
AWS
re:Invent

ARC317

Applying the principles of the AWS Well-Architected security pillar

Garvit Singh

Solutions Developer

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

AWS Well-Architected Framework – Security pillar

Reference implementations

- AWS Security Hub automated response and remediation solution
- Centralized WAF and security group management solution

Demo

Key features

Call to action



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The 5 pillars of the Well-Architected Framework



See also re:Invent 2020 session SEC314 – Security Best Practices / Ben Potter



Detection

- Identify potential security misconfigurations, threats, or unexpected behavior
- Ensure the highest security standards and fulfill compliance obligations
- Automate detection and remediation techniques to help you scale



Infrastructure protection

- Protection at layers 3–7 for your network resources and applications
- Ensure consistent security posture across your organization
- Automate infrastructure protection to help you scale

AWS Security Hub automated response and remediation



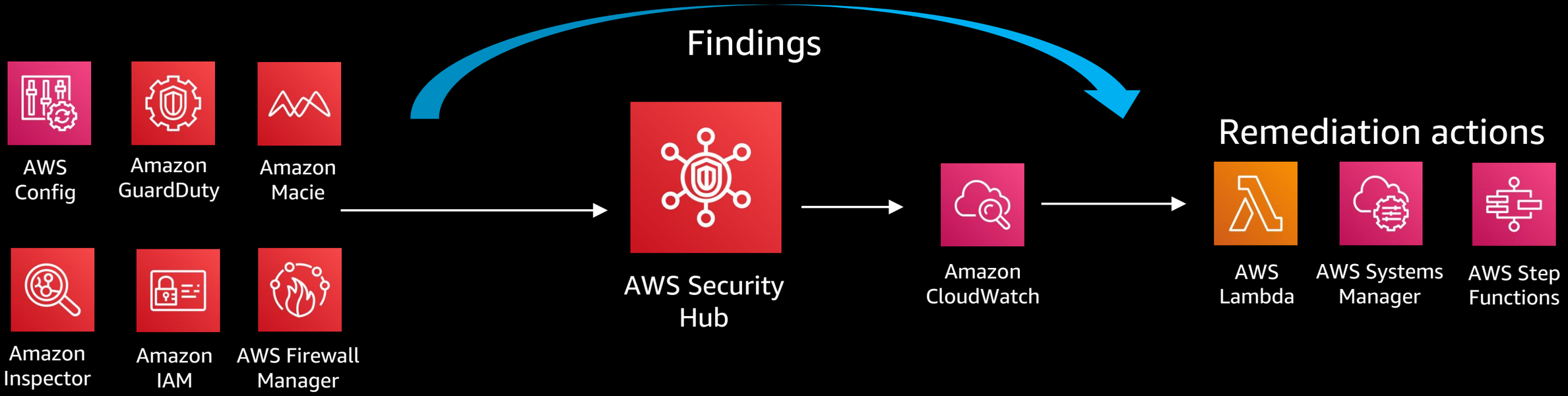
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Hub



Centralized detection and management of security alerts
Automate compliance checks and remediations



https://aws.amazon.com/security-hub/

AWS Security Hub Automated Response and Remediation

View implementation guide

What does this AWS Solutions Implementation do?

