Identity

Zero Trust Model- It operates on the principle of trust no one, verify everything.

In zero Trust Model Identity becomes the primary security perimeter.

What is the Primary Security Perimeter?
The primary or new security perimeter defines the first line of defense and its security controls that protect a company's cloud resources and assets.

Network-Centric (Old way): Firewalls, VPNs, employees can only access the service within the work station

Identity Centric (New Way): Since time is changing with all the new options of remote work etc. Bring you own device is much more common so we use methods like MFA or provide provisional access based on the level of risk.

Identity Centric does not replace but augments Network Centric.

Identify Security Controls you can implement on AWS to meet the Zero Trust Model.

AWS Identify and Access Management (IAM)

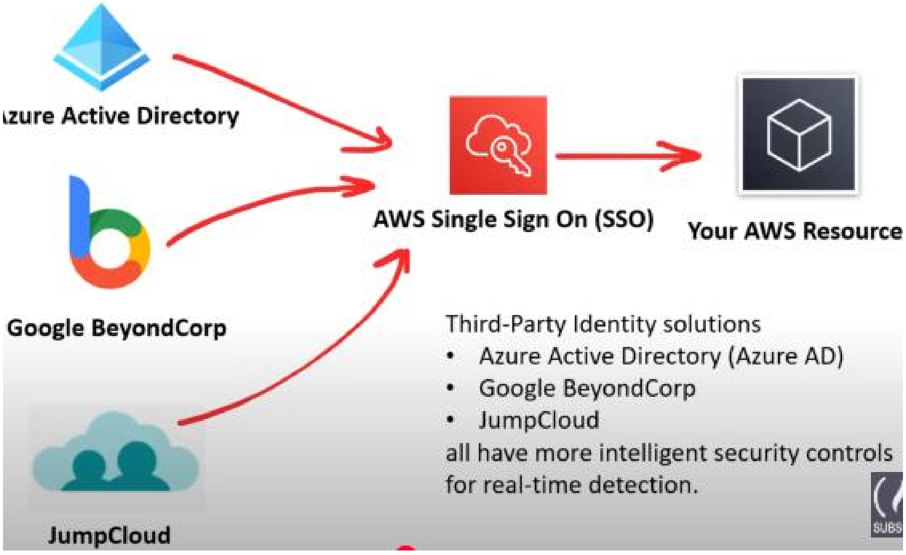
I am polices
Permission Boundaries
Service Control Policies (Organization-wide policies)
IAM Policy Conditions
-aws:Sourcell-Restrict on IP address
-aws:RequestRegion-Restrict on Region
-aws:MultiFactorAutPresent-Restrict if MFA is turned off
-aws:CUrrentTime-Restrict access based on time of day.

Zero Trust on AWS with Third Parties

AWS does not technically implement a zero trust model but does not allow for intelligent identity security controls.

For Eg- Azure directory has Real-Time and calculated risk detection based more points than AWS.

Third Party Solution



Third-Party Identity solutions

- Azure Active Directory (Azure AD)
- Google BeyondCorp
- JumpCloud

all have more intelligent security controls for real-time detection.

Directory Service

A directory service maps the names of network resources to their network address.
A directory service is shared information infrastructure for locating managing administering and organizing resources.
Well known services are
DNS
Microsoft Active Directory

Identity Providers (Idps)- a system that creates maintains and manages identify information. EG-Facebook, amazon, google, twitter..etc

Federated Identify is a method of linking a user identify across multiple separate identify management system.

EG-OpenID, OAuth2.0, SAML (An important use case for SAML is Single-Sign on via web browser)