Cloud Checkr

whitepaper

Hackproof Your Cloud:
Preventing 2017 Threats for a New Security Paradigm

When your company's infrastructure was built on the model of a traditional on-premise data center, security was pretty straightforward; you had processes and tools for securing your infrastructure, the applications, and the data it housed. Everything you did security-wise rested on the idea that resources were physical and static, with well-defined IP addresses. There was a clear "inside and outside" of the infrastructure, and you focused on protecting that by preventing attackers from getting in, and detecting them when they did.

If your company is like many, it increasingly depends on the cloud for its computing, storage and network infrastructure. But in the cloud, infrastructure scales up and down based on your needs. Resources are ephemeral as your workloads get assigned to different instances depending on what's available at the time it's needed. The idea of a perimeter that defines what you protect all but goes away. As a result, many of the tools and processes you used to secure your on-premise data center no longer do the job, or must be modified to work in the cloud.

Industry experts say that by 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

These differences provide opportunity for perhaps even better security for your workloads and data, but the structure of the cloud and the way it operates necessitate a very different approach to security.

In this paper, you'll learn:

- **The key differences between the cloud and on-premise security**
- **Why traditional security tools and processes are ineffective in the cloud, and what you must consider to manage security in the cloud**
- **Which tools provided by AWS, as well as purpose-built solutions, can help you further secure your workloads in the cloud**

Security in the Cloud is Different

According to Forbes, former U.S. federal chief information officer (CIO) Vivek Kundra said, "Cloud computing is often far more secure than traditional computing." He asserted that it was because cloud companies like Amazon can attract and retain high quality cyber security employees. While Kundra's statement is true, the cloud is also inherently more secure by virtue of how it is set up differently from the on-premise data center.

What you protect is different

With Amazon's "Shared Responsibility Model," AWS takes ownership of some data security—for example, disposal of hard drives, fire suppression systems to protect the infrastructure from damage, and security guards around the AWS infrastructure. While AWS protects what's outside the virtual private cloud (VPC), you protect what's within the VPC (more on this below). You also must monitor the AWS APIs that instruct AWS what instances to create, S3 buckets to set up, and what actions to take to control the infrastructure.

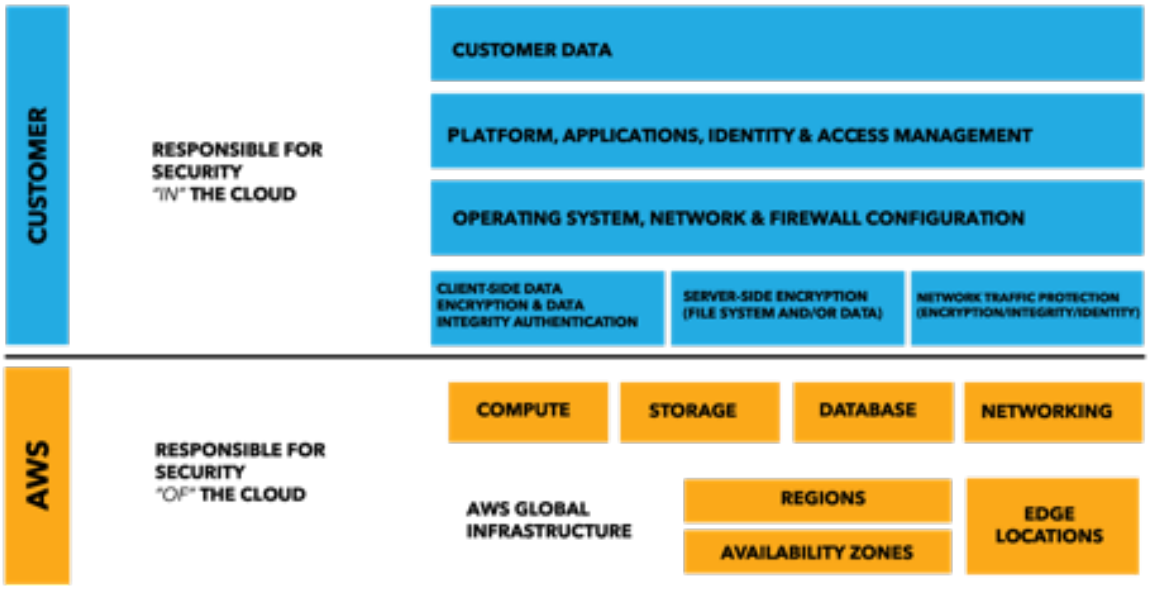

Figure 1. Shared Responsibility Model for Security

How you monitor is different

Differences in what you protect also require you to change how you approach security in the cloud. As noted earlier, in the cloud, there's no defined perimeter to lock down and scan. Further, because infrastructure is shared with other tenants, AWS won't allow you to scan your infrastructure whenever you want because of its impact on the other tenants. This forces you to make two adjustments: you need to understand where to look and you need permission to aggressively test once you do know where to look.