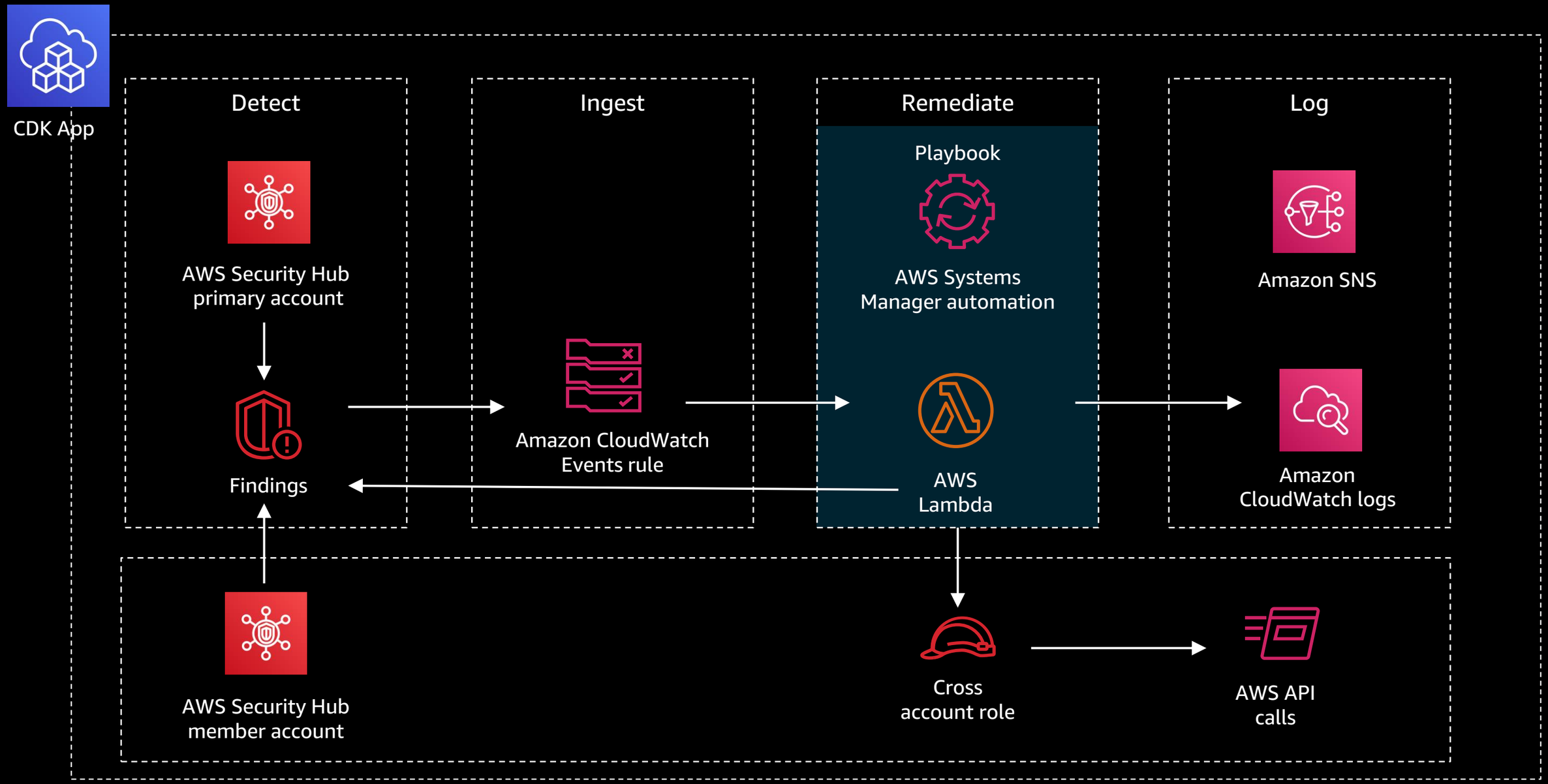
The continued evolution of security threats makes it difficult, expensive, and time-consuming for security teams to react. The AWS Security Hub Automated Response and Remediation solution addresses this challenge by providing predefined response and remediation actions based on industry compliance standards and best practices.

AWS Security Hub Automated Response and Remediation is an add-on solution that works with AWS Security Hub to provide a ready-to-deploy architecture and a library of automated playbooks. The solution makes it easier for AWS Security Hub customers to resolve common security findings and to improve their security posture in AWS.

The solution creates an AWS Service Catalog Portfolio of predefined security response and remediation actions called *playbooks*. Customers choose the individual playbooks they want to deploy in their Security Hub primary account. Each playbook contains the necessary custom actions, Identity and Access Management (IAM) roles, Amazon CloudWatch Events, Systems Manager Automation documents, AWS Lambda functions, and AWS Step Functions needed to start a remediation workflow within a single AWS account, or across multiple accounts.

AWS Solutions Implementation overview

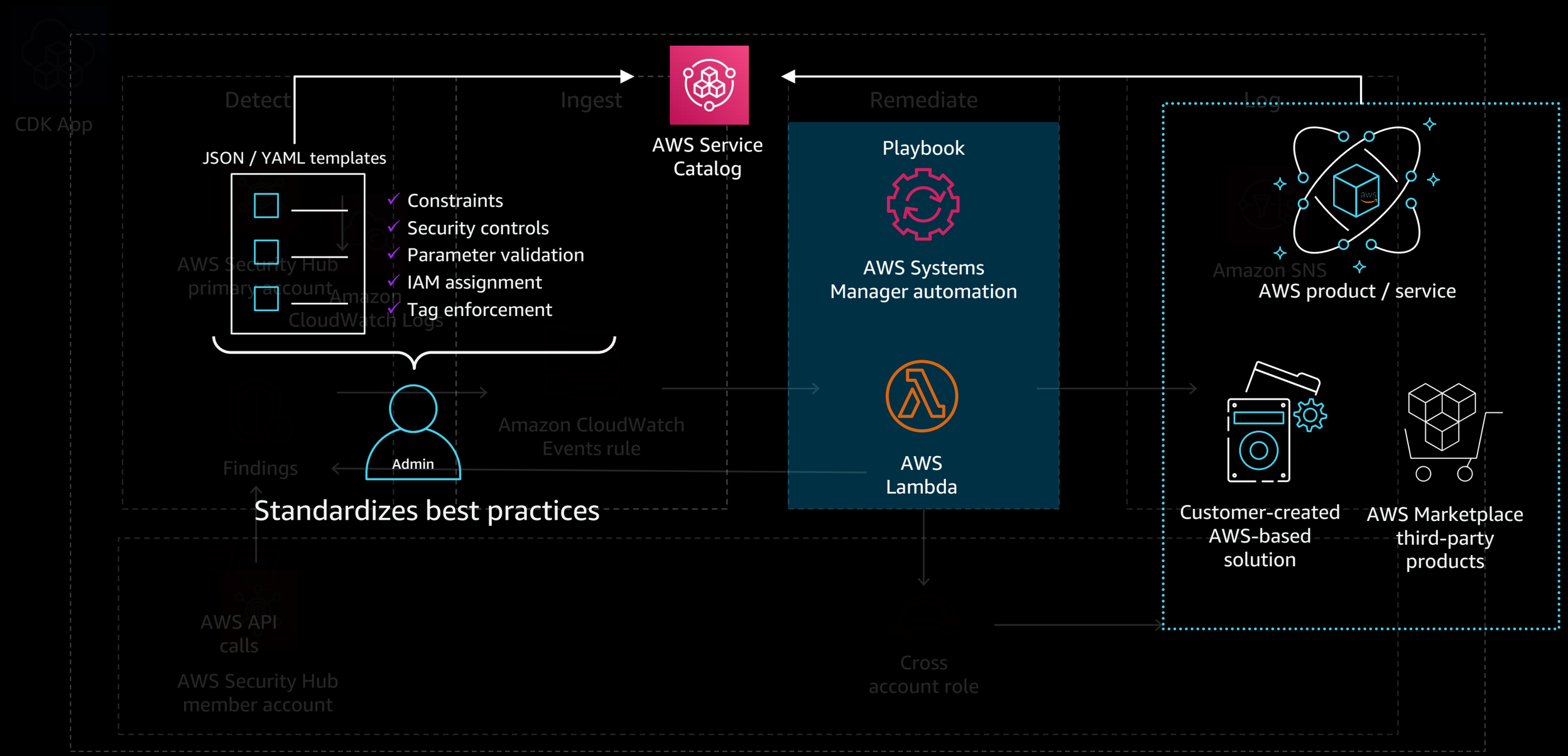
Architecture



Design decisions



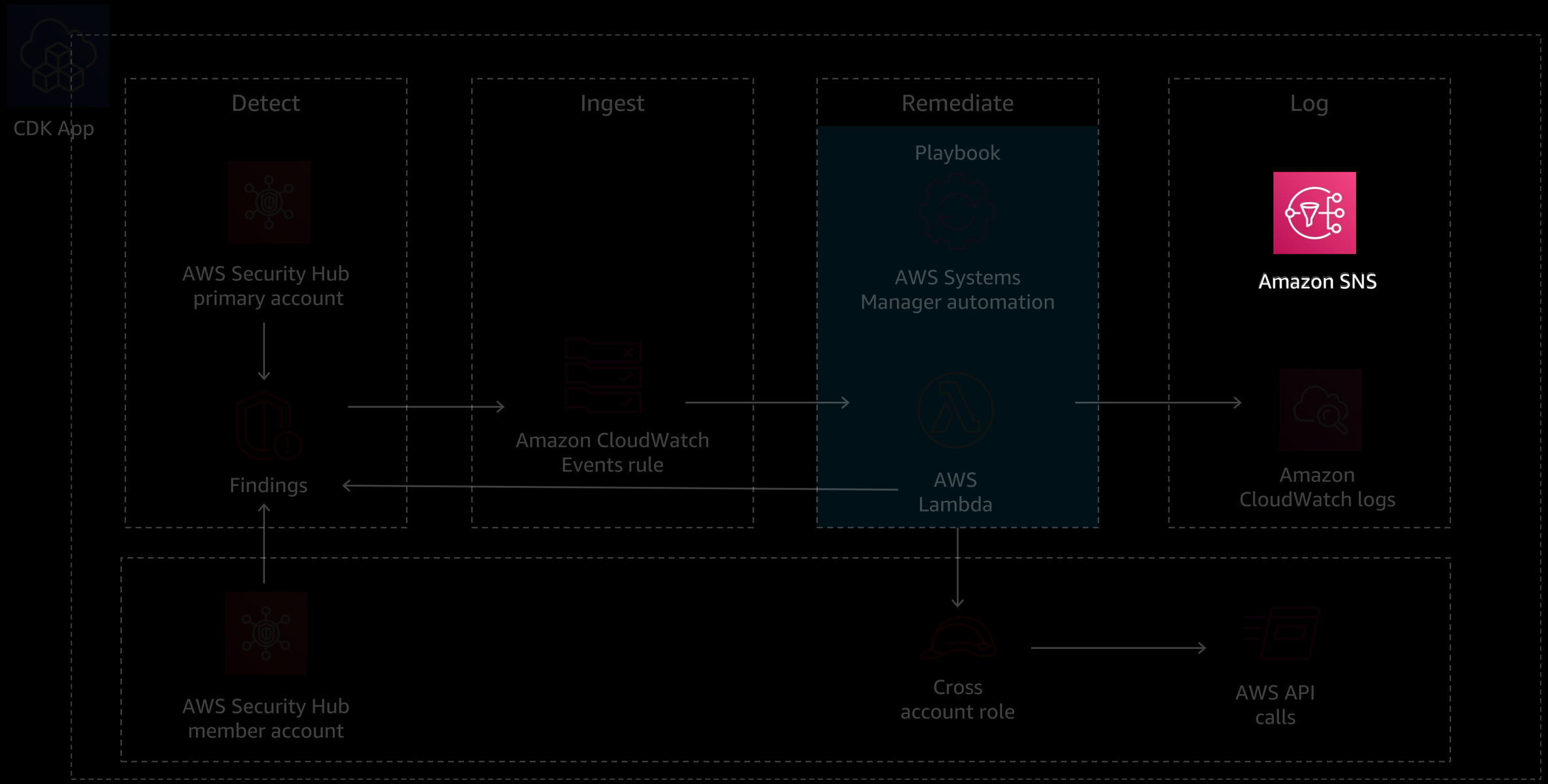
Design decisions



Design decisions



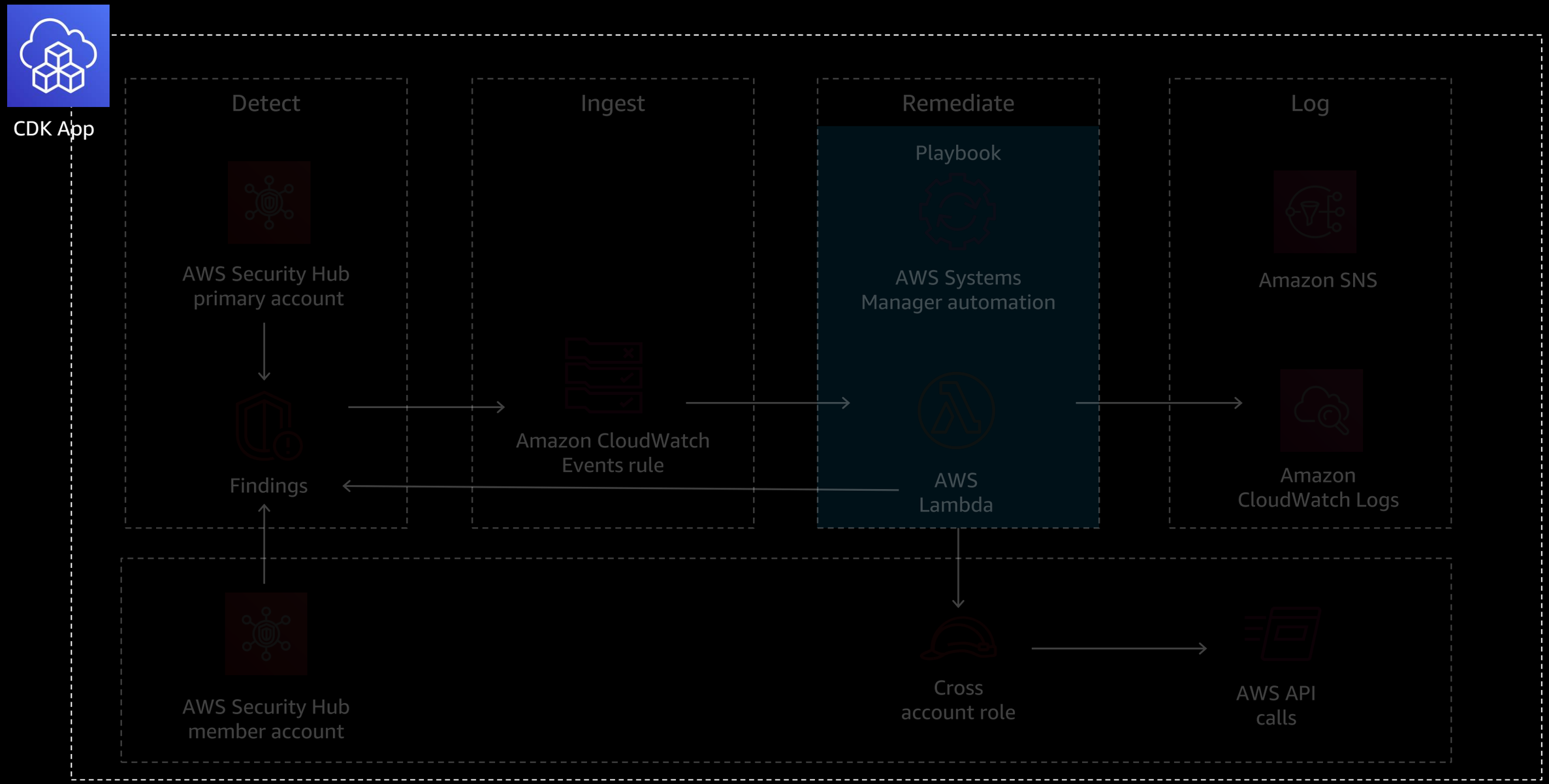
Design decisions



Design decisions



Design decisions



Key features



- Remediates Security Hub findings from the AWS console
- Deploys easily across Security Hub member accounts
- Remediates findings across accounts
- Supports automatic and immediate remediation in response to new findings
- Supports many of the CIS v1.2.0 controls
- Uses AWS CDK constructs, open sourced, to allow solution extension

