
AWS
re:Invent

MGT301

Best practices for securing your multi-account environment

Balaji Palanisamy
Global Identity Services Specialist
AWS

AWS re:Invent

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

This session is for you if…

- You are familiar with multi-account architecture for AWS
- You want to understand how AWS Organizations can help you get started **securely**

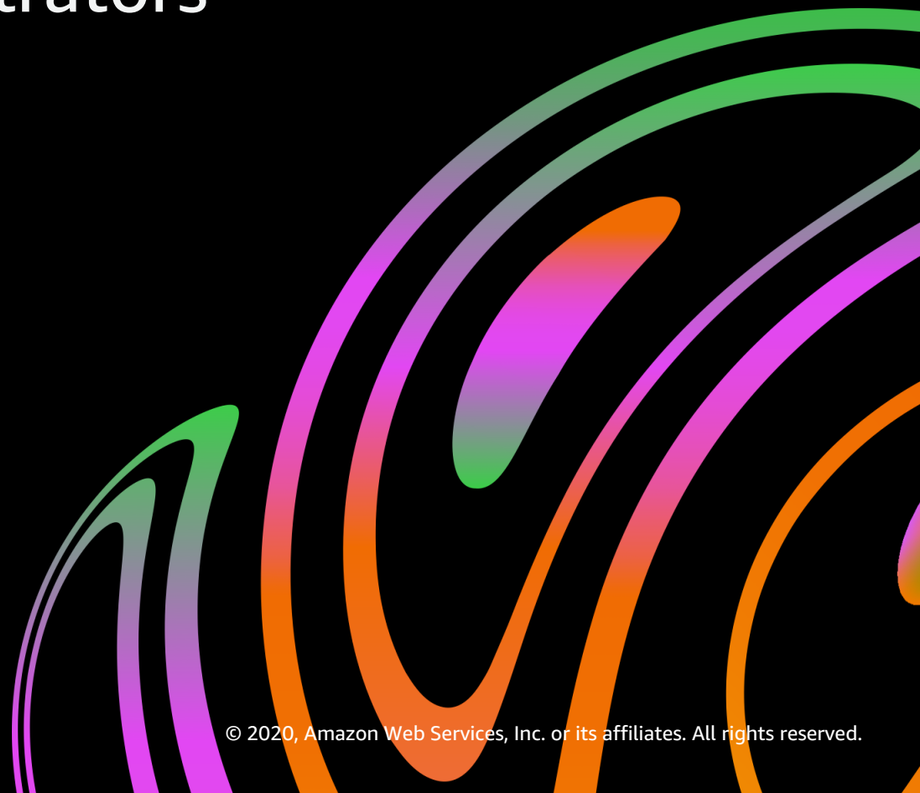
I will focus on five Organizations features to get started



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

Five features to securely launch multi-account environments

- Create security organizational units (OU) and accounts
- Enable security services and delegate administrators
- Deploy resources across multiple accounts
- Enforce controls with Organizations policies
- Manage access; share resources securely



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

Really short intro … really



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

Multi-account environments



Many teams

Support rapid innovation with resources provisioned quickly and exclusively for each team



Business process

Organize AWS accounts to reflect business processes with different operational, regulatory, and budgetary requirements



Isolation and security control

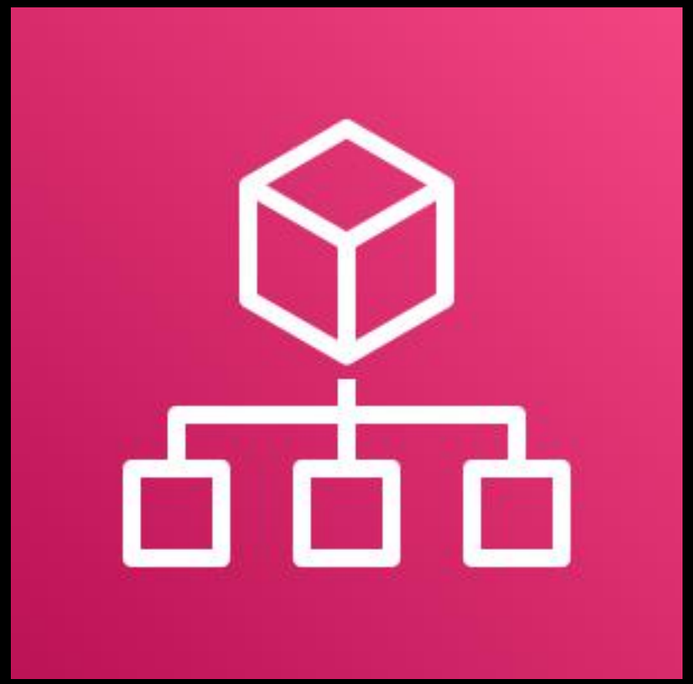
Support tight security boundaries, enforce preventive controls, and centralize security and monitoring



