Introduction to Security on AWS

This whitepaper outlines AWS security, covering infrastructure security, data encryption, identity and access control, and compliance. It highlights AWS security products, monitoring tools, DDoS mitigation.

Security of the AWS Infrastructure

The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. AWS ensures that these controls are replicated in every new data center or service.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of our most security-sensitive customers. This means that you get a resilient

infrastructure, designed for high security, without the capital outlay and operational overhead of a traditional data center.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure, and you are responsible for securing workloads, you deploy in AWS (Figure 1). This gives you the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data or deploy less stringent controls for information you want to make public.

Security Products and Features

AWS and its partners offer a wide range of tools and features to help you to meet your security objectives. These tools mirror the familiar controls you deploy within your on-premises environments. AWS provides security-specific tools and features across network security, configuration management, access control and data security. In addition, AWS provides monitoring and logging tools that provide full visibility into what is happening in your environment.

Infrastructure Security

AWS provides several security capabilities and services to increase privacy and control network access. These include:

- Network firewalls built into Amazon VPC let you create private networks and control access to your instances or applications. Customers can control encryption in transit with TLS across AWS services.
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment.
- DDoS mitigation technologies that apply at layer 3 or 4 as well as layer 7. These can be applied as part of application and content delivery strategies.
- Automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities.

Inventory and Configuration Management

AWS offers a range of tools to allow you to move fast, while still enabling you to ensure that your cloud resources comply with organizational standards and best practices. These include:

- Deployment tools to manage the creation and decommissioning of AWS resources according to organization standards.
- Inventory and configuration management tools to identify AWS resources and then track and manage changes to those resources over time.
- Template definition and management tools to create standard, preconfigured, hardened virtual machines for EC2 instances.

Data Encryption

AWS offers you the ability to add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. These include:

- Data at rest encryption capabilities available in most AWS services, such as Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker
- Flexible key management options, including AWS Key Management Service, that allow you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your own keys
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to help satisfy your compliance requirements
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS

In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

Identity and Access Control

AWS offers you capabilities to define, enforce, and manage user access policies across AWS services. These include:

- AWS Identity and Access Management (IAM) let's you define individual users with permissions across AWS resources AWS Multi-Factor Authentication for privileged accounts, including options for software- and hardware-based authenticators. IAM can be used to grant your employees and applications federated access to the AWS Management Console and AWS service APIs, using your existing identity systems, such as Microsoft Active Directory or other partner offering.
- AWS Directory Service allows you to integrate and federate with corporate directories to reduce administrative overhead and improve end-user experience.
- AWS IAM Identity Center (successor to AWS Single Sign-On) allows you to centrally manage workforce access to multiple AWS accounts and applications.

AWS provides native identity and access management integration across many of its services, plus API integration with any of your own applications or services.

Monitoring and Logging

AWS provides tools and features that enable you to see what's happening in your AWS environment. These include:

- With AWS CloudTrail, you can monitor your AWS deployments in the cloud by getting a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred.
- Amazon CloudWatch provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes. You no longer need to set up, manage, and scale your own monitoring systems and infrastructure.
- Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Amazon GuardDuty exposes notifications via Amazon CloudWatch so you can trigger an automated response or notify a human.

These tools and features give you the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment.

Security Products in AWS Marketplace

Moving production workloads to AWS can enable organizations to improve agility, scalability, innovation, and cost savings — while maintaining a secure environment. AWS Marketplace offers security industry-leading products that are equivalent, are identical to, or integrate with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments

Security Guidance

AWS provides customers with guidance and expertise through online tools, resources, support, and professional services provided by AWS and its partners.

