ORACLE KPMG

Demystifying the Cloud Shared Responsibility Security Model

Oracle and KPMG Cloud Threat Report 2020 series

Volume 2

Research conducted in partnership with ESG

Contents

Executive Summary

Welcome to the second installment of the Oracle and KPMG Cloud Threat Report series. The first report, Addressing Secure Configurations Amidst a State of Constant Change, highlighted the need for a cultural shift to close the cloud security readiness gap. That gap has resulted in a series of data breaches associated with misconfigured cloud services. A specific set of DevSecOps leading practices were prescribed as a means of automating leading practices to secure the configuration of cloud services. Successful secure DevOps initiatives are, however, predicated on organizational alignment between the lines of business and the IT and cybersecurity teams so that security is implemented as a shared responsibility.

As digital transformation initiatives go into overdrive to support remote workers who rely on cloud services more than ever, it is critical that organizations understand the shared responsibility model (SRM) associated with the consumption of cloud services. As we explore how service providers and subscribers share the responsibility for securing cloud services, the call to action remains the same: The broad adoption of cloud services to enable business agility requires a cultural shift. It is in that context that we aim to demystify the most important cloud security construct, the shared responsibility model.

The cloud security shared responsibility model (SRM) is inherent to the use of cloud services: while in traditional on-premises data center deployments, customers had full physical and logical control over the environment, in the cloud, a customer's security responsibility is limited to certain operational areas that vary depending of the nature of the cloud services being utilized. It is essential that subscribers of cloud services be fluent in, and up to date on, how they and their service providers share the responsibility for securing their cloud footprint. It boils down to developing an accurate understanding of who is responsible for what security functions (e.g., patching malware scanning, log analysis, user provisioning, etc.) As the SRM varies by the type of services, and in many instances, between providers of similar cloud services, the ability of a business to develop an accurate understanding of the SRM is critical to its ability to secure its IT operations.

It is essential that subscribers of cloud services be fluent in, and up to date on, how they and their service providers share the responsibility for securing their cloud footprint.

Oracle and KPMG wanted to gauge to what degree businesses understand the cloud security shared responsibility model, whether a year's time has helped organizations clarify areas of confusion around cloud security, and whether ongoing confusion has had a material impact on the security of business information. Our findings show that, there is work to do within the cloud industry collectively.

This report explores the following research findings:

The cloud security shared responsibility model varies by service type and provider.

The absence of a single model across the diverse landscape of cloud services requires businesses to take a more proactive approach to understand the SRM.

Confusion grows as businesses struggle to understand and operationalize the model.

Increased confusion about how a subscriber and a cloud service provider (CSP) coordinate securing the cloud is further evidence of a problematic cloud security readiness gap that is preventing businesses from operationalizing their obligations.

The ramifications of confusion about the shared model are serious.

The implications of confusion are not trivial, including misconfigured cloud services, resulting in possible data loss, introduction of malware, failed audits, and more.

Subscribers seek more transparency from their cloud service providers.

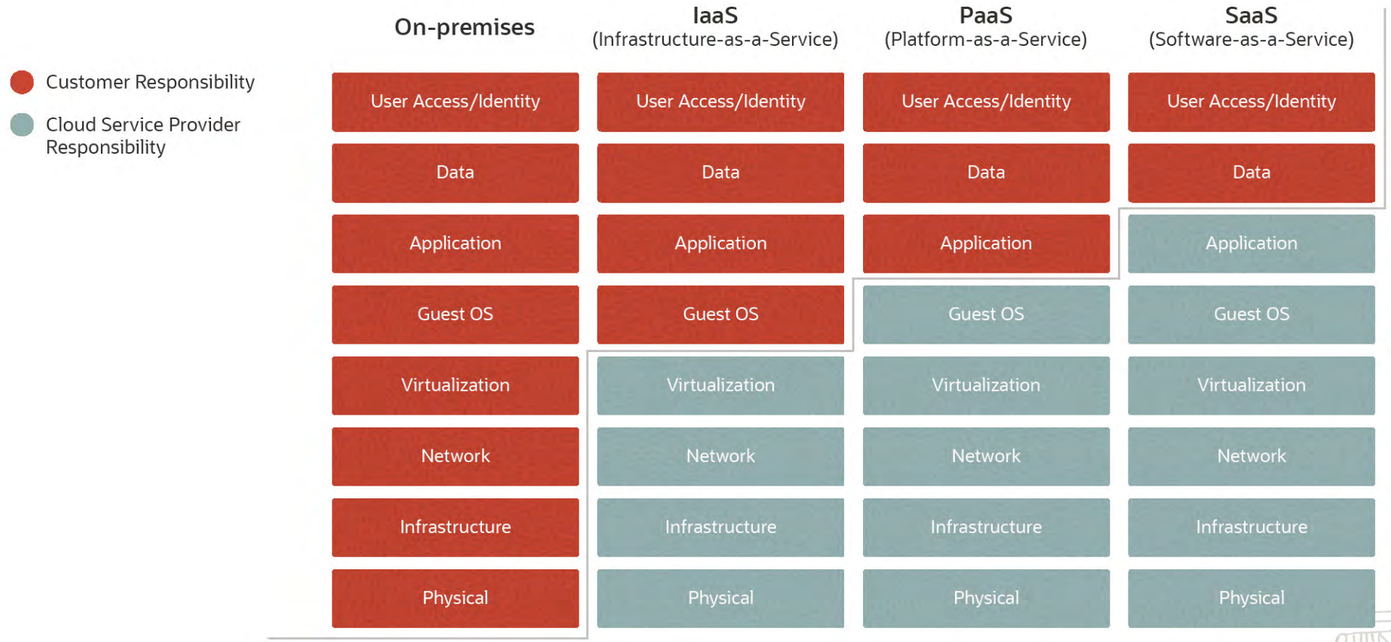
The abstract nature of cloud computing leaves many subscribers wanting to better understand the successes of their CSP's SecOp programs.