Centralized WAF and VPC security group management



AWS re:Invent

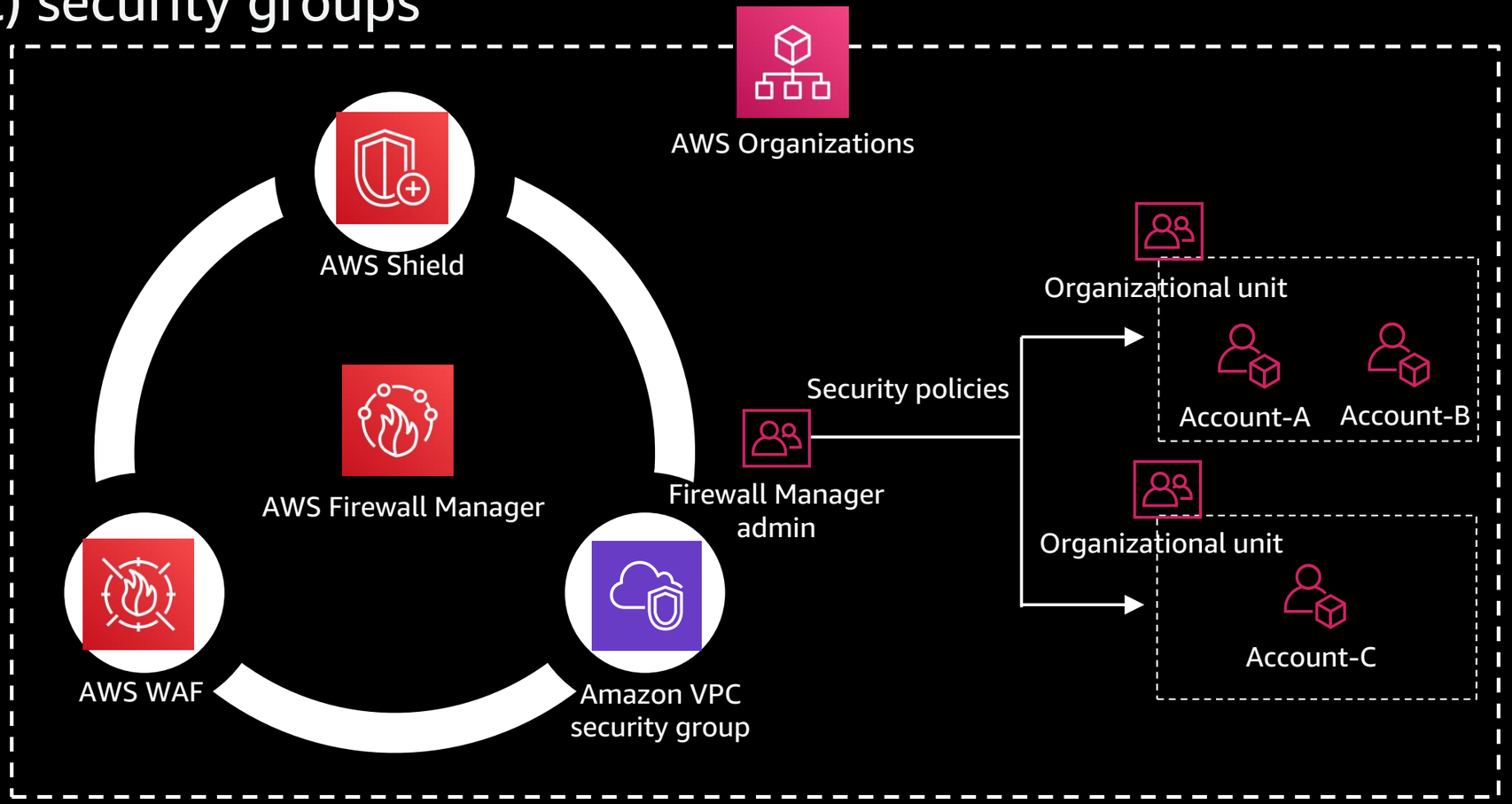
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Firewall Manager



Configures, manages, and audits firewall rules across your accounts

Deploys managed rules for WAF and audit checks for virtual private cloud (VPC) security groups



https://aws.amazon.com/firewall-manager/

AWS Centralized WAF and VPC Security Group Management

View implementation guide

What does this AWS Solutions Implementation do?