- **AWS Trusted Advisor** is an online tool that acts like a customized cloud expert, helping you to configure your resources to follow best practices. Trusted Advisor inspects your AWS environment to help close security gaps, and finds opportunities to save money, improve system performance, and increase reliability.
- **AWS Account Teams** provide a first point of contact, guiding you through your deployment and implementation, and pointing you toward the right resources to resolve security issues you may encounter.
- **AWS Enterprise Support** provides 15-minute response time and is available 24×7 by phone, chat, or email; along with a dedicated Technical Account Manager. This concierge service ensures that customers' issues are addressed as swiftly as possible.
- **AWS Partner Network** offers hundreds of industry-leading products that are equivalent, are identical to, or integrate with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, as well as hundreds of certified AWS Consulting Partners worldwide to help with your security and compliance needs.
- **AWS Professional Services** houses a Security, Risk and Compliance specialty practice to help you develop confidence and technical capability when migrating your most sensitive

workloads to the AWS Cloud. AWS Professional Services helps customers develop security policies and practices based on well-proven designs and helps ensure that customers' security design meets internal and external compliance requirements.

- **AWS Marketplace** is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. AWS Marketplace Security products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on- premises environments.
- **AWS Security Bulletins** provides security bulletins around current vulnerabilities and threats and enables customers to work with AWS security experts to address concerns like reporting abuse, vulnerabilities, and penetration testing. We also have online resources for vulnerability reporting.
- **AWS Security Documentation** shows how to configure AWS services to meet your security and compliance objectives. AWS customers benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations.
- **AWS Well-Architected Framework** helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. The AWS Well-Architected Framework includes a security pillar that focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. Customers can use the AWS Well-Architected Tool from the AWS Management Console or engage the services of one of the APN partners to assist them.
- **AWS Well-Architected Tool** helps you review the state of your workloads and compares them to the latest AWS architectural best practices. This free tool is available in the AWS Management Console, and after answering a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization. The AWS Well-Architected Tool then provides a plan on how to architect for the cloud using established best practices.

Compliance

AWS Compliance empowers customers to understand the robust controls in place at AWS to maintain security and data protection in the AWS Cloud. When systems are built in the AWS Cloud, AWS and customers share compliance responsibilities. AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1.i. Additionally, AWS also has assurance programs that provide templates and control mappings to help customers establish the compliance of their environments running on AWS, for a full list of programs, see AWS Compliance Programs.

We can confirm that all AWS services can be used in compliance with the GDPR. This means that, in addition to benefiting from all the measures that AWS already takes to maintain services security, customers can deploy AWS services as part of their compliance plans. AWS offers a Data Processing Addendum (DPA) in the AWS Service Terms that applies automatically, whenever AWS customers use AWS services to process personal data uploaded to their AWS account. The GDPR-compliant terms of the AWS DPA are considered a high watermark for privacy compliance worldwide and we are confident they exceed requirements of most other data protection laws. This means customers will achieve at least an equivalent – if not higher - compliance standard to that required by most data protection laws.

By operating in an accredited environment, customers reduce the scope and cost of audits they need to perform. AWS continuously undergoes assessments of its underlying infrastructure—including the physical and environmental security of its hardware and data centers—so customers can take advantage of those certifications and simply inherit those controls.

In a traditional data center, common compliance activities are often manual, periodic activities. These activities include verifying asset configurations and reporting on administrative activities. Moreover, the resulting reports are out of date before they are even published. Operating in an AWS environment allows customers to take advantage of embedded, automated tools like AWS Security Hub, AWS Config and AWS CloudTrail for validating compliance. These tools reduce the effort needed to perform audits, since these tasks become routine, ongoing, and automated.

By spending less time on manual activities, you can help evolve the role of compliance in your company from one of a necessary administrative burden, to one that manages your risk and improves your security posture.

Security at the Edge

AWS provides services and features you can use to help you create secure architectures, workloads, and services to elevate your security from edge to cloud. Security at AWS starts with core infrastructure, which is built for the cloud and designed to meet the most stringent security requirements in the world. For example, all data flowing across the AWS global network that interconnects data centers and Regions is automatically encrypted at the physical layer before it leaves AWS secured facilities.