The Cloud Security Shared Responsibility Model Varies by Service Type and Provider

The notion of a shared responsibility seems at first to be a simple concept.

In a cloud security context, the shared responsibility model conveys how a cloud service provider is responsible for managing the security *of* public-cloud while the subscriber of the service is responsible for securing what is *in* the cloud. But complexity creeps in due to differences between the types of cloud services and, in some cases, variance between service providers. Additionally, some domains, such as configuration management and compliance, are typically shared, with both parties having substantive mutual functional responsibilities.

Shared Responsibility Security Model



The shared responsibility model conveys how a cloud service provider is responsible for managing the security *of* public-cloud while the subscriber of the service is responsible for securing what is *in* the cloud.

Subscribers Maintain Ultimate Responsibility for Configurations

The first report in this series focused on the need to maintain secure configurations, a topic that spans the tiers listed in the above graphic depicting the model. While subscribers may look to the cloud services provider or other sources for technical assistance, the customer is ultimately responsible for securing configurations in the part of the technical stack they are responsible for.

An illustrative example is the case of setting the appropriate access control lists (ACLs) on object stores. Per the graphic depicting the model, securing access to the data inside an object store with tightly scoped ACLs is the customer's responsibility. However, to assist customers in properly securing access to object-based storage, some CSPs monitor and notify the customers of configuration settings that could be problematic. These notifications often offer advice on how to best remediate the issue.

CSPs may also notify cloud subscribers of other issues, including:

- Multi-factor authentication (MFA) not being used for access to the management console.
- Server workloads exposed to the external internet and thus subject to port scanning.

Because configuration management in the cloud has proven to be a significant challenge that has led to incidents of data loss, it warrants noting the bottom line: Many service providers will offer a lending hand helping customers implement the proper controls, but the customers are ultimately responsible for *how* the services they consume are securely configured.

Many service providers will offer a lending hand helping customers implement the proper controls, but the customers are ultimately responsible for *how* the services they consume are securely configured.

IaaS and PaaS Responsibility Is Workload-based

The main difference between securing the use of IaaS and PaaS is the definition of a workload. The notion of serverless services such as functions-as-a-service (FaaS) and databases-as-a-service (DBaaS) further conflates the distinction since the CSP is managing the underlying server instance. Subscribers need to be diligent in understanding who is responsible for managing what. Let's start by looking at how the shared responsibility model applies to IaaS.

For IaaS, the service provider is responsible for securing everything physical—data center access, network, and bare metal—up to and including the hypervisors that virtualize instances. In the case of application containers, the CSP is also responsible for securing the host operating systems underneath the containers. Such virtualized instance services, be they virtual machines or containers, as well as the applications and code running in them are the security domain of the subscriber.

Given this line of demarcation, customer responsibilities include but are not limited to:

Securely configuring cloud server workloads.

Identifying and remediating known vulnerabilities.

Implementing segmentation rules

Applying runtime preventative, detective, and corrective controls.

In contrast, in a PaaS environment, the CSP is also managing the guest operating system to enable the subscribers to focus on application development and delivery. As such, customers need not worry about whether the workload has been hardened, but they are responsible for managing application security. In this case, the customers may and should opt to use development-time application security tools such as composition analysis as well as static and dynamic analysis for the code they create. When commercial off-the-shelf software is being used, customers should assess the security assurance practices of their vendors to determine the security suitability of the application they wish to operate in the cloud. As code gets built into applications that move into production, runtime controls, such as web application firewalls (WAFs) can be applied by the subscriber via configuration controls to provide additional level of security.

Securing Identities and Data Is the Customer Remit

Moving from left to right in the graphic that depicts the shared responsibility model, it is clear that some security activities apply regardless of the type of cloud service: user access, identities, and data security are always in the customer's remit, with, as noted, an assist from the provider. Assuring a cloud service has been securely configured requires a lifecycle approach to both the human and nonhuman identities (e.g., service accounts, API keys, or bots) that are accessing the service.

Managing the identity lifecycle includes granting the appropriate privileges upon account provisioning, decommissioning stale accounts, revisiting permission levels as roles change and new functionality is provisioned, and monitoring user activity when the most critical and sensitive cloud resources are accessed.

These core identity and access management (IAM) leading practices are challenged by the decentralized nature of cloud adoption in which business units subscribe to diverse cloud services without the involvement of their IT and cybersecurity teams. In such cases, the user accounts for these IT cloud services are often not connected to the company's directory, resulting in silos of identities. Identity sprawl—cloud accounts that are neither federated nor centralized—also means these identities are managed by individuals who are not concerned with or aware of properly scoped IAM configurations.

Cloud IAM is not just about who has access, but right-sizing privileges based on role, task, and sensitivity of the service and data accessed. The concept of zero-trust has gained favor as a strategic approach to authentication, monitoring, and implementing least-privileged management to narrowly scope access to applications and data. Zero-trust also challenges "trust, but verify" authentication and auditing by not trusting, and verifying continuously and adaptively based on context.

Privilege access management (PAM) for SaaS applications presents another example of service-specific policies. Beyond basic read, write, and change privileges, a few examples of such privileges include:

- Sharing documents via an enterprise file sync and share (EFSS) service.
- Creating a new channel in the corporate messaging platform.
- Assigning tickets in an IT service management (ITSM) application.

