Secure IAM on AWS with Multi-Account Strategy

Sungchan Yi Advisor: Prof. Chung-Kil Hur

Dept. of Computer Science and Engineering, Seoul National University

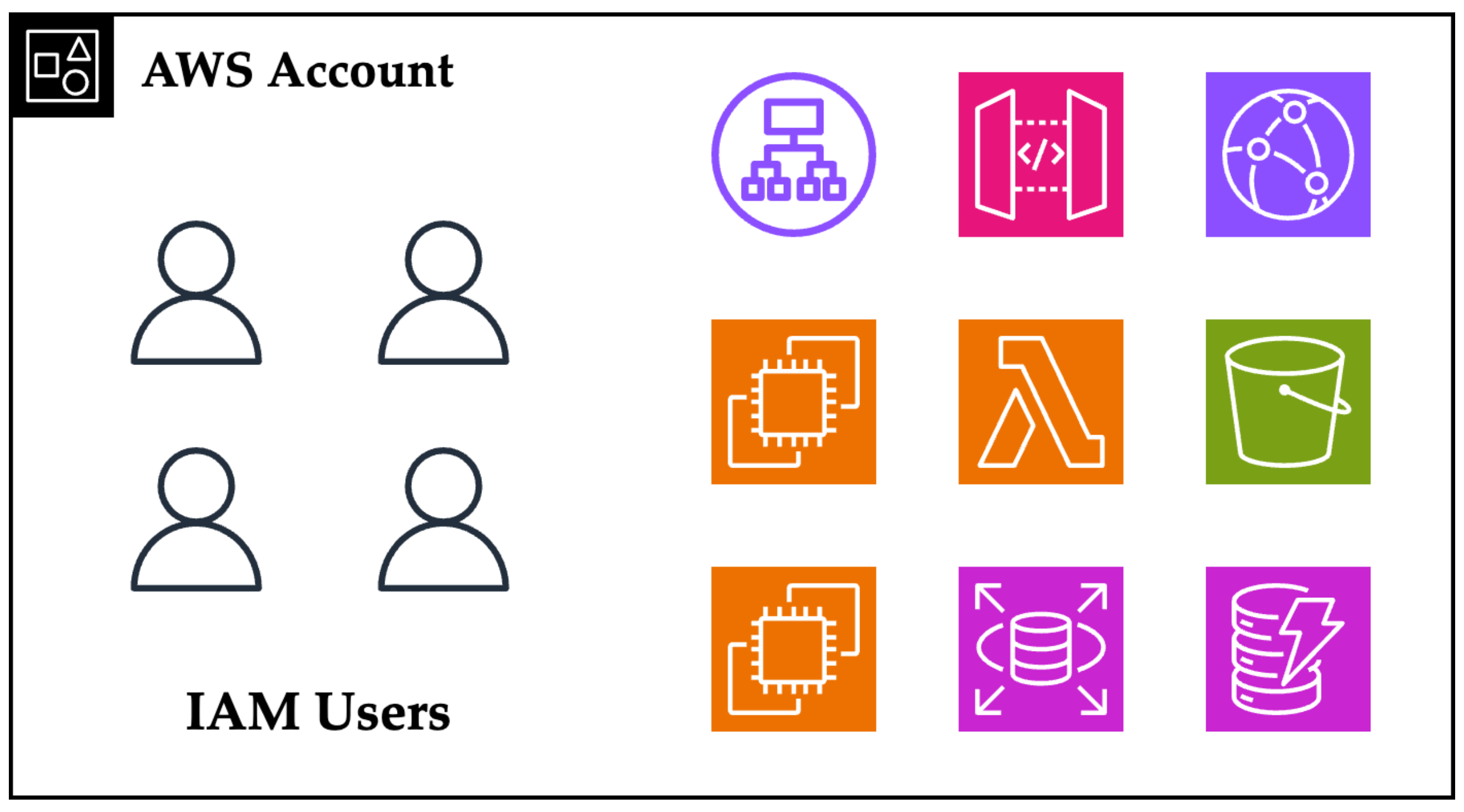
Introduction

- Many businesses use cloud services to operate their product, and thus cloud assets have become a new attack surface.
- Cloud security is emerging as an important concept. Insecure cloud architectures can lead to privacy leakage, service unavailability, or law enforcements.
- Small organizations often don't have enough resources to design a secure cloud architecture.
- Using **multi-account strategy** is recommended. It contributes to security by enhancing access control, through separation of assets and elimination of redundancies in policy management.
- Multi-account structures bring security benefits and requires little operation costs, which is adequate for small organizations.

