An Executive's E-Guide to Protecting Workloads and Data on AWS

With Prisma Cloud

paloalto NETWORKS | aws

Table of Contents

Introduction: The State of Cloud Security

In almost every industry, cloud computing is the new reality, enabling greater speed, agility, innovation, and scalability. Using the inherent advantages of the cloud, companies can rapid- ly respond to changing business needs, capture new market opportunities, and continuously differ- entiate their offerings. It's no wonder that today nearly 9 in 10 enterprises have a cloud- first strategy,[1] and 68% of enterprises are running workloads on Amazon Web Services (AWS®).[2]

With cloud usage a given, IT leaders must focus on an effective security and governance strat- egy, not only for the cloud but across the entire IT architecture. To do so, they need to under- stand two salient facts. First, the responsibility for cloud security is shared between cloud service providers and their customers. Second, attackers are location agnostic—their focus is to gain access to an organization's IT infrastructure, wherever it is, and execute their end goal.

As an IT leader, you need to understand your organization's responsibilities for cloud security and identify the necessary controls and pro- tections available today for securing your cloud applications (also known as workloads) and data. You'll learn about all these areas and more in this e-guide, where Palo Alto Networks and AWS join forces to separate fact from fiction about cloud security as well as provide proven recommenda- tions on how to secure and govern at the speed of the cloud.

Fact or Fiction: Is the Cloud Secure?

Fact: Cloud computing infrastructure is generally more secure than most enterprise data centers. AWS has achieved dozens of national and industry security certifications and meets more than 2,600 audit requirements. Most private data centers can't or choose not to attempt this level of security vigor.

Does this make your application running in the cloud secure? The short answer is that it depends on you and whether your organization is fulfilling its cloud security responsibilities.

In the race to the cloud, many enterprises make mistakes that impact the security of their workloads and data. Just as the cloud helps accelerate and scale development and innovation, it also can scale those mistakes, omissions, and misconfigurations. Some of the common security missteps made by enterprises when moving to the cloud include:

- Missing or incorrect access controls for confidential data, leading to data leakage
- Misconfigured access rights for applications, enabling inappropriate access
- Use of unpatched, vulnerable applications and development tools, which could expose them to exploits

Through 2022, at least 95% of cloud security failures will be the customer's fault.[3]

Dispelling Cloud Security Myths

Table 1: Cloud Security Myths vs. Realities	
Myth	**Reality**
The cloud is inherently secure/unsecure.	The cloud is secure, but your workloads and data in the cloud are only as secure as you make them.
Cloud service providers are responsible for securing customer workloads and data.	You are in complete control of and responsible for securing your workloads and data in the cloud.
The cloud introduces new security risks.	If you ignore any part of your cloud security responsibilities, your workloads and data could be exposed.
The security controls and tools provided by the cloud service provider are sufficient.	You are responsible for the security of your workloads and data, which requires appropriate governance and additional layers of defense based on your organization's data classification policy.
Heavily regulated industries can't use the cloud because of compliance requirements.	Compliance requirements can be fulfilled in the cloud with the right strategy, tools, and gover-nance.
The same security tools, policies, and processes used to secure private data centers can also secure the cloud.	Not all traditional tools, policies, governance, and processes were designed for the cloud, nor can they adapt to the speed, agility, and automation requirements of cloud deployments.

Understanding Your Cloud Security Responsibilities

One of the biggest cloud security challenges enterprises face is not understanding their role in the cloud service provider's approach to security. Called the shared responsibility model and recognized across the industry, this approach shares accountability and ownership for security between the subscribing customer and the cloud service provider.

In the cloud, providers such as AWS own and secure the infrastructure, physical network, and hypervisor. The enterprise owns and secures the workload operating system (OS), applications, virtual network, access to the tenant environment/account, and data.

