



Demystifying Cloud Security With AWS

Fundamentals and Best Practices

Vishal Alhat

SSE, Forcepoint



<https://www.linkedin.com/in/vishalalhat>



[@WeShallAWS](https://twitter.com/WeShallAWS)

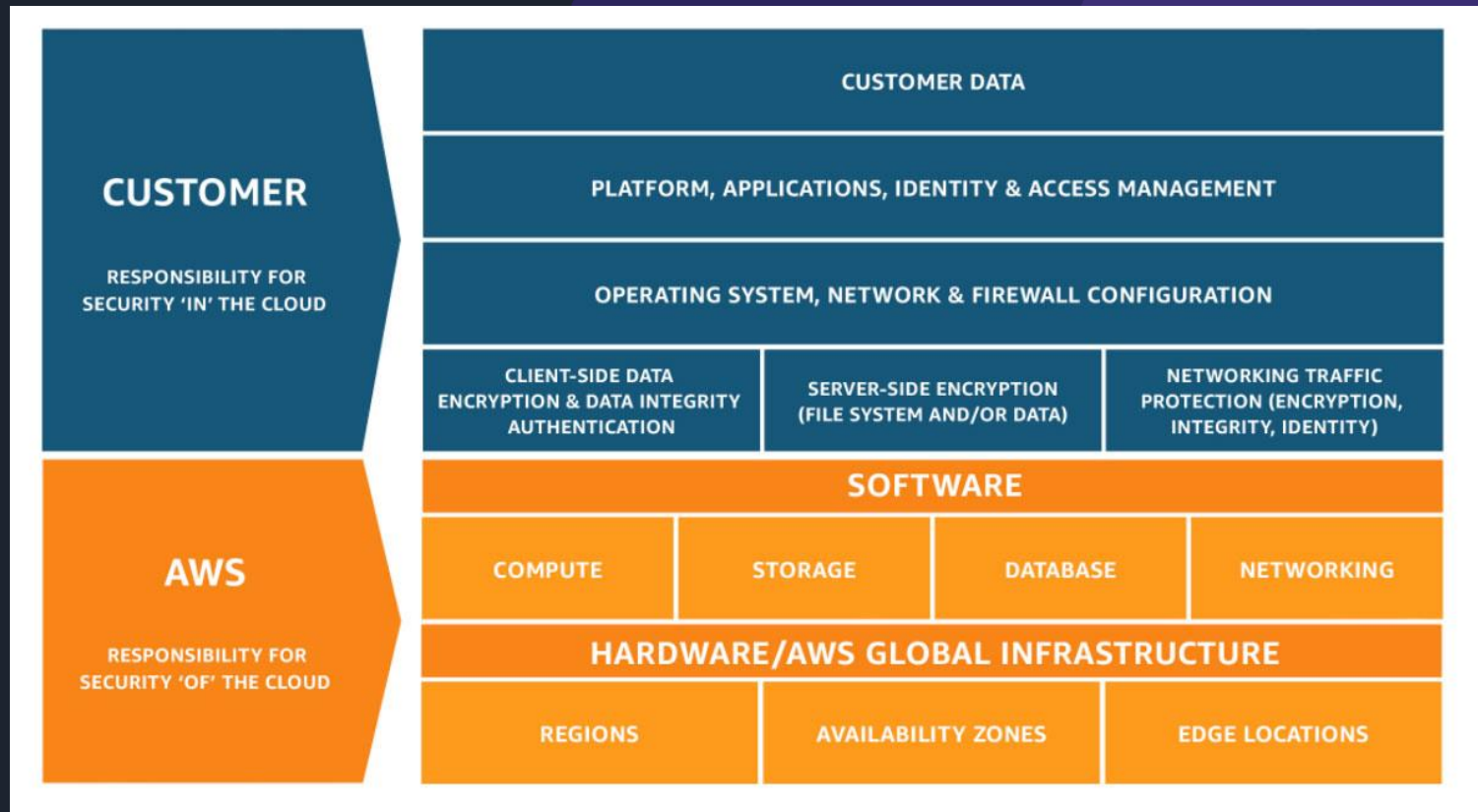