The Multi-Account Strategy

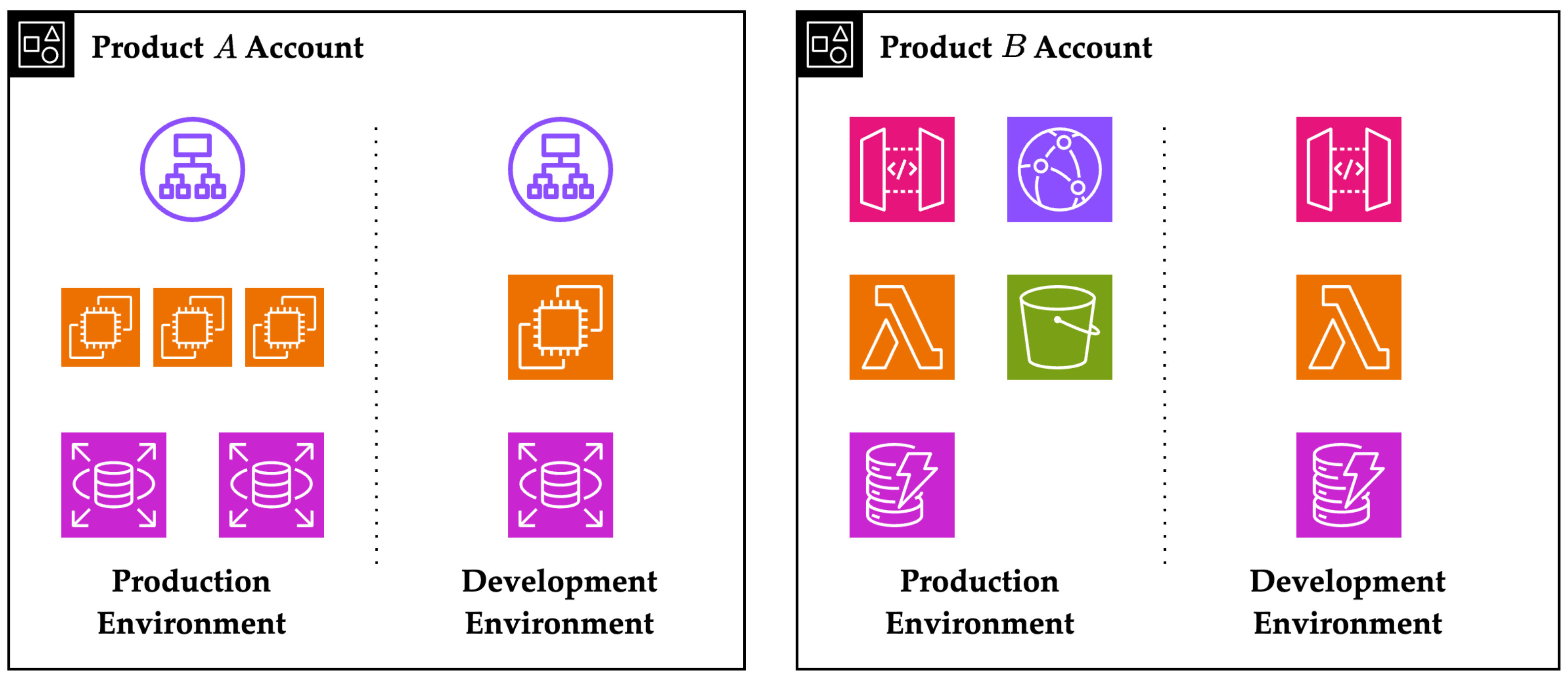
Main Strategy: Use multiple accounts to explicitly separate assets.

