ARMOR™

BETWEEN YOU AND THE THREAT

Completing your AWS Cloud

SECURING YOUR AMAZON WEB SERVICES ENVIRONMENT

Introduction

Amazon Web Services (AWS) provides Infrastructure as a Service (IaaS) cloud offerings for organizations. Using AWS, your organization can stand up and launch a new website or application quickly, and then scale its resources up or down on demand as processing, storage, or other needs change. This flexibility makes AWS incredibly valuable.

Before using AWS, it's important to understand that as an IaaS provider, AWS is only responsible by default for the security of its cloud infrastructure. AWS goes through great efforts to make customers aware of their responsibilities through the AWS Shared Responsibility Model. The webpages explaining the basics of AWS services frequently reference the model to offer complete transparency into which responsibilities are always taken care of by AWS and which are to be handled by the customer.

The AWS Shared Responsibility Model makes it clear that AWS customers are responsible for selecting and acquiring all the security controls for their operating systems, applications, and data residing on top of the AWS infrastructure, as well as all of their network use. These controls are usually provided by a combination of AWS, third parties, and your organization. Failure to fulfill all the responsibilities specified in the model means that your AWS-hosted applications and data will be more susceptible to data breaches and other compromises, with potentially disastrous results.

This white paper is intended to help you make better-informed decisions about the security control options for AWS usage so you can choose the best combination of controls for your organization's situation and needs.

Cloud Infrastructure Security

AWS is responsible for keeping its infrastructure secure. This includes the following:

- **Physical security.** This involves restricting who enters the cloud hosting facilities and what they can access, as well as monitoring the facilities through cameras, sensors, and other means.
- **Basic filtering of inbound network traffic.** AWS blocks certain types of unwanted network traffic from entering its servers. This is mainly accomplished using distributed denial of service (DDoS) mitigation systems to prevent large-scale attacks from disrupting customer availability.
- **Hypervisor security.** AWS manages the hypervisors that provide the foundation for the customer operating system instances, applications, and data. Responsibilities include securing the hypervisors to prevent external attackers from breaching them and customers from breaching each other, and monitoring the hypervisors to ensure they remain secure and any issues are dealt with quickly.

Security Control Selection

It's important to take the time to choose whose security controls you should use for protecting your organization's operating systems, applications, and data hosted on the AWS cloud infrastructure. For every control, there are options. AWS offers some security control technologies above the infrastructure layer, controls may be acquired from third parties, and your organization may have existing controls or want to acquire new ones to meet AWS needs.

It may be tempting to handle all the security technologies yourself or to have AWS or a third party provide all those technologies on your behalf. However, in most cases those aren't the best approaches. Let's look at the issues with a single provider model:

- AWS can't be the sole provider of security for its IaaS customers because it doesn't offer the full range of security controls needed to safeguard their operating systems, applications, and data. Also, in many cases organizations aren't allowed to give another organization complete access to all of its sensitive information hosted in the cloud, including authentication credentials and cryptographic keys.
- One or more third parties can provide the complete range of security technologies to protect your organization's AWS usage, but as stated above, it's unlikely that your organization would be allowed to do so because of compliance requirements, regulations, etc.
- Your own organization can deploy and manage all the necessary security technologies. However, some non-cloud security technologies won't work in cloud environments, and putting cloud versions of these technologies in place can be quite expensive, not to mention the need to manage and monitor the technologies on a 24x7 basis. Add to this the need for your security architects and administrators to have a strong understanding of cloud technologies and AWS security, and this option may not be practical.

In most cases, you will find it's best to employ a combination of security technologies offered by AWS, your organization's own technologies, and third-party services. This allows you to pick the individual security technologies and services that are optimal for your needs and environment. The exact combination of security controls may be unique due to laws, regulations, organizational policies, and other relevant requirements and recommendations. The next sections of this paper cover the most important categories of security controls, show you how you can take advantage of these controls to use AWS securely, and make recommendations for which source you should use for each type of control.

Restricting access

Your organization needs to restrict access to its operating systems, applications, and data hosted by AWS. Even if applications and data are intended to be used by anyone, access still needs to be restricted to support availability, prevent application file and data tampering, and avoid other forms of compromise that could seriously harm your organization.

Network firewalling. Network firewalling should permit each operating system (OS) instance to be contacted only by the appropriate hosts on only the appropriate network ports. AWS offers Amazon Virtual Private Cloud (VPC), which provides some firewalling capabilities by isolating a group of OS instances from external hosts.

In many cases, however, you may want more granular control, including separating your OS instances from each other to prevent a compromise in one instance from rapidly spreading to others. You can best achieve this by deploying host-based firewalls within each OS instance and configuring each firewall to allow only the necessary network traffic into and out of the associated OS instance.

User authentication and access control. At a minimum, user authentication and access control should include single-factor authentication for users and multifactor authentication for administrators, and fine-grained access control for user access to applications and data. AWS offers a service called Identity and Access Management (IAM). IAM can provide all of these capabilities, and it can also link to your organization's existing enterprise authentication services. Many third-party authentication and access control services are also available. Which option—AWS, third party, or your own services—is best for any given situation is heavily dependent on your applications' usage and security needs.

Encryption services. Encryption services should include both storage encryption and cryptographic key management. Storage encryption technologies, including file encryption and database field encryption, are available from AWS and third parties, and capabilities are built into many OSes and database management systems. AWS and third parties also offer key management services, which handle everything from key creation and rotation to secure key storage and key usage auditing. Many organizations choose to handle their own key management, or at minimum key storage, so that they can keep their keys separate from the data they encrypt, a generally recommended practice.