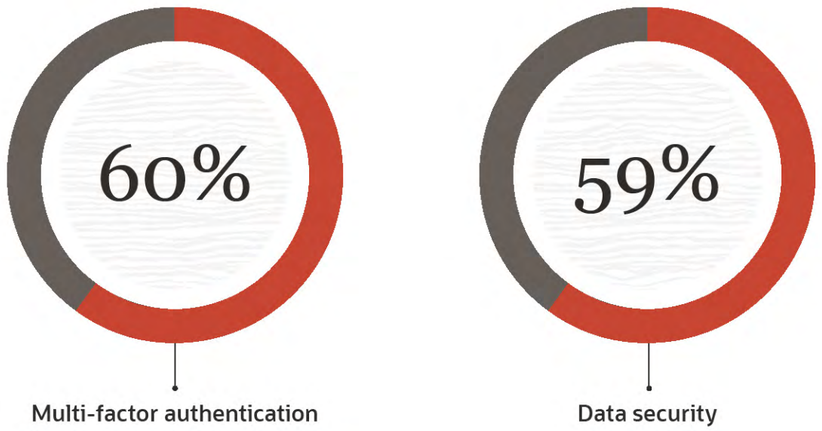
Assuring a cloud service has been securely configured requires a lifecycle approach to both the human and nonhuman identities (e.g., service accounts, API keys, or bots) that are accessing the service.

These examples of zero-trust policies to secure access to cloud services require that the subscriber of the service implements the requisite controls, which may be provided by the CSP. For example, MFA should be configured for secure access to an organization's most critical cloud resources, proactively up-leveling authentication requirements in response to the detection of anomalous behaviors and enabling additional verification to perform a privileged task.

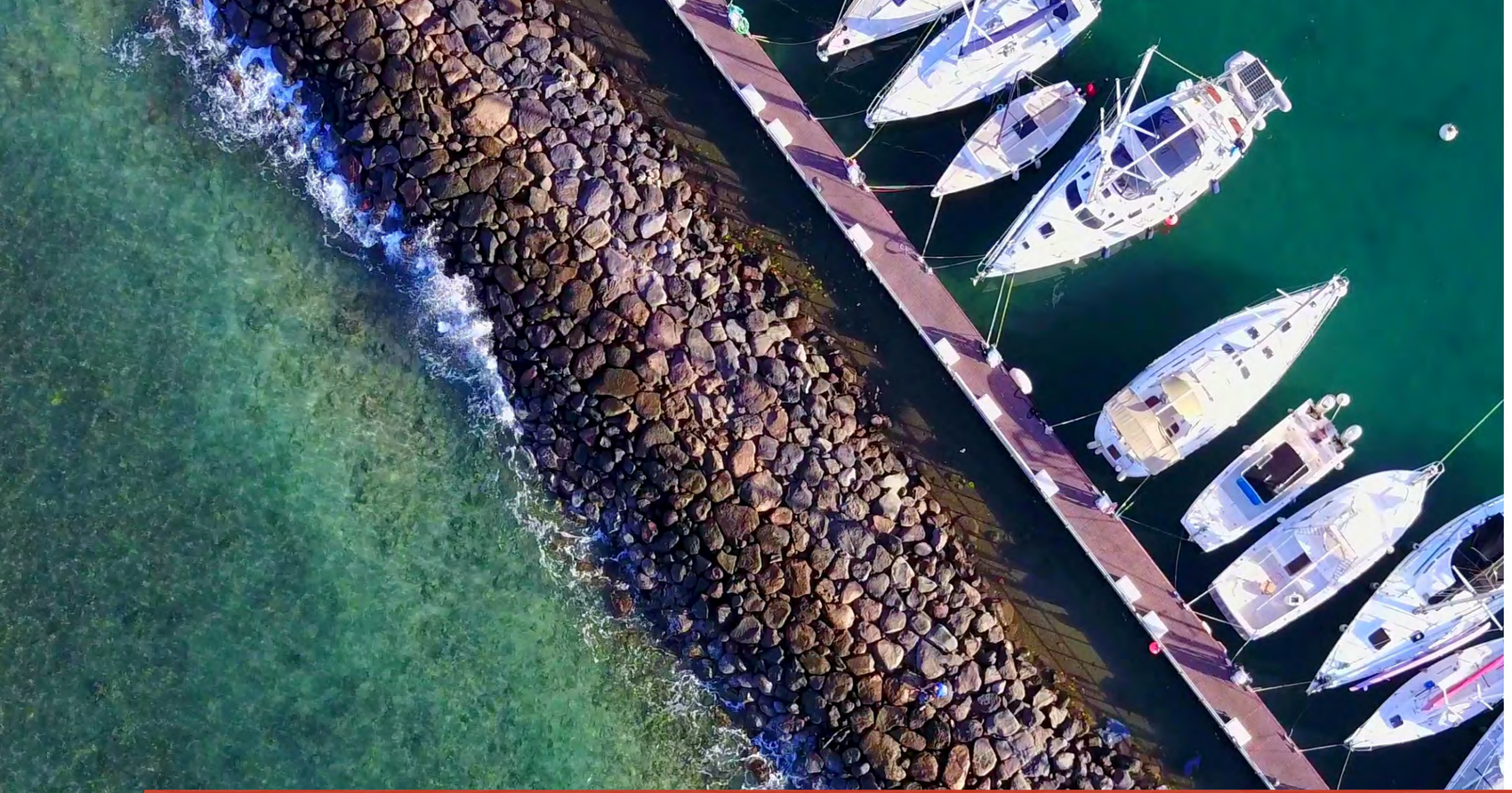
Research respondents view MFA and data security as technologies that support a zero-trust strategy.[1] In fact, data security joins user access and identities as tiers of the cloud security shared responsibility model for which the subscriber is always responsible, inclusive of data discovery and classification, encryption, key management, and data loss prevention (DLP).