Agenda

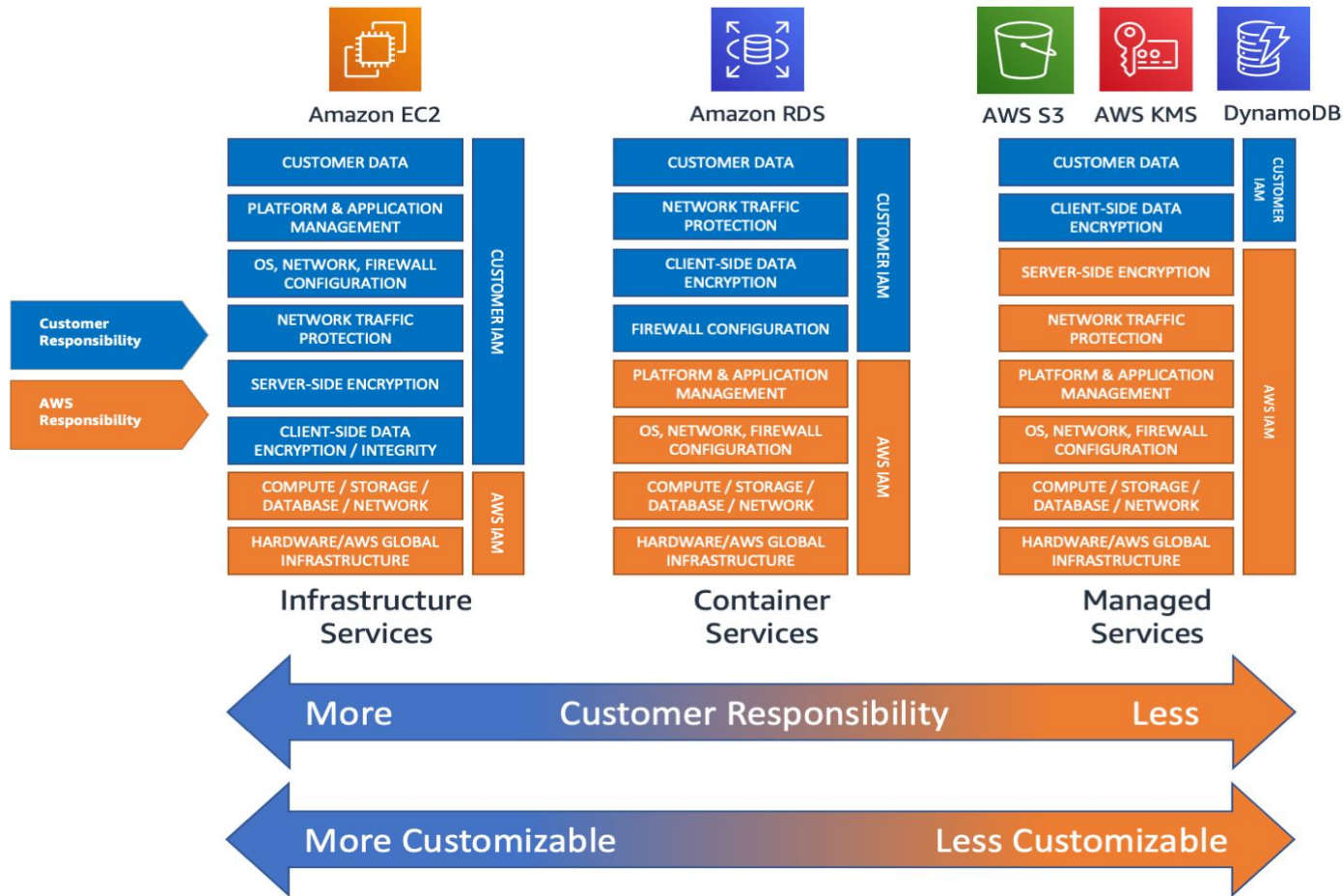
- ✓ Introduction
- ✓ AWS Shared Responsibility model
- ✓ Security Best Practices
- ✓ AWS Data Security
- ✓ AWS Servers Security
- ✓ AWS Applications Security
- ✓ Monitoring with AWS



