



Learning Days

State, Local, Education and Health

Security is top priority

Columbus, OH | May 9th 2023

Matt Duncan

Solutions Architect
WWPS - SLG/EDU
Amazon Web Services

David Stielstra

Solutions Architect
WWPS - SLG/EDU
Amazon Web Services

How AWS thinks about security



Security is the top priority



Security is everyone's responsibility



Guardrails, not gates

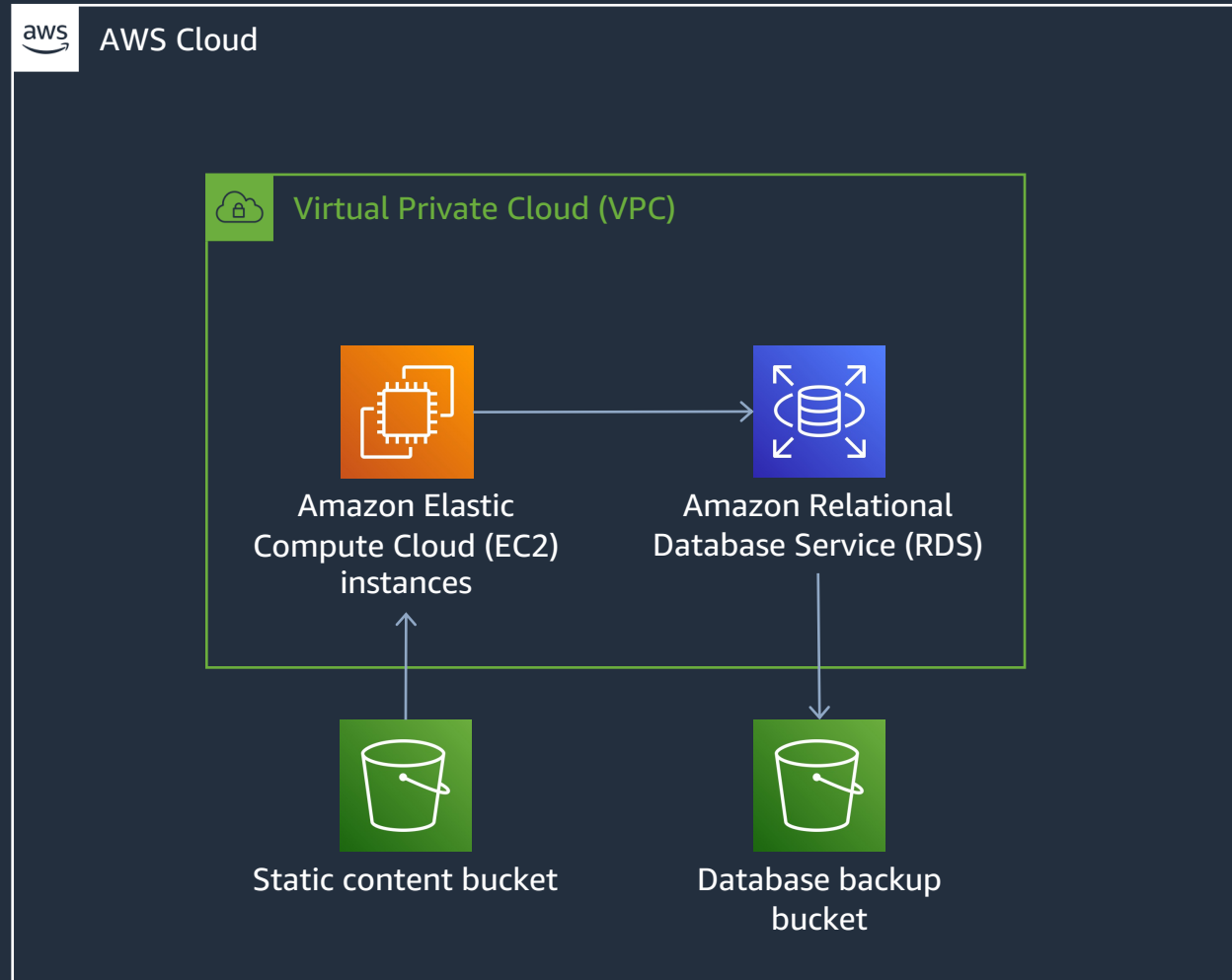


Security is a journey

Introducing Bob



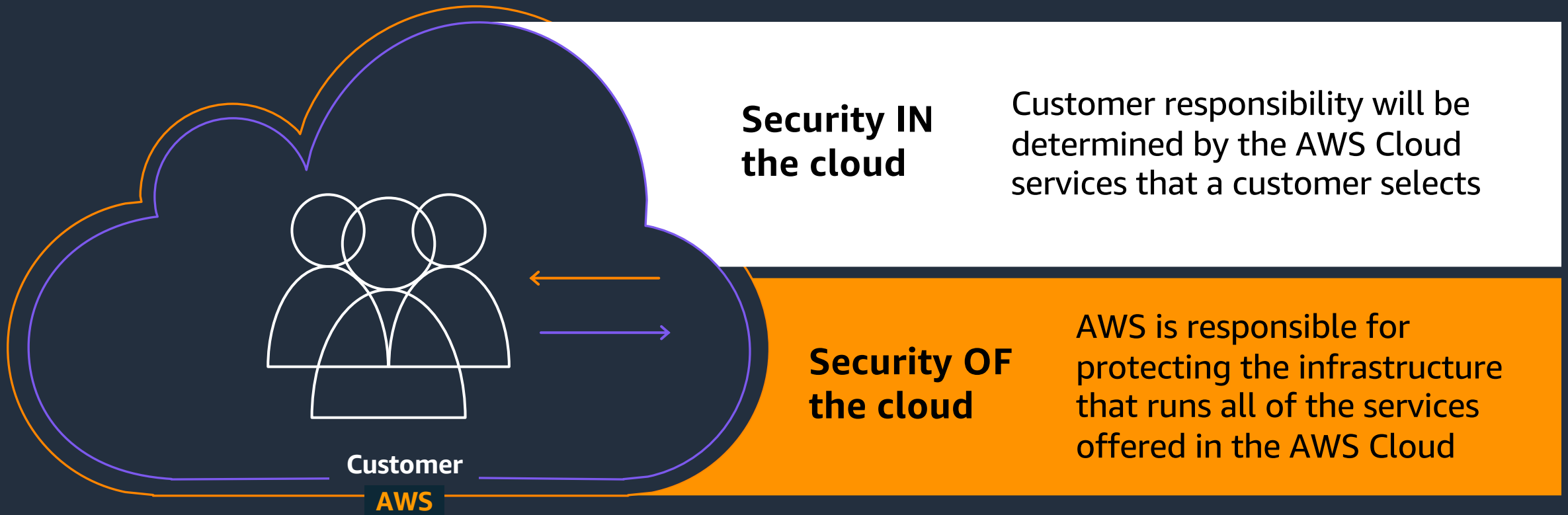
- Bob
- Chief Engineer
- Doesn't know much about security



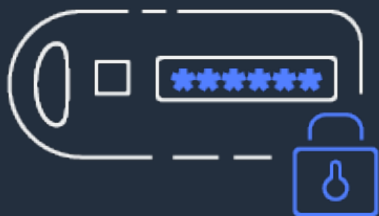
The AWS Shared Responsibility Model



AWS Shared Responsibility Model



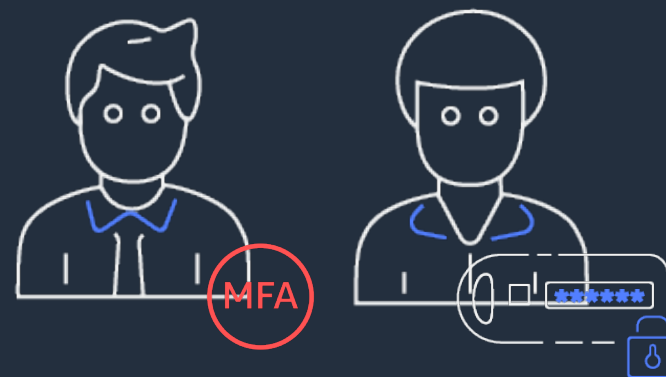
Protect your root user



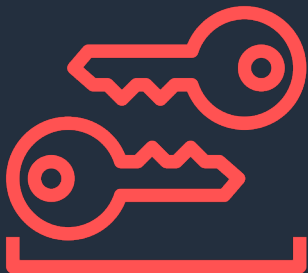
Use a complex password



Turn on multi-factor authentication (MFA)



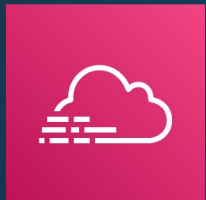
Separate password and MFA holder



Delete access keys



Set up alarms

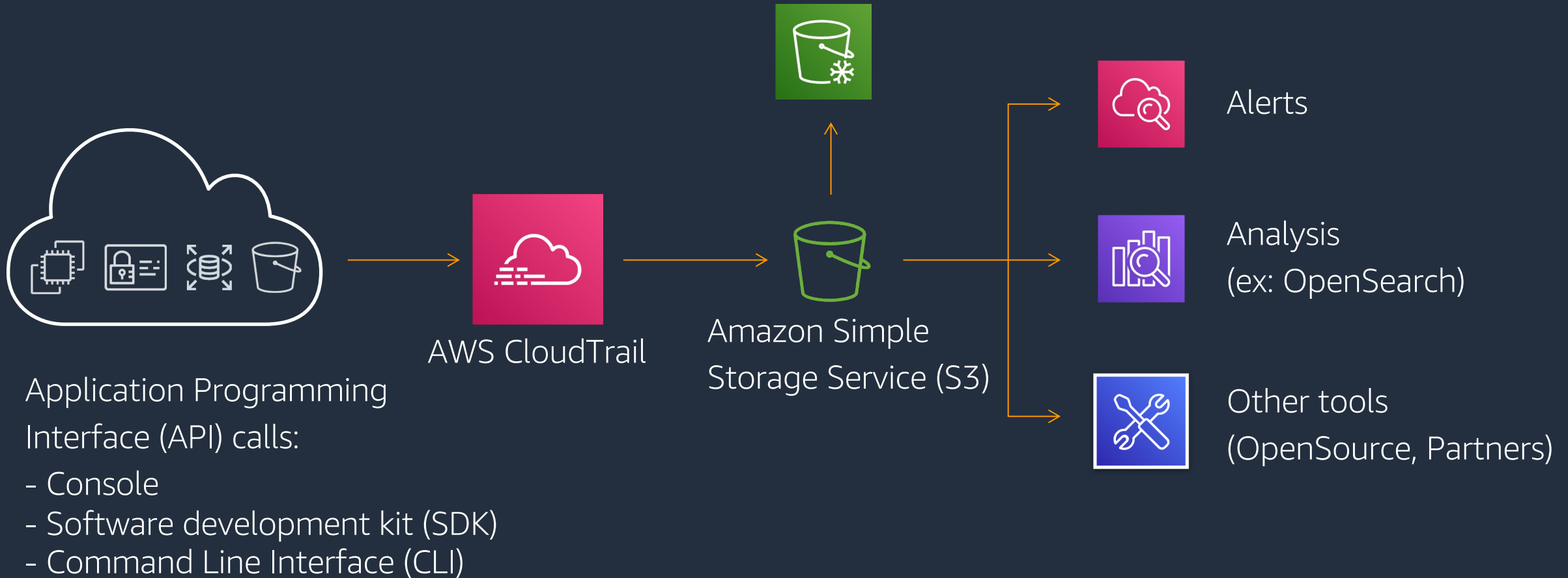


AWS CloudTrail



© 2024, Amazon Web Services, Inc. or its affiliates.