This does not mean the service provider isn't there to help with recommended practices, frameworks, and controls. For example, it is quite common for CSPs to provide native data encryption controls. Some CSP services encrypt by default, but some do not—an example of the variance between providers and services that customers must understand. In that same vein, a service provider may also offer key management-as-a-service (KMaaS) as well as single- and multi-tenant key stores, but the use of those services to follow key management leading practices such as rotation, decommissioning, and separation is the domain of the subscriber. While providers may notify the subscriber of potential issues and provide controls native to their service, the subscriber is ultimately responsible for identity and access management and data security.

Does your organization use – or is it considering – any of the following technologies to support its "zero-trust" strategy? (Percent of respondents, N=246, multiple responses accepted)



1 Source: ESG Master Survey Results, Network Security Trends, March 2020.



Security of the Full Stack is a Shared Responsibility

Since a cloud service provider can represent a strategic and thus critical aspect of an organization's digital supply chain, a subscriber's due diligence on a provider may reasonably include their compliance with one or more industry regulations. Customers must ensure that they are meeting and maintaining compliance with applicable regulations. As such they must assess the security practices of their CSPs as well as develop and maintain the required controls in the context of the SRM to meet their compliance needs. While part of the stack that the CSP is responsible for may have passed an audit, how customers build on the stack, how they configure services, how they control access to and audit use of that service, and the type data they place in the cloud are not in the scope of a CSP's compliance program. As such, subscribers in regulated industries need to consider whether what they put in the cloud will be in regulatory scope and apply the appropriate controls and processes regardless of whether or not the service provider provides attestation of compliance with the same regulation.

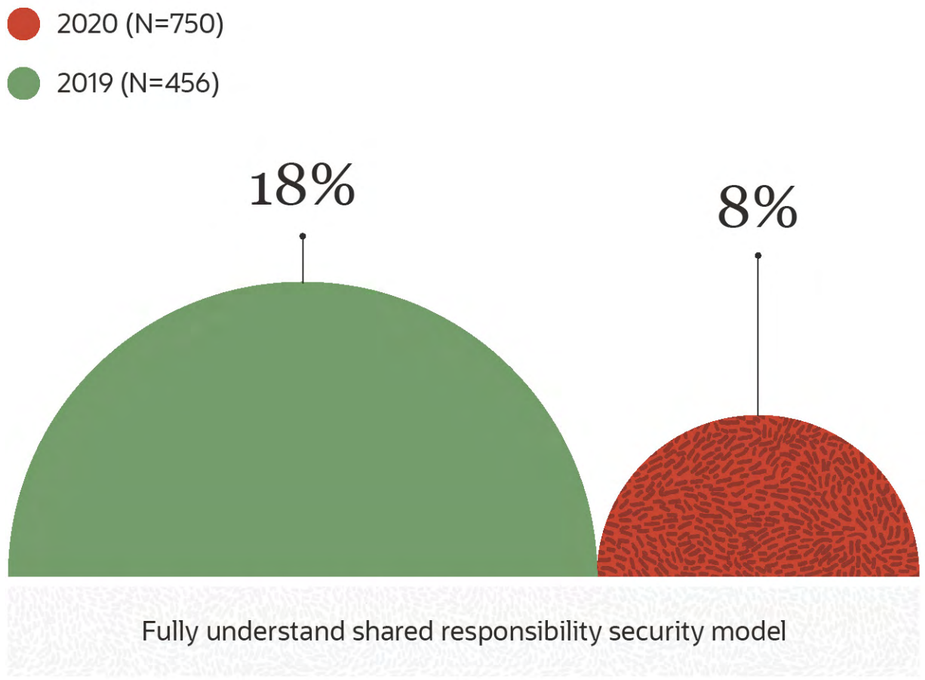
Subscribers in regulated industries need to consider whether what they put in the cloud will be in regulatory scope and apply the appropriate controls and processes regardless of whether or not the service provider provides attestation of compliance with the same regulation.

Confusion Grows as Businesses Struggle to Understand the Model

As a term, “the cloud security shared responsibility model” is reasonably familiar to our respondents, with 55% saying they are very familiar with the term and 41% saying they are pretty familiar with the term. However, our findings have shown that any level of familiarity does not equate to expertise. In last year’s Oracle and KPMG Cloud Threat Report 2019, only 18% said they fully understand the model for all types of cloud services, which we found disconcerting. It is further concerning that only 8% of this year’s research participants said they fully understand the shared responsibility model for all types of cloud services, a notable 10% degradation.

CISOs have not yet emerged as experts as one would hope, with only 7% saying they fully understand the model. Note: We will take a closer look at how cloud has impacted the role of CISO in a future report in the Cloud Threat Report series, The Mission of the Cloud-centric CISO.

A comparative of general Shared Responsibility knowledge, mapped against CISO knowledge from last year to this year.



