Barracuda
Your journey, secured.

The five pillars of a Well Architected AWS Security Framework

WHITE PAPER

PUBLIC CLOUD SECURITY

Overview

As you migrate your compute infrastructure to the public cloud, one of the biggest challenges you face is the need to translate your on-premises security framework to a cloud-based one that provides the same or higher level of security for your network, applications, and data. Solutions designed for traditional, on-premises infrastructures may not work in the cloud, or may introduce too much latency or complexity.

To get the most benefits, you want a solution that can incorporate and integrate with the many security services offered by public cloud infrastructure providers. And finally, to operate securely in the cloud you need to adopt a new set of principles based on the new contexts that the cloud enables.

AWS has defined its Well Architected Security Framework with seven principles and five pillars. The principles behind the AWS Well Architected Security Framework are:

1. Implementing a strong identity foundation
2. Enable traceability
3. Apply security at all layers
4. Automate security best practices
5. Protect data in transit and at rest
6. Keep people away from data
7. Prepare for security events

Instituting these principles falls into five best-practice areas which form the five pillars of this framework.

The Five Pillars of a Well Architected AWS Security Framework

These key pillars are:

1. IAM – Identity Access Management
2. Detective Controls
3. Infrastructure Protection
4. Data Protection
5. IR – Incident Response

Addressing each pillar in sequence is the best way for you to achieve a well architected security infrastructure. First, ensure IAM requirements are understood and resolved before moving onto Detection Controls, etc. A piecemeal approach is more likely to result in unnoticed gaps in your security posture as a whole.

To succeed, you need to understand how each element of this framework applies to your specific situation. The purpose of this white paper is to help you understand each of the five pillars, so that you can apply them to your own situation to systematically establish a strong security posture in AWS.

IAM (Identity Access Management)

Traditionally, organizations look at IAM from the standpoint of users, with intersecting categorizations into groups and roles, associated with various levels of access permissions.

As you move to the cloud, however, you have to understand that the various services you make use of require their own IAM policies—that you need to secure them by thinking in terms of how they are accessed and managed.

Within the AWS infrastructure, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user and programmatic access to AWS services and resources. Within AWS, you should also require strong password practices, such as complexity level, avoid re-use, and enforce multi-factor authentication (MFA).

To develop a well architected IAM pillar, customers must:

- Manage credentials and authentication
- Control human access
- Control programmatic access

https://wellarchitectedlabs.com/Security/Quest_Managing_Credentials_and_Authentication/README.html?ref=wellarchitected-ws

Detective Controls

Detective Controls focus on intrusion, and are more commonly known as Intrusion Detection Systems (IDS). Automated IDS solutions are designed to monitor and analyze network traffic, and to generate an alert in response to activity that either matches known malicious patterns or is anomalous. Some IDS controls go further: they will trigger automated processes that can include recording suspicious activity or scanning the computers involved to try to find signs of compromise.

IDS controls are very valuable to resource managers and IT not just because they allow a timely response to compromises, but because they offer the capability to identify devices that are in imminent danger of compromise. To do so, IDS controls need some kind of feedback loop, with a security provider, to learn to spot the latest malicious activities and recognize them when detected.

Within the AWS infrastructure, there are a number of detective controls which run the gamut from processing logs to monitoring, automated analysis, and alarms.

To monitor metrics with alarming:

- CloudTrail logs
- AWS API Calls
- CloudWatch

Configuration history

- AWS Config

Managed detection threat service with continuous monitoring

- Amazon GuardDuty

Service-level logs, i.e. logging access requests

- Amazon Simple Storage Service (Amazon S3)

To develop a well architected Detective Controls pillar, customers must:

- Understand how they will detect and investigate security events
- Defend against emerging security threats

https://wa.aws.amazon.com/wat.question.SEC_4.en.html

https://wa.aws.amazon.com/wat.question.SEC_5.en.html

Infrastructure Protection (NetSec)

Many organizations make the mistake of beginning their security framework discussions around Infrastructure Protection (aka NetSec), as this was traditionally how they secured on-premises infrastructure. In the cloud, firewalls and WAFs that provide security to cloud-based users are different than on-premises devices that secure users—very few companies have a strategy that leverages the same code and controls for both. NetSec can also describe benchmark policies such as CIS Benchmark for AWS and leveraging AWS policies to detect any information security policy violation.

In AWS, you can implement both stateful and stateless packet inspection at a very basic protection level—by deploying either AWS-native technologies or a number of third-party partner products and services that you can acquire through the AWS Marketplace.

The Amazon Virtual Private Cloud (Amazon VPC) provides a private, secured, and scalable environment designed to allow you to define your own specific topology. With the VPS environment, it's easy to define and protect gateways, routing tables, and both public and private subnets. You can deploy persistent defenses by hardening configurations you develop in either Amazon EC2, ECS, or Elastic Beanstalk instances with containers and then applying these configurations to an Amazon Machine Image AMI. Then, all new instances launched via this AMI will receive the same hardened configuration.

To develop a well architected infrastructure protection pillar:

- Understand how you will protect your networks
- Understand how you will protect your compute resources

https://wa.aws.amazon.com/wat.question.SEC_6.en.html

https://wa.aws.amazon.com/wat.question.SEC_7.en.html

Data Protection

Data protection for the network is often equated to backup, but the two functions are actually somewhat different. Data backup is a snapshot in time of selected, any, or all data in a cloud infrastructure. This is data at rest, and as such, it is only accurate to the point of the backup. When backups are deployed to rectify a compromise, i.e., a data restore, significant time may have elapsed between the date of the most recent backup and the date a restoration is initiated.