The tools you use are different

While many facets of protecting your data and infrastructure may be different for the cloud, the threats are the same. Advanced persistent threats (APTs) and attacks that can be prevented by patching, like SQL injection and application-level attacks, are still a consideration. However, traditional tools aren't as effective, or are totally ineffective.

In the cloud, for example, you can't do the deep packet content inspection that was formerly sufficient with network packet sniffing (although AWS does provide VPC flow logs, which will be discussed later). You can't use network devices for intrusion detection systems (IDS) or intrusion prevention systems (IPS) because they create a bottleneck for anything on the subnet or network you're trying to protect. Agent-based security is impractical because you'd need to install them on all your workloads, which are a constantly moving target as you scale up and down into the 10,000+ range. Vulnerability assessment (VA) tools damage the performance of an instance and could hurt other tenants sharing the hardware that you're using. Although AWS will allow you to perform a limited assessment, you must first go through a time-consuming approval process, which is unrealistic if you have numerous instances.

Understanding the Structure of the Cloud

To better grasp what you have to protect, it's important to understand how AWS cloud is structured and how it operates. Figure 2 shows the structure of the AWS cloud. In that structure, VPCs connect to the outside AWS world through an internet or VPN gateway. Inside the VPC, you have subnets that logically group things, like web servers or database servers. Routing tables define how to move traffic around the VPC. Access control lists serve as a basic firewall to allow or deny network packets.

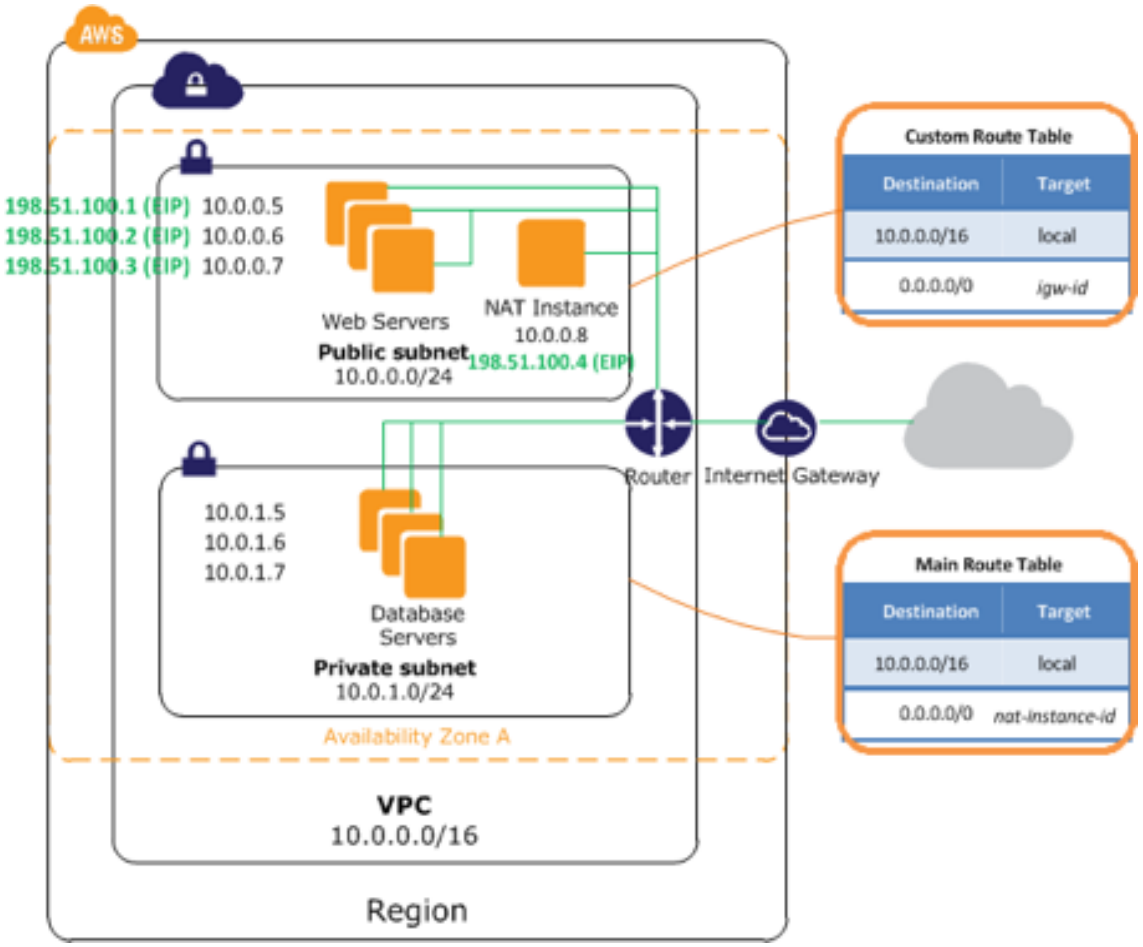

Figure 2. Structure of the AWS cloud

Securing Your VPCs

The way AWS' shared responsibility model works, AWS is responsible for everything outside of your VPC, and you're responsible for your securing your VPC—the network, inventory, configuration, data, access control. You're also responsible for securing what's in your VPC; specifically, your applications and your content.