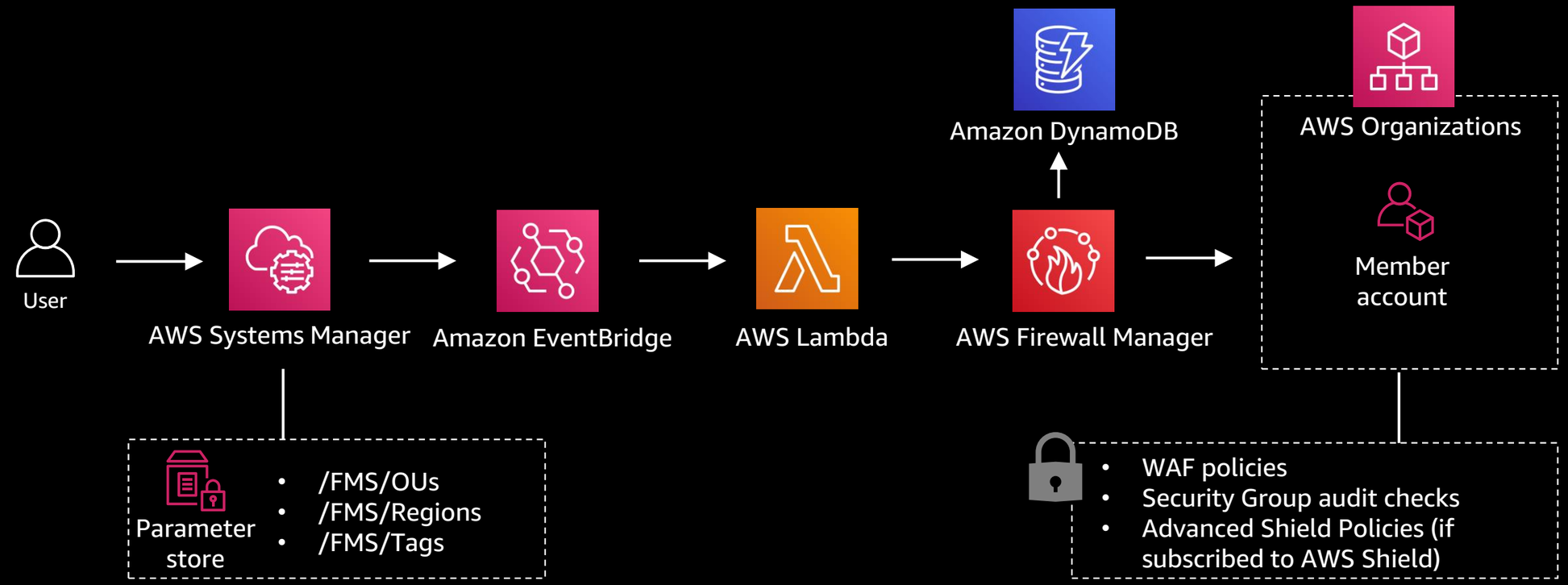
The AWS Centralized WAF and VPC Security Group Management solution allows you to centrally configure, manage, and audit firewall rules across all your accounts and resources in AWS Organizations. This solution is a reference implementation to automate the process to setup AWS Firewall Manager security policies.

This solution provides pre-configured rules that can be deployed across accounts to (1) configure application-level firewalls for Web Application Firewall (WAF) and (2) audit unused and overly permissive virtual private cloud (VPC) security groups. It allows you to automatically enable the prerequisites required to use Firewall Manager, so you can spend more time focusing on your specific security needs.

This solution helps AWS enterprise customers create a quick baseline of firewall security rules across Layers 3-7 resources and maintain a consistent security posture within their organization. Additionally, this solution deploys Shield Advanced policies for customers who subscribe to AWS Shield Advanced, to protect against Distributed Denial of Service (DDoS) attacks to their AWS accounts.

Note: This solution must be installed in your Firewall Manager admin account. If you have not already set up Firewall Manager, refer to the Implementation Guide for the steps.