Recent legislation such as GDPR has caused security professionals to look beyond protection of data at rest and address the much more difficult task of protecting data in motion, also called data in transit. Data in motion is very often data moving out of the network, or between nodes, making it vulnerable to malicious activity as a part of transport.

Encryption is the most popular method of protecting data both at rest and in transit, but it is not a total solution. Network security controls add another layer of protection, as do data policies. You can apply specific policies to data classified as at-risk whenever it is accessed or moved, ranging from alerts to full blocks against access or transit. Going further, data classification can be leveraged as a way to organize data based on self-described levels of sensitivity, and ultimately automating encryption tools and access.

To develop a well architected Data Protection pillar:

- Have complete visibility of information and data stored in AWS
- Establish and maintain version control of data
- Protect data at all times
- Encrypt data at all times

There are multiple means to encrypt data at rest and in transit in AWS. There is service-side encryption, as well as HTTPS encryption or SSL termination that can be handled by Elastic Load Balancing (ELB).

When developing your data protection pillar, you need to consider the following:

- How you will classify data and automate security such as encryption
- How you will protect data at rest, as well as data in transit

https://wa.aws.amazon.com/wat.question.SEC_8.en.html

https://wa.aws.amazon.com/wat.question.SEC_9.en.html

https://wa.aws.amazon.com/wat.question.SEC_10.en.html

IR (Incident Response)

Incident Response includes the ability to quickly identify, find, eliminate, and prevent future occurrences of malicious traffic. Companies with poorly architected IR infrastructures can go months before identifying potentially devastating data breaches caused by email or other malicious traffic.

But within a well architected cloud framework, IR is more focused on spotting and responding to security gaps and non-compliant policy configurations. As cloud deployments grow more complex and more dependent on multiple service configurations, these are the sorts of incidents expected to result in the majority of breaches.

IR capabilities can take many forms, from simple identification and rectification, or prevention, to changes in policies and strategies that avoid future similar incidents. If you leverage a well architected cloud framework as a basis to enforce security and workflow best practices, you can use IR to identify where best practices aren't being followed and why. In that way, IR becomes part of a continuous feedback loop to help keep a well architected cloud framework secure.

Within the AWS infrastructure, several practices can help facilitate effective incident response:

- Detailed logging including file access and changes
- Automated processing of events through AWS APIs
- Leveraging AWS CloudFormation to create a "clean room" in which you can carry out forensics in an isolated environment
- Leveraging AWS Lambda to create rules that will trigger automated responses
- Using AWS Detective, a new service, to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities

To develop a well architected IR pillar, customers must understand first how they will respond to an incident, including access to their InfoSec team and a means to automatically isolate instances.

https://wa.aws.amazon.com/wat.question.SEC_11.en.html

Conclusions and Next Steps

IT organizations are typically staffed to keep their respective companies or users secure and productive and to operate within a defined company framework. Even if your team includes extensive security understanding and cloud experience, you are best served by engaging with security-architecture partners.

Once your organization has completed the exercise of defining how you execute on the five pillars of well architected security, develop a strategy to close any gaps you identify during this process. Then you can work with a specialized partner to implement the tools and processes you've identified as keys to your well architected AWS security framework. These partners can also ensure that hybrid frameworks don't hamper your ability to migrate to and fully leverage the cloud, but instead remain integral parts of your overall security framework.

Your organization is then able to focus on the real value you intend to extract from the cloud: digital and operational transformation. Organizations who understand their IAM framework, for example, can feel secure leveraging AWS services such as Amazon ML (machine learning) or artificial intelligence such as Amazon Comprehend, Amazon Personalize, and Amazon Textract to build new and transformational workloads without compromising their own security frameworks.

What are your next steps in this process? Besides identifying a partner or partners to shoulder part of the burden and ensure you aren't bogged down by developing this well architected framework, you should:

1. Identify the key processes within each of these pillars that affect your business operations
2. Identify information that you must initially gather to create these pillars (as example, the roles and permissions they need to extend across users and groups, or the definition of "at-risk" data, etc.)
3. Identify "holes" in your existing security strategy and assess the criticality of each issue as well as which pillars it affects
4. Identify both third-party and native AWS services that you can leverage to address security challenges
5. Build out a timeline to deploy services, procedures, and policies and execute building your well architected security framework.

About Barracuda Networks

For AWS frameworks, Barracuda provides a suite of solutions that address common challenges that organizations encounter when building a Well Architected AWS Security Framework:

CloudGen Firewall – the industry's first built-for-the-cloud network firewall, which combines SDWAN capabilities, virtually unlimited remote access, and all the security and management parameters with which IT organizations are familiar from their on-premises architectures—but built to provide security and visibility to and through AWS.

CloudGen WAF – a highly scalable web application firewall to provide Layer-7 security for web-facing applications, along with automated remediation and highly granular rule-sets that you can tailor by user and application.

Cloud Security Guardian – a service that operates at the data plane level, and can configure and manage security controls and practices across an organization's entire cloud architecture, including centralized management of CloudGen Firewalls and WAFs, as well as other cloud infrastructures.

Barracuda Networks is the only security provider with two AWS Security Competencies—tested and proven to enhance your AWS security. Barracuda leverages built-in AWS cloud features, is certified on GovCloud (part of AWS' ATO initiative), and offers licensing to match your cloud deployment. More information on Barracuda's AWS security solutions is available on the Barracuda website at www.barracuda.com/AWS.

Barracuda
Your journey, secured.