Shared Responsibility Model






Shared Responsibility Model and Service Categories



AWS security best practices



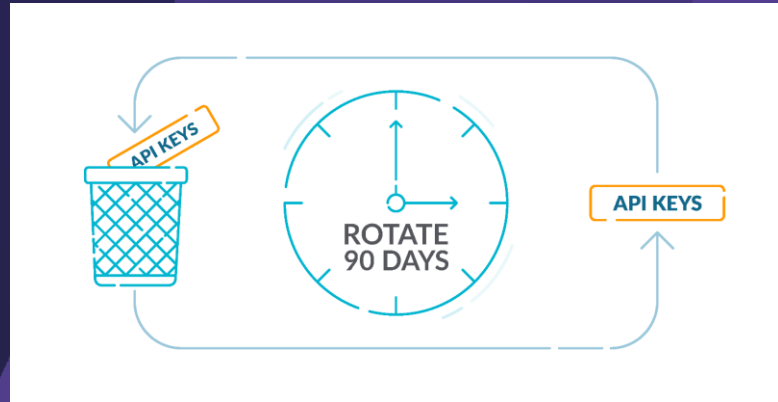
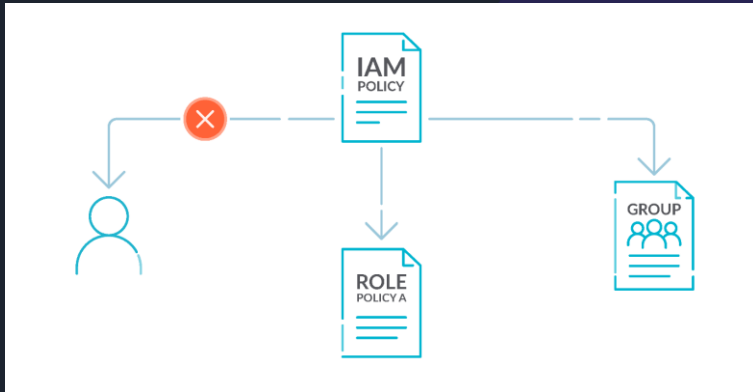
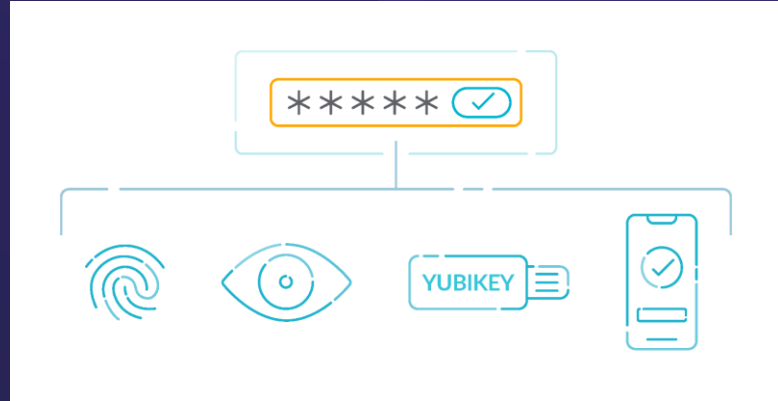
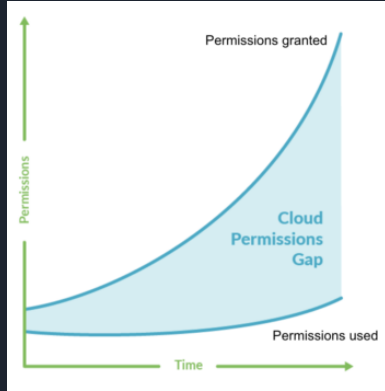
AWS security best practices by service

	High Risk 	Medium Risk 	Low Risk 
AWS IAM	<ul style="list-style-type: none">IAM policies should not allow full “*” administrative privilegesIAM root user access key should not existHardware MFA should be enabled for the root user	<ul style="list-style-type: none">IAM users’ access keys should be rotated every 90 days or lessMFA should be enabled for all IAM users that have a console passwordPassword policies for IAM users should have strong configurationsUnused IAM user credentials should be removed	<ul style="list-style-type: none">IAM users should not have IAM policies attached



