



# CLOUD SECURITY SHOWDOWN

AWS VS. AZURE

# Identity: The New **Perimeter**

How they handle the keys to the kingdom.

- > **AWS IAM: Resource-Centric.** Uses complex JSON policies. Highly granular but has a steep learning curve.
- > **Azure AD (Entra ID): User-Centric.** Flat structure designed for Enterprise. Native Office 365 integration.
- > **Verdict:** AWS is for *Builders*. Azure is for *Corporate IT*.



# Infrastructure & Network

- > **Isolation:** AWS uses **VPC** vs Azure's **VNet**. Both provide logical isolation.
- > **Firewalls:** AWS **Security Groups** (Instance-level). Azure **NSGs** (Subnet-level).
- > **DDoS:** AWS **Shield Standard** is "always on" and free. Azure requires a paid tier for similar advanced protection.



# Threat Detection

- > **AWS GuardDuty:** A focused service. Uses ML on CloudTrail/VPC logs to detect anomalies. "Set and Forget."
- > **Azure Sentinel:** A full cloud-native **SIEM**. It ingests data from the entire enterprise (on-prem + cloud) and offers orchestration (SOAR).
- > **Key Difference:** GuardDuty is a *sensor*. Sentinel is a *platform*.



# Strategic Verdict

FEATURE AREA	AWS APPROACH	AZURE APPROACH
Identity	Developer-First (IAM)	Enterprise-First (Entra ID)
Hybrid Tech	Outposts (Hardware)	Market Leader (Arc)
SIEM Strategy	Partner-Heavy (Splunk, etc)	Native Platform (Sentinel)
Best For...	Cloud-Native Startups	Hybrid Enterprises