevention (DLP), file integrity monitoring and CASBs, are slower to adapt to cloud environments and less likely to be natively offered by providers.

### Security-as-a-Service

As discussed earlier, security is also being hosted in the cloud. Security-as-a-service (SecaaS) is an application well suited for the cloud, offering organizations the ability to offload monitoring, detection, updating and patching support for both internal and cloud-based applications.

In this survey, the top six security controls implemented in the cloud as a service include application security controls/firewalls, vulnerability scanning, anti-malware, log management, IDS/IPS/SIEM and CASBs. Over the next 18 months, vulnerability scanning, multifactor authentication, DLP and log management functions will continue to be strong and hopefully carry over from the physical to the cloud environment. See Figure 16.

**What additional services do you plan on shifting to a cloud-based security-as-a-service in the next 18 months? Select all that apply.**

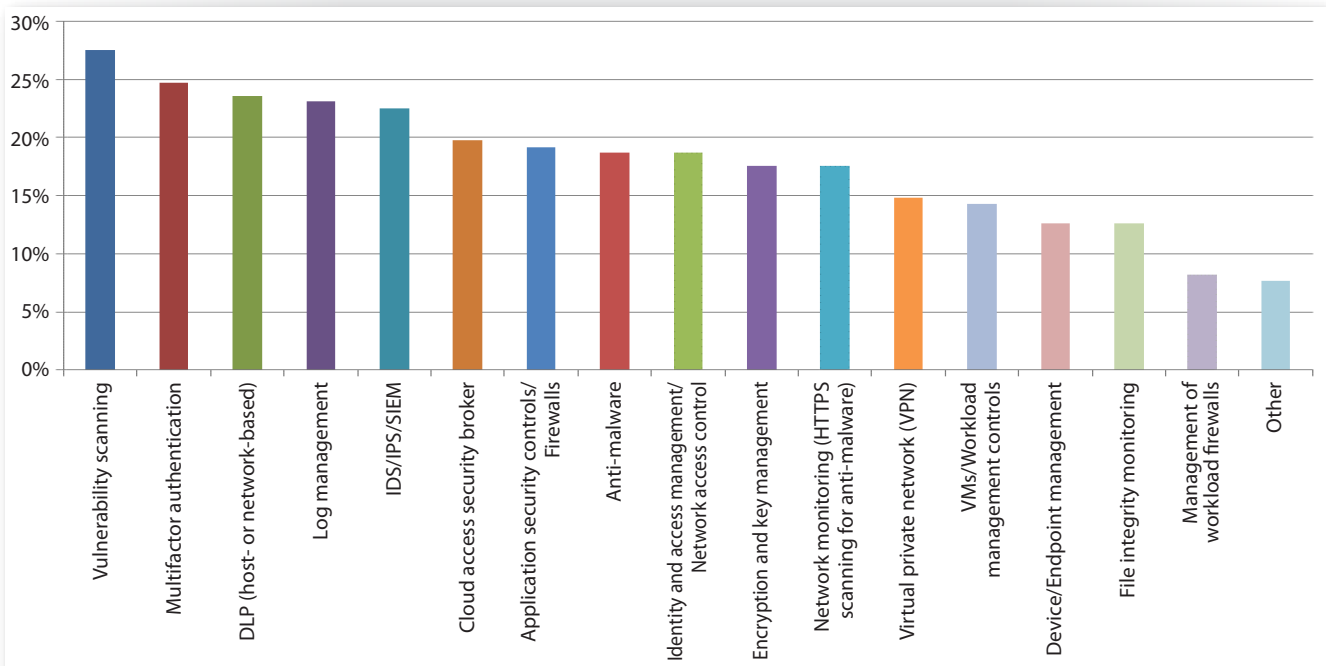


Figure 16. Future SecaaS Investment

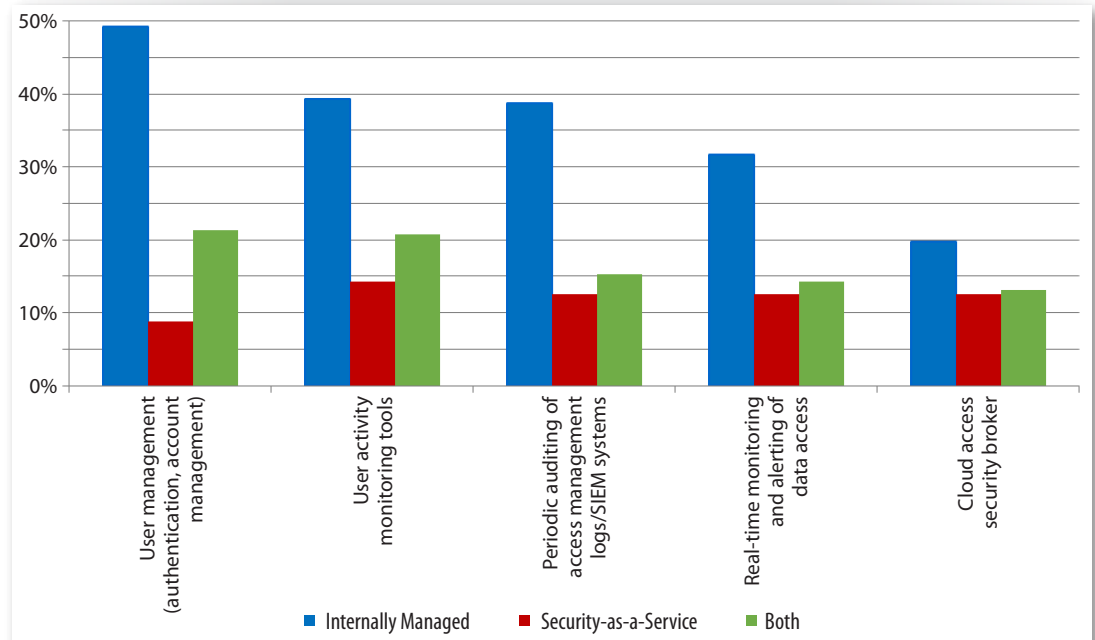
This aligns with the Gartner Hype Cycle report, which shows these technologies maturing rapidly, with more effective vendor offerings appearing all the time.



### Control Access

Many organizations are worried about the use of cloud services by employees, especially when some services (like cloud-based storage or messaging) have neither been approved for use nor safely configured. SecaaS is beginning to make inroads as a viable control originator for user account management, which, although still primarily handled in-house, is originated by SecaaS for 14% of respondents. Overall, 45% are implementing CASB options for monitoring, primarily with internal management. Figure 17 shows the types of monitoring organizations are implementing.

**If you control and monitor cloud usage by employees, please indicate whether these tools and processes originate from within your organization (internally managed), your cloud provider (security-as-a-service) or both.**



*Figure 17. Cloud Activity Monitoring Options*





## How to Build Better Cloud Defenses (CONTINUED)

While it's obvious that security teams are focusing on monitoring employee use of the cloud, controlling and monitoring data traversing between employee devices and cloud services can be difficult. Most (54%) require the use of a network-based VPN or a proxy to gain access to corporate resources in the cloud, while 41% secure data during transport via a proxy. Others have focused on the endpoints themselves, separating content and applications, using DLP tools or restricting applications that can be installed (whitelisting). Figure 18 illustrates the methods survey respondents use to monitor data in transit between employee devices and the cloud.