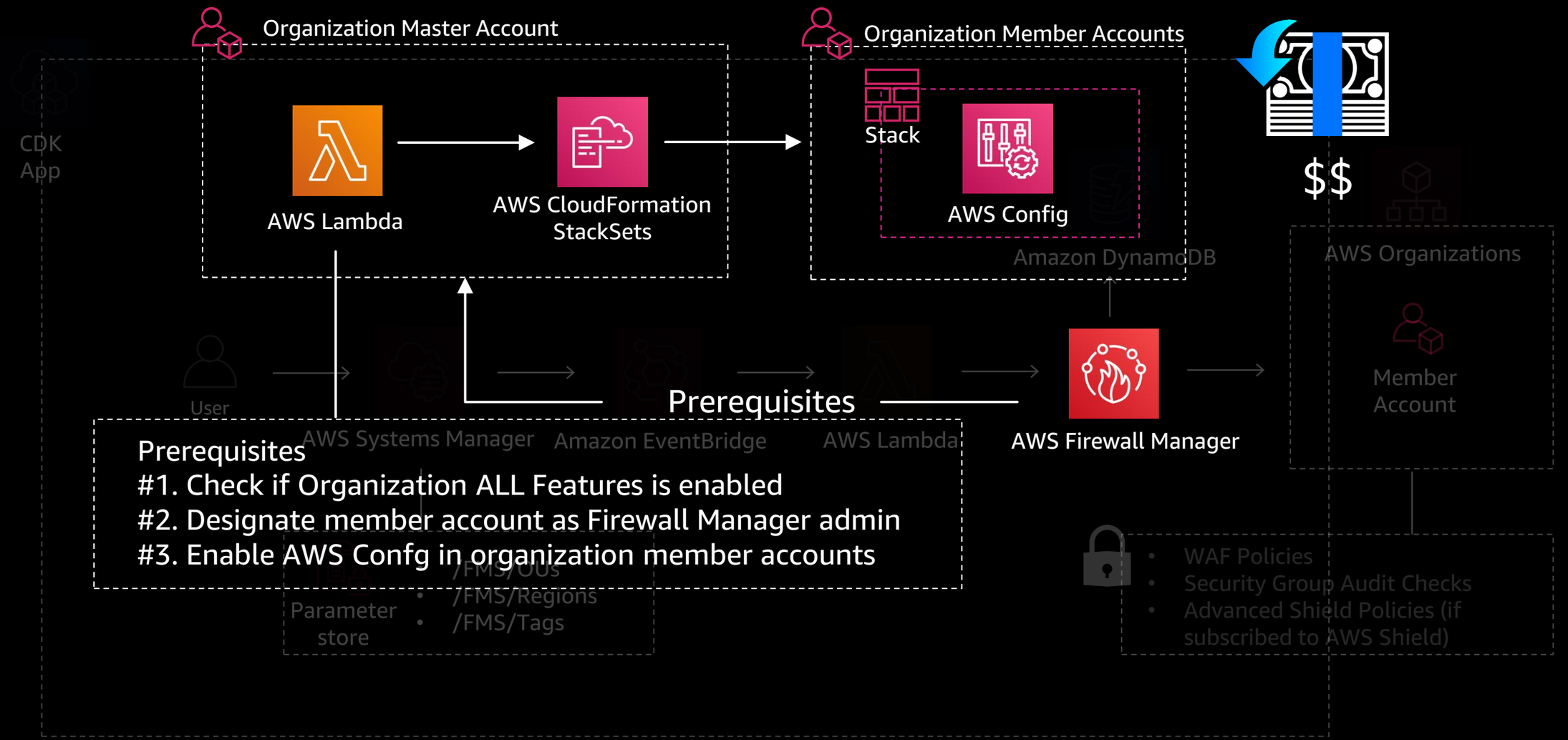
Architecture



Design decisions



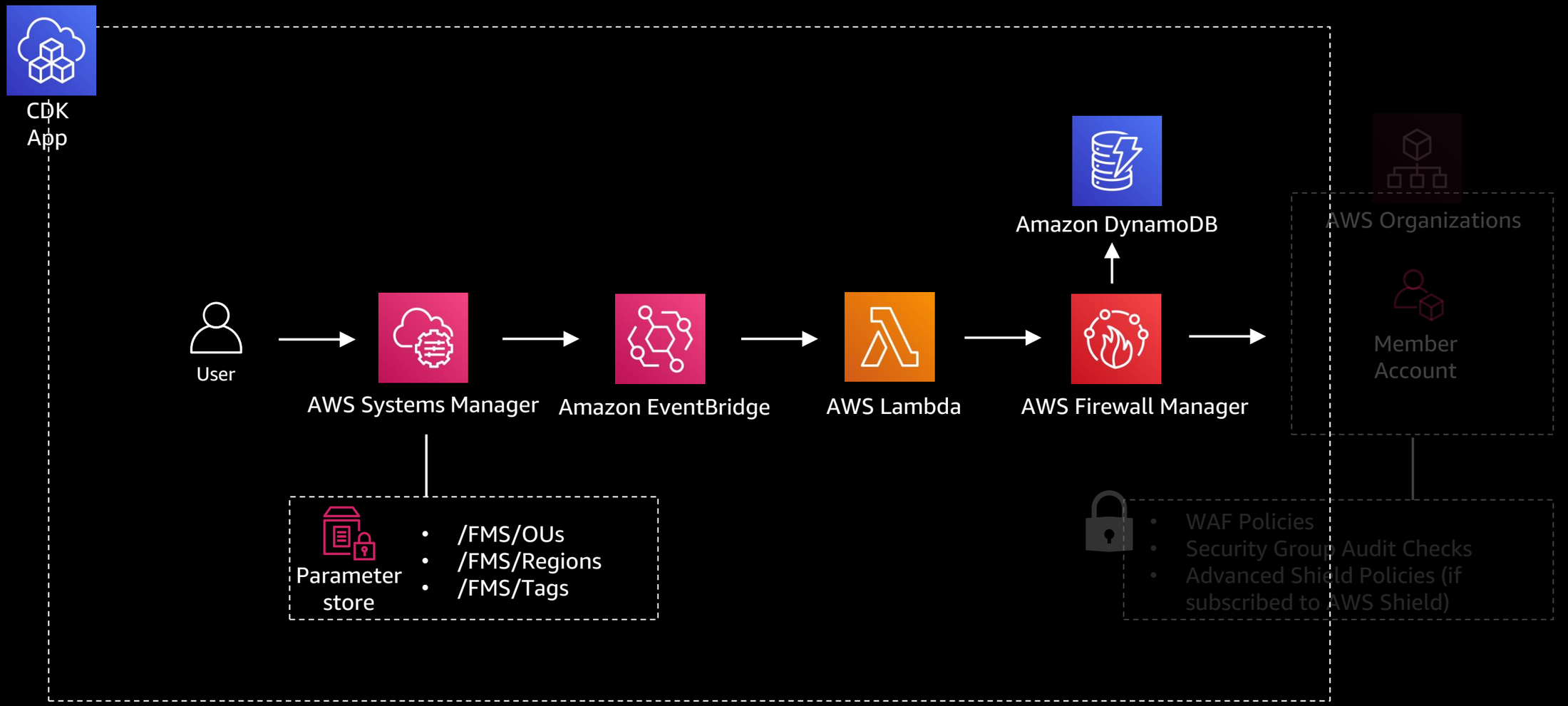
Design decisions



Design decisions



Design decisions



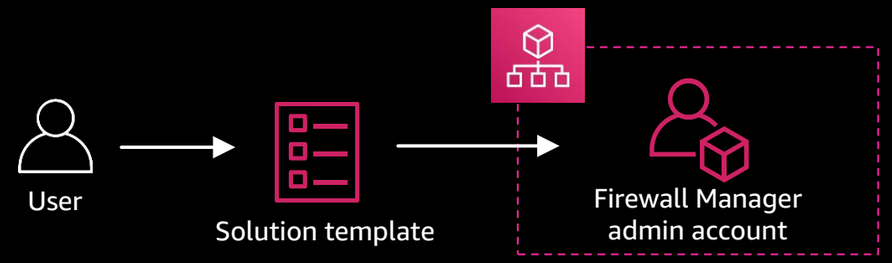
Design decisions



Design decisions

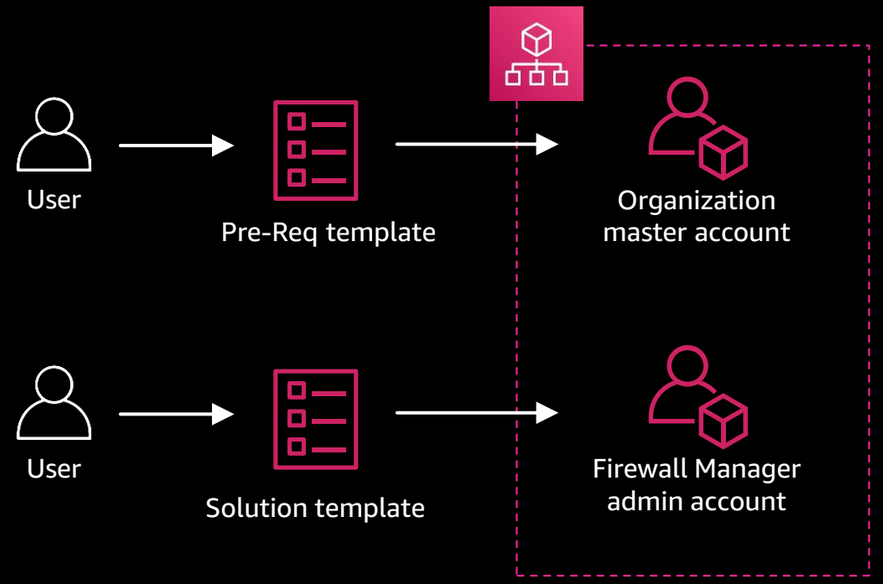
Already using Firewall Manager?

Install the solution primary template in your Firewall Manager Administrator account



Want to set up Firewall Manager?

Install the prerequisite template in your Organization Master account first



Key features



- Automates the set up for Firewall Manager service
- Uses AWS Managed Rules for baseline security posture
- Supports WAF, Shield Advanced, and Security Group policies
- Offers different deployment modes for existing and new AWS Firewall Manager service customers
- Uses AWS CDK constructs, open sourced, to allow solution extension

Call to action!



Move fast AND Stay secure

Review your workload, AWS Well-Architected Tool