The Shared Model for Securing SaaS Applications Is the Most Confusing

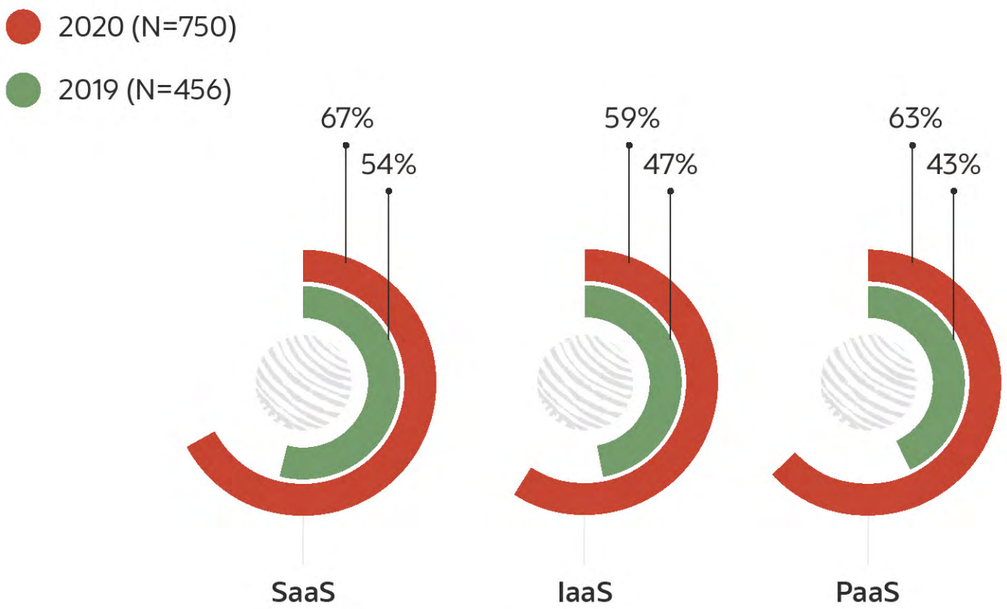
Where is the most confusion? Ironically, it is where the customer has the least amount of responsibility: SaaS applications. And SaaS applications are also the type of cloud services for which year-over-year confusion increased the most.

Let's unpack what is driving confusion around this cloud security construct. For starters, most enterprises and their IT and cybersecurity teams are charged with managing and securing a complex, multi-cloud environment comprised of disparate data centers. Such heterogeneity drives complexity but also provides benefits in the area of high-availability without an over reliance on a single data center. To this point, nearly two-thirds of research respondents stated that their IT environment is more complex today than it was two years ago.[2]

A contributing factor to complexity is the diversity of most companies' cloud portfolios. For example, just two years ago, half of the businesses who participated in an annual spending intentions research study noted they were using infrastructure-as-a-service (IaaS). As we probed IaaS adoption intentions for 2020, we found a notable increase to two-thirds of organizations using IaaS.[3]

A contributing factor to complexity is the diversity of most companies' cloud portfolios.

For which of the following types of cloud services do you find the shared responsibility security model the most confusing? (Percent of respondents, N=750, multiple responses accepted)

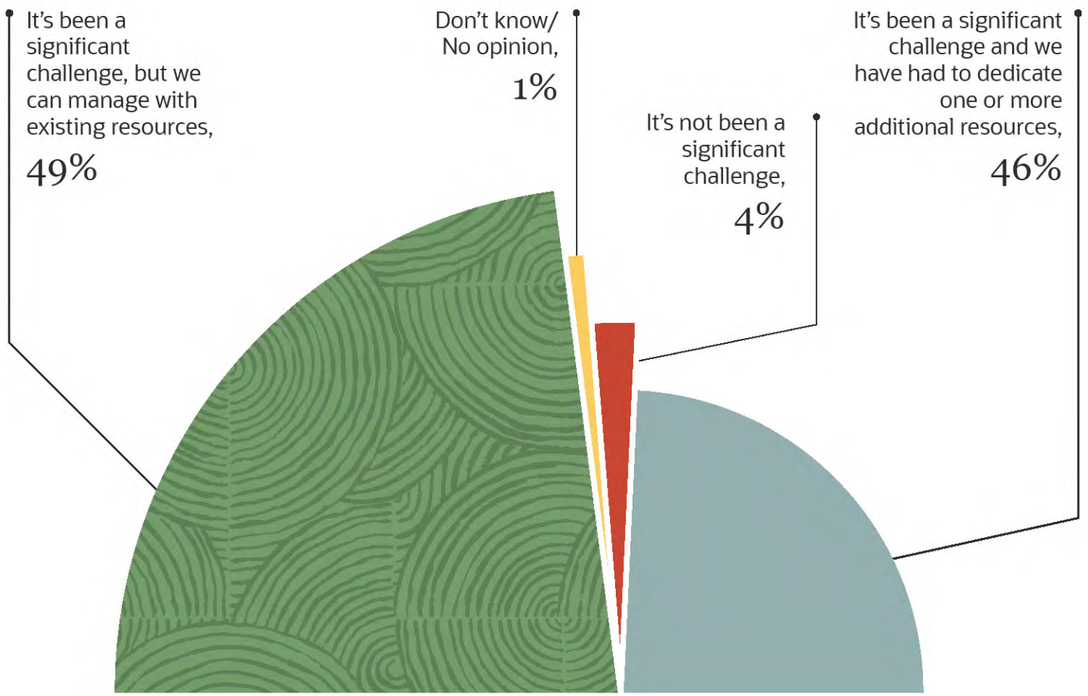


2 Source: ESG Master Survey Results, 2020 Technology Spending Intentions Survey, January 2020.
3 Ibid.

With respect to SaaS applications, we have seen not only an increase in usage, but the migration of those applications from on-prem to public cloud solutions. This is an important point: Front-, middle-, and back-office applications that run the business necessitate the involvement of the IT and cybersecurity teams. This inflection point has brought about an epiphany for many—the consumption of cloud services to host and deliver business-critical applications necessitates understanding the implications of outsourcing and leads to a realization that the division of labor for securing those applications is often murky.

We can also assume that the ongoing shortage of cybersecurity skills[4] makes retooling skills to develop expertise in shared responsibility models challenging. As such, our respondents shared that they are taking action to address confusion with resourcing. Nearly half of this year's respondents shared that in order to maintain a clear understanding of the variance in models between CSPs, they have had to dedicate one or more additional resources.