You have two main ways to secure your VPC: your network access control lists, and the security groups you create. Network access control lists define how you allow or deny packets in or out of the VPC, and can be thought of as the uber-security level for the VPC. By using your access control lists, you have the advantage of being able to set and apply your rules to everything within a VPC or subnet. Security groups are a bit more granular. These are rules that you assign to actual server instances within a subnet of VPCs. So now you're setting security at the instance level.

Strategies and Tips for Managing the Security of Your Workloads

AWS provides many ways for you to manage the security of your workloads in the cloud, but there are also some strategies you can use to improve security—often more easily than you could with on-premise infrastructure.

"Through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers." [1]

While it's not practical to do vulnerability assessments, you can do something that accomplishes the same goal of finding and fixing vulnerabilities. You can create an image of all the settings one of your workloads is based on, scan it in a test environment to identify vulnerabilities, fix them, and update with the latest security patches. You can then make that image a template that you apply to any future workloads. Be sure to update the template to catch any vulnerabilities that may have arisen between template versions.

Network Access Control Lists

So why not just secure the instances with security groups and forget about the network access control lists? When you use security groups alone, if someone spins up a new instance without setting up the security group on it properly, you have a security hole in your network. The best advice is to use both—secure at the perimeter, or VPC level, and then fine tune as needed at the security group level.

In the on-premise datacenter, keeping up with patching was almost impossible due to resource issues. Patching in the cloud becomes much easier. Rather than patching individual servers, you simply apply the template to the server each time DevOps re-provisions a workload on that server. In fact, by writing a script, you can use automation to re-deploy hundreds of servers based on a new, patched template in just hours.

Tips for Security for Other AWS Services

VPCs are just one of over 80 services offered by AWS. AWS provides a centralized Identity and Access Management (IAM) service for VPCs, which allows you to lock down access to VPCs in just the way you need. Unlike VPCs, many of these other services have their own versions of authorization and access control that can supersede the centralized IAM in AWS. With these services, automating access and authorization settings for each can be your best bet. This will save time otherwise spent manually examining 80 services for security holes solely related to access.

[1] Kasey Panetta, "Is the Cloud Secure?", Gartner, 2017

Here are some considerations about security for a select few of those services:

Amazon Relational Database Service (RDS)

When you secure your VPCs, you've locked down your EC2 instances and your Amazon Relational Database Service (RDS) so that it can't be attacked on your SSH port or Telnet port. However, RDS has the option to be publicly accessible, which leaves many ways to be exploited. Make sure this option is not enabled. If you do need it to be public, restrict it to a specific IP address. Be aware that hackers can exploit via your database snapshots, and if your database is locked down, they'll target these snapshots. Make sure you lock down your snapshots, too.

Amazon Simple Storage Service (Amazon S3)

Amazon S3 sits physically outside of the VPC, which makes it more vulnerable. However, AWS offers the ability to put endpoints for S3 on your VPC. An endpoint is a virtual device that lets you create a private, secure connection between your VPC and another AWS service—in this case, your S3—without requiring an Internet gateway, network address translation (NAT) instance, or a virtual private gateway in your VPC.

Unfortunately, many people don't use these endpoints, which means that if someone knows your S3 storage name, they can try to connect to it from their computer. To prevent outside access, you must properly configure four levels of access control, set up multiple layers of encryption, enable support for HTTPS, and enable server access logs. If you don't use endpoints for S3 and have assets available with read/write permissions, hackers can easily access and re-upload them with a macro virus, for example.

Good to Know: User Permissions

With all services, if you create a permission for Authenticated Users, understand that this user category means anyone with an AWS account—whether they're from your company or not. Never set a bucket of permissions for Authenticated Users; if you do, anyone with a credit card and burner phone can become a serious security threat.

Amazon Simple Queue Services (SQS) and Amazon Simple Notification Service (SNS)

These services don't live in an AWS region and don't have the option for an endpoint like S3. They're simply public URLs that are obscure, but not secure. Obscurity is never a good practice for security, especially when the threat comes from inside. While it's unlikely an outsider may guess your URL, an insider has full access. With SQS or SNS, set service policies in addition to the IAM policies that specify who can access it; this also facilitates more granular access rules. Don't set SQS or SNS access to "Everyone," as that allows someone to use these service for an SQL injection or any other attack vector.