https://a.co/5MUhIM3

Collaborate with us on open-sourced projects
https://bit.ly/3enTY8b

Automate detection and compliance
https://a.co/3uiUh0K

Curated library of solutions
https://a.co/3v7xRTt

Automate infrastructure protection
https://a.co/4YVRvQv

AWS solutions implementations

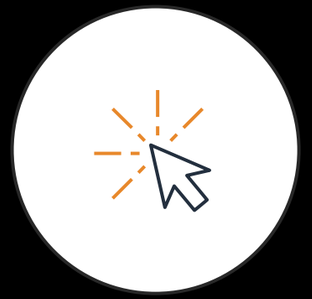
OVER 240 VETTED REFERENCE ARCHITECTURES, AVAILABLE FOR SELF-DEPLOYMENT VIA THE AWS SOLUTIONS LIBRARY



Detailed architecture diagram



Full deployment guide



One-click and manual deployment options



Downloadable source code

References

AWS Solutions Library (https://aws.amazon.com/solutions/)

AWS Security Hub automated response and remediation

- Landing page (https://amzn.to/38zWhnE)
- Github (https://bit.ly/2GTHA3q)

AWS Centralized WAF and security group management solution

- Landing page (https://amzn.to/38zIqOb)
- Github (https://bit.ly/3eWR8XZ)

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.