Billing

Simplify billing where resources used within an AWS account can be allocated to the business unit that is responsible for that account

AWS Organizations



Provides the underlying infrastructure and capabilities to build and manage multi-account environments

Over 90% of enterprise customers have multiple accounts and use Organizations

Benefits



Centrally provision accounts and resources



Secure and audit your environment for compliance



Share resources and control access to accounts, regions, and services



Optimize costs and simplify billing

Five features to securely launch multi-account environments

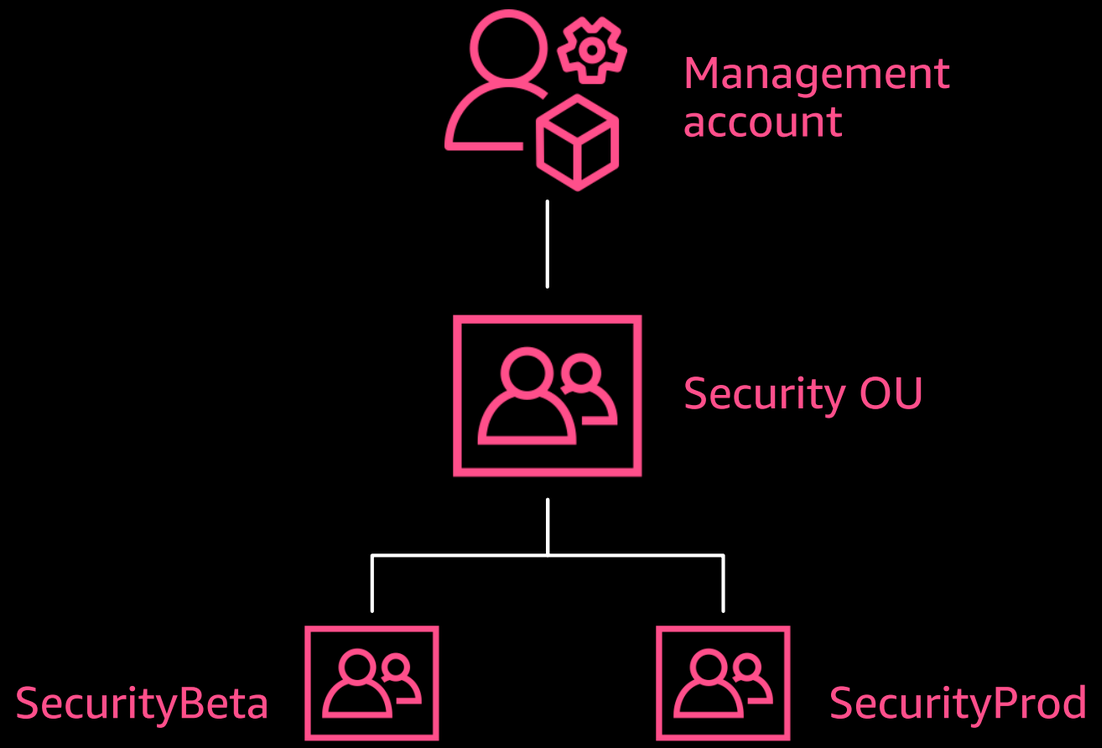


AWS re:Invent

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

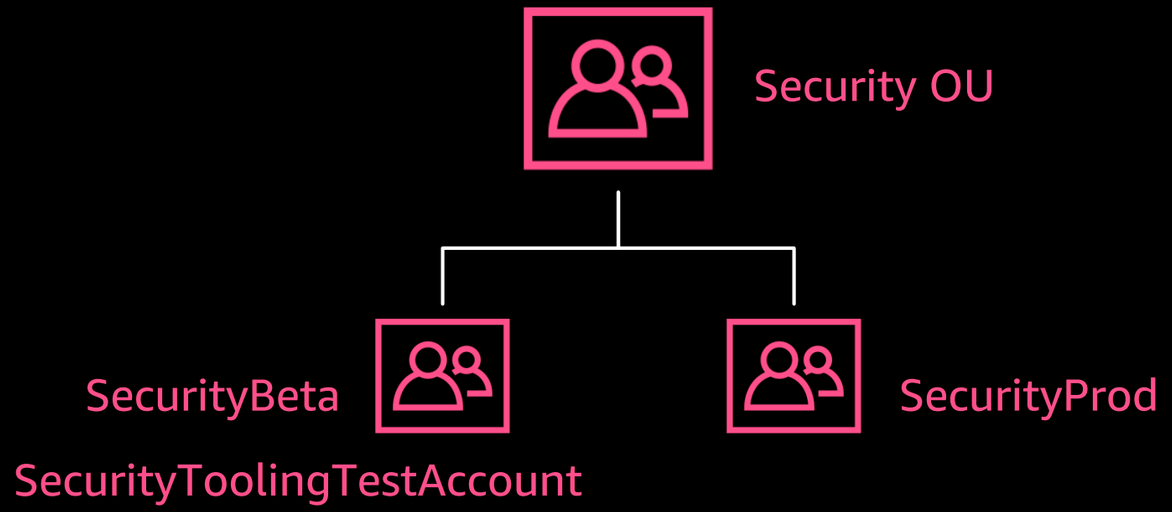
Create a security organizational unit

- Organizational units (or OUs) are containers for a group of accounts
- Create a security OU using the management account
- Create nested OUs for Beta and Prod accounts



Security accounts – Beta OU

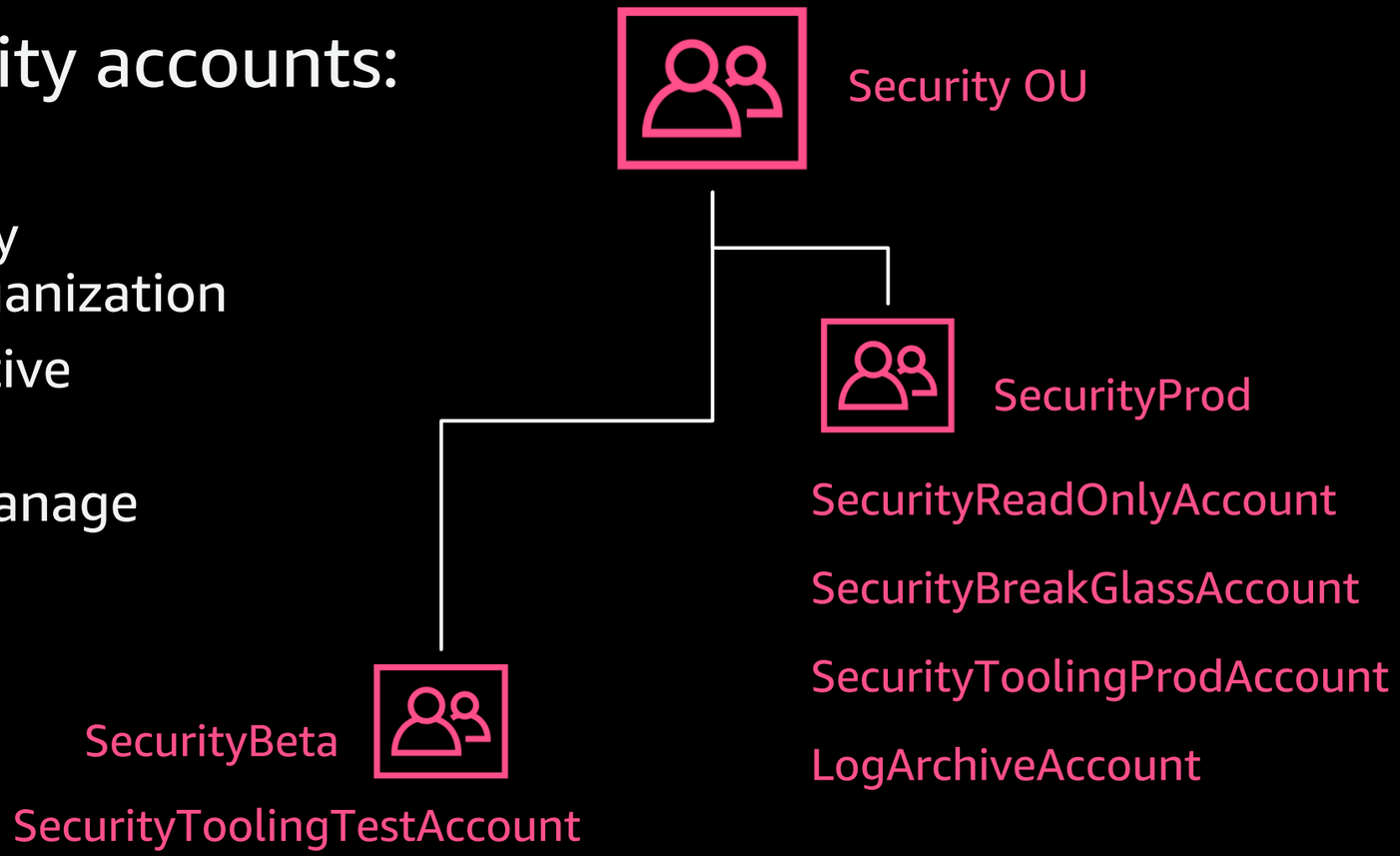
- Create an account to test security tooling and services
- SecurityToolingTest