AWS CloudTrail: Audit of actions



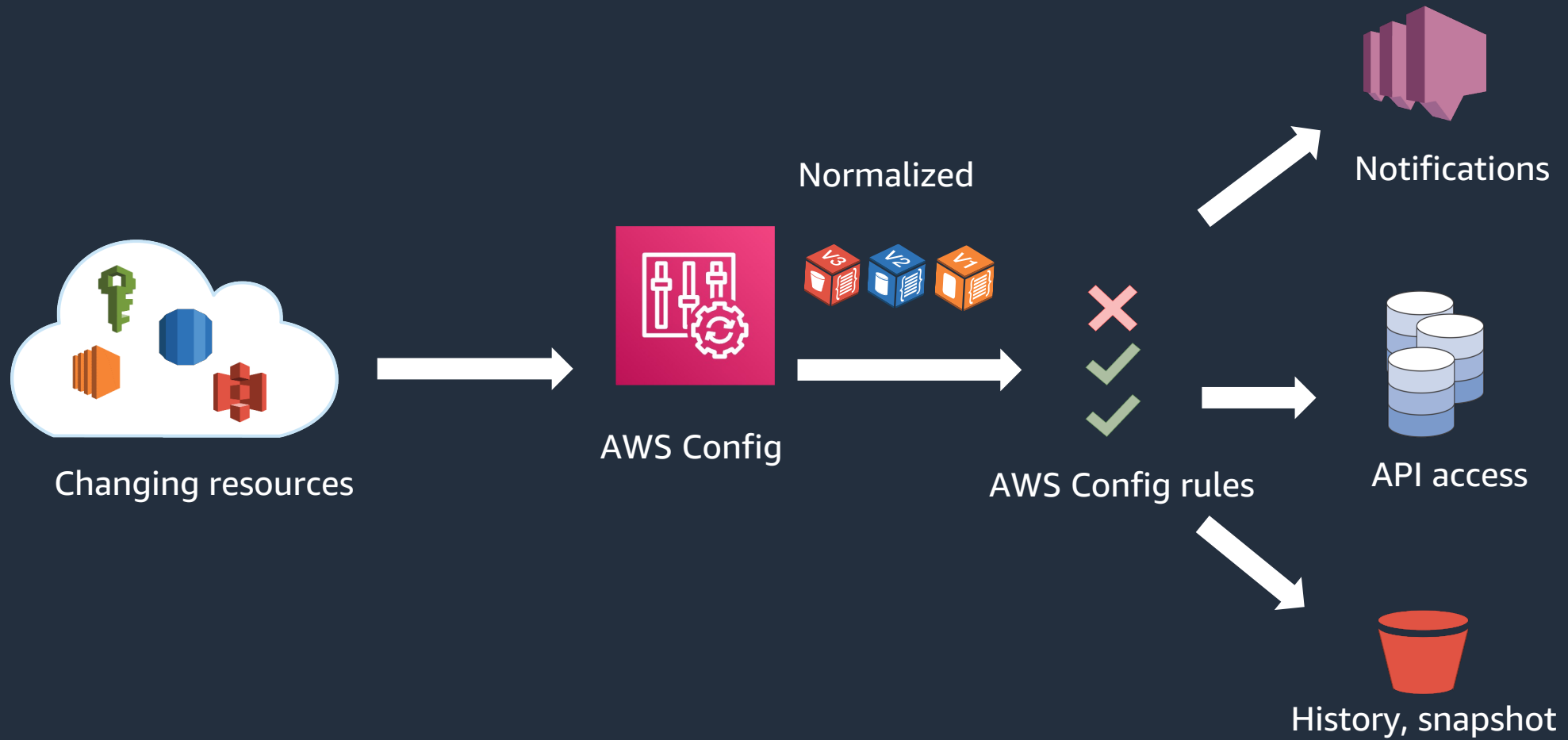


AWS Config



© 2024, Amazon Web Services, Inc. or its affiliates.

AWS Config





AWS Trusted Advisor

AWS Trusted Advisor

LEVERAGE TRUSTED ADVISOR TO ANALYZE YOUR AWS RESOURCES FOR BEST PRACTICES FOR AVAILABILITY, COST, PERFORMANCE, AND SECURITY.

Trusted Advisor

Recommendations

Cost optimization

Performance

Security

Fault tolerance

Service limits

▼ Preferences

Manage Trusted Advisor

Notifications

Checks summary

⊗ 9

Action recommended

Info

⚠ 22

Investigation recommended

Info

⊖ 0

Checks with excluded items

Info

Security checks

Filter by tag key [Learn more about using tags](#)

Tag Key

Tag Value

Reset

Apply filter

Search by keyword [Info](#)

Source

View

Filter checks

All sources

All checks

< 1 2 3 4 5 6 7 ... 14 >

▶ ⊗

Amazon ECS Containers should only have read-only access to its root filesystems

Last updated: an hour ago

🔄

Checks if ECS Containers are limited to read-only access to its mounted root filesystems.

2 of 2 resources failed this Security Hub control.

▶ ⊗

Amazon ECS task definitions should have secure networking modes and user definitions.

Last updated: an hour ago

🔄

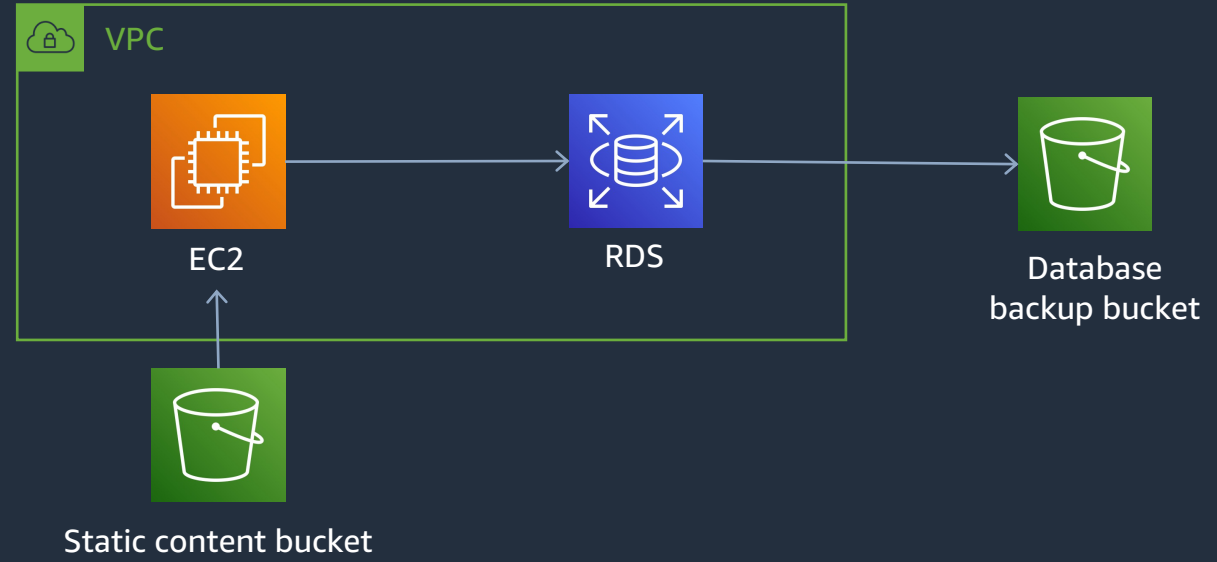
Checks if an Amazon ECS Task Definition with host networking mode has "privileged" or "user" container definitions.

