Foundational Security Principles and Best Practices

The services described best practices outlined in the design principles of the AWS Well-Architected Framework Security Pillar to secure the edge devices and applications themselves. Together, implementation of these services provides a strong defense in depth strategy to secure edge devices and applications.

Topics:

Foundational Security Principles

- **Implement a strong identity foundation** — Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with AWS resources. Centralize identity management and aim to eliminate reliance on long-term static credentials. AWS Identity and Access Management (AWS IAM) and Amazon Cognito help configure secure access to edge applications.
- AWS IAM provides a seamless process for multi-layer security and identity and access management, either using pre-configured policies or customized policies. IAM Roles and Permissions can be used to limit who can make changes to your network environment, such as CloudFront, AWS WAF, and Route 53. Amazon Cognito enables the addition of user sign up/sign in supporting multi-factor authentication and data encryption. Roles can be defined and users mapped to give applications access to the exact resources authorized for each user. AWS edge services can be configured to verify that only traffic from CloudFront reaches your infrastructure.
- **Enable traceability** — Monitor, alert, and audit actions and changes to an environment in real time. Integrate log and metric collection with systems to automatically investigate and take action. Available and integrated services such as AWS IoT Device Defender continuously audit edge Internet of Things (IoT) configurations to verify security best practices, while CloudTrail logs and monitors account activity across your AWS infrastructure.

Amazon GuardDuty monitors for malicious activity and unauthorized behavior to provide threat detection. AWS Config enables you to assess, audit, and evaluate the configurations of your AWS resources.

AWS WAF has full logging of all web requests it inspects. With this feature, logs are stored in S3. You can integrate the logs with SIEM and log analysis tools.

With Amazon CloudFront, you can log the requests that come to your CloudFront distributions or log the CloudFront service activity into your AWS account. Use Amazon EventBridge to centralize events into a location for processing, providing more traceability.

- **Apply security at all layers** — Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code). At the edge, secure content delivery, application and network protection, and DDoS mitigation strategies cover Layers 3, 4, and 7 for a comprehensive approach.
- **Automate security best practices** — Automation is one of the key securities benefits of the cloud, and those benefits extend out to the edge. Automated software-based security mechanisms improve the ability to securely scale more rapidly and cost-effectively.

  Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates. AWS WAF, for example, can be completely administered through APIs that make security automation easier, enabling rapid rule propagation and fast incident response.

  The AWS WAF Security Automations solution uses AWS CloudFormation to automatically deploy a set of AWS WAF rules designed to filter common web-based attacks. Users can select from preconfigured protective features that define the rules included in an AWS WAF web access control list (web ACL). After the solution deploys, AWS WAF begins inspecting web requests to the user's existing Amazon CloudFront distributions or Application Load Balancers and blocks them when applicable.

  AWS Firewall Manager also has automation features, such as automatically enforcing mandatory security policies that you define across existing and newly created resources, and automatically protecting against various types of DDoS attacks such as UDP reflection attacks, SYN flood, DNS query flood, and HTTP flood attacks across accounts.

  Firewall Manager enables you to generate policies that ensure any new resources created by developers automatically have the correct Security Group, AWS Shield, or AWS WAF policies. Firewall Manager can integrate with AWS Security Hub, allowing for a centralized view of the policies that apply to your AWS environment.

- **Keep people away from data** — Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling or modification and human error when handling sensitive data. Machine learning (ML) tools and services, such as Amazon Macie, automate discovery of sensitive data, providing constant visibility into the security of your data and lowering the cost of protecting data.
- **Prepare for security events** — Prepare for an incident by having incident management and investigation policy, and processes that align to organizational requirements. Run incident response simulations and use tools with automation to increase speed for detection, investigation, and recovery.
- Amazon Detective automatically collects log data from your AWS resources, including AWS CloudTrail and Amazon GuardDuty, and uses ML, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.
- AWS Shield Advanced enables proactive engagement from the Security Response Team (SRT) when a DDoS event is detected. With proactive engagement, the SRT will directly contact you if an Amazon Route 53 health check associated with your protected resource becomes unhealthy during an event that is detected by Shield Advanced. Use Security Hub to collect security data from across AWS accounts, services, and supported third-party products, analyze security trends, and identify the highest priority security issues.
- **Protect data in transit and at-rest** — Classify data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control, where appropriate. AWS encryption solutions such as AWS Key Management Services (KMS) help keep data at the edge encrypted at rest and in motion. AWS KMS enables you to easily create and manage cryptographic keys and control their use in applications across services. AWS Certificate Manager provisions, manages, and deploys SSL/TLS certificates at the edge for use with AWS services and internal resources. AWS CloudHSM is useful for managing encryption keys.