Security accounts – Prod OU

Create four production security accounts:

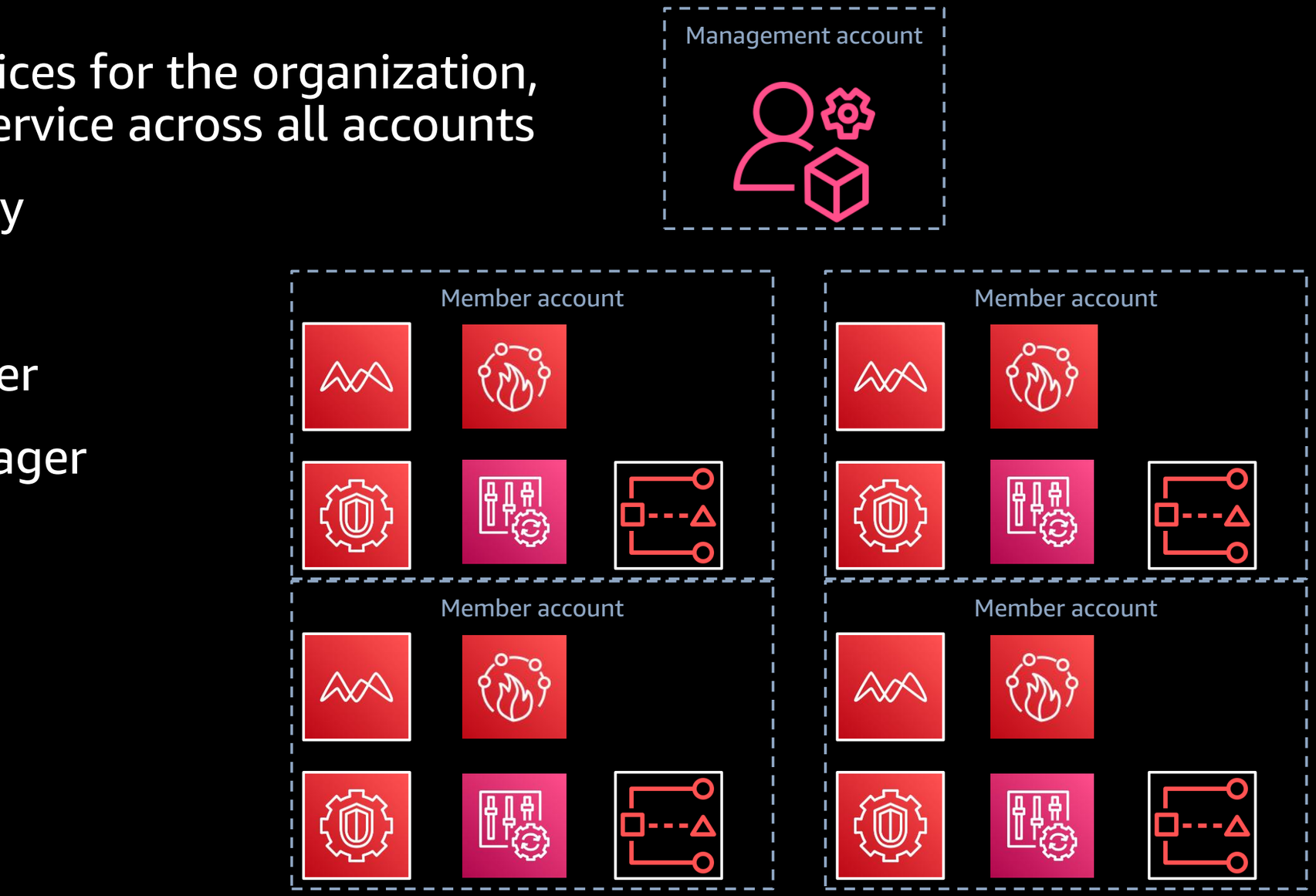
- SecurityReadOnly – has read-only access to accounts within the organization
- SecurityBreakGlass – used for active security events
- SecurityToolingProd – used to manage delegated security services
- LogArchive – used to store and search archives



Enable security services for the organization

Activate security services for the organization, which activates the service across all accounts

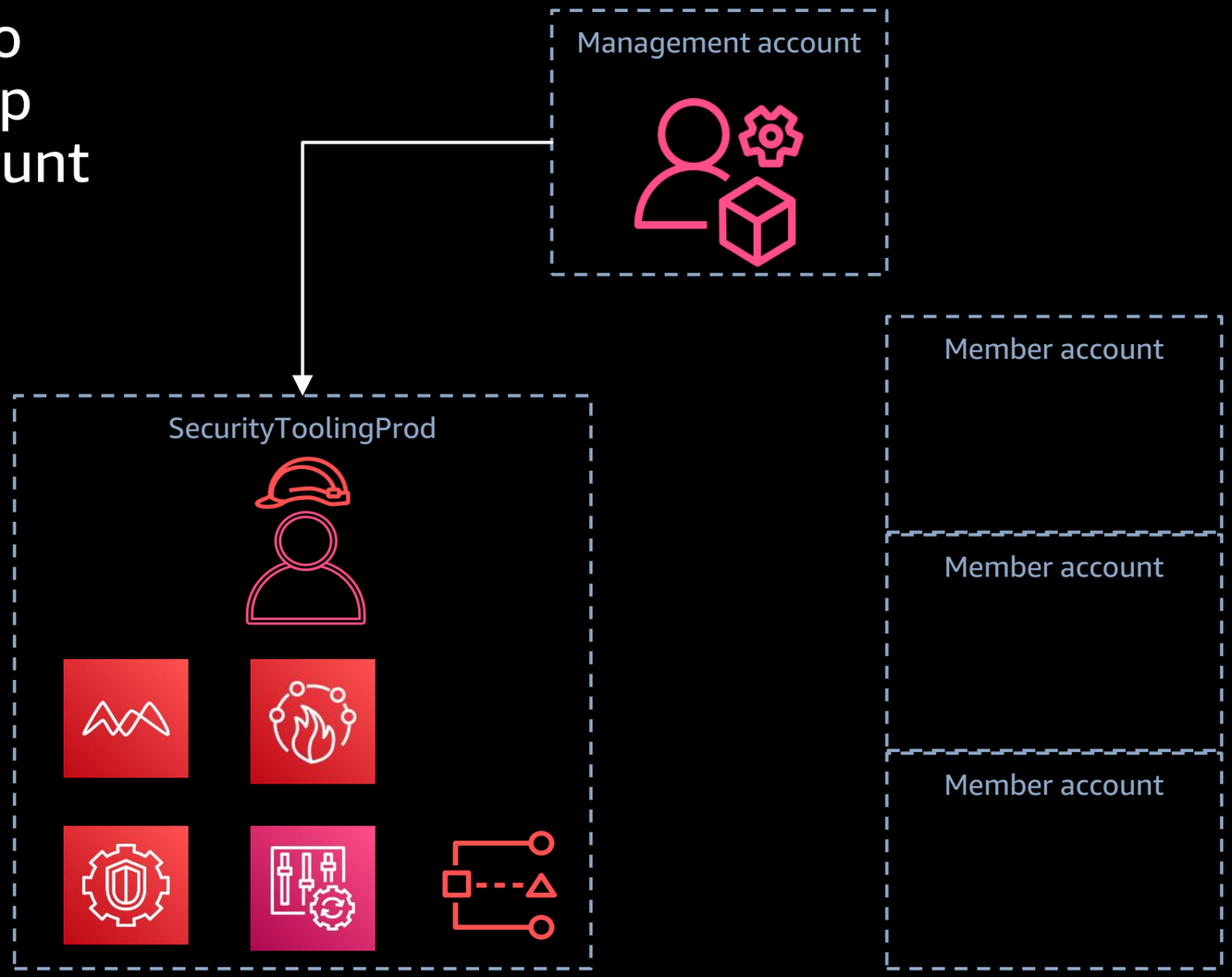
- Amazon GuardDuty
- Amazon Macie
- IAM Access Analyzer
- AWS Firewall Manager
- AWS Config
- And many more…



Delegate administration for security services

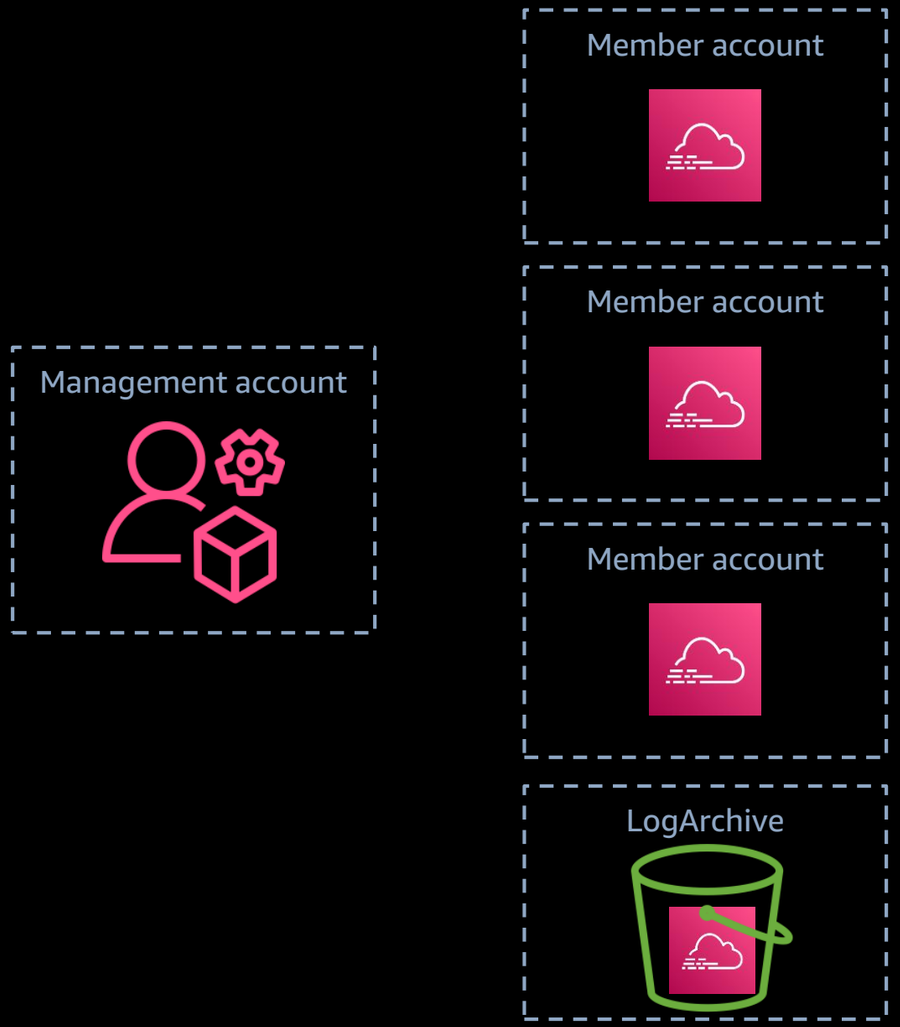
- Use a delegated administrator to assign security tooling ownership to the SecurityToolingProd account

- This means that your security team can manage these services on behalf of the organization