At the edge, AWS offers services that address the different aspects of edge security, including preventive security mechanisms like encryption and access control, continuous monitoring mechanisms like configuration auditing, and physical security like tamper-evident enclosures. Customers that need to store and process data on premises, or in countries where there are no AWS Region, can do so securely with AWS edge services. This capability can help you comply with data handling or data residency requirements.

AWS Cloud security principles are fundamental and apply regardless of where an organization operates. These principles are discussed here. AWS offerings combine a high security bar with agility to adapt rapidly as needed. AWS customers working at the edge have access to over 200 fully featured, integrated cloud and device services, many of which have specific edge capabilities.

AWS services with Points of Presence (PoP) at edge locations — globally scaled and connected through the AWS network backbone — provide a more secure, performant, and available experience. AWS also offers services that run on the edge, which enable you to deliver content. AWS edge services, which provide infrastructure and software that deliver data processing, analysis, and storage at endpoints comprise a comprehensive set of cloud services that support the secure deployment and management of edge devices.

Security at the edge has the same principles as cloud security. By extending cloud services to the edge, AWS gives you a way to operate safely, with strong security infrastructure and safeguards. AWS-owned infrastructure is monitored 24/7 to help safeguard the confidentiality, integrity, and availability of our customers data. Moving cloud workloads to edge devices or endpoints provides you with more control and visibility and mitigates risk.

A defense in depth model (for example, using multiple independent layers of specialized security controls) provides layers of protection. In addition to the design principles of the AWS Well-Architected Framework's Security Pillar, this paper highlights three aspects of edge protection whose PoP is at AWS edge locations. The three highlighted edge protections that help secure the connection points between the origin infrastructure, edge services, and customer edge devices or applications are:

- Secure content delivery
- Network and application layer protection
- Distributed Denial of Service (DDoS) mitigation

The design principles also cover the security of edge devices and applications. A comprehensive defense in depth strategy should include services that account for the security of both AWS edge locations, and edge devices and applications.

Secure content delivery

Secure content delivery provides content, such as data, videos, applications, and APIs, quickly and securely to customers. These should be delivered over secure transport, using the recommended version of Transport Layer Security (TLS) to encrypt communications between endpoints. If necessary, there are several methods you can use to help secure that same content through restricted access, including signed URLs, signed cookies, and token authentication.

Amazon CloudFront, a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to viewers with low latency and high transfer speeds, addresses these areas of security when it is deployed at AWS edge locations.

To create a more secure CDN, organizations can gain protection against L3/L4 DDoS attacks using AWS Shield. AWS also offers AWS Shield Advanced, which provides additional detection and mitigation against large and sophisticated DDoS attacks, near-real-time visibility into attacks, and integration with AWS WAF, a web application firewall service, to protect against application layer (L7) attacks. Together, these services create a flexible, layered security perimeter.

CloudFront offers security capabilities, including field-level encryption and HTTPS support, seamlessly running with AWS Shield Advanced, AWS WAF, and Amazon Route 53 to protect against multiple types of attacks, including network and application layer DDoS attacks. For more details about CloudFront and Route 53, see the Appendix.

Network and Application Layer Protection

Edge networks are architected outside of the security perimeters of traditional clouds. Extending security to edge end devices requires network and application security and continuous monitoring, as well as encryption of data in transit and at rest.

Edge customers should define trust boundaries for networks and accounts and verify secure system configurations and other policy-enforcement points, including web application firewalls (WAFs) and API gateways. This can be done by blocking well-known exploits, implementing protections

specific to applications, responding to new threats, and performing ongoing monitoring.

There are two important aspects to network and application layer protection at the edge:

- Protections from well-known exploits and attacks that could affect an organization's applications
- Visibility and control of workloads

A WAF deployed at AWS edge locations can help to set fundamental protections, customize them to the applications, and help organizations quickly visualize actions so they can create a dynamic security posture. With AWS WAF, you can use the AWS pre-configured rules (Managed Rules), use Marketplace Rules, or create your own custom rules to protect against common attack vectors.