Compliance and the Shared Responsibility Model

The Shared Responsibility Model (SRM) is an important concept applied to the relationship and security responsibilities between AWS and its customers. AWS provides and protects the foundational hardware, infrastructure, and software aspects of the cloud – including the edge – that customers build their applications on. However, it is the customer's responsibility to choose how they architect their applications on AWS, and how they choose to expose those applications to the internet. Security at the edge focuses on a defense in depth strategy.

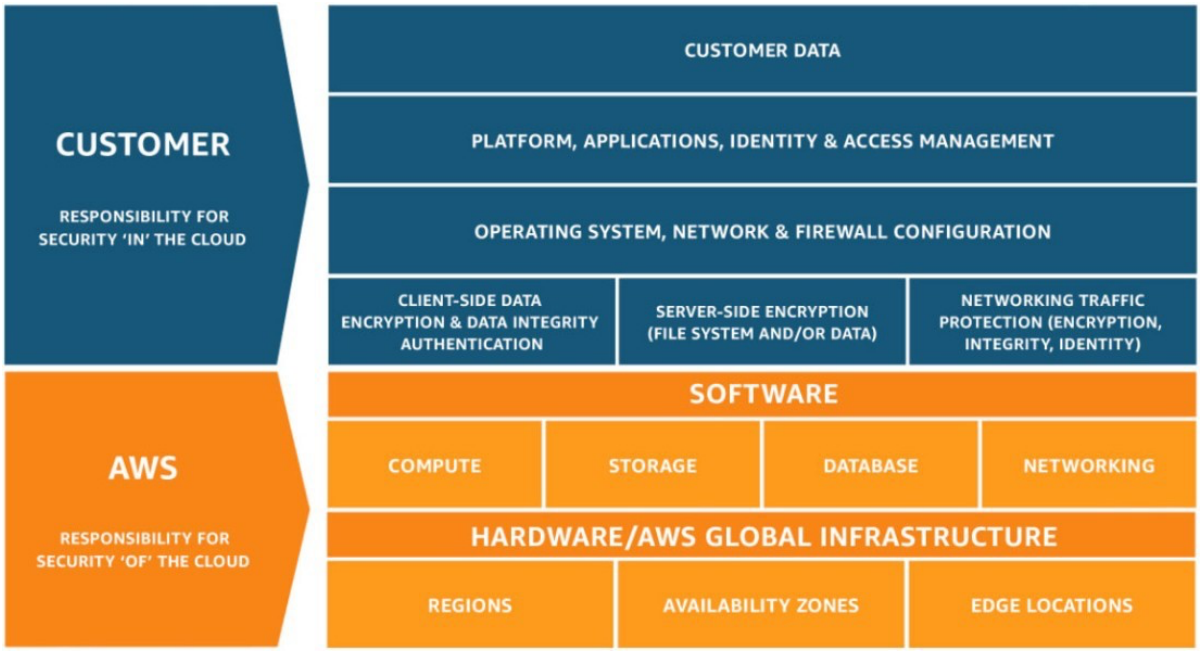

Figure 1: AWS Shared Security Responsibility Model

Customers always control their data, including encryption, storage, movement, and retention. AWS services can help customers guard identity and access, protect data, secure applications, and meet their compliance objectives.

Similar to its high bar for security, AWS has high standards for compliance that extend to the edge. AWS regularly achieves third-party validation for thousands of global compliance requirements that are continually monitored to help customers meet standards for finance, retail, healthcare, government, and beyond.

AWS customers also receive access to tools they can use to reduce the cost and time to run their own specific security assurance requirements. For example, some of the AWS key edge services, such as CloudFront, have many security standards and certifications, including PCI DSS Level 1, HIPAA, FedRamp, ISO 9001, 27001, 27017, 2701.

Credit to: AWS Documentation