76% of organizations believe (incorrectly) that their cloud service providers take care of all data privacy and compliance regulations.[4]

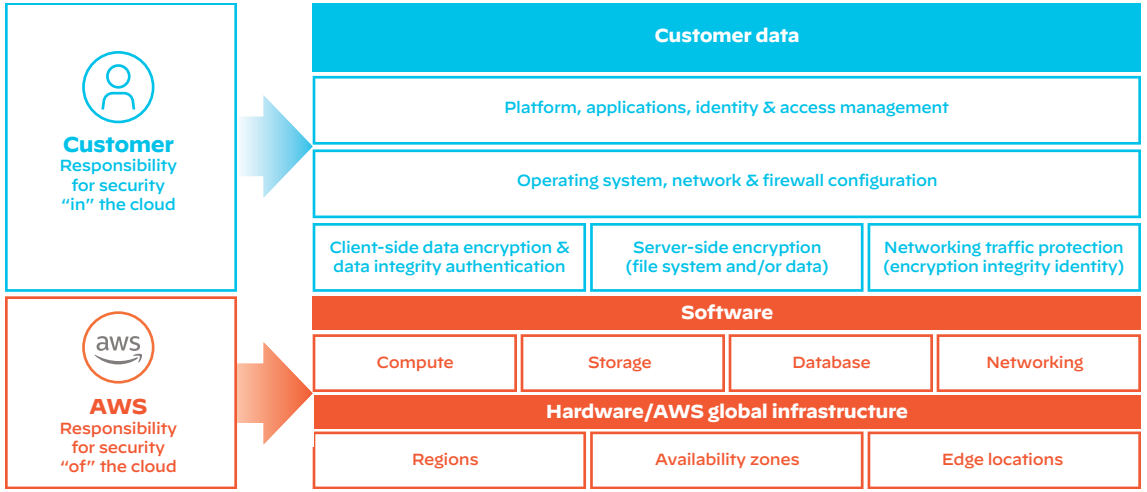

Figure 1: AWS shared responsibility model

This model makes securing your workloads and data in the cloud no different from securing them on-premises. Just like in your own data center, you are in complete control of which security measures to implement. This means that the onus is on your organization to take steps to safeguard your workloads and data, based on the nature of the content and how your organization classifies it.

To help you meet your security responsibilities, you can use third-party cloud security offerings that complement and extend AWS security services and controls to maintain the level of protection and governance that your enterprise and its compliance requirements mandate.

With the shared responsibility model in mind, let's look at some recommendations for securing your workloads and data on AWS.

83% believe (incorrectly) that their organization's cloud service provider takes care of protecting their data in the cloud.[4]

Recommendation #1: Build an Organizational Culture Around Security

For the shared responsibility model to work effectively, your organization must be prepared to take responsibility for securing everything you put in the cloud. The first step in taking responsibility is to create the right organizational culture—one that frictionlessly embeds security and governance in everything you do.

To create an effective culture around cloud security, begin by:

- Assessing your organizational needs
- Identifying teams that may need to be formed, as well as the required skill sets
- Defining individual responsibilities for cloud security within your organization and ensuring everyone knows what is required
- Conducting training and education on cloud computing and security in the cloud, including the shared responsibility model

Table 2: Responsibilities for Cloud Security by Team	
Teams	**Responsibilities**
Executive(s)	Executive sponsorship is critical to obtain the resources you need, the authority to take action, and visibility for security and governance needs across the company.
Cloud center of excellence (COE)	This team works together to apply security and governance requirements across the cloud and IT networking and infrastructure environments. The team defines and enforces appropriate policies that securely enable the business to use the cloud without becoming a bottleneck to productivity and efficiency.
Line-of-business (LOB) manager(s)	LOB leaders ensure that the organization's cloud security and governance requirements are understood and adhered to within their respective areas of the business.
DevOps teams	By having a security champion as part of the DevOps organization and/or a member of the cloud COE, these teams understand and consider any applicable security and governance policies at the beginning of a project and integrate/automate them into the application delivery workflow.
Individual end users	End users should be trained to follow corporate governance with respect to cloud security and compliance by understanding risks in the cloud and safeguarding the data with which they have been entrusted.