AWS Managed Rules give you protection against common web application attacks. They are curated by multiple points of intelligence across multiple sources within AWS.

Marketplace Rules are written, updated, and managed by third-party security experts, and can be used on their own or in conjunction with AWS Managed Rules. AWS WAF, which integrates with AWS Shield Advanced at no extra cost, provides easy setup, low operation overhead, minimal latency impact, and customizable security. It also uses advanced automation to analyze web logs, identify malicious requests, and automatically update security rules.

In addition to preventing incidents, visibility into traffic coming into and out of a network is a second key aspect of network and application layer protection. There are multiple options available to get insights and metrics: CloudWatch metrics, sampled web requests, and logs.

With CloudWatch, you can monitor web requests and web access control lists (ACLs) and rules. CloudWatch collects and processes raw data from AWS WAF and Shield Advanced into readable, near-real-time metrics. AWS WAF supports full logging of all web requests inspected by the service, which can then be stored in the cloud for compliance and auditing purposes and used for debugging and additional forensics. You can also integrate the logs with your security information and event management (SIEM) and log analysis tools. For details, see AWS WAF Launches New Comprehensive Logging Functionality.

For more details about AWS WAF, see the Appendix.

DDoS Mitigation

DDoS mitigation as a defense layer is important for organizations operating at the edge with mission-critical operations that cannot afford downtime. DDoS mitigation helps ensure continued availability of those operations and services. DDoS attacks are deliberate attempts to exhaust infrastructure or application resources, so they are unavailable to users. Common types of DDoS attacks are SYN floods that exploit the TCP protocol; reflection or amplification attacks that use the connectionless nature of User Datagram Protocol (UDP) for its purposes; and HTTP floods that target web servers' capacity to manage requests.

AWS services include basic DDoS protection as a standard feature. All AWS customers using CloudFront, Application Load Balancers, Network Load Balancers, Global Accelerators, Elastic IPs, or Route 53 receive basic DDoS protection against common network and transport layer attacks.

This protection is always on, but is preconfigured, static, and provides no reporting or analytics. Mitigations are configured with pre-assigned limits based on the service being targeted. For example, if your Elastic Load Balancing (ELB) is targeted by an infrastructure layer DDoS attack, a mitigation that is configured based on ELB service limits to ensure the resource remains operational is placed. This mitigation is effective at blocking many known vectors of attack and protecting the underlying resource. The nuance is that the limits of your application may differ from the limits of the ELB, resulting in the resource remaining operational, but your application still being impacted.

Shield Advanced is a managed service that builds a customized DDoS protection capability specifically for your applications' needs, based on the resources you specified either in Shield Advanced or through an AWS Firewall Manager Shield Advanced policy. Shield Advanced can be deployed at AWS edge locations, and you get tailored detection based on the specific traffic patterns of your application, protection against Layer 7 DDoS attacks at no additional cost, access to 24x7 specialized support from the Shield Response Team (SRT), centralized management of security policies through AWS Firewall Manager, and cost protection to safeguard against scaling charges resulting from DDoS-related usage spikes. You can also configure AWS WAF to integrate with Shield Advanced to create custom rules.

Some DDoS events can be mitigated by scaling applications to absorb the additional traffic or by using a web application firewall. (For more information, see *AWS Best Practices for DDoS Resiliency*.) Unless encrypted traffic ends with a network-layer device, these devices are generally unable to inspect encrypted requests. This can allow bad actors to use expansive web requests or large volumes of web requests to generate a flood that is challenging to fingerprint, challenging to block or absorb, or both.

Using Amazon CloudFront or AWS Global Accelerator to distribute request handling across many AWS edge locations and AWS WAF to temporarily block source IP addresses that exceed a pre-defined limit can help secure applications targeted by this type of DDoS attack. These events are detected when an Amazon CloudFront distribution or Application Load Balancer (ALB) is protected by AWS Shield Advanced.

Credit to: AWS Documentation