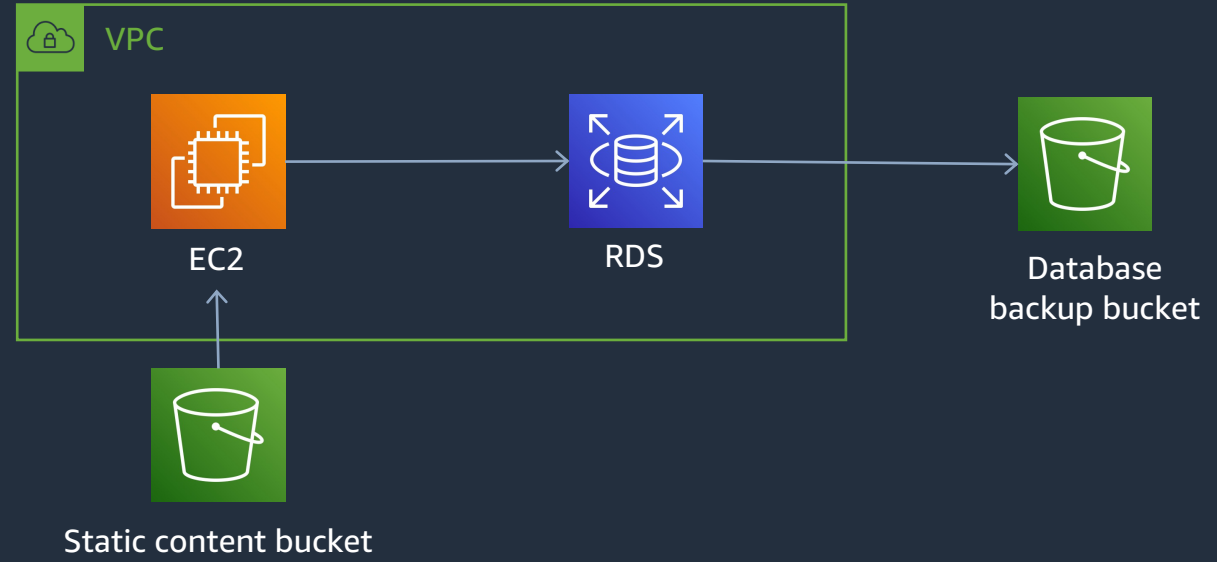
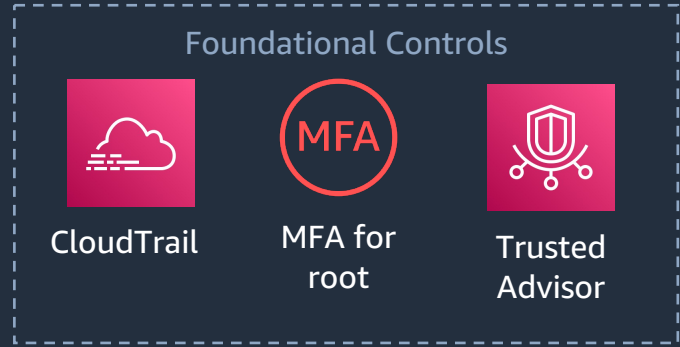
2 of 2 resources failed this Security Hub control.

© 2024, Amazon Web Services, Inc. or its affiliates.



Bob





Well Architected Framework Pillars

Identity and Access Management





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

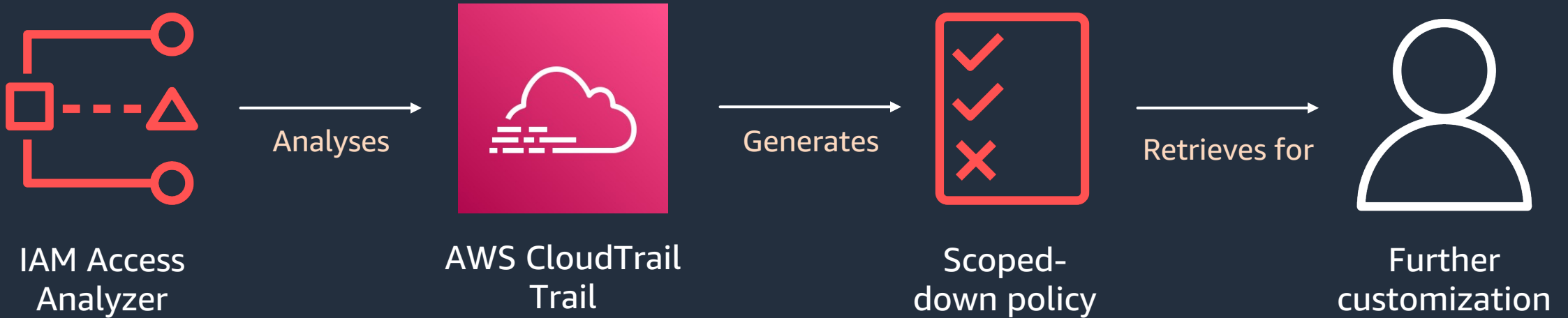


AWS Resource Access Manager

Simple, secure service for sharing AWS resources

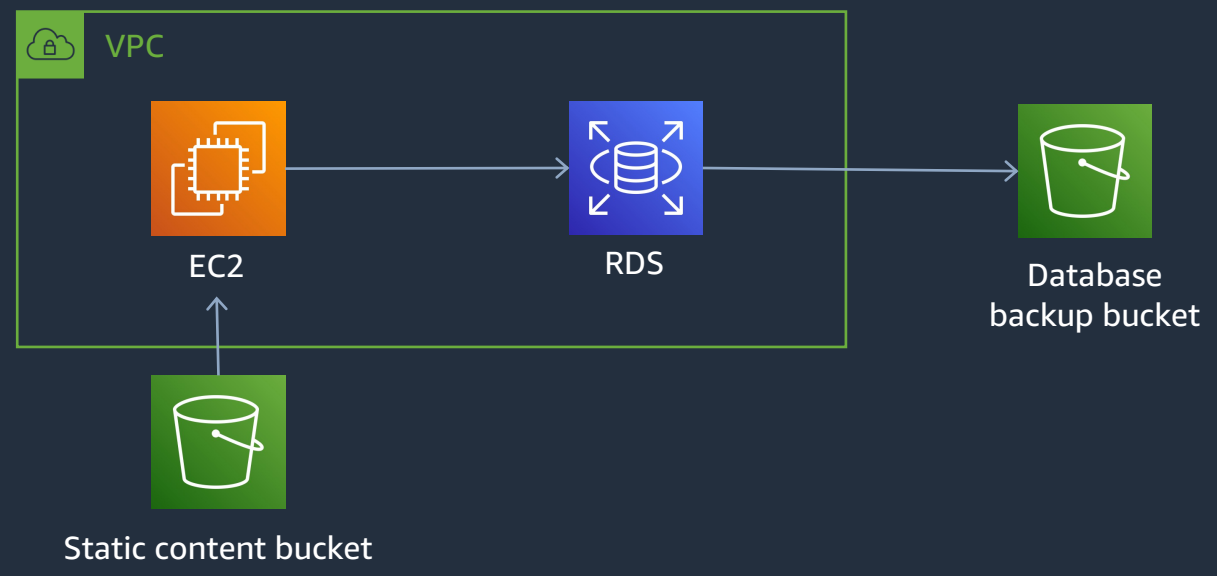
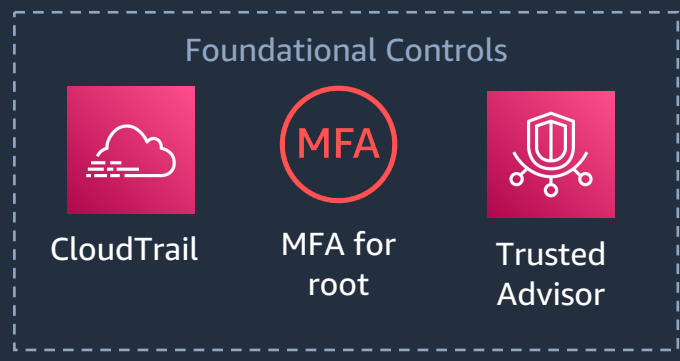
IAM Access Analyzer - Generate policies based on access activity

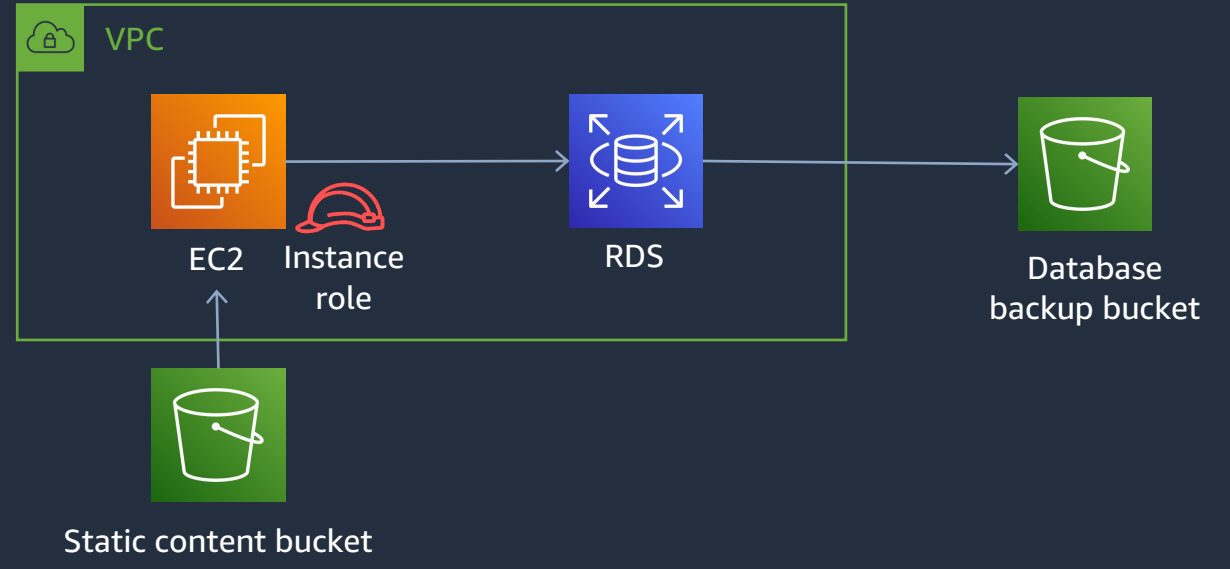
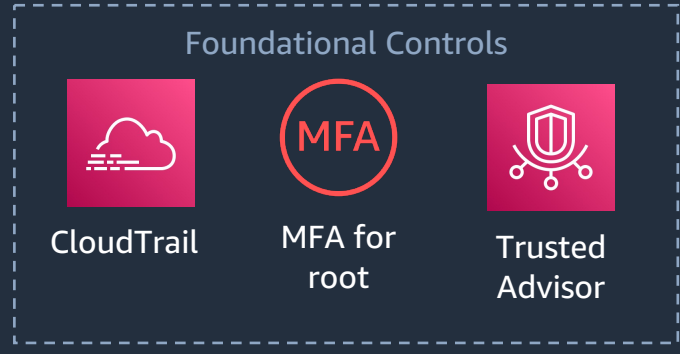
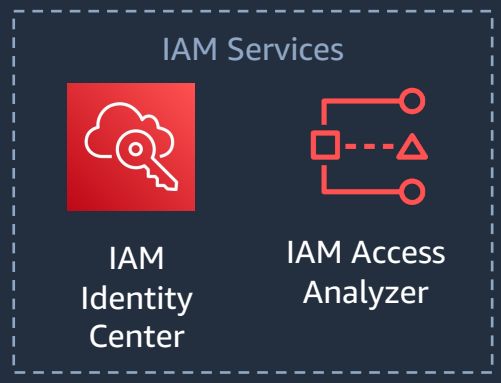
IAM Access Analyzer reviews your AWS CloudTrail logs and generates a policy template that contains the permissions that have been used by the entity in your specified time frame





Bob





Well Architected Framework Pillars

Detection





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.



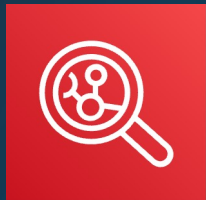
Amazon GuardDuty



© 2024, Amazon Web Services, Inc. or its affiliates.

How GuardDuty works





Amazon Inspector

Amazon Inspector

AUTOMATED AND CONTINUAL VULNERABILITY MANAGEMENT AT SCALE

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.



AMAZON ELASTIC COMPUTE CLOUD (EC2)

CONTAINER IMAGES RESIDING IN AMAZON ELASTIC
CONTAINER REGISTRY (AMAZON ECR)

AWS LAMBDA FUNCTIONS

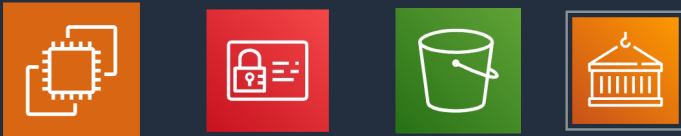


AWS Security Hub

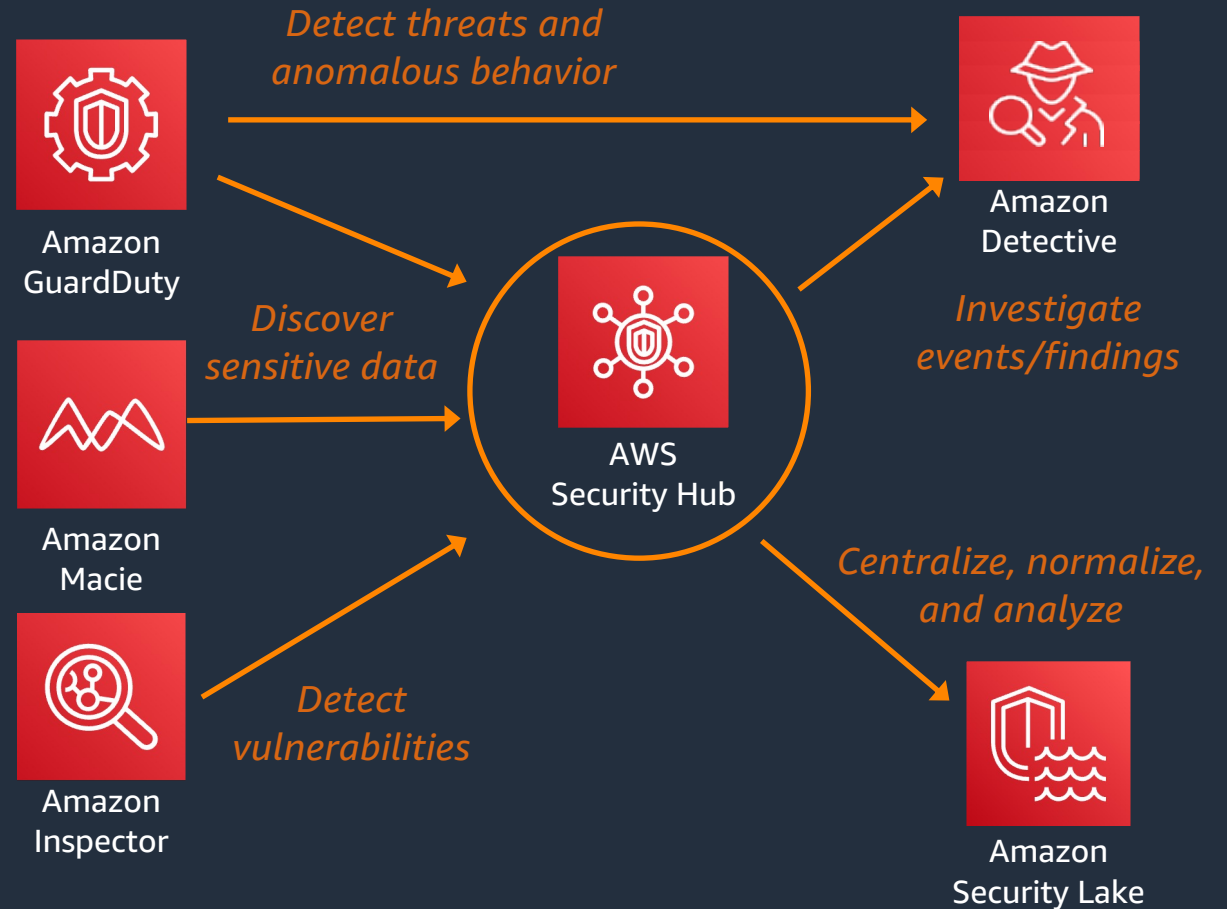
Threat detection, monitoring, and response



Security monitoring and threat detection



Integrated with AWS Workloads in an AWS Account, along with identities, and network activity



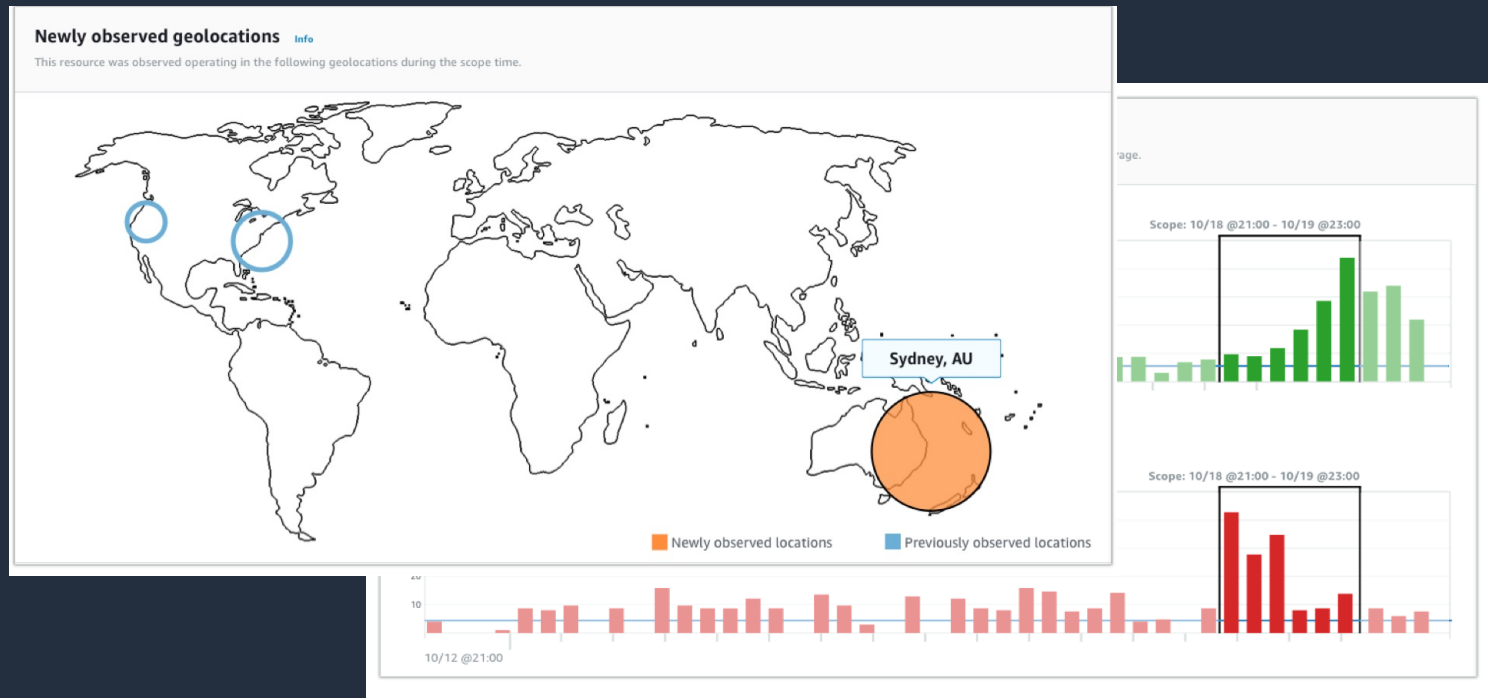


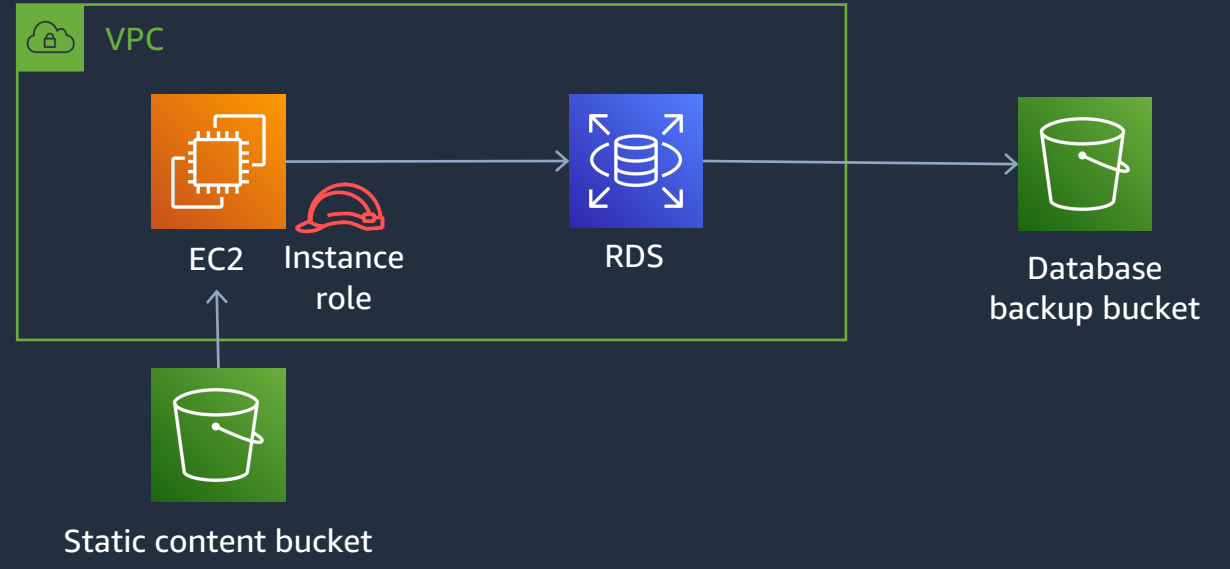
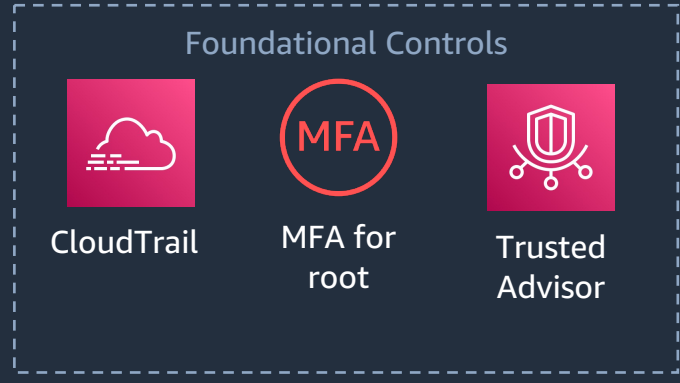
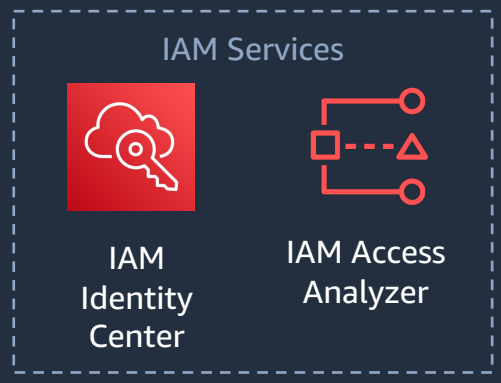
Amazon Detective

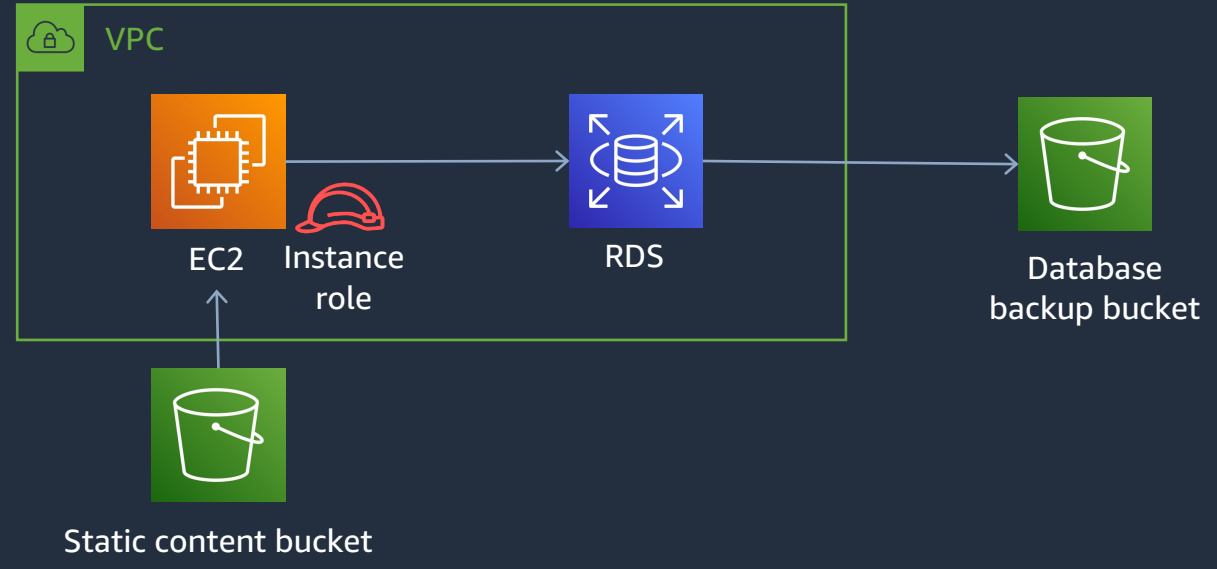


Amazon Detective

Analyze and visualize security data to rapidly get to the root cause of potential security issues







Well Architected Framework pillars

Infrastructure security





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 (Web Access Firewall)

Protects your web applications from common exploits.



Amazon Virtual Private Cloud

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



AWS PrivateLink

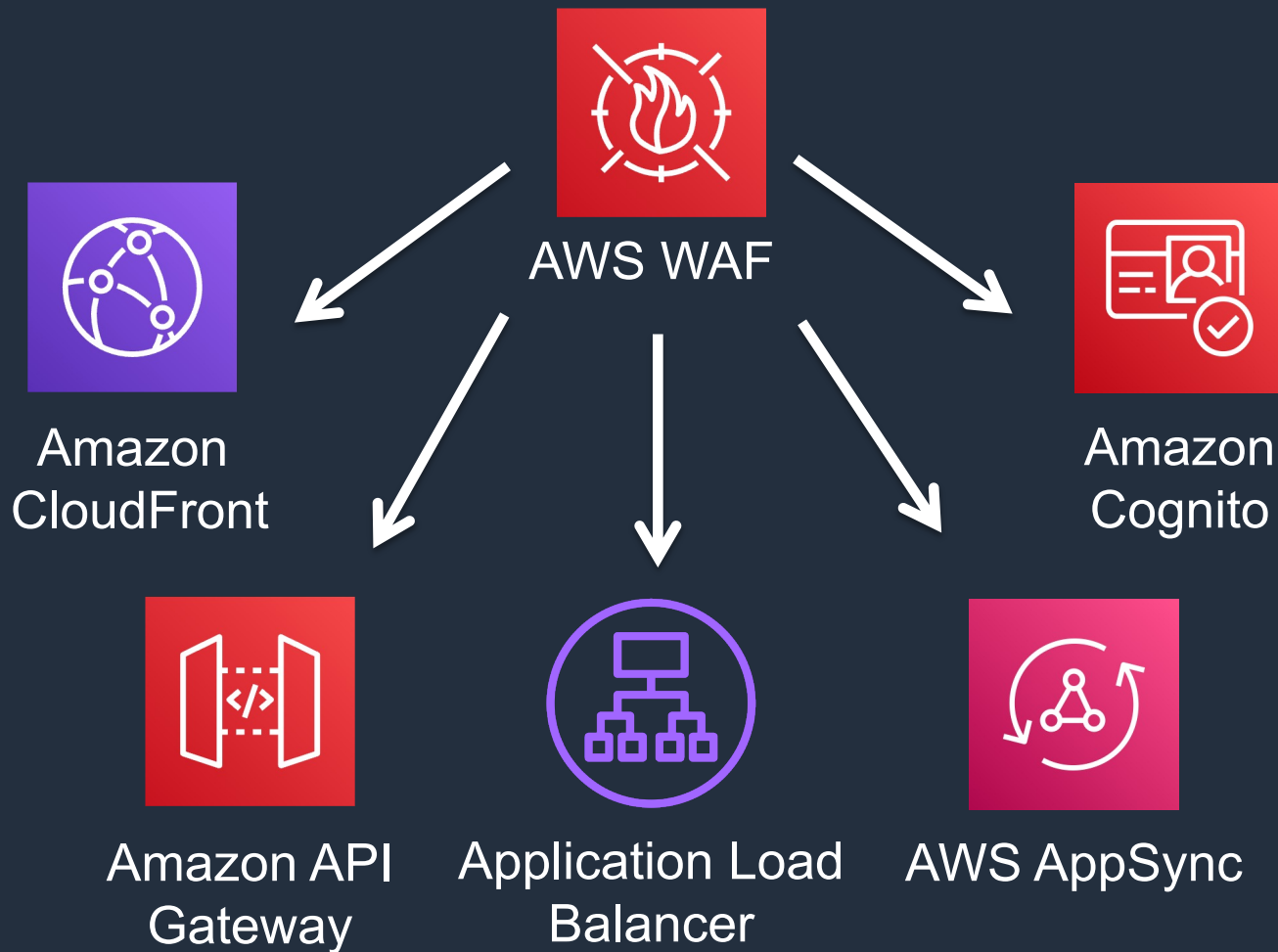
Establish connectivity between VPCs and AWS services without exposing data to the internet.



AWS Systems Manager

Gain operational insights into AWS and on-premises resources.

AWS WAF - Layer 7 protection



- Managed, elastic, and integrated WAF
- Pay-as-you-go
- Rules managed by AWS
+ Custom rules
+ Provided by partners



DDoS protection with AWS Shield

Standard



Available to all AWS customers at no additional cost

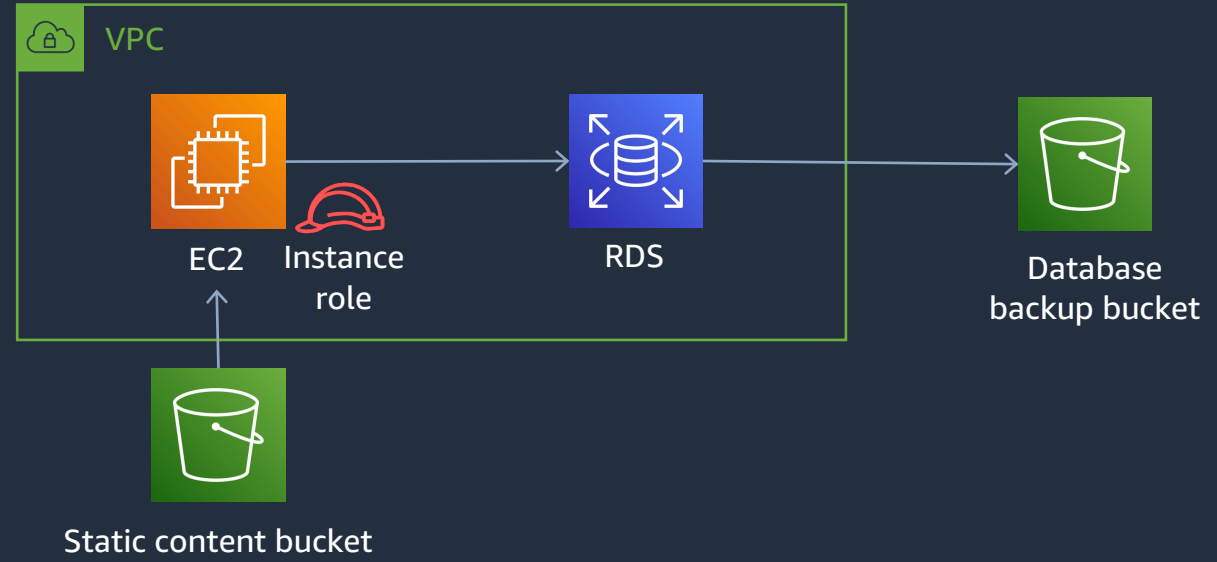
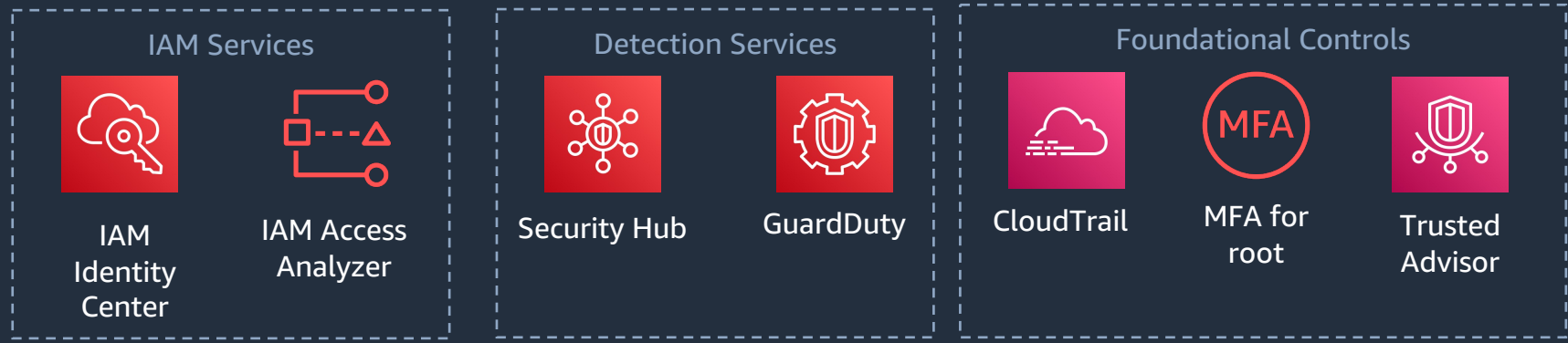
- Protection against the most common attacks (SYN/UDP Floods, Reflection Attacks, etc. Layer 3/4)
- Automatic detection and mitigation

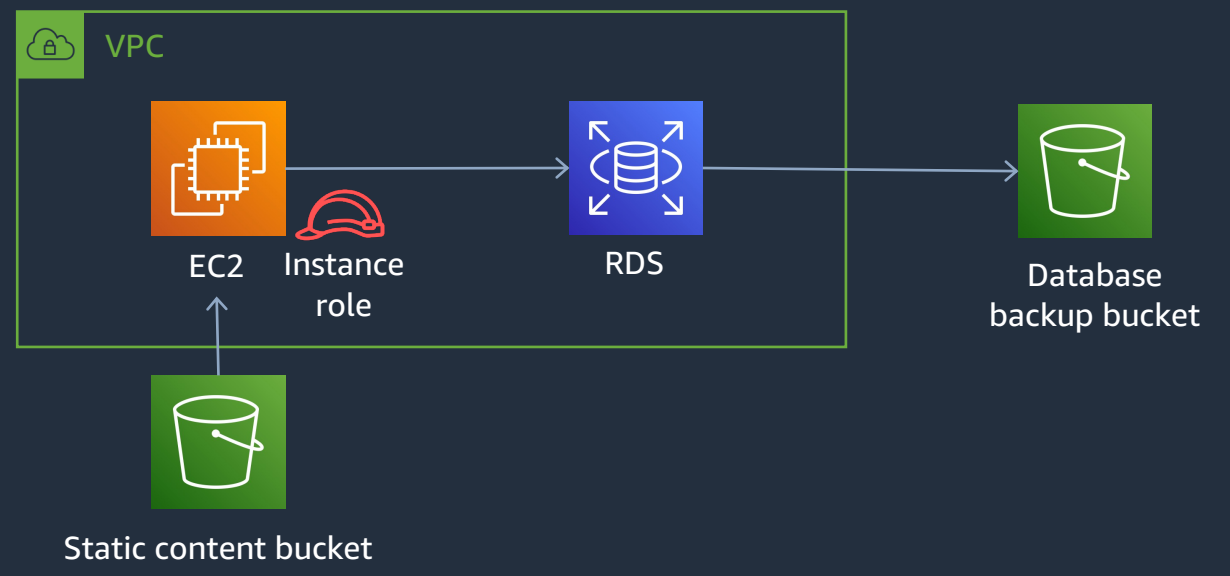
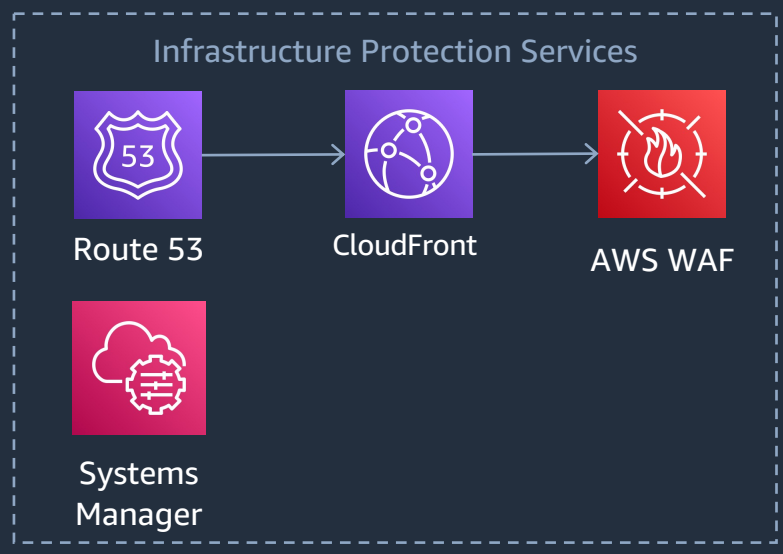
Advanced



Paid service that provides additional protection against sophisticated attacks

- + Protection against advanced attacks (Layer 7)
- + 24x7 DDoS Response Team (proactive/reactive)
- + Cost protection
- + Faster mitigation/better visualization
- + Includes WAF and Firewall Manager





Well Architected Framework Pillars

Data protection





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.





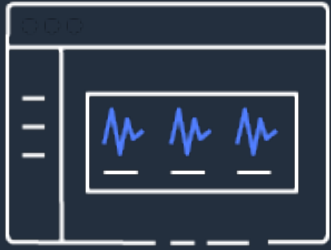
Amazon Macie



© 2024, Amazon Web Services, Inc. or its affiliates.

Amazon Macie

Discover and protect your sensitive data at scale



Gain visibility and evaluate

- Bucket inventory
- Bucket policies



Discover sensitive data

- Inspection jobs
- Flexible scope



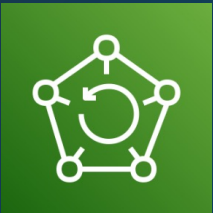
Centrally manage at scale

- AWS Organizations
- Managed and custom data detections



Automate and take actions

- Detailed findings
- Management APIs



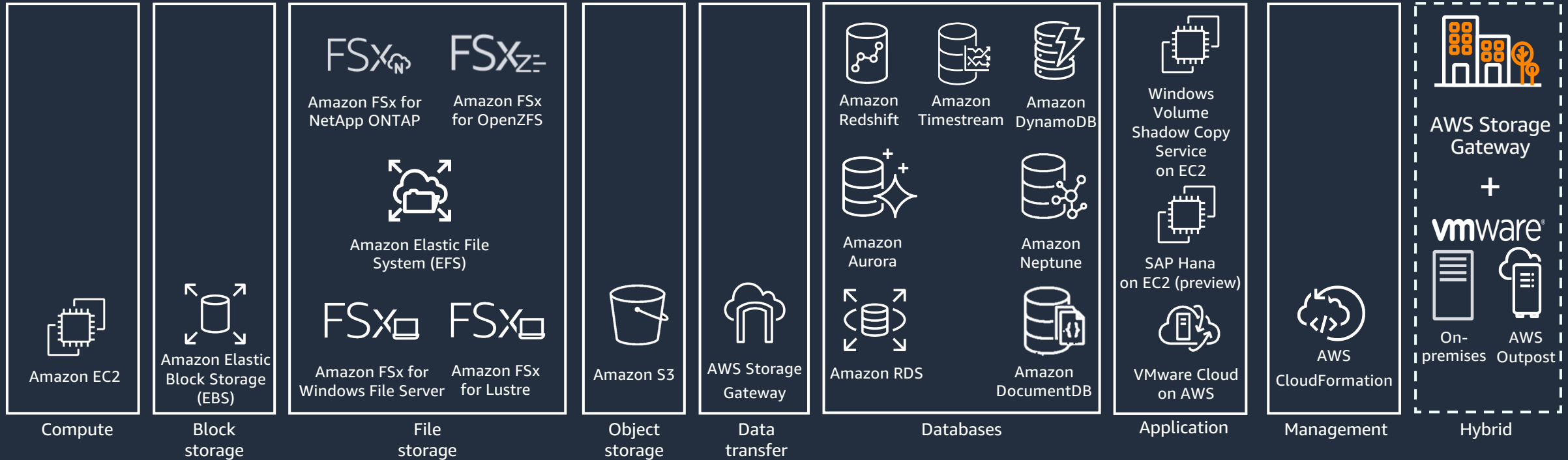
AWS Backup

Overview of AWS Backup



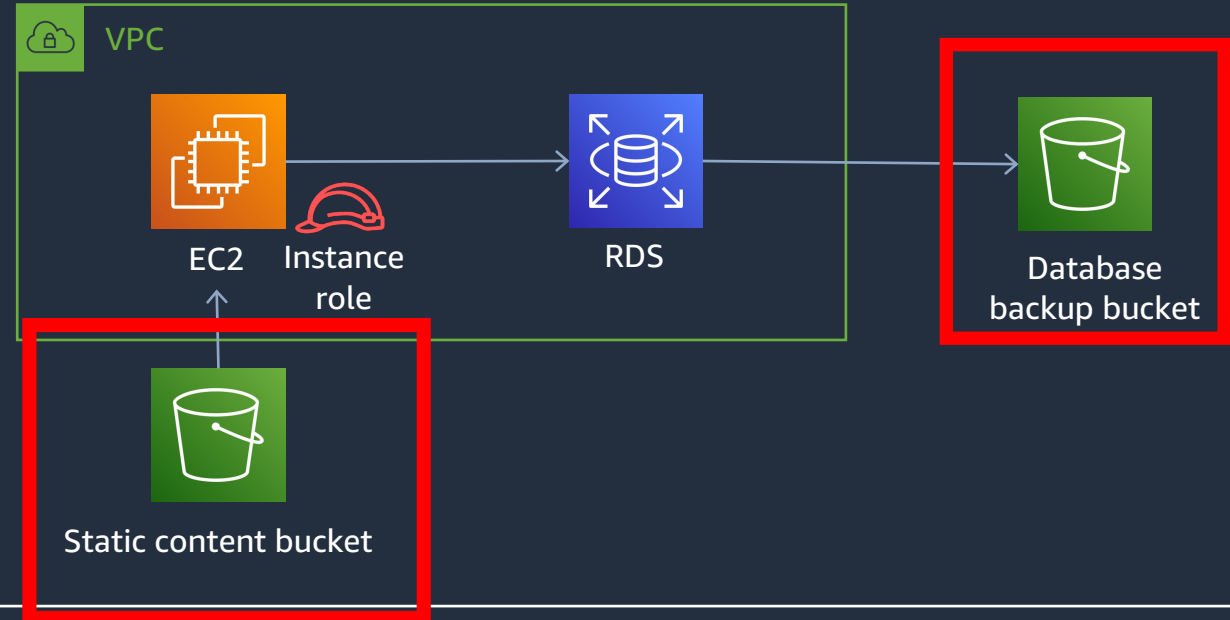
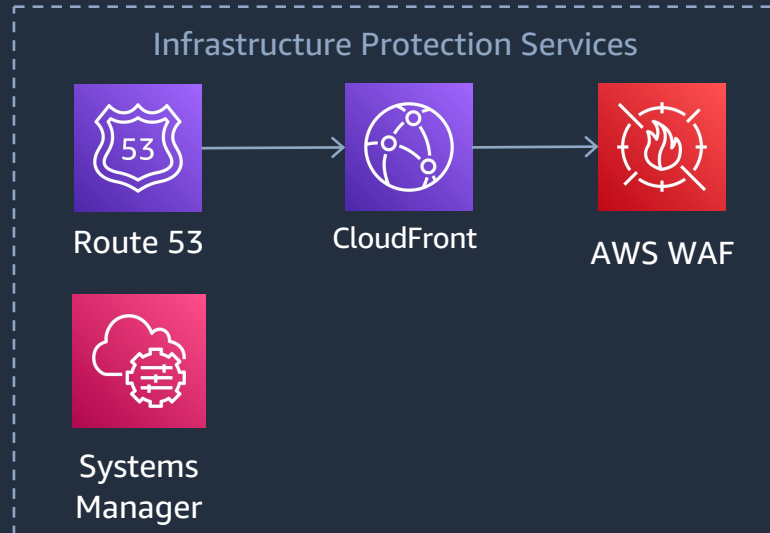
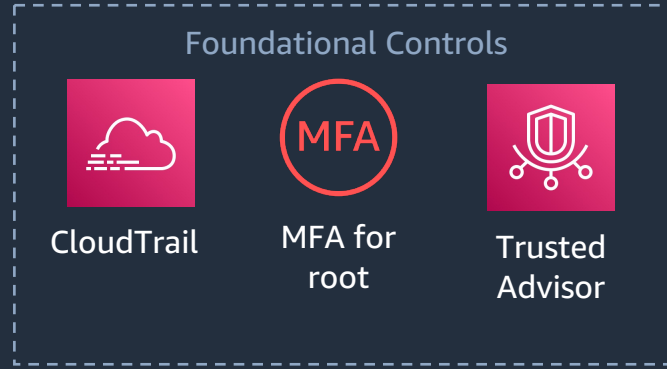
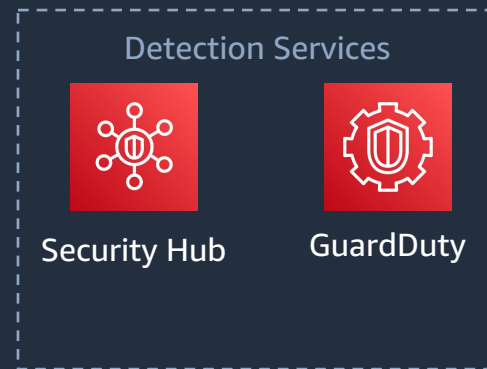
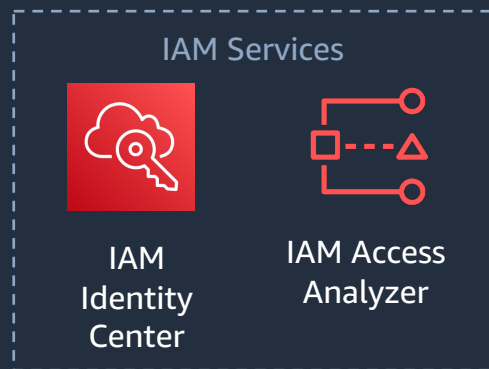
AWS Backup

A fully managed, policy-based backup service that makes it simple to centrally manage and automate the backup of data across multiple AWS services and hybrid workloads



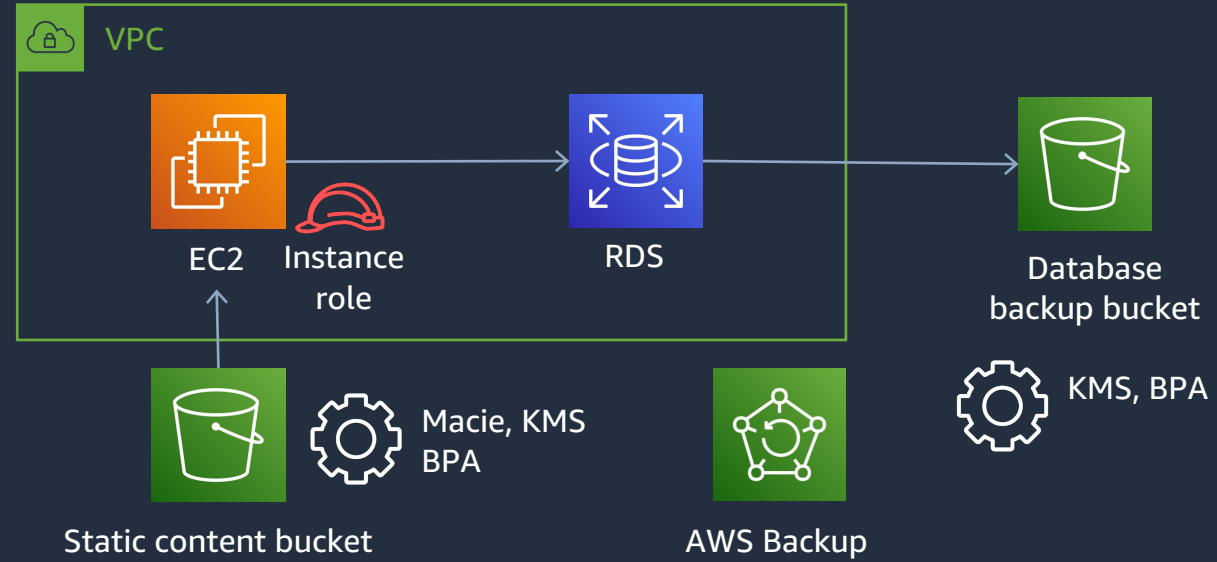
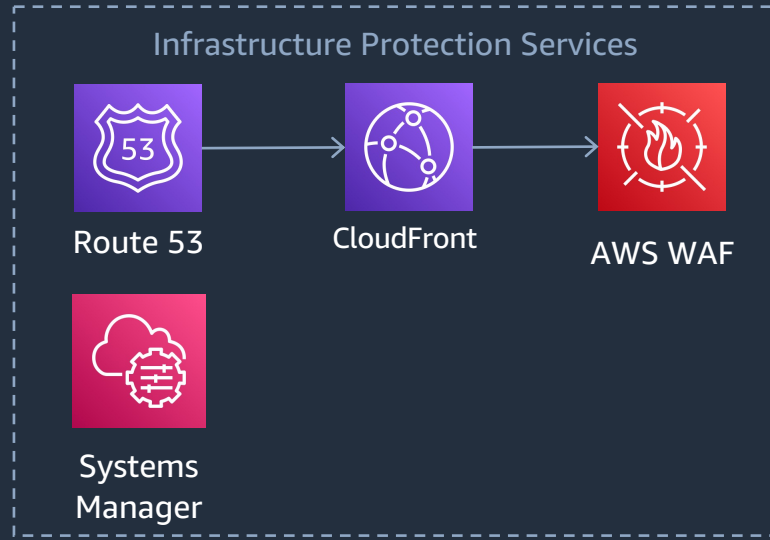
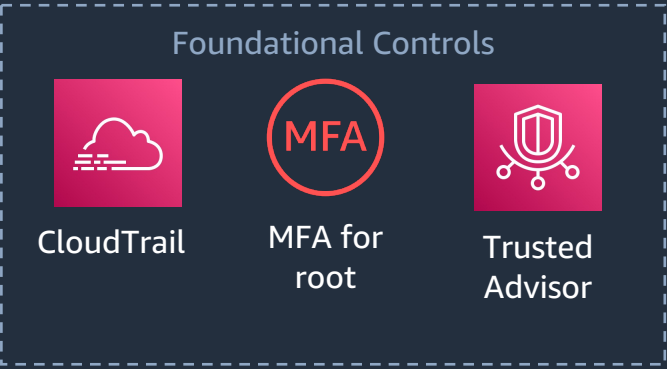
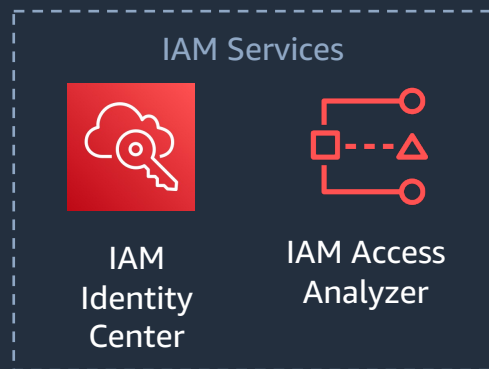