Identifying and correcting security weaknesses

Your organization must regularly identify and correct security weaknesses within its OS instances and applications. Without robust capabilities for this, data breaches and other serious compromises are far more likely to occur. Important technologies and processes include the following:

- **Patch management.** OS and application software need to be checked frequently to see if any security patches are missing, then ensure that the missing patches are acquired and installed quickly.
- **Software version management.** Each OS instance and application needs to be checked periodically to see if it's outdated. For example, a software version may no longer be maintained by its vendor, meaning there are no patches to correct vulnerabilities. Another example is software that has been replaced with a new version offering superior security features.
- **Security configuration management.** OS instances and applications need to be checked often, ideally on a continuous basis, to verify they are using the right security configuration settings. Any incorrect settings must be fixed as quickly as possible.
- **Vulnerability assessment.** Vulnerability assessment is a periodic verification that known vulnerabilities have been addressed. Vulnerability assessment can be performed by several means, including internal or external vulnerability scans and penetration testing.

Your organization is likely to already have robust capabilities in all of these areas, either directly performed by your staff or managed by a third party, and if so, there's no compelling reason to look for alternatives. Use your existing technologies and processes to identify and correct security weaknesses.

On the other hand, if your organization is missing some of these capabilities, you will benefit from acquiring services from a third party or from AWS. AWS offers Amazon Inspector, a paid agent-based service that can identify missing patches, outdated software, and security configuration errors.

The major drawbacks of Amazon Inspector are that it can't be used to correct problems and its ruleset can't be customized to use your organization's policies or other requirements when identifying deviations from what's acceptable. Third-party services offer more robust and customizable capabilities that merit serious investigation for filling any gaps in your organization's existing security technologies.

ARMOR™

Monitoring security events and responding

Your organization must ensure around-the-clock monitoring of security events and responses to significant events such as blocking attacks or identifying successful compromises. One aspect of this is preventing and detecting compromises within your OS instances. The necessary security controls depend on the OS (Windows, Unix, etc.), but examples include antimalware software and file integrity monitoring utilities. AWS does not offer these because they reside within the customer's OS instances, so these need to be handled by your organization or a third party on your organization's behalf.

Another aspect of monitoring and response is preventing and detecting compromises carried within application network traffic. The primary security control for this is a web application firewall (WAF). AWS offers a WAF service for a fee that you can fine tune to understand your applications' characteristics. However, this service requires use of the Amazon CloudFront content delivery service, and it can only check unencrypted network traffic. Many organizations instead choose to deploy software-based WAFs within their OS instances, which enables the WAFs to see the contents of network traffic after it's been decrypted but before it reaches the application software.

Finally, it's critical to have around-the-clock security monitoring so that any security problems can be rapidly resolved and so that your organization can meet its auditing and compliance requirements. In terms of technologies, AWS offers CloudWatch to do logging and automatically generate alerts, but this is insufficient for most organizations that need a single enterprise-wide view of security, plus humans are still needed at all times to respond to alerts. It's much more common for organizations to monitor their AWS usage either with their existing security information and event monitoring (SIEM) solution and operations staff, or with a third-party monitoring service.

The Big Picture

As you've seen from the observations on protecting AWS usage by restricting access, identifying and correcting security weaknesses, and monitoring security events and responding to significant events, there are many separate components involved in AWS security. Each component is important and necessary, and any failure to Now consider the needs to have all of these components work together, to have staff members with a strong understanding of AWS security, and to adjust all of these components over time as changes occur to AWS architecture and security, any of the components, or your organization's requirements, such as a new compliance or regulatory effort being imposed.

Many organizations find it incredibly helpful to rely on a third party with strong AWS security knowledge and expertise to help facilitate their secure adoption and usage of AWS. Such a third party not only helps you select the right mix of security components and component providers, but that third party also helps you integrate all those disparate components into a single robust security solution, as well as maintaining that level of security as changes inevitably occur. Engaging a third party to help with your AWS security may provide a much stronger solution that prevents breaches and ultimately saves your organization's time, resources, and reputation.

Making Your Job Easier: Industry Benchmarks and Checklists

Whether your organization is going to implement and manage all its own AWS security controls or have AWS and third parties handle almost all of them on its behalf—or any arrangement between those two extremes—you will benefit from using industry benchmarks and checklists for AWS security. These documents, which explain how customers' security controls should be implemented, configured, managed, and maintained in AWS environments, can be incredibly helpful not only for the people with those responsibilities, but also for auditors and others who are responsible for making sure that AWS and third parties supporting your organization's AWS security are meeting the organization's security requirements.

One checklist you should definitely utilize is AWS's auditing checklist named "Introduction to Auditing the Use of AWS." This provides a comprehensive, high-level overview of several categories of security controls, including network and system security, logical access control and encryption, security logging, incident response, and disaster recovery. For each category, the AWS checklist lists specific tasks to be performed or considered, but omits any details on how to do those tasks because they are necessarily organization-specific. You can best use this to plan security controls and to audit those security controls on a regular basis to ensure they are performing as needed.

Another valuable resource for you is the AWS Foundations Benchmark from the Center for Internet Security (CIS). This benchmark is a strong complement to the AWS auditing checklist because it provides low-level, detailed recommendations and implementation and auditing guidance on the configuration settings that are most likely to be needed by AWS customers. Areas covered by the CIS benchmark include password policies, logging and alarming, and basic firewalling rules.

You should strongly consider using the AWS checklist to plan your organization's security controls, the CIS benchmark to help implement those controls, and both documents to audit those controls regularly. Many other sources of guidance are also available. One word of caution—because security threats and vulnerabilities change over time, as does the AWS environment, make sure to get the latest version of any AWS security checklist or benchmark before following it.