Category	What is it	AWS service
Identity and access management	Securely manage access to services and resources	AWS Identity and Access Management (IAM)
	Manage workforce access across AWS accounts and apps	AWS IAM Identity Center (successor to SSO)
	Identity management for your apps	Amazon Cognito
	Managed Microsoft Active Directory	AWS Directory Service
	Simple, secure service to share AWS resources	AWS Resource Access Manager
	Central governance and management across AWS accounts	AWS Organizations

AWS security best practices

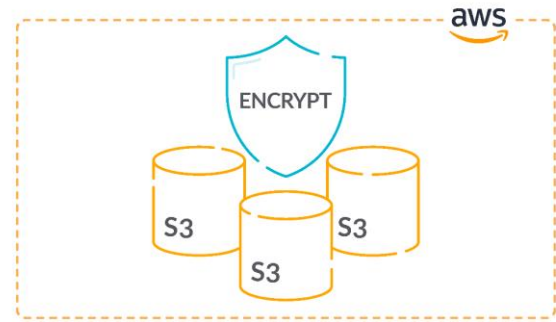


AWS security best practices



73%




of cloud accounts contain
publicly exposed S3 buckets



AWS security best practices






AWS security best practices by service

	High Risk 	Medium Risk 	Low Risk 
AWS S3	S3 buckets should have server-side encryption enabled - configure your buckets with server-side encryption	S3 Block Public Access setting should be enabled using ACLs S3 Block Public Access setting should be enabled at the bucket level using bucket level policies	

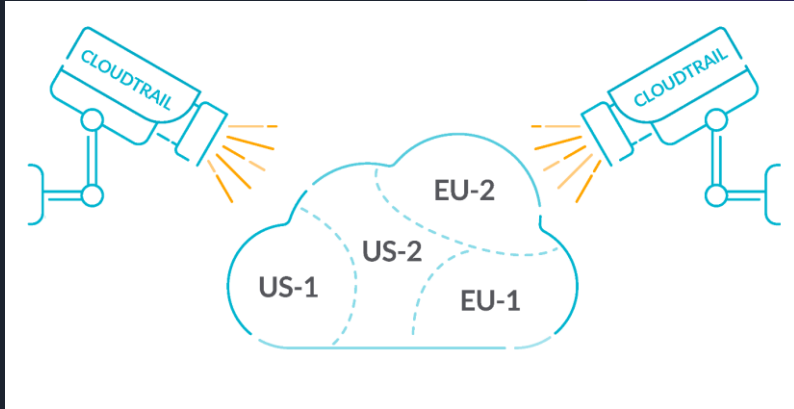
AWS security best practices



AWS security best practices by service

	High Risk 	Medium Risk 	Low Risk 
AWS CloudTrail	CloudTrail should be enabled and configured with at least one multi-Region trail	CloudTrail should have encryption at rest enabled Ensure CloudTrail log file validation is enabled	
AWS Config	AWS Config should be enabled		




AWS security best practices



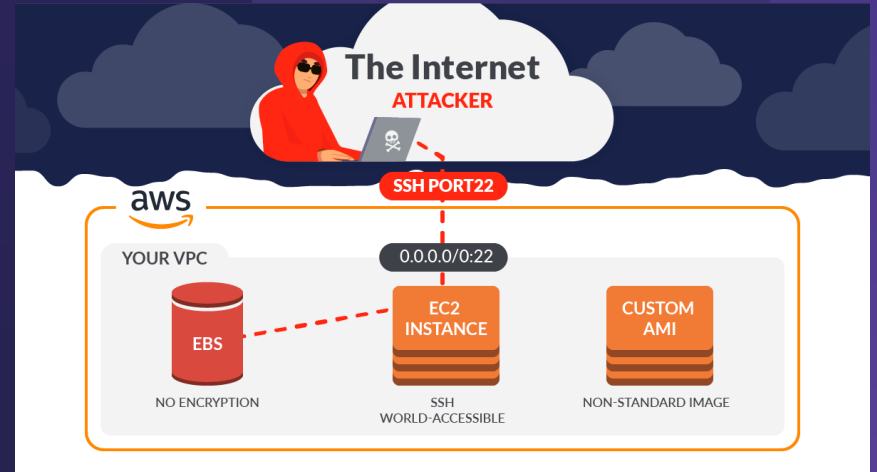
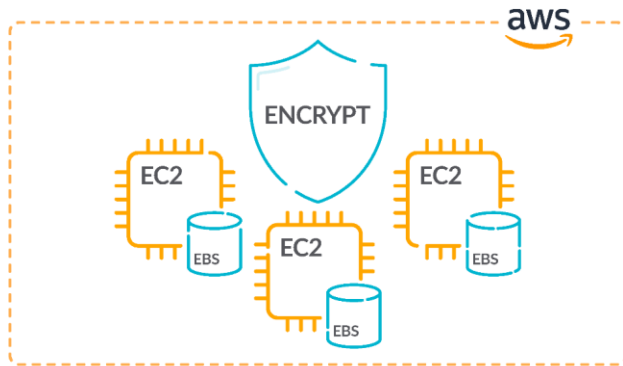
AWS security best practices