Which of the following best represents the effort required to maintain a clear understanding of the differences in the shared responsibility security model between different cloud service providers (CSPs)? (Percent of respondents, N=719)



4 Source: ESG Master Survey Results, 2020 Technology Spending Intentions Survey, January 2020.

Problem solving starts with awareness:

Our respondents are aware of the issue and thus are starting the process of educating themselves and their colleagues on what their obligations are to secure their cloud footprint. Once again, doing so is predicated on a cultural shift that brings all stakeholders into the cybersecurity conversation. Moving forward, business unit, DevOps, IT, legal, compliance, and cybersecurity organizations all need to be involved from the inception of cloud adoption and work collaboratively on developing a core competence in understanding the cloud security shared responsibility model for each service in use.

Adoption of cloud services cannot be the sole decision of the LOB based on operational requirements alone: security requirements must be understood from the onset. Unfortunately, in a haste to adopt cloud services, many organizations do not consider security requirements until they engage in the contract negotiations with the CSP. Very often this means, that purchasing departments are left with issuing vague and ambiguous security requirements that do not properly align with the intended risk posture of the organization.

Business unit, DevOps, IT, legal, compliance, and cybersecurity organizations all need to be involved from the inception of cloud adoption and work collaboratively on developing a core competence in understanding the cloud security shared responsibility model for each service in use.

Connected Applications, Further Confusion, and Configuration Issues

Confusion, from the onset, about how security is shared between a provider and subscriber means mistakes will be made when a cloud service is first enabled and configured. Some mistakes, such as misconfigurations of identity and access management roles, and granting of excessive privileges, persist, contributing to a significant attack surface. As the use of a given service expands across a business, and new functional capabilities are employed, such configuration mistakes are compounded. As such, organizations need to plan for not only the initial rollout of a cloud service, but also how changes over time impact their security obligations. Let's look at a few examples.

When it comes to customer relationship management (CRM) applications, many organizations start with the core CRM functionality of managing the lifecycle of their customer base. As the implementation matures and the business has confidence in the accuracy and integrity of its customer data, teams are likely to add layered SaaS applications that are connected to the base CRM instance. This could include a third-party analytics application to gain insights into customers and marketing automation software to execute prospect nurturing campaigns. In the case of marketing automation, a member of the sales operations team may provision administrative access to the marketing automation application to a member of the marketing team, who now has escalated privileges.

The use of enterprise resource planning (ERP) applications often track to a similar usage pattern. With base ERP functionality enabled, an organization may choose to add a supply chain module—another example of a layered and connected SaaS application—in which users may be granted excessive privileges. Yet another example is a financial application used to manage a business's general ledger and accounts payable and receivable processes that gets connected to an asset management module.

The market of third-party add-on applications is robust and represents yet another layer of abstraction that can introduce confusion around who has responsibility for securing what application stacks. While the service provider for one of those layers may provide IAM or data security controls, it bears repeating that the use of such controls is up to the subscriber to secure the vertical stack of connected SaaS applications.

While the service provider for one of those layers may provide IAM or data security controls, it bears repeating that the use of such controls is up to the subscriber to secure the vertical stack of connected SaaS applications.

Confusion About the Shared Model Can Have Serious Ramifications

But does confusion matter?

That is, just how exposed are businesses that fail to develop a competency in understanding and acting upon the specifics of the cloud security shared responsibility model? It is clear that confusion around the model causes multiple negative outcomes, highlighting the need for organizations to gain clarity.

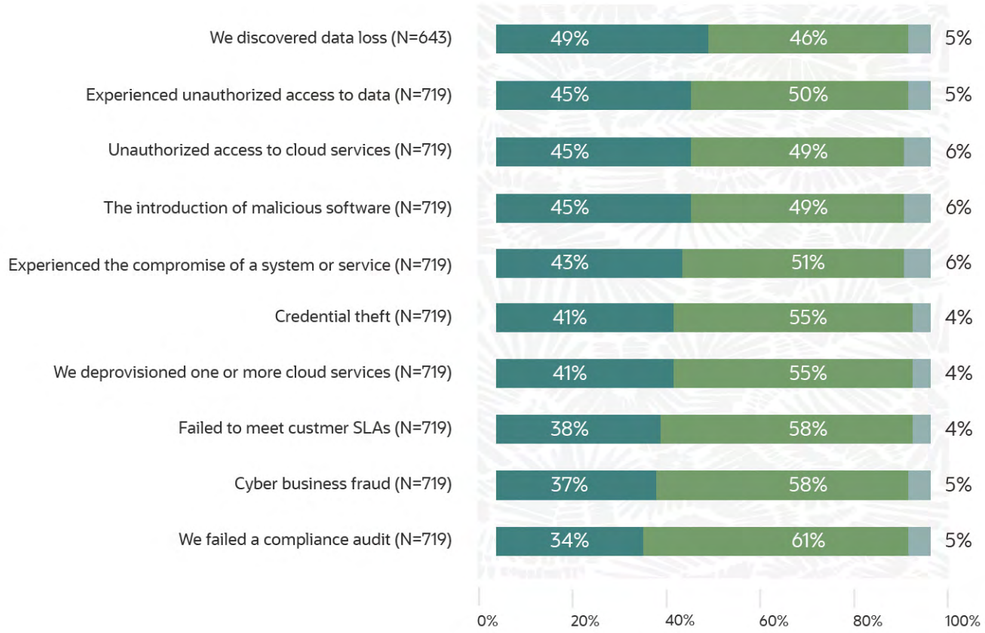
From Confusion Comes Data Loss, Malware, and Stolen Credentials

As more data is stored using cloud services, including that deemed to be sensitive, cloud data security becomes increasingly important. To that point, 89% of our research participants shared that at least half of their cloud-resident data is sensitive. Unfortunately, three trends lines are heading in the same direction:

1. The percentage of cloud-resident data considered sensitive.
2. Increasing confusion over the cloud security shared responsibility model.
3. Data loss attributed to confusion over the model.

