Westcon – AWS

Security Whitepaper

Westcon | aws

Contents

The purpose of this document

Nowadays, modern businesses tend to migrate their workload from traditional IT environments to the cloud. As we all know, the security and compliance of the cloud environment is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the service operates. However, there is still a fair bit of work that needs to be taken care of by the customer.

This document will go through the AWS security competency checklist and outline important consideration points that any AWS customer should assess to improve the security posture in their cloud environment.

Identity And Access Management

Identity Governance & Administration

When a customer creates an AWS account, the first thing to consider is the security of the root account. The best practice guidelines when using the root user include but are not limited to:

1. Using root account only for setting up identity federation in IAM and the billing & cost management purposes.
2. Enable MFA for the AWS account root user.
3. Remove AWS account root user access keys.
4. Periodically change the AWS account root user password.
5. Use a long and strong password for the root account.

Typically, the customer will choose to create individual IAM accounts with assumed roles for daily operation tasks. When creating the user accounts, it is recommended to have strong identity governance and secure administration like below:

1. Implement least privilege and separation of duties across the lifecycle of joiners, movers, and leavers.
2. Scan the networks or policies to provide a list of AWS services and roles that can access the Internet.
3. Enable MFA for the user accounts.
4. Federate internal and external users to AWS accounts and business applications.
5. Manage passwords, keys, and other secrets to avoid a customer storing credentials in plain text on an instance.
6. Have visibility of how identity access rights map to resources.

Cloud Infrastructure Entitlements Management

In addition, cloud infrastructure entitlements management plays a vital part in Identity and Access Management, the customer should:

1. Enforce policies for entitlements using guard rails across multiple environments, including AWS.
2. Implement policies for entitlements across multiple environments, including AWS.
3. Control access for humans, machines, and applications across multiple environments including AWS.
4. Use historic logs to recommend policy updates in line with least privilege.
5. Detect and alert customers based on anomalous access patterns (e.g., outside of work hours or from a new location).

AWS Control Tower

The AWS account management can become very complex and time-consuming, especially when the customer has multiple accounts and teams. AWS Control Tower becomes very popular for the customer who needs an easy way to set up and govern a secure multi-account AWS environment. The built-in guardrails service automatically and continuously enforce the policies using service control policies (SCPs) and detect policy violations using AWS Config rules. The integrated dashboard will reveal a top-level summary of policies applied to the AWS environment. Not to mention, AWS Control Tower automatically creates a secure data bunker (only members of the security team have access to this account) which allows CloudTrail for the organisation to send these logs to the bucket in the secure data account.

Threat Detection and Response

Distributed Denial of Service (DDoS)

With the growth of the DDoS attack, it has been a huge concern for customers who are running their own service on AWS environment. DDoS protection for the applications running in a customer's AWS accounts is recommended, in order to stop bad actors consuming resources and impacting application performance. The mitigations that the customer is choosing must adapt to user interactions from layer 3, 4, and 7 attacks at Internet scale.

When considering the security services edge, technologies like Cloud Access Security Brokers (CASB), Secure Web Gateway (SWG) and Zero Trust Network Access (ZTNA) are often on the table.

- CASB provides inline content filter, via proxy or API, to protect enterprise users' outbound connections from malicious content, data leakage, and advanced threats.
- SWG provides protection for inbound as well outbound connections using advanced malware protection, data leakage prevention, application control, geo-awareness, HTTPS inspection, SSL decryption, and blocklist URL filtering.
- ZTNA removes implicit trust in the network based on physical or network location and replace it with a focus on users, assets, and resources, as well as secures workloads that are not located on the same network such as remote workers and bring your own device

Network Security Policy Management

Even though all the technologies and tools are provided, the customer still needs a proper network security policy management to further enhance the security posture and reduce operational overhead by:

1. Providing a comprehensive view of network security policy from firewalls and other rules-based security solutions across AWS Cloud and other environments.
2. Identifying rules that are redundant or out of date and provide a process for simplifying those rules.
3. Providing a visualisation of the network edge where managed policies reside.

The customer should consider the following service to enhance Threat Detection and Response:

1. Amazon GuardDuty
2. AWS Firewall Manager
3. AWS Network Firewall
4. AWS Shield
5. AWS WAF – Web application firewall
6. Amazon Virtual Private Cloud
7. AWS PrivateLink
8. AWS Systems Manager

Data Protection

The services that have been mentioned in Threat Detection and Response can be unitised for data protection.

Database Security

Database security is very important to a customer as it contains all valuable data related to the business. A good database security solution should:

1. Provide a visual dashboard for users to see where their data is stored, the configuration compliance with active policy, and the type of data.
2. Has the capability of discovering and classifying the sensitive data stored in AWS.
3. Be able to scan databases for misconfigurations, patch levels, lack of encryption, lack of back-ups, and identity and access control issues that allow for privilege escalation.

Email Security

Email as another critical service in a business needs to be secured for data protection purposes. The solution normally includes detection, remediation actions, and training.

1. Scan email for malicious code or attachments as well as data leakage.
2. Encrypt email based on content filter policies.
3. Scan email for malicious messages and common phishing tactics.

Data Loss Prevention (DLP)

In addition, the customer must understand where sensitive data resides and how it moves over time when thinking about data loss prevention. It is a good idea to regularly scan data at rest (storage) and data in motion (network) to determine when sensitive data is improperly used or exchanged.

Amazon S3 Malware Scanning

S3 is a well-known AWS data storage service, Malware scan can help to maintain the data integrity in an API-based, Event-based, or scheduled approach. Tokenisation and Masking are mechanisms for customers to use after identifying sensitive information, and replace it with non-sensitive information in the same data format using a reversable process.

Keys and Secrets Management

Finally, keys and secrets management are a must when considering securely store, transmit, and audit secrets.

1. AWS customers require a policy for implementing AWS privacy controls, including advanced access, encryption, and logging features.
2. A policy for flexible key management that includes use cases for Customer Selected Keys.
3. The policy needs to cover TLS/SSL cert monitoring for expiration, secure storage, and use under HSTS (HTTP Strict Transport Security) by default.
4. Provide details on how the policy manages keys, including rotation and recovery strategies.

Compliance and Privacy

Even though the AWS Shared Responsibility model is very well-known, the business still needs to have regular internal training on the understanding of responsibilities taken by AWS and those taken by the customer.

For the customer to take good care of their responsibility, the following points must be taken into consideration:

1. A playbook is required for incident response, and the ability to create self-policing guard rails and/or the ability to detect "configuration drift" away from a standard are vital.

2. The AWS environment must be designed and built thoroughly to obtain a third-party certification, attestation, or pass a third-party audit such as PCI or SOC 2. The customer can seek help from AWS Artifact and AWS Audit Manager.

3. A properly built Cloud Workload Protection provides a single pane of glass for protection based around the workload as it operates across AWS and on-prem environments The scope should cover protections across OS/Hardware hardening, network firewalling, system integrity, application control, exploit prevention, server EDR, HIPS, and anti-malware scanning.

4. Cloud Security Posture Management requires:
    - Automated processes to remediate resources that are out of compliance.
    - Compliance checking against third-party standards including CIS benchmarks.
    - Alert when a resource changes configuration in a way that takes it out of compliance with an active policy.
    - Check and alert on scenarios with un-encrypted databases, data storage exposed to the Internet, and MFA for root access.

5. Attack Surface Management provides control of customer attack surface through continuously discovering, classifying, and monitoring the resource inventory from an external perspective (i.e., malicious hacker viewpoint).

6. Container Security Configuration Scanning is important for modern business that leverage microservices.
    - Be alerted when container configurations shift or drift from the approved baseline and playbooks to execute in this event.
    - Protect containers and integrate with the AWS container services - Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), or AWS Fargate.

Perimeter Protection

Layered Edge Services Defence

Layered security posture for customer accounts, assets and distributions is required at the Edge using AWS services includes AWS Shield and AWS WAF. Additional recommended components are Amazon CloudFront and AWS BOT Control.

The investigation policies and processes must align to organisational requirements. There must be processes for running incident response simulations, including tools, automation, detection techniques, investigation process, and recovery procedures.

AWS Global Accelerator can be used to securely distribute AWS request handling across AWS edge location. Customisation of security rules for edge computing (like AWS Managed Rules, Marketplace Rules, or custom rules) to address the appropriate level of protection. Secure content delivery needs to be considered from AWS Edge locations:

1. Implement TLS (SSL) encryption, signed URLs, signed cookies, or token authentication.
2. Protect the CDN against Layer 3/4 DDoS events with AWS Shield and against L7 DDoS events, BOTs, and Web Application exploits with AWS WAF.
3. Use AWS Firewall Manager to centrally configure and manage firewall rules across accounts and applications in AWS Organisations.

Security Information Event Management (SIEM)

Security Information Event Management (SIEM) is often used to audit, monitor, alert, and report changes to an environment in real-time. The systems API can automatically investigate and take actions. The logs and metrics must be ingested into the SIEM system including AWS CloudTrail Logs, Amazon VPC Flow Logs, Amazon CloudWatch logs, AWS WAF logs and AWS Shield events.

Security Operations Centre (SOC)

Customers need a Security Operations Centre (SOC) solution to support their AWS environments. A 24/7 SOC service will include engineers with security skills in WAF rule writing, mitigation, escalation, and log parsing.

Core Security Considerations

SOC Implementation and Incident Response

1. Standard incident response playbooks define how the customer analyses AWS telemetry including AWS CloudTrail, Amazon GuardDuty Findings, AWS WAF Logs, AWS S3 Access Logs, Amazon VPC Flow Logs, as well as OS and Application logs.
2. AWS customers must also integrate these security workflows, alerts, and logs into a centralised SIEM and ticketing system.
3. The SOC can outline common events and the associated responses, as well as escalations up to the board or owners.
4. Documented process for investigating an incident and collecting evidence on AWS workloads.

Business Continuity (BC)

1. The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
2. The organisation's mission, objectives, stakeholders, and activities are understood and prioritised; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
3. The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified, categorised, and managed consistent with their relative importance to business objectives and the organisation's risk strategy.
4. Examples of written process for recovering back-ups, written frequency of testing COOP plan, written plan for on-prem or multi-cloud recovery into AWS.
5. The customer has a policy and process for validating that the back-ups are isolated from the production network with separate access roles and separate MFA access, like audit accounts.

Ransomware Protection

1. Provide anti-Ransomware software deployment documentation and/or automation that is used by individuals in their company or equivalent assets in their application.
2. Detail mitigations of host and network attack vectors as well as policy enforcement such as patch management.
3. Include inventory of digital assets, logging, reporting, vulnerability management, and event detection.
4. Include secure backup, immutable storage, investigation, and analytics capabilities.
5. Software Composition Analysis (SCA).

   For the Open-Source Software (OSS) SCA
   - The customer can identify all the third-party software, including OSS, within an application.
   - Solutions will also provide visibility into the software licensing imbedded in the software, such as the GNU General Public Licenses (GPL).

Have an enquiry?

Contact us

Allan Kivell *(Cloud Development Manager)*
Email: allan.kivell@westcon.com
Phone: +64 21 497 558

As an AWS authorised distributor, we will work with you and a qualified Reseller Partner to help with your cloud journey