



Silicon   
Overdrive

# Security in the Cloud



by Gareth Bowers, Silicon Overdrive

CEO, and AWS Brand Ambassador

# Agenda



- **Shared Responsibility, Compliance**  
by Radhir Nundlall, AWS
- **Security in the Cloud**  
By Gareth Bowers, Silicon Overdrive
- **Q & A (Questions & Answers)**  
By Gareth Bowers and Radhir Nundlall







Silicon   
Overdrive

# Security in the Cloud



# Security in the Cloud

- **Security and compliance standards do not change, whether you're on-prem or in the cloud and what you are needing to build:** AWS handles security of the infrastructure and provides multiple tools to assist with security in the cloud.
- **Shared Responsibility Model:** Being with a cloud service provider helps you meet your compliance requirements but doesn't make you compliant.
- **Always architect and build securely:** Be clear if you are building a throw-away PoC or a PoC to transition to MVP and full product.



# Security in the Cloud

- **Public versus Private Subnets:** Understand costs versus security and ease for developers.
- **Encryption at rest:** When should this not be used?
- **Encryption in transit:** What does Business or Compliance require?
- **Automate and script as much as possible:** From the infrastructure to testing, automate where it will save on iterative tasks and improve security.





# AWS Security, Identity, and Compliance Solutions



## Identity and access management

- AWS Identity and Access Management (IAM)
- AWS IAM Identity Center
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager
- Amazon Verified Permissions

## Detective controls

- AWS Security Hub
- Amazon GuardDuty
- Amazon Security Lake
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

## Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF
- Amazon VPC
- AWS PrivateLink
- AWS Systems Manager
- AWS Verified Access

## Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Private CA
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

## Incident response

- Amazon Detective
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery

## Compliance

- AWS Artifact
- AWS Audit Manager







## Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources.



### AWS Identity and Access Management (IAM)

Securely manage access to AWS services and resources.



### AWS IAM Identity Center

Centrally manage SSO access to multiple AWS accounts and business apps.



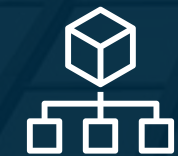
### AWS Directory Service

Managed Microsoft Active Directory in AWS.



### Amazon Cognito

Add user sign-up, sign-in, and access control to your web and mobile apps.



### AWS Organizations

Policy-based management for multiple AWS accounts.



### AWS Resource Access Manager

Simple, secure service for sharing AWS resources.

### Amazon Verified Permissions

Fine-grained permissions and authorization for your applications.







## Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment.



### AWS Security Hub

Automate AWS security checks and centralize security alerts.



### Amazon GuardDuty

Protect your AWS accounts with intelligent threat detection.



### Amazon Inspector

Automated and continual vulnerability management at scale.



### Amazon CloudWatch

Observe and monitor resources and applications on AWS, on premises, and on other clouds.



### AWS Config

Assess, audit, and evaluate configurations of your resources.



### AWS CloudTrail

Track user activity and API.



### VPC Flow Logs

Capture info about IP traffic going to and from network interfaces in your VPC.

### Amazon Security Lake

Automatically centralize your security data in a few steps.







## Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS.



### AWS Firewall Manager

Centrally configure and manage firewall rules across your accounts.



### AWS Network Firewall

Deploy network firewall security across your VPCs.



### AWS Shield

Maximize application availability and responsiveness with managed DDoS protection.



### AWS WAF

Protects your web applications from common exploits.



### Amazon Virtual Private Cloud

Define and launch AWS resources in a logically isolated virtual network.



### AWS PrivateLink

Establish connectivity between VPCs and AWS services without exposing data to the internet.



### AWS Systems Manager

Gain operational insights into AWS and on-premises resources.

### AWS Verified Access

Provide secure access to corporate applications without a VPN.







## Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.



### Amazon Macie

Discover and protect your sensitive data at scale.



### AWS Key Management Service (AWS KMS)

Create and control keys used to encrypt or digitally sign your data.



### AWS CloudHSM

Manage single-tenant hardware security modules (HSMs) on AWS.