On the last point, the year-over-year trend is troubling—more than doubling from the 23% who reported last year that confusion over the shared responsibility model led to data loss to nearly half of the those who reported the same this year.

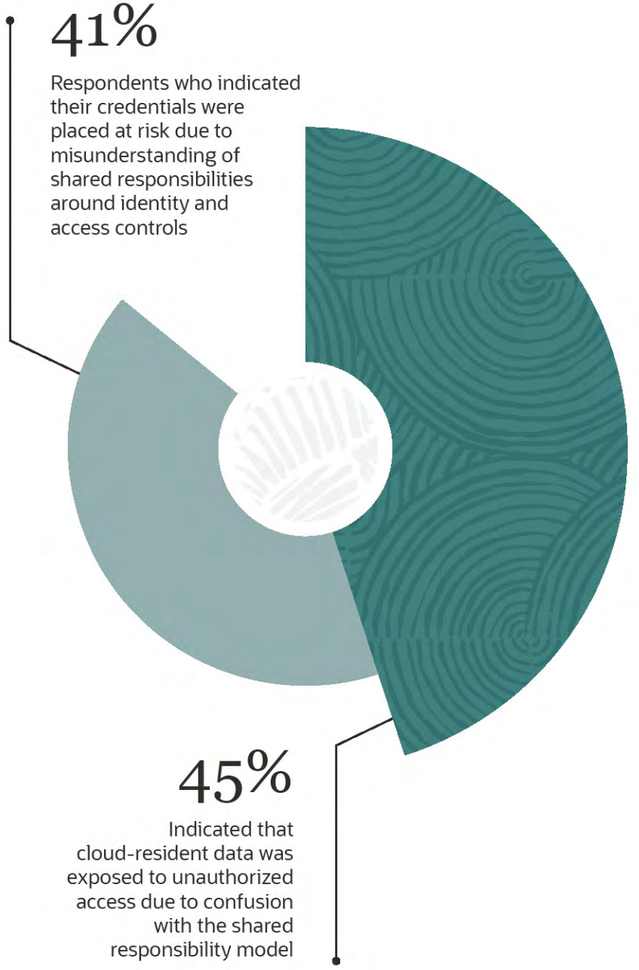
Has confusion about the shared responsibility security model resulted in any of the following events in the past? (Percent of respondents)



Another aspect of compromised cloud-resident data is unauthorized access, an issue 45% of research participants reported due to confusion around the shared responsibility model. More broadly, unauthorized access to cloud services in general due to confusion is also a notable issue for the same number of respondents. In an IT reality where lines of business self-provision a SaaS application, a lack of attention to privilege management can result in unauthorized access to data. The root of the issue is the use of cloud services for collaboration with both internal constituents and third parties, a workflow more common with the increase in a remote workforce.

In addition to putting data at risk, confusion opens the door for malware, per the 45% who noted this outcome. If customers do not understand that, in the context of privilege management, they are responsible for server workload configurations, including the instrumentation of host-based security groups, malware is more likely to move laterally to vulnerable servers. And when subscribers do not fully understand that they are responsible for IAM, cloud credentials are more likely to get stolen, another result of confusion that was reported by 41% of respondents.

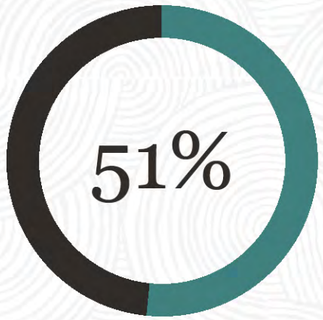
In an IT reality where lines of business self-provision a SaaS application, a lack of attention to privilege management can result in unauthorized access to data.



Confusion Leads to Weak Configurations

Those respondents who reported that they discovered misconfigured cloud services were generally less literate on the cloud security shared responsibility model. More specifically, 72% of respondents who noted they discovered over-privileged SaaS accounts are most confused about how the model applies to SaaS applications. The outcome? As discussed in the prior report in this series, Addressing Secure Configurations Amidst a State of Constant Change, more than half (51%) of the respondents who said they discovered a misconfigured cloud service reported that it led to data loss. Note: We will take a closer look at how cloud has impacted the efforts of the CISO in mitigating data loss in a future report in the Cloud Threat Report series, The Business Impact of the Modern Data Breach.

With respect to the lack of understanding of the model for IaaS, there is also a connection between configuration missteps and confusion. Two-thirds of the organizations who reported discovering open SSH ports (versus 59% of all respondents) cited confusion around how the model applies for securing their use of IaaS, indicating a lack of clarity on which party is responsible for securing cloud-resident server workloads.



of the respondents who said they discovered a misconfigured cloud service reported that it led to data loss

Those who failed a compliance audit are also more confused than other respondents.

- **76%** who failed a compliance audit found shared responsibility model for SaaS confusing—10% more than the average.
- **66%** who failed a compliance audit found shared responsibility model for IaaS confusing—9% more than the average.

And, finally, those who have experienced cyber business fraud due to confusion are also more confused than others. Note: We will take a closer look at how the use of cloud services has led to an increase of cyber business fraud incidents in a future report in the Cloud Threat Report series, *Addressing Cyber-risk and Fraud in the Cloud.*

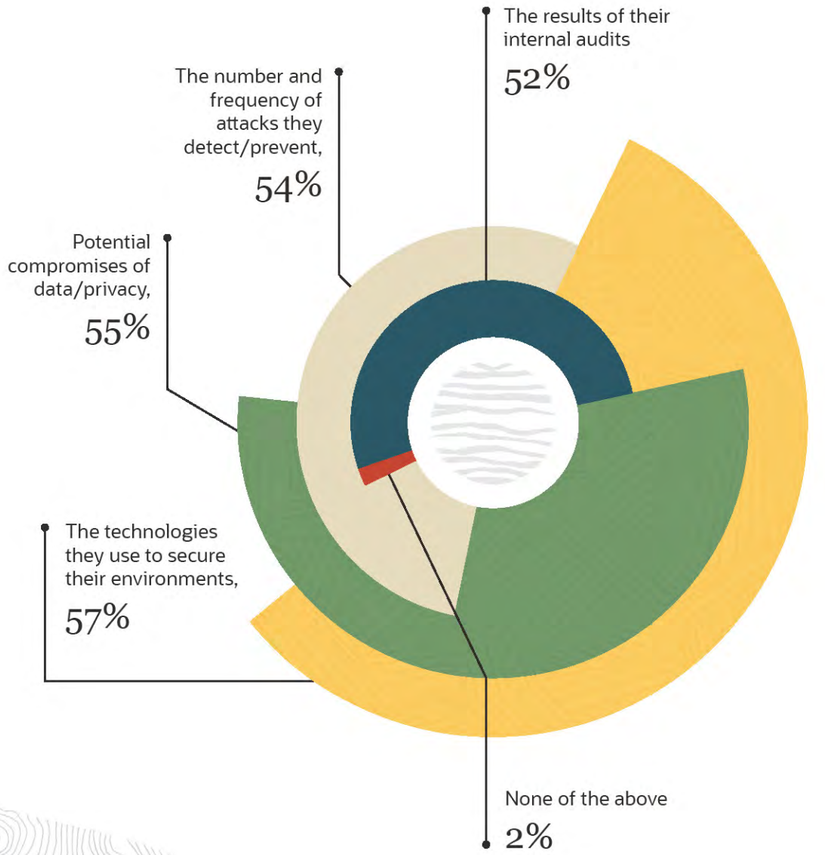
Subscribers Seek More Actionable Intelligence from Their Cloud Service Providers

For many, the cloud is an uncomfortable level of abstraction.

The lack of physical access to infrastructure now operating in someone else's data center is a brave new world. As such, perhaps due to confusion around the shared responsibility model, our respondents want more actional information from their service providers. Subscribers should start that dialog with a prospective service provider by asking that CSP to complete a Consensus Assessment Initiative Questionnaire (CAIQ), a Request for Information (RFI) templated defined by the Cloud Security Alliance (CSA). A completed CAIQ will help the subscriber better understand the security practices of the CSP and ultimately determine the suitability of the cloud service considering the organization's security requirements. As previously-noted, organization's purchasing departments are often left with issuing vague and ambiguous security requirements at the time of the contract. The use of a CAIQ, prior to entering the contractual phase, will help the organization gather accurate information about the security practices of the CSPs, and help determine the security suitability of the cloud service being considered.

At the top of the list, customers want to know what technologies cloud service providers use to secure their infrastructure. Customers also want to determine whether the CSP is able to detect and prevent attacks. While customers want more visibility into the potential for compromises of data and privacy in general, it is important noting that this data is largely irrelevant as it is likely an indication of how poorly cloud subscribers are securing their environment, as opposed to how effective the CSP is at securing the environment it is responsible for.

Does your organization need more transparency from its cloud service providers (CSPs) in any of the following areas? (Percent of respondents, N=750, multiple responses accepted)



In Summary: Culture Is the Catalyst to Close the Readiness Gap

A secure journey to the cloud requires that organizations develop a core competency around understanding the cloud security shared responsibility model. The dynamic nature of the cloud means such a competency must also account for change. Fluency in the model then, inclusive of variations and nuances, must always be current so organizations can adapt and stay secure.

As we have discussed, the shared responsibility model does not offer a clear break between provider and subscriber, but rather a dovetailing of how the two entities can collaborate to keep cloud properties safe.

To gain more clarity subscriber responsibilities, some practices to demystify confusion include:

Cadence: Regularly review with the cross-functional team how changes in your business's use of cloud services impacts your obligations.

Configuration management: Treat configuration management as a set of core leading practices, appreciating that your CSP may provide guidance and controls, but you are responsible for how your company uses the cloud.

Understand Identity and data security: Fully understand that IAM and data security is the subscriber's responsibility, including how these domains impact the ability to meet and maintain compliance with applicable industry regulations.

Compliance: Assess the security practices of the CSPs as well as develop and maintain the required controls in the context of the SRM is the subscriber's responsibility. Compliance requirements may be performed by both provider and subscriber but are not transferrable. Attestation from a CSP does not extend to your use of its cloud.

Knowledge Exchange: Leverage the knowledge of others who have paved the way by following documented leading practices as well as frameworks prescribed by your cloud service providers and industry organizations.

Control evaluation: Evaluate the native controls provided by your CSP in light of your organization's risk posture and augment native cloud controls with business process and IT general controls that together represent a defense in depth approach to meeting your part of the shared responsibility model.

In conclusion, IT professionals must be change agents for a cultural shift that treats your cloud service providers as partners and creates a climate that emphasizes cybersecurity as a shared responsibility among all internal stakeholders.

ORACLE KPMG

Research conducted in partnership with ESG