AWS security best practices by service

	High Risk 	Medium Risk 	Low Risk 
Amazon EC2	<p>Attached EBS volumes should be encrypted at rest</p> <p>EBS default encryption should be enabled</p>		<p>VPC flow logging should be enabled in all VPCs</p> <p>The VPC default security group should not allow inbound and outbound traffic</p>
AWS DMS	<p>AWS Database Migration Service replication instances should not be public</p>		




AWS security best practices



AWS security best practices






AWS security best practices by service

	High Risk 	Medium Risk 	Low Risk 
Amazon EBS	Amazon EBS snapshots should not be public, determined by the ability to be restorable by anyone		
Amazon OpenSearch Service-(successor to Elasticsearch)	Elasticsearch domains should have encryption at rest enabled		
Amazon SageMaker		SageMaker notebook instances should not have direct internet access	

AWS security best practices



AWS security best practices by service

	High Risk 	Medium Risk 	Low Risk 
AWS Lambda		Lambda functions should use supported runtimes	
AWS KMS		AWS KMS keys should not be unintentionally deleted	
Amazon GuardDuty		GuardDuty should be enabled	



Data Security Best Practices

- ✓ Encryption
- ✓ Use KMS
- ✓ Rotate your keys
- ✓ Classify your data
- ✓ Secure data in transit
- ✓ S3 bucket permissions



Servers Security Best Practices

- ✓ Use IAM roles for EC2
- ✓ Use ELB
- ✓ Security group configuration
- ✓ Use Web Application Firewall (WAF)
- ✓ Secured access
- ✓ Backup and recovery
- ✓ EC2 termination protection



Application Security Best Practices

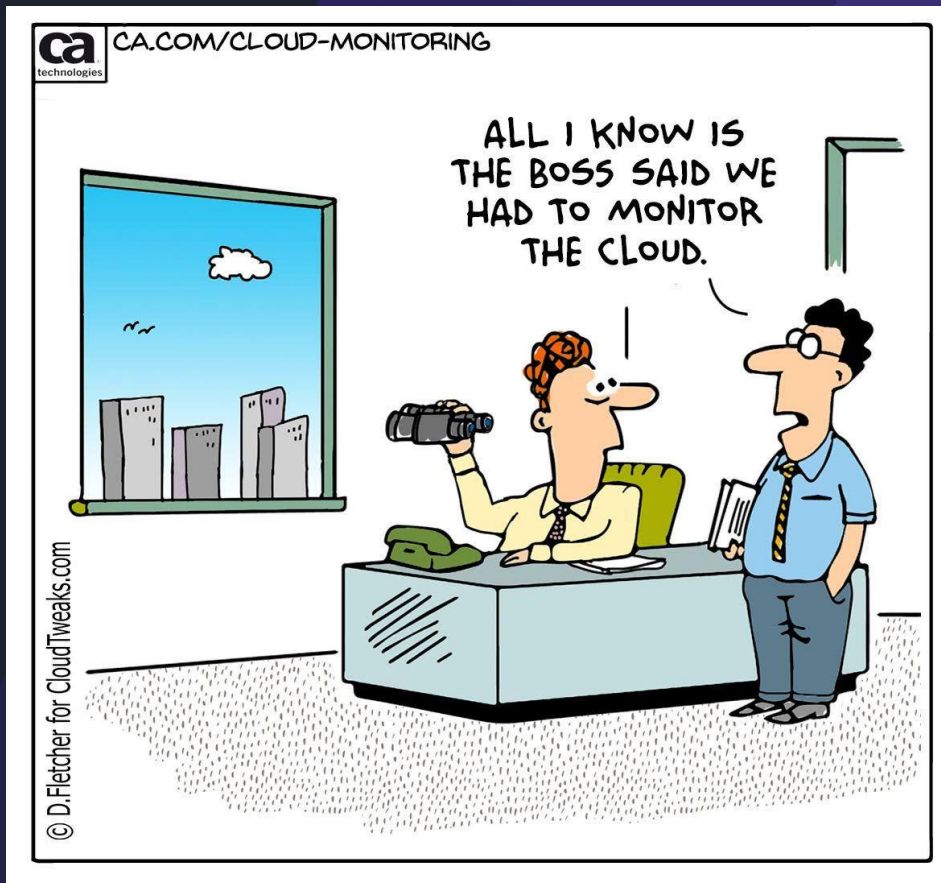
- ✓ Use web application firewall
- ✓ Amazon Inspector
- ✓ Penetration testing
- ✓ Utilize AWS security tools