Don't force information security's old processes to be adopted by DevOps developers. Instead, plan to integrate continuous security assurance seamlessly into the developer's continuous integration/continuous development (CI/CD) toolchain and processes.[5]

Recommendation #2: Embrace the Shared Responsibility Model

With the right teams and culture in place, you can build policies and processes that help you correctly set up and securely use your AWS resources. These best practices can help you get started.

Take a Holistic Approach to Your AWS Account Structure

A well-defined AWS account structure lets you optimize both resource usage and security while enabling the structure to evolve as your enterprise's needs change. Start by defining and categorizing all of your assets running on AWS, including bringing any shadow IT accounts under your corporate security and governance umbrella. Use a tagging strategy that assigns metadata, such as owner, purpose, cost center, data classification, or other criteria to AWS resources to help you organize and manage them effectively. Once categorized and tagged, set up role-based access control (RBAC) policies for access to AWS accounts and resources.

Implement Infrastructure-Level Security Controls

To protect your workloads and data running in AWS, apply security best practices at the AWS infrastructure level. For example, you can use security groups to begin the process of segmenting workloads and data based on Zero Trust principles. Create appropriate access restrictions and policies to protect sensitive data against unauthorized access. Restrict outbound access for resources associated with security groups to prevent accidental data loss or exfiltration in the event of a breach. Don't forget to set up encryption for data at rest.

Gain Full Visibility into Your Cloud Environment

Monitor and report on security and compliance to detect and remediate risks across configurations, infrastructure, and users. Utilize AWS services to help you monitor and audit your AWS configuration.

Security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.[6]

Recommendation #3: Take a Cloud-Centric Approach to Availability

As part of the triad of confidentiality, integrity, and availability—a well-known model for guiding security policy—availability ensures reliable access to enterprise applications.

The concepts of high availability and resilience don't change in the cloud, but how they can be achieved does. It requires taking a cloud-centric approach: utilizing the cloud provider fabric and its inherent resilience and elasticity features, such as load balancing and auto scaling, to quickly and seamlessly accomplish the end goal of high availability. Using this approach, you'll leverage native architectures for load balancing, scaling, and availability for your workloads and data.

Equally important will be ensuring that these capabilities are correctly configured using infrastructure-level security controls to protect your workloads and data from unauthorized access.

51% of organizations were found to have at least one publicly exposed cloud storage service.[7]

Recommendation #4: Implement the Right Security Tools

To fulfill your part of the shared responsibility model, you'll need to have the right security tools in place. Most enterprises will find that they need a combination of native AWS capabilities and third-party product offerings to meet all of their security and governance requirements.

Start by understanding the options available.

Native Cloud Security

AWS offers native security services—including logging, AWS Identity and Access Management (IAM), encryption, and AWS Web Application Firewalls (WAFs)—to help you fulfill some of your responsibilities to protect your workloads and data in the cloud. For more comprehensive protection, you may need third-party tools that complement native AWS security offerings and help you manage and govern your AWS accounts.

Legacy Security Tools

Legacy security vendors claim to offer an adequate level of protection to secure your cloud environments, but these options aren't integrated with the cloud, negating the on-demand nature of the cloud and agility benefits. Plus, legacy tools typically lack the automation required to enable consistent, frictionless security across your entire environment.

Do-It-Yourself (DIY) Security

Some organizations choose a DIY approach to securing their cloud workloads and data, using scripting and visibility tools to protect deployments. Potential disadvantages to this strategy include lack of resources and expertise to develop, deploy, and manage in-house offerings, and potential lack of access to support via a community-based approach in the event of a security breach.

Third-Party Security, Natively Integrated

AWS security provides a great starting point for protecting your workloads and data; however, third-party offerings exist to provide added security over and above native capabilities. Inline security provides more granular controls and threat prevention. API-based offerings can span multiple vendors, providing a richer set of analytics and reporting. Workload-based security prevents advanced threats, improves visibility and supports segmenting of workloads, and scales automatically based on demand. Regardless of the approach taken, the goal is to protect your workloads and data on AWS and help you fulfill your shared responsibilities for security.

A Checklist for Cloud Security Tools

The tools you select for cloud security should provide:

- Granular visibility and control of the AWS environment (including accounts and regions) and workloads on AWS
- Detailed analytics on usage to mitigate the risk of data leakage and compliance violations
- Context-aware policy controls to drive enforcement and quarantine if a violation occurs
- Cloud workload protection that prevents exploits and threats in real time
- Real-time threat intelligence on known threats and detection of unknown threats to prevent new malware insertion points
- Automation of deployment workflows to make security frictionless, including support for AWS CloudFormation Templates and third-party automation tools, such as Jenkins, Ansible, and Terraform
- Integration with native AWS logging, monitoring, and security tools

Recommendation #5: Automate Security

In the fast-paced, dynamic world of the cloud and DevOps, making sure that security best practices are implemented can cause delays that induce friction, slowing deployments or, worse, weakening security if the deployment can't wait for security change control to happen.

The answer to this challenge is automation. By automating security in the cloud, organizations can eliminate security-induced friction and, at the same time, take advantage of the flexibility and agility benefits the cloud offers. Using cloud native or third-party automation tools, you can achieve touchless deployments that will create the AWS environment from scratch, complete with a fully configured set of native and third-party security controls, resulting in secure, compliant, and isolated virtual networking environments on AWS.

In addition to automating the deployment workflow and integrating with your DevOps tools, the right cloud security offering lets you automate discovery, analysis, incident response, and other repetitive security tasks to enable your security team to do more, faster, and with greater accuracy.

84% of enterprises are committed to increasing security automation efforts in the future.[8]

Next Steps

As the massive migration to the cloud continues, it's imperative for organizations to understand and embrace the shared responsibility model and deploy appropriate security tools and best practices to protect their workloads and data in the cloud.

Together, AWS and Palo Alto Networks can help your organization secure and govern your AWS workloads and data at the speed of the cloud.

Ready to experience the security power first-hand?

- Prisma™ Cloud by Palo Alto Networks provides continuous visibility, compliance monitoring, and threat defense in the cloud. Start your 30-day free trial.
- VM-Series Virtualized Next-Generation Firewalls allow allows you to integrate security in your development workflow. Start your 15-day free trial.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Notes

1. Reisinger, Don, "How Cloud Computing Impacts Corporate Security for Better or Worse," in *eWeek*, April 20, 2018.
2. "2018 State of the Cloud Report," RightScale, 2018.
3. Smarter with Gartner, "Is the Cloud Secure?" March 27, 2018, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure.
4. "2017 Truth in Cloud Report," Veritas, research conducted by Vanson Bourne, 2017.
5. "10 Things to Get Right for Successful DevSecOps," Gartner, October 2017.
6. AWS Cloud Security, accessed October 23, 2019, https://aws.amazon.com/security.
7. "Cloud Security Trends," Unit 42 Cloud Research Team, May 2018.
8. Reisinger, Don, "How Cloud Computing Impacts Corporate Security for Better or Worse," a KPMG and Oracle survey as reported in *eWeek*, April 20, 2018.

Prisma by Palo Alto Networks

Governed access, plus pervasive protection for data, applications, hosts, containers, and serverless—this is the proper foundation for the journey to the cloud. As a comprehensive cloud security suite, Prisma helps our customers secure every step of their journey.

Prisma provides unprecedented visibility into assets and risks, consistently securing access, data, applications, and modern workloads, regardless of location. The suite helps customers deploy and adapt quickly with speed and agility as well as control operational costs and reduce complexity with a radically simple architecture.

Prisma™ is the most complete cloud security suite for today and tomorrow.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com