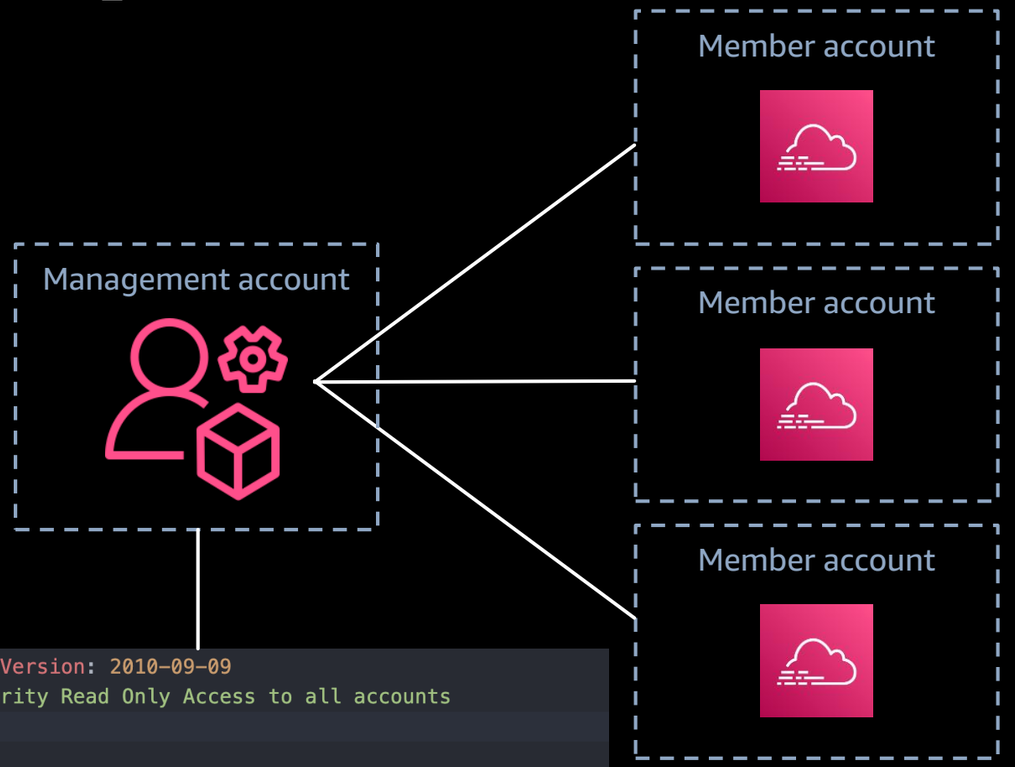
Enable audit trails

- Create an “organization trail” for all accounts in the organization
- Store logs in an S3 bucket accessible from the LogArchive account
- All account activity within your organization is recorded and searchable, and logs cannot be modified or turned off



Deploy resources across multiple accounts

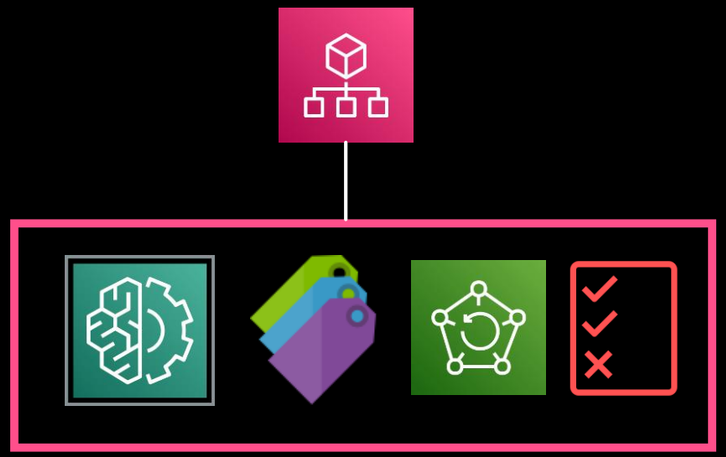
- Create an AWS CloudFormation template for the role
- Enable trusted access for StackSets
- Deploy AWS CloudFormation template from the management account




```
AWSTemplateFormatVersion: 2010-09-09
Description: Security Read Only Access to all accounts
Resources:
  SecurityROrole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: SecurityReadOnlyRole
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          -
            Effect: "Allow"
            Principal:
                AWS:
                  - arn:aws:iam::<Security RO Account Number>:root
            Action: sts:AssumeRole
      Path: "/MyOrgsDemoAc/SecurityROrole/"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

Enforce controls with Organizations policies

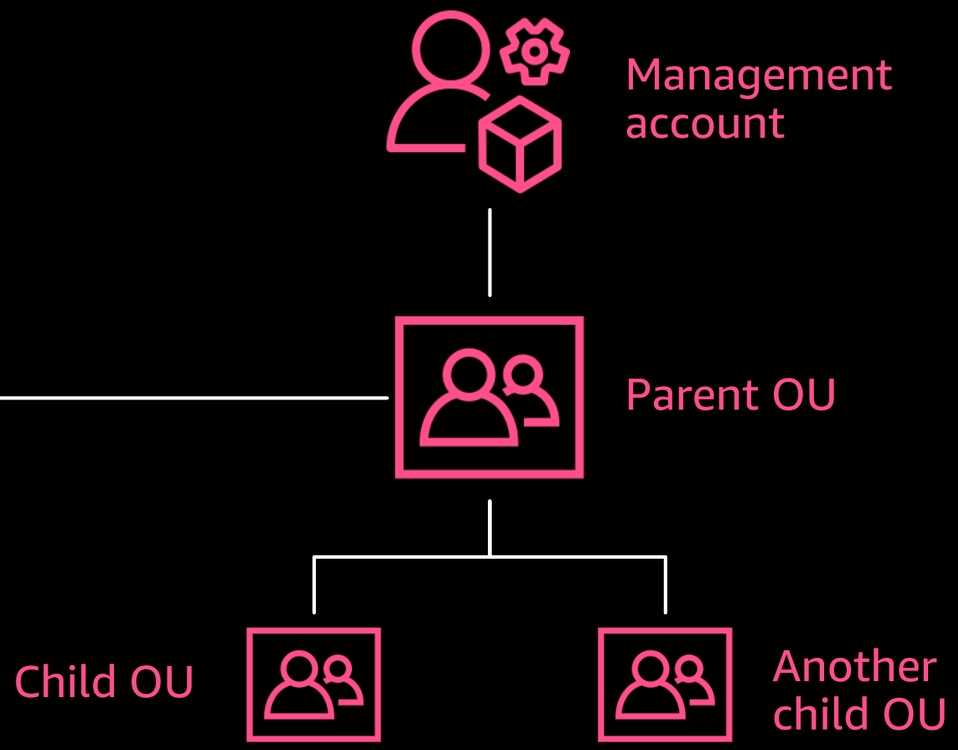
- Implement granular control over backups
  - Backup policies
- Maintain tag consistency
  - Tag policies
- Control how your data is used with artificial intelligence (AI) services
  - AI services opt-out policies
- Centrally control the maximum available permissions for your AWS accounts
  - Service control policies (SCP)



Preventive control with SCP

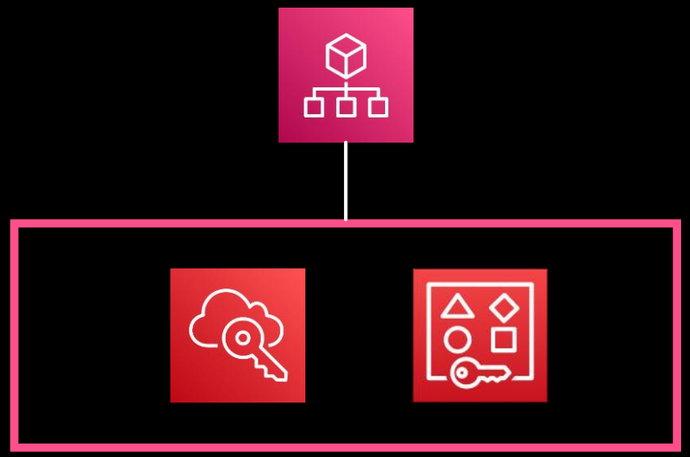
- Create an SCP to prevent tampering with the security read-only role
- Deploy the policy at the parent OU

```
{  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyChangesToSecurityRORole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
      ...
              ],
      "Resource": [
        "arn:aws:iam::*:role/SecurityReadOnlyRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/<trusted role>"
        }     }     } ]   }
```



Manage access; share resources

- Provide access to accounts and resources and customize permissions based on separate job roles
  - AWS Single Sign-On
- Share resources securely at scale and reduce duplicate resources
  - AWS Resource Access Manager



Recap

- Create security organizational units (OU) and accounts
- Enable security services and delegate administrators
- Deploy resources across multiple accounts
- Enforce tag, backup, and access controls with Organizations policies
- Manage access; share resources within your organization

What next?

- Manage service limits
- Manage billing and costs
- And more



Additional multi-account support

Some customers want additional assistance or guidance to build and manage their multi-account environment

For those customers, AWS launched a new service in 2019:



AWS Control Tower
https://aws.amazon.com/controltower/

References

Best practices for multi-account and Organizations

https://aws.amazon.com/organizations/getting-started/best-practices

https://aws.amazon.com/blogs/mt/best-practices-for-organizational-units-with-aws-organizations/

https://aws.amazon.com/blogs/mt/governance-risk-and-compliance-when-establishing-your-cloud-presence/

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html

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.