Drawbacks of Single Account Structures

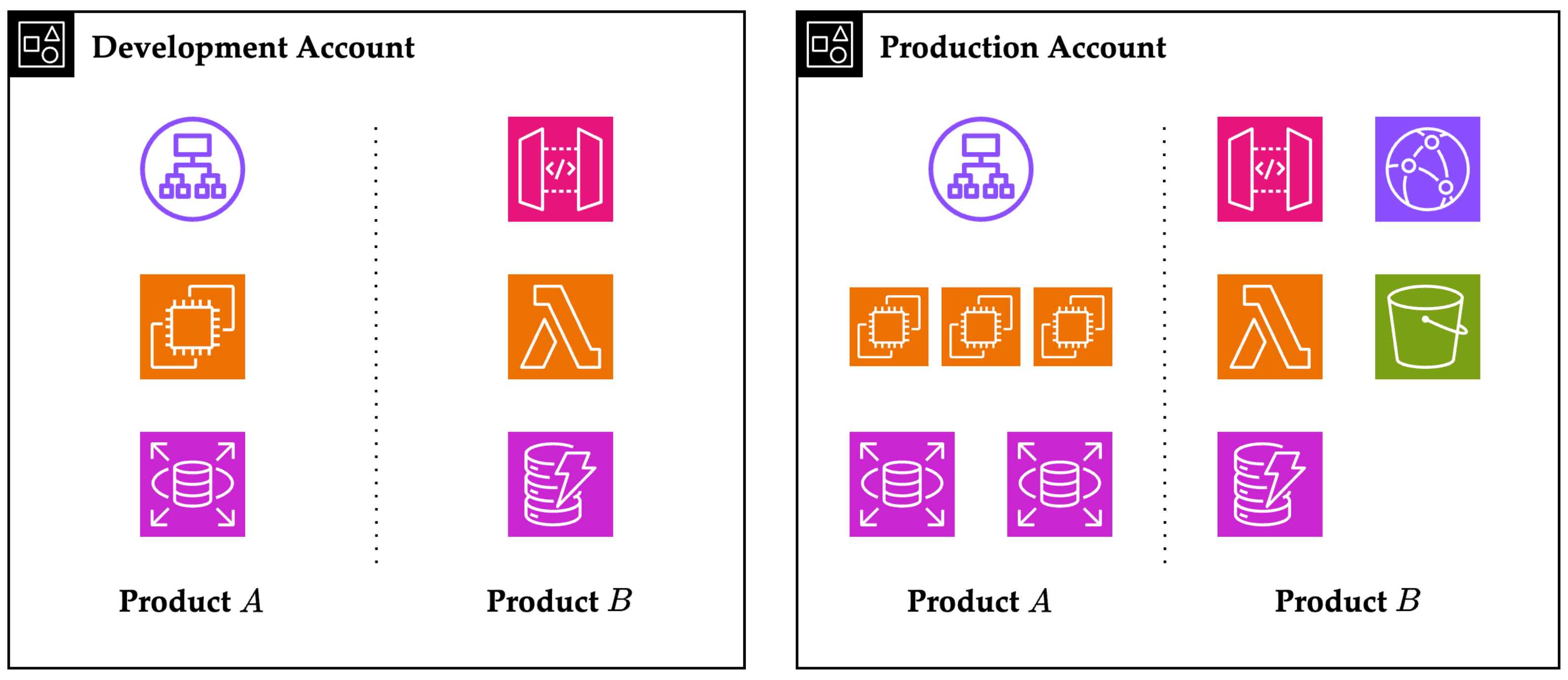


Single account structures put all resources and users inside the same account. This approach causes problems in **visibility** and **environment separation**. All resources are visible without access control, and incidents potentially have a large area of impact.