Application Security Best Practices

- ✓ Use web application firewall
- ✓ Amazon Inspector –vulnerability management service
- ✓ Penetration testing
- ✓ Utilize AWS security tools

Monitoring in Cloud

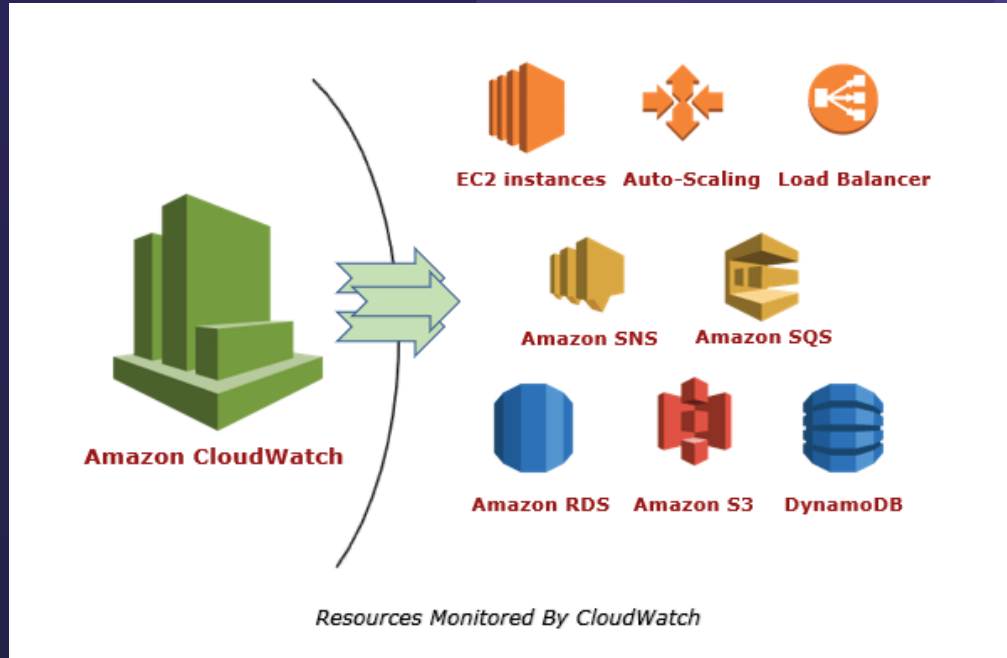


Monitoring With AWS

AWS Allows you to monitor all your resources in cloud, such as your servers and your AWS services, Along with applications running with these services through its fully managed monitoring service – AWS CloudWatch.

AWS CloudWatch provides

- ✓ Metrics
- ✓ Dashboard
- ✓ Events
- ✓ Alarms
- ✓ Log monitoring



Thank you!

Q & A





Please complete
the session
survey