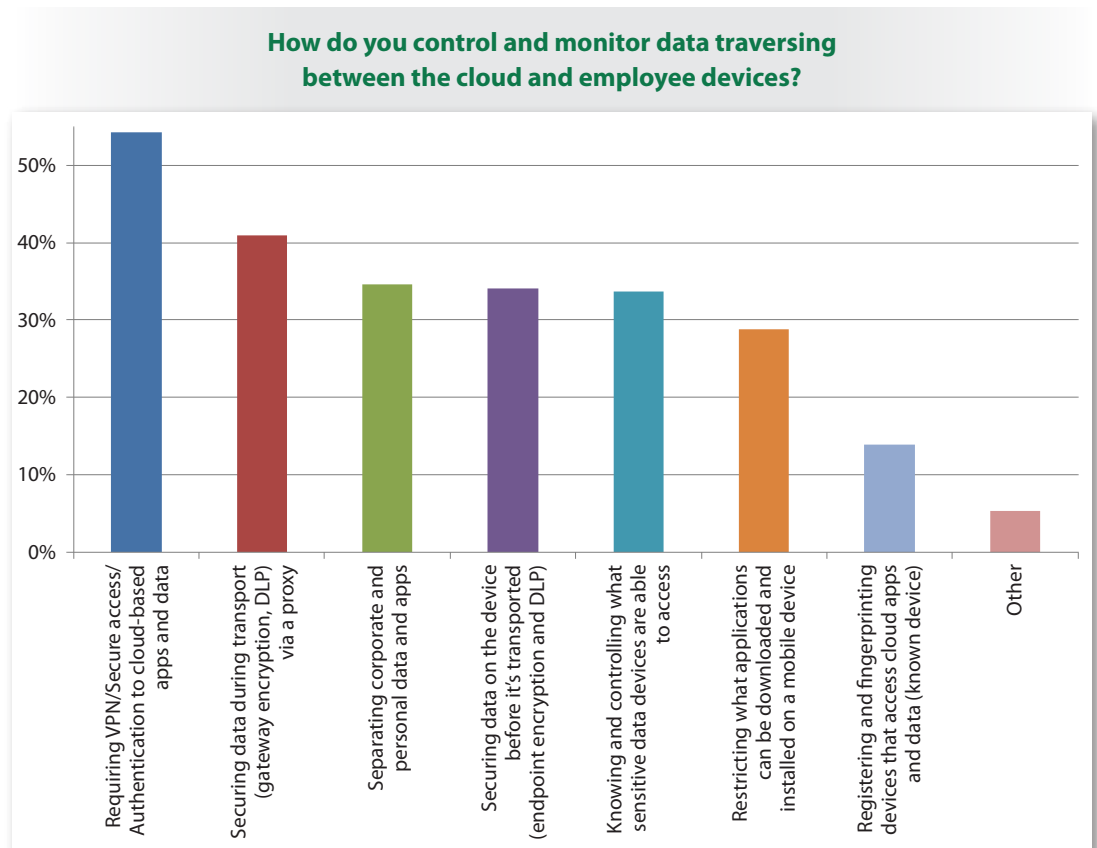


Figure 18. Employee Device Monitoring for Cloud Service Use



## How to Build Better Cloud Defenses (CONTINUED)

### TAKEAWAY:

To improve the efficacy of layered security controls, check into provider-offered controls such as logging, multifactor authentication, encryption, and other products and services that can function natively in the cloud infrastructure.

Using network-based approaches for controlling access to applications, systems and data in the cloud represents one layer of today's security stack—and it will continue to grow and change over time as the nature of cloud access and use changes. Right now, many security professionals see a shift in the nature of how their layered security controls work when moving to cloud environments.

Organizations that want to improve the efficacy of their layered security controls should look into controls offered by providers, such as logging, multifactor authentication, encryption and compatible products and services that work natively within their cloud infrastructure. The use of SecaaS controls are also expected to increase, especially as providers partner with security service companies to offer more seamless integration and functionality.



# Conclusion

*Security teams will need to adopt more automation and API-compatible security controls that can help bridge the gap between internal security tools and processes and those running in cloud or SecaaS environments.*

SANS survey respondents provided significant feedback to the analyst team on challenges they face and thoughts they have on migration to the cloud. Not surprisingly, some respondents are leery of moving to cloud environments, with many citing lack of visibility into cloud provider practices and controls as a reason.

A number of respondents also specifically mentioned the need for greater security automation, whereby security teams have access to tools and scripts that integrate with provider and SecaaS APIs to better secure and monitor their cloud assets. Security teams are struggling to get enough visibility into cloud provider infrastructure, controls and processes through contracts and audit reports, and say the nature of organizations' "defense in depth" security stack has to change as well.

Security teams are facing the reality that business leadership wants to move into using cloud services—it's already happening at a rapid pace. Many organizations are moving sensitive data there, too, meaning security teams will need to carefully review what kinds of data they're charged with protecting in the cloud and what security controls (encryption, DLP, CASB services, etc.) are available to help protect it. Pushing cloud providers for more insight into their controls and processes, both contractually and through standard audit reports like SSAE 16 SOC, can help organizations determine the general security posture of potential providers, but security professionals should still be looking at protective controls that they can manage as well.

Security teams need to pay close attention to their organizations' cloud accounts because attackers are actively seeking to breach cloud services and compromise data. Protect data in transit with VPN and other encryption options, and monitor what types of cloud services employees are using. More vendors are adapting their products to cloud environments all the time, and SecaaS is filling the gaps in many cases.

Endpoint security tools and controls, SecaaS offerings that leverage APIs to integrate with cloud providers, and on-premises controls such as cloud encryption gateways and vulnerability management solutions will need to work flexibly with new controls offered by the cloud providers themselves. In fact, as the adoption of hybrid cloud models grows—and this seems to be the case—security teams will need to adopt more automation and API-compatible security controls that can help bridge the gap between internal security tools and processes and those running in cloud or SecaaS environments.



## 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:*

CloudPassage

 evident.io



The Intel Security logo, featuring the word 'intel' in blue lowercase font inside a blue oval, followed by the word 'Security' in blue uppercase font and a small red shield icon with a white 'M'.





# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS SEC460: Enterprise Threat	San Diego, CAUS	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
Security Awareness Summit & Training 2017	OnlineTNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced