WHITE PAPER

YOUR ORGANIZATION'S ROLE IN THE SHARED RESPONSIBILITY MODEL

A Guide to Understanding and Taking Control

CloudCheckr

TABLE OF CONTENTS

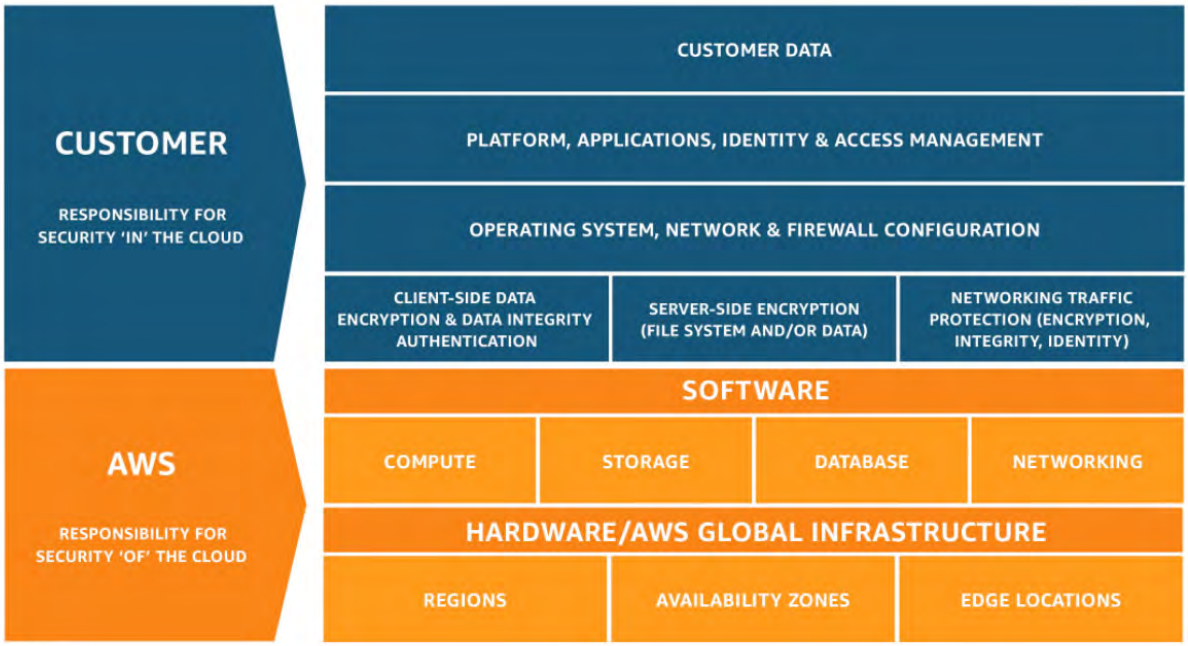
OVERVIEW

Public cloud providers have had no choice but to take their security and compliance responsibilities very seriously. While initially there were many concerns about the security of data in multi-tenant architectures and on infrastructures not directly under the enterprise's control, cloud providers have done a good job of convincing users that their infrastructures are as secure as—if not more secure than—on-premises data centers. As a result, we are seeing more and more highly-regulated sectors such as finance and healthcare deepening and broadening their cloud profiles. Perhaps the strongest endorsement for the security capabilities of the cloud providers was the CIA's strategic decision to go all-in on the cloud, using a private AWS cloud deployment.

However, the two leading cloud providers, AWS and Microsoft Azure, have made it clear that their responsibility for security and compliance goes only so far. Customers are left having to close the data security loop. AWS and Microsoft Azure have articulated a shared responsibility model for security and compliance, which has been adopted by the other cloud providers as well.

This white paper looks at how AWS and Azure have divided the security and compliance responsibilities between the cloud providers and their customers as well as what enterprises need to do to properly secure their cloud-based assets.

FIGURE 1:
AWS Shared Responsibility Model



THE SHARED RESPONSIBILITY MODEL ACCORDING TO AWS AND MICROSOFT AZURE

There are virtually no differences between Amazon's and Microsoft's visions of the shared responsibility model. As shown in Figures 1 and 2, both companies take responsibility for the security of their infrastructure and managed services. The user is responsible for the security of the software it chooses to run on that infrastructure. They are also responsible for the security of their data—in-transit and at-rest.

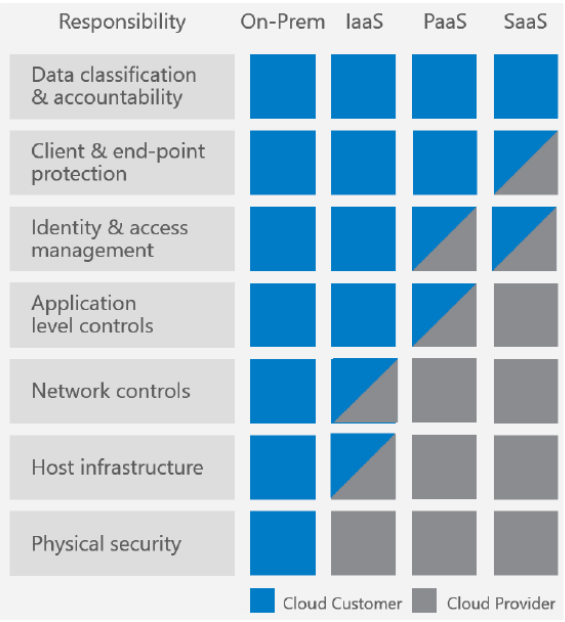
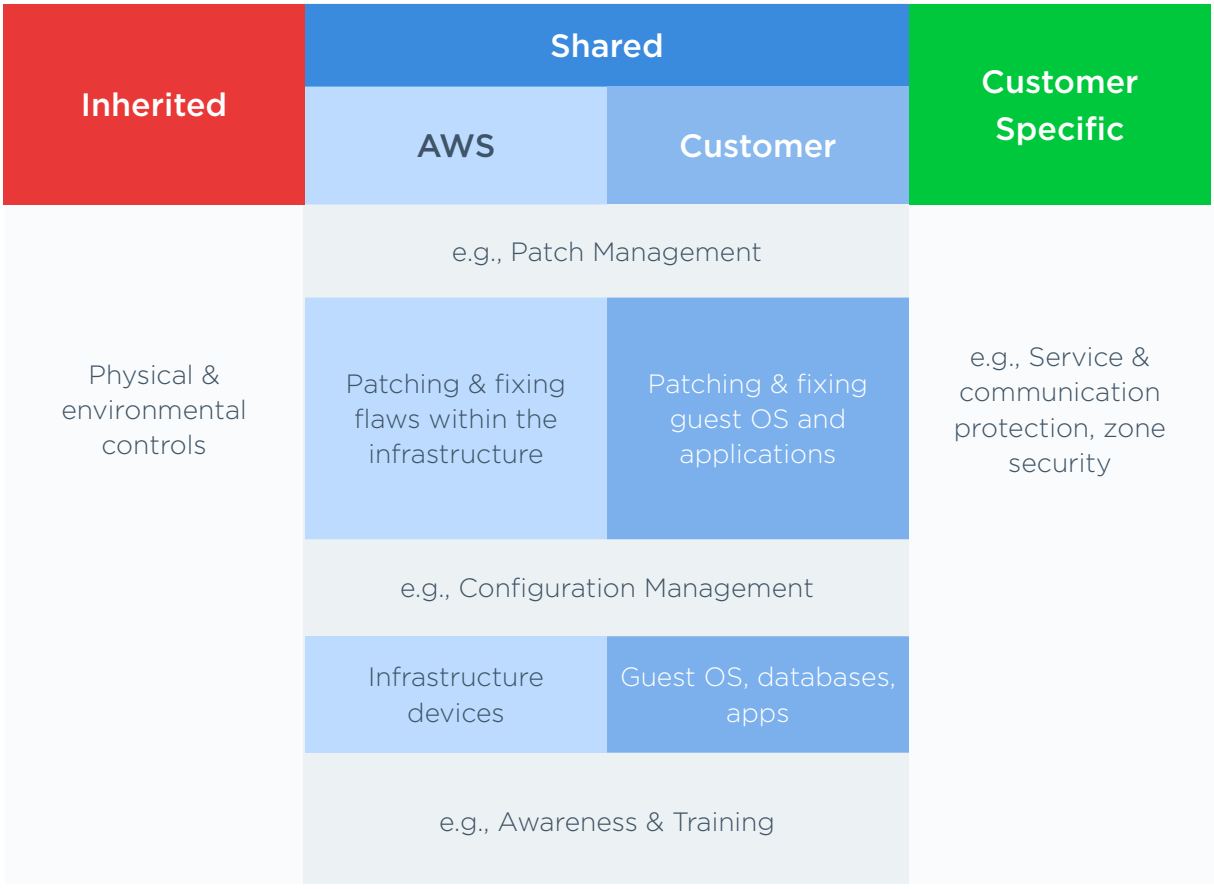


FIGURE 2:
Azure Shared Responsibility Model

AWS explains the shared responsibility model by differentiating between Security **of the** Cloud (for which it takes responsibility) and Security **in the** Cloud (for which the customer is responsible). To provide a secure cloud, AWS manages and controls the host operating system, the virtualization layer, and the physical security of its facilities. To ensure security within the cloud, the customer configures and manages the security controls for the guest operating system and other apps (including updates and security patches), as well as for the security group firewall provided by AWS. The customer is also responsible for encrypting data in-transit and at-rest.

As shown in the table below, AWS categorizes security controls based on those that are fully inherited by a customer from AWS, those that are shared, and those that are customer-specific.



The Azure rendition of the shared model (see Figure 2) effectively illustrates how the boundary of responsibility shifts depending on the level of cloud deployment:

› In an IaaS framework, the provider is completely responsible for the physical layer and shares responsibility with the customer for the security of the host infrastructure and network; all the rest is the responsibility of the customer.

› In a PaaS framework, the provider also takes full responsibility for host infrastructure and network security, but it also shares responsibility with the customer at the application and access control levels.

› In a SaaS framework, the provider takes full responsibility for application controls while sharing responsibility with the customer for access control as well as client/endpoint protection.

No matter what the framework is, the customer is always fully accountable for classifying and protecting its own data.

Another context within which the customer bears responsibility for security is the Amazon Machine Image (AMI). AMI provides the initial configuration for an EC2 instance (OS and app runtime parameters), including security controls related to confidentiality and compliance. It is recommended that the customer build a catalog of AMIs with security configuration baselines that ensure each instance conforms to the organization's security policies. It is also the customer's responsibility to keep its AMIs updated to the latest security patches.

Both AWS and Azure provide best practice guidelines and an array of services and tools to help their customers uphold their end of the shared security responsibility. The following table describes some of the leading AWS and Azure tools and services.

AWS and Azure Tools and Services

	AWS	Azure
Configuration Control	**AWS Config:** Fully managed service that provides an AWS resource inventory, configuration history, and configuration change notifications.	**Operations Management Suite Automation and Control:** Manages all automation and configuration assets from a centralized repository.
Compliance	**AWS Service Catalog:** IT services approved for use on AWS for consistently meeting compliance requirements.	**Secure Development Lifecycle (SDL):** Helps developers build more secure software and address security and compliance requirements.
Encryption	**AWS CloudHSM:** Securely generates, stores and manages cryptographic keys. **Server-Side Encryption (SSE):** Encrypts data with a key generated by AWS or a key supplied by the customer.	**Azure Rights Management (RMS):** Uses encryption and authorization policies to secure files and email. Customers can provide its own keys. **Azure Key Vault:** Safeguards cryptographic keys and other secrets.
Access Control	**AWS Identity Access Management (IAM):** Secures control of user and app access to AWS resources.	**Azure Active Directory (AD):** Provides multi-factor authentication, ID protection, and role-based access control.
Audits	**AWS CloudTrail:** Records AWS API calls in log files for security analysis and compliance auditing.	**Azure Activity Logs:** Data can be exported to Security Incident & Event Management (SIEM) systems for analysis.
App Security	**Amazon Inspector:** Automated security assessment service improves security and compliance of apps deployed on AWS. Includes a knowledge base mapped to security, best practices and vulnerability definitions.	**Azure Security Center:** Integrates security monitoring and policy management.

THE KEY CHALLENGES OF CLOUD SECURITY

While it may be possible to "lift and shift" infrastructures and workloads to the cloud with little or no refactoring, migrating traditional security tools is a more complicated process. The cloud introduces a whole new set of security challenges and requires an entirely new way of thinking about security.

The challenges start with the unprecedented velocity of change that the cloud allows as a result of its on-demand resources and streamlined provisioning processes. Traditional security tools cannot handle this "chaos," and configuration and policy management become overwhelming tasks. Access and other security controls are weakened and become unreliable.

The next challenge is the transient nature of networks in the cloud. Virtual instances are spun up instantaneously and torn down just as quickly. Network identifiers, such as IP addresses, are no longer stable control points, and the encryption of data in-transit to and from the cloud reduces the visibility into application behavior. Perimeter-based security tools cannot do their job when the perimeter has, for all intents and purposes, disappeared. In short, traditional network-centric security tools cannot provide a suitable measure of protection for cloud-based assets.

The cloud is complex in even the simplest deployment framework, i.e., working with a single public cloud provider. The complexity increases exponentially in multi-cloud or hybrid deployments, which are quickly becoming the norm. Analyzing security incidents—or even tracking an administrator's activities—across a multitude of cloud entities, configuration files, event logs, networks, and so on is impossible for legacy data center security tools.

Last but not least, with the cloud providers responsible—at a minimum—for securing the infrastructure, the host OS, and the networks to and from their facilities, customers have far less visibility and control than they would in their own environments. This too undermines the ability of on-premises-oriented security tools to do their job.

What You Can Do to Close the Gaps

Given the sheer size of the target, cloud-based enterprise data is a magnet for malicious security threats from attackers both within and outside of organizations. So, if cloud data theft is not uncommon, which entity is not holding up its end of the shared responsibility model?

According to a recent Gartner report, the answer is very clear: the customer. It is expected that over the next five years, at least 95% of cloud security failures will be the customer's fault. Based on the European Union's GDPR data privacy legislation that came into effect May 25, 2018, we can also say that regulators place the onus of securing personal data squarely on the shoulders of the data owner, i.e., the entity that collects the data. It is the data owners who are liable for data security breaches and it is their responsibility to ensure that their cloud providers have suitable security and compliance measures in place.

With that in mind, listed below are some best practices that can enhance the security of cloud-based assets:

- **Data governance:** A 2017 State of Data Governance survey indicates that only about 50% of organizations have dedicated data governance programs. It is entirely the enterprise's responsibility to put in place and enforce policies for cloud data ownership and responsibility. At the most basic level, the enterprise must understand and classify its data so that the appropriate security measures can be implemented according to the varying levels of data sensitivity.

- **Keep software current:** It is the customer who is responsible for the security of the software that it runs on top of the cloud. Patching is the bread-and-butter of security, and it's no different in the cloud.

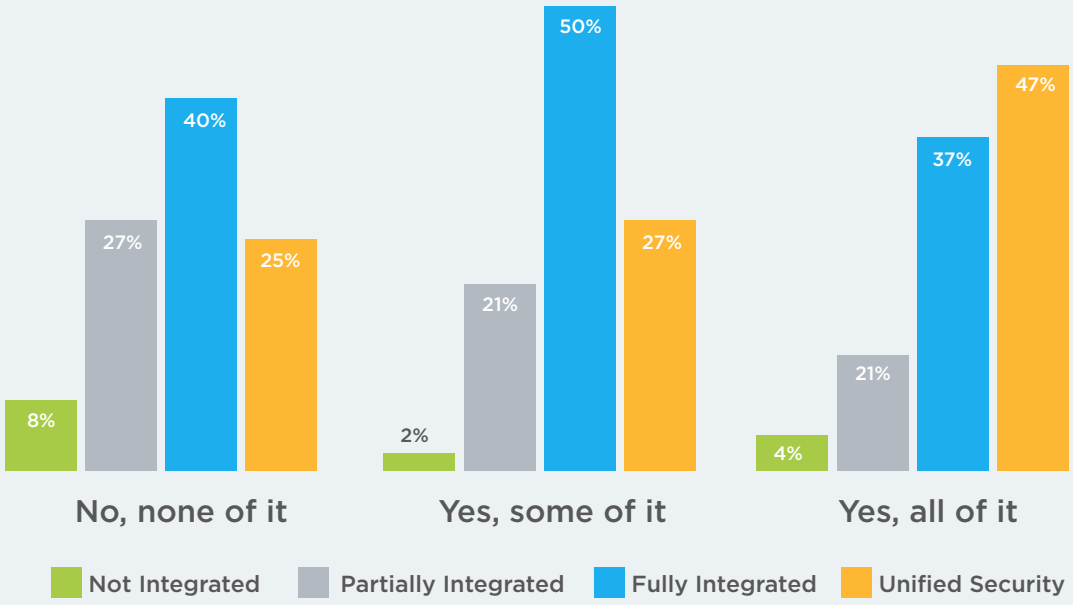
- **Ensure that security is built into apps, operational processes, and enterprise workloads:** Since it is no longer feasible or useful to monitor network activity, the security focus has to shift to the entities that are running in the cloud and the processes used to deploy and manage them. Winning organizations are embracing a shift-left approach to app development and deployment, with DevSecOps teams building security into apps and processes at the design and coding stages.

- **Diligent management of identity and access controls:** Identity and access management (IAM) in the cloud is substantially more complex than it is in closed, monolithic environments. Cloud providers offer best practice guidelines as well as tools and managed services to help organizations handle IAM, but it's up to the organization to use them effectively.

- **Realtime configuration management:** Here is a concrete example of why this best practice is so important. Several years ago, an American healthcare provider began using a cloud-based productivity suite. Due to misconfiguration, its email module bypassed the check that prevents personal health information from being transmitted externally. The oversight was detected only in a quarterly configuration audit because the healthcare provider had not deployed a cloud security solution that automatically and immediately alerted the staff about critical configuration changes. In addition to being a serious breach, the oversight also cost the healthcare provider a hefty seven-figure non-compliance fine.

Does your organization's public cloud service store your organization's sensitive data?

(split by level of integration of security solutions)



Source: https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#570866391848

The Importance of Automation

According to that same Gartner report, in 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures. A 2017 Intel Security survey indicates that there is a high correlation between an organization's willingness to store its most sensitive data and the extent to which it has embraced an integrated and unified security solution.

As the speed of business continues to accelerate, automation across all IT functions will be critical. We're seeing this need in app development and operations, and it is starting to have an impact on security functions as well.

Even the most experienced and well-educated system administrator can only manage so many servers, databases, and storage systems at a time. The only way to manage a growing cloud infrastructure, at scale, is through automation.

CONCLUSION

Next generation automated cloud monitoring and security management tools like CloudCheckr are essential for providing effective protection in the face of cloud complexity and velocity. CloudCheckr's self-healing automation capabilities can detect, and remedy security misconfigurations. Their "Fix Now" button corrects the issue and "Always Fix" can do so whenever such an issue is detected, without human intervention. For example, if a user makes an S3 bucket public, automated Best Practice Checks detect the permissions issues, correct them, and emails the administrator with news of the correction. Alerts can be enabled to notify appropriate personnel of any specific configuration change.

The cloud providers are constantly investing in innovative solutions to strengthen their security profiles. In order to hold up their end of the shared responsibility model, their customers must do the same.

See automated security in action.
Schedule a custom demo with one of our cloud experts. **cloudcheckr.com/demo**

CloudCheckr

342 N GOODMAN ST,
ROCHESTER, NY 14607

1-833-CLDCHCK

CLOUDCHECKR.COM