### AWS Certificate Manager

Provision and manage SSL/TLS certificates with AWS services and connected resources.



### AWS Secrets Manager

Centrally manage the lifecycle of secrets.



### AWS VPN

Connect your on-premises networks and remote workers to the cloud.



### Server-Side Encryption

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

### AWS Private CA

Create private certificates to identify resources and protect data.







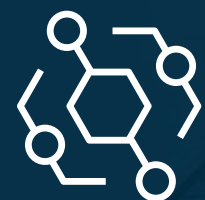
## Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice.



### Amazon Detective

Analysis and visualization of security data to get to the root cause of potential security issues quickly.



### Amazon EventBridge

Serverless event bus that makes it easier to build event-driven applications to scale your programmed, automated response to incidents.



### AWS Backup

Centrally manage and automate backups across AWS services to simplify data protection at scale.



### AWS Security Hub

Out-of-the-box integrations with ticketing, chat, SIEM, SOAR, threat investigation, incident management, and GRC tools to support your security operations workflows.



### AWS Elastic Disaster Recovery

Fast, automated, cost-effective disaster recovery.







## Compliance

AWS supports security standards and compliance certifications to help you satisfy compliance requirements for virtually every regulatory agency around the globe.



### **AWS Artifact**

No-cost, self-service portal for on-demand access to AWS compliance reports.



### **AWS Audit Manager**

Continuously audit your AWS usage to simplify how you assess risk and compliance.





# Large Community of Security Partners & Solutions



## Network and infrastructure security

ALERT LOGIC  
Security. Compliance. Cloud.

APPGATE

ARMOR

Barracuda

Check Point  
SOFTWARE TECHNOLOGIES LTD.

CISCO

ExtraHop

FORTINET

Guardicore

paloalto  
NETWORKS

PROTECTWISE

SKinfosec co., Ltd.

SOPHOS

zscaler

## Identity and access control

okta

onelogin

Ping  
Identity

SAVIYNT

## Vulnerability and configuration analysis

bridgecrew

ExtraHop

Qualys

RAPID7

tenable

threat stack

## Logging, monitoring, SIEM, threat detection, and analytics

ALIEN VAULT

LACEWORK

McAfee  
Together is power.

SECURONIX  
Security Analytics. Delivered.

splunk

sumo logic

## Host and endpoint security

CROWDSTRIKE

Symantec

TREND  
MICRO

SentinelOne

## Application security

Barracuda

Checkmarx

f5

## Data protection and encryption

CYBERARK

Data Sunrise  
Data & Database Security

gemalto  
security to be free

HashiCorp

PRIVITAR

THALES





Silicon   
Overdrive

# Q & A



# About Silicon Overdrive

Founded in 1995, Silicon Overdrive has over 25 years of experience as a leading IT Managed Services business.

Silicon Overdrive has significant experience and expertise in helping customers migrate, secure, optimize, and manage their AWS infrastructure, as well as achieve and maintain security and compliance, including POPIA, GDPR, PCI DSS, ISO 27001, and HIPAA.

We have been awarded the AWS Public Sector Partner of the Year – Sub-Saharan Africa 2021 and AWS Consulting Partner of the Year – Sub-Saharan Africa 2020.



- Public Sector
- Immersion Day
- Solution Provider
- DevOps Services Competency

- Education Services Competency
- Migration Services Competency

- Well-Architected Partner Program
- Amazon EC2 for Windows Server Delivery







Silicon   
Overdrive

# Thank You

## South Africa



[www.overdrive.co.za](http://www.overdrive.co.za)



+27 21 448 5759



[aws.sales@overdrive.co.za](mailto:aws.sales@overdrive.co.za)



5 Hares Avenue, Woodstock  
Cape Town, South Africa

## Kenya



[www.overdrive.co.ke](http://www.overdrive.co.ke)



+254 726 284 477



[aws.sales@overdrive.co.ke](mailto:aws.sales@overdrive.co.ke)



Keystone Park, 95 Riverside Drive,  
Riverside, Nairobi, Kenya