Security Actions to Take Today

1. Turn on VPC Flow Logs to start capturing network information immediately.
2. Check access control lists to apply rules within a VPC or subnet.
3. Configure security groups to ensure security at the instance level.
4. Create and apply image templates to scan for vulnerabilities within workloads.
5. Employ and automate server patch templates.
6. Enable CloudTrail logs across regions.
7. Set up security alerts to monitor for suspicious activities or events.
8. Ensure holistic perimeter assessment (VPC as well as S3, SNS, SQS, etc.) to identify all possible access points.
9. Set endpoints for S3.
10. Set SQS policies in addition to the IAM policies.
11. Enable and manage CloudWatch logs.
12. Don't underestimate the significance of culture on security—ensure alignment across IT, security, and operations.

Security Tools from AWS

In addition to the centralized IAM service, AWS provides you with several other security tools that you should use. These tools include AWS CloudTrail, Amazon CloudWatch Logs, Amazon VPC Flow Logs, AWS Inspector, and AWS Config.

AWS CloudTrail

AWS CloudTrail is a service that records AWS API calls for your account and delivers log files that include details of that call to you. Turn on AWS CloudTrail to provide activity monitoring for any actions and changes made within AWS API. In the past, you had to turn it on for each region, but now you can click a single button to enable monitoring for all regions. With this feature turned on, CloudTrail will automatically become enabled as new regions get added. This will ensure proactive alerting for any unusual activity occurring in regions that may be of concern.

Amazon CloudWatch Logs

Amazon CloudWatch Logs ensures compliance with many regulations and mandates, such as the Payment Card Industry Data Security Standard (PCI), that require a record of maintained logs for a certain amount of time. This service captures all activity across your instances, even if those instances were spun down and the logs deleted. It ships all logs from the operating system to a central repository to mitigate any regulatory compliance issues. You will need to manage the size of the repository for these logs, as eventually the repository can get quite full.

Amazon VPC Flow Logs

Amazon VPC Flow Logs help you monitor what's happening on the network—for example, if someone is trying to break in by accessing ports or IPs that you've specifically blocked. If you monitor these logs for "Deny Connections," you can see if someone is trying to attack from the outside or inside. While you can't do much more than monitor the activity happening from the outside, access attempts from the inside can notify you to proactively address and mitigate risks. VPC Flow Logs get shipped to your CloudWatch service.

AWS Inspector

AWS Inspector provides visibility to improve security across cloud environments, offering best practices and recognizing vulnerabilities. The tool ensures your security posture is proactively maintained by checking for vulnerabilities before and during deployments. Amazon Inspector is agent-based, API-driven, and delivered as a service, which allows DevOps teams to integrate it within their workflow.

AWS Config

AWS Config provides inventory, historical data, and change notifications about resources and configurations. Track and view existing or deleted resources, as well as configuration across the environment. You can automatically check that resources are configured to specified settings, and determine overall compliance posture at any point. Setting up alerts to notify you of changes can help turn this insight into action.

Comprehensive Cloud Governance & Monitoring

Beyond AWS-provided tools, third party tools are invaluable for ensuring total cloud governance. Some are recognized with specific AWS Security Competency status, with a proven track record of success in the cloud. When choosing a cloud management tool, this can be great validation for meeting security requirements and compliance standards.

CloudCheckr offers a unified cloud governance platform, providing actionable insights to manage security and compliance, while saving money and automating your cloud. The CloudCheckr platform collects and unifies AWS data, including AWS API data from CloudTrail and AWS Config, operating system logs from CloudWatch, and network traffic information from VPC Flow Logs. This enables a complete picture of resources, permissions, configurations, and exposures. CloudCheckr automates scheduled reporting and alerts for existing and potential vulnerabilities, security risks, and configuration issues across all data sources. CloudCheckr's comprehensive solution also automates tasks to clean up security groups and turn best practices into action.

As an Advanced Technology AWS Partner with Security Competency recognition, CloudCheckr provides solutions to ensure organizations in the government, finance, retail, healthcare, and other highly regulated industries meet security & compliance requirements including NIST 800-50, PCI-DSS, HIPAA and many more. With over 400 best practice checks to identify weaknesses, mitigate risks and provide actionable recommendations, CloudCheckr keeps your cloud in check.

About CloudCheckr

CloudCheckr Inc. is a Rochester, NY software company that specializes in bringing clarity to cloud deployments for enterprise cloud users. CloudCheckr Inc. leveraged its team's expertise and knowledge to develop CloudCheckr (www.cloudcheckr.com).

CloudCheckr uses read only credentials to fully inventory your cloud deployment. It then formats this information into actionable knowledge, cost, and best practice reports and checks.