Benefits of Multiple Account Structures



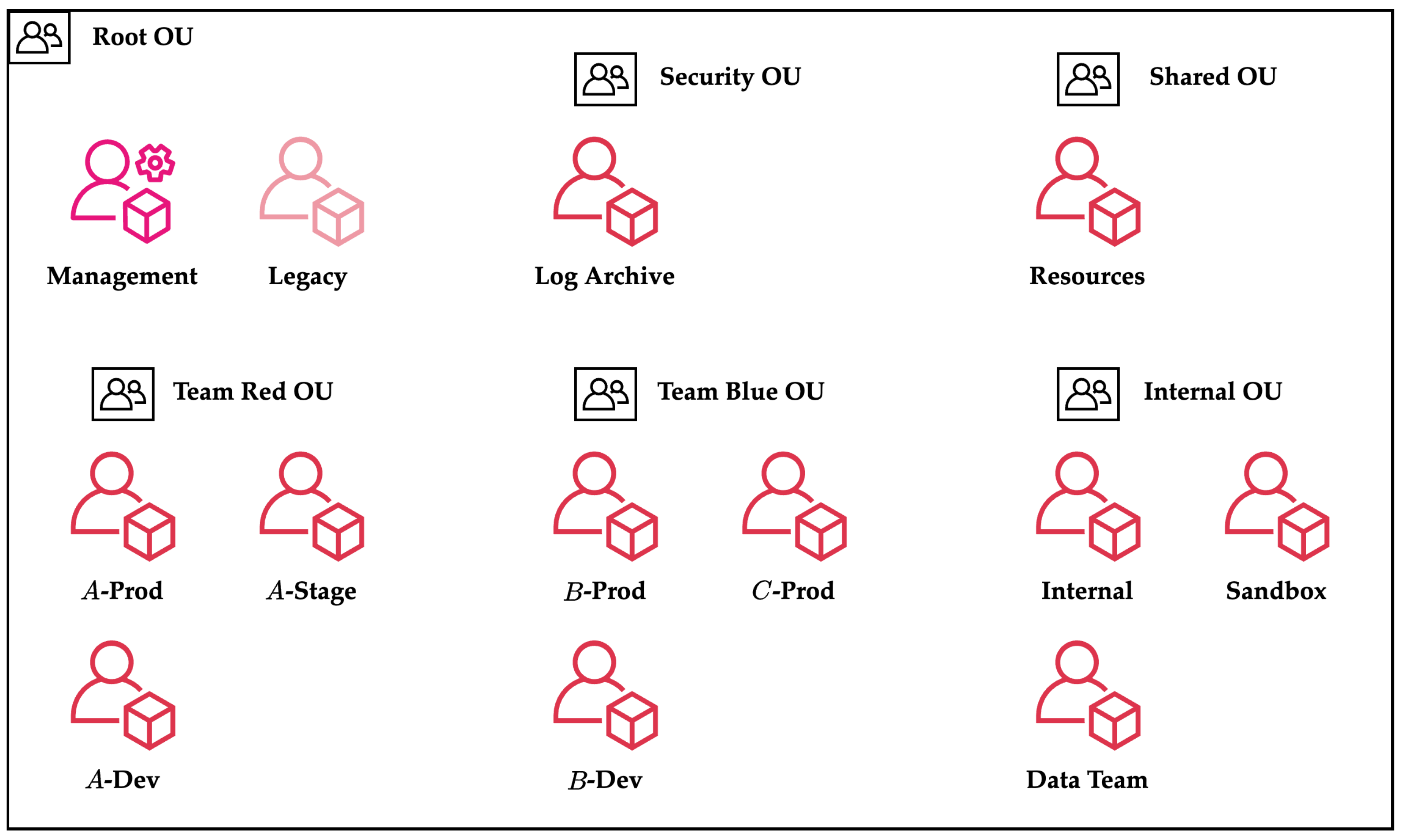
Separation by product solves the visibility problem. Resources are visible only inside the boundary of an account, providing automatic access control.



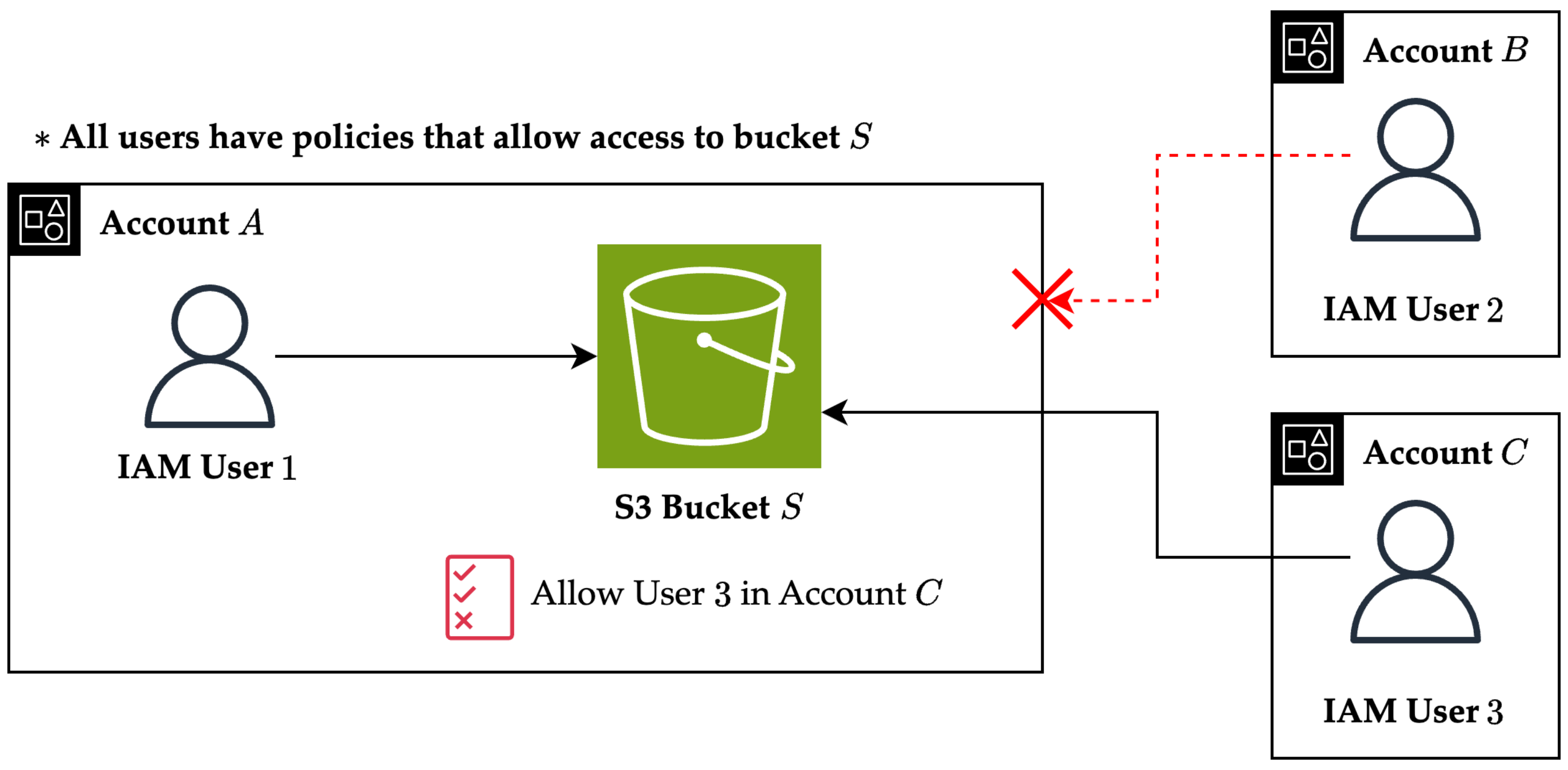
Separation by environment greatly reduces the area of influence to a single account, enhancing availability of products.

Configuring Multi-Account Structures

AWS provides methods to reduce multi-account overheads.