Bob





Bob



Well Architected Framework Pillars

Incident response





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

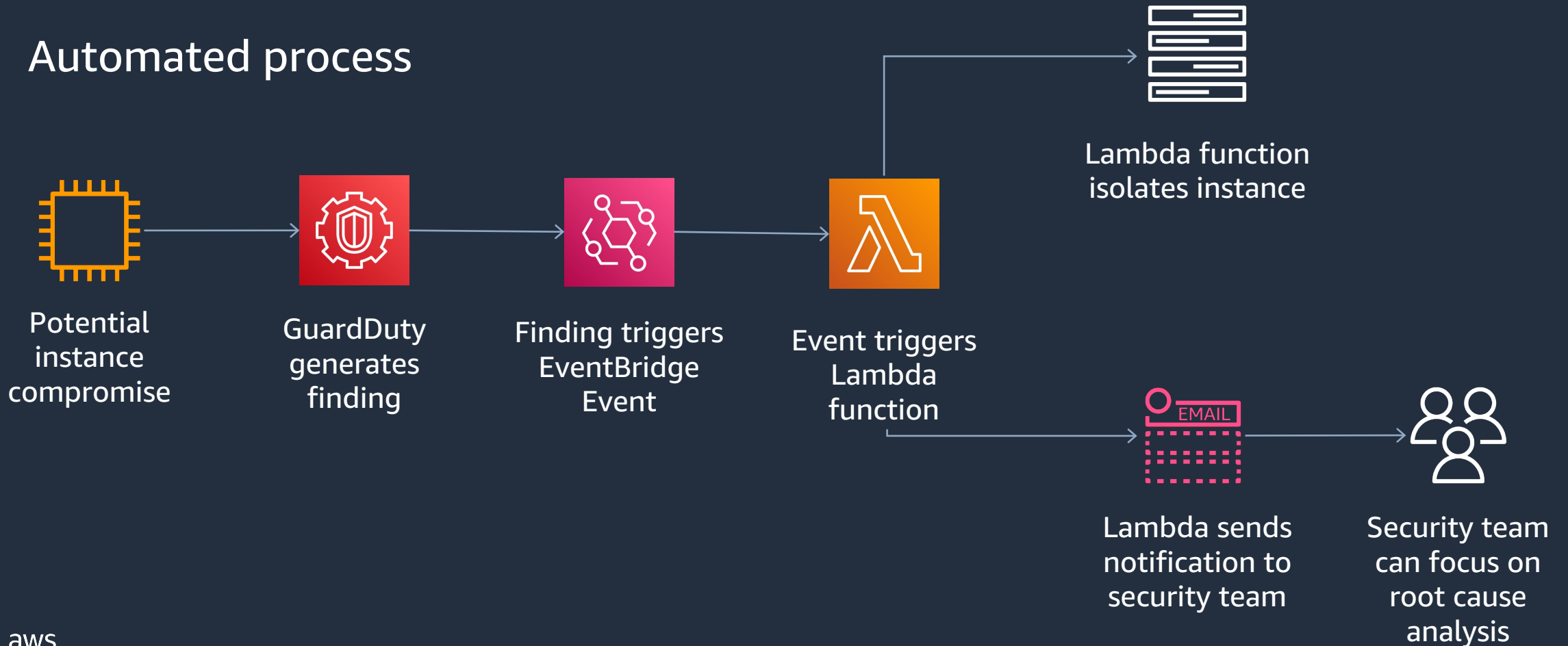


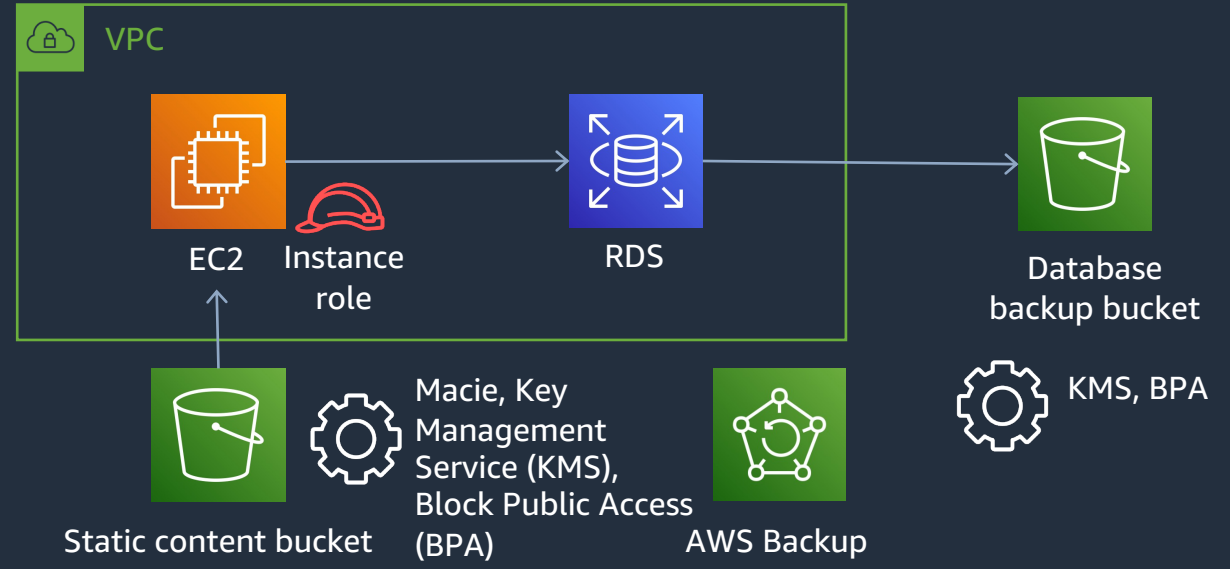
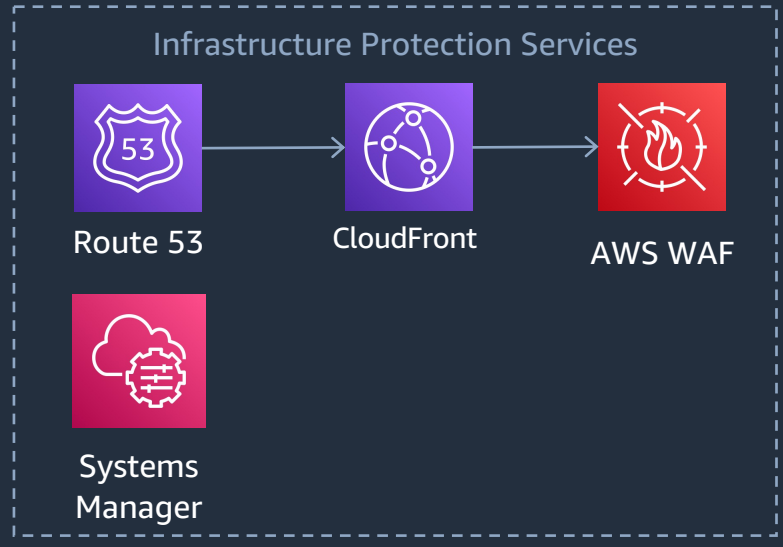
AWS Elastic Disaster Recovery

Fast, automated, cost effective disaster recovery

Automated Incident Response – simple example

Automated process







Bob




Mary




Incident response runbooks



IAM Services



IAM Identity Center



IAM Access Analyzer

Detection + IR Services



Security Hub



GuardDuty

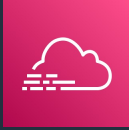


EventBridge




Lambda


Foundational Controls



CloudTrail

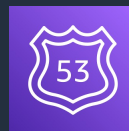


MFA for root

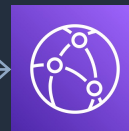


Trusted Advisor


Infrastructure Protection Services




Route 53



CloudFront

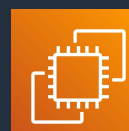


AWS WAF




Systems Manager

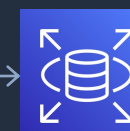
VPC



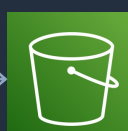
EC2



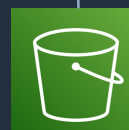
Instance role




RDS




Database backup bucket




Static content bucket



Macie, Key Management Service (KMS), Block Public Access (BPA)



AWS Backup



KMS, BPA

Call to action

- Connect with the account team
- Ask the Experts

AWS Services Discussed

AWS Services Presented	Additional Information
AWS CloudTrail	https://aws.amazon.com/cloudtrail/
AWS Config	https://aws.amazon.com/config/
AWS Trusted Advisor	https://aws.amazon.com/premiumsupport/technology/trusted-advisor/
Amazon GuardDuty	https://aws.amazon.com/guardduty/
Amazon Inspector	https://aws.amazon.com/inspector/
AWS SecurityHub	https://aws.amazon.com/security-hub/
Amazon Detective	https://aws.amazon.com/detective/
AWS WAF	https://aws.amazon.com/waf/
AWS Shield	https://aws.amazon.com/shield/
Amazon Macie	https://aws.amazon.com/macie/
AWS Backup	https://aws.amazon.com/backup/
Amazon EventBridge	https://aws.amazon.com/eventbridge/
AWS Lambda	https://aws.amazon.com/lambda/



Thank you!

Matt Duncan

dncmatt@amazon.com

David Stielstra

dstiel@amazon.com

Please complete this survey:



Session: Security is top priority