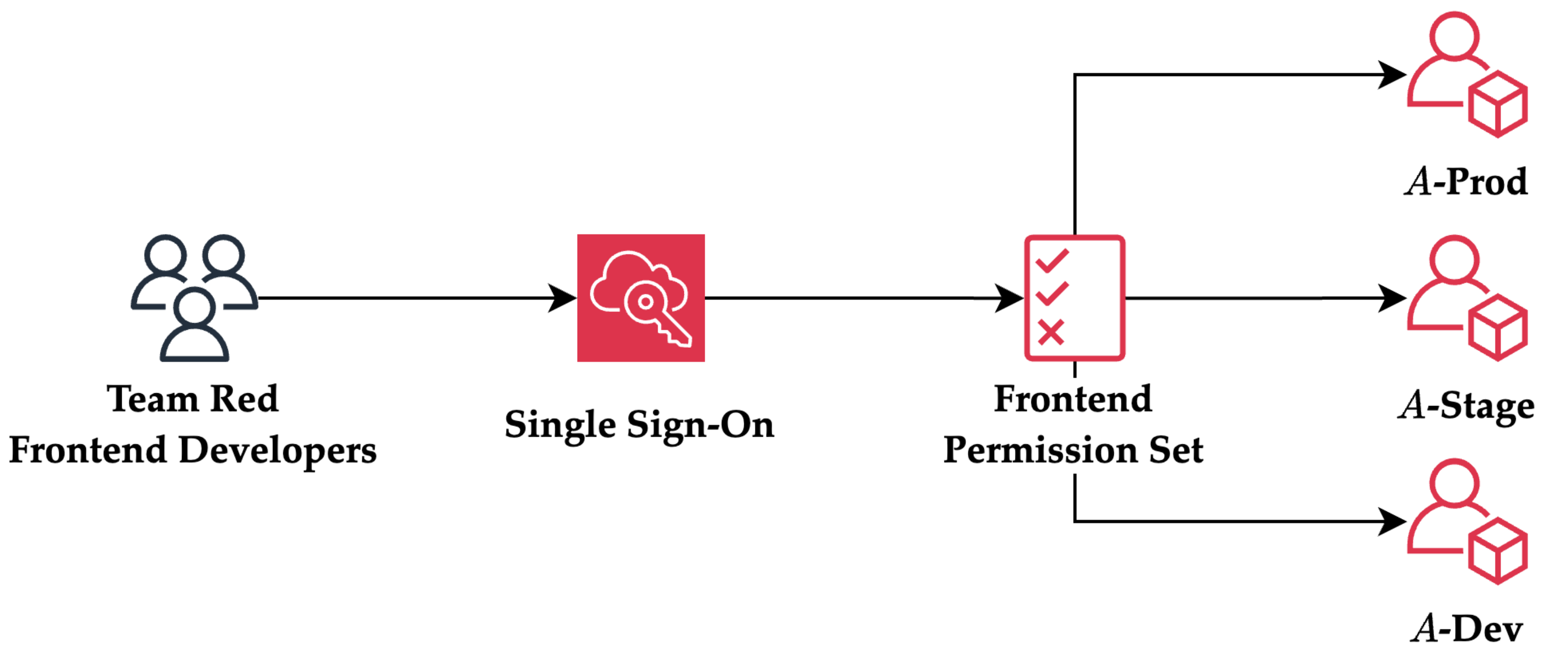


The **AWS Organizations** service provides organizational features. It simplifies account provisioning, groups accounts into organizational units for management. Also, it provides organization-wide control policies and consolidated billing.


∗ All users have policies that allow access to bucket *S*
Account *A*
IAM User 1
S3 Bucket *S*
Allow User 3 in Account *C*
Account *B*
IAM User 2
Account *C*
IAM User 3

When a cloud resource must be shared between multiple accounts, it need not be replicated in each account. Configuring the **resource-based policy** or using the **Resource Access Manager** allows cross-account resource sharing.

Single Sign-On (SSO)



The **single sign-on** feature reduces repeated configurations and account switching overheads. Assigning **permission sets** to user-account or group-account pair allows the user/group to access an account with the given permissions. These can be reused, eliminating redundancies in policy management.

Managing Multiple Accounts

- Policies should be managed according to the **principle of least privilege**.
- **IAM Access Analyzer** checks unused privileges and generates the least privileged permissions of a user.
- The multi-account structure and the given permissions should be documented in detail, as a general security guide for users.
- **AWS CloudTrail** provides audit logs for tracking and detecting malicious activity on the cloud.