aws INNOVATE

DATA EDITION

23 August, 2022

Data protection fundamentals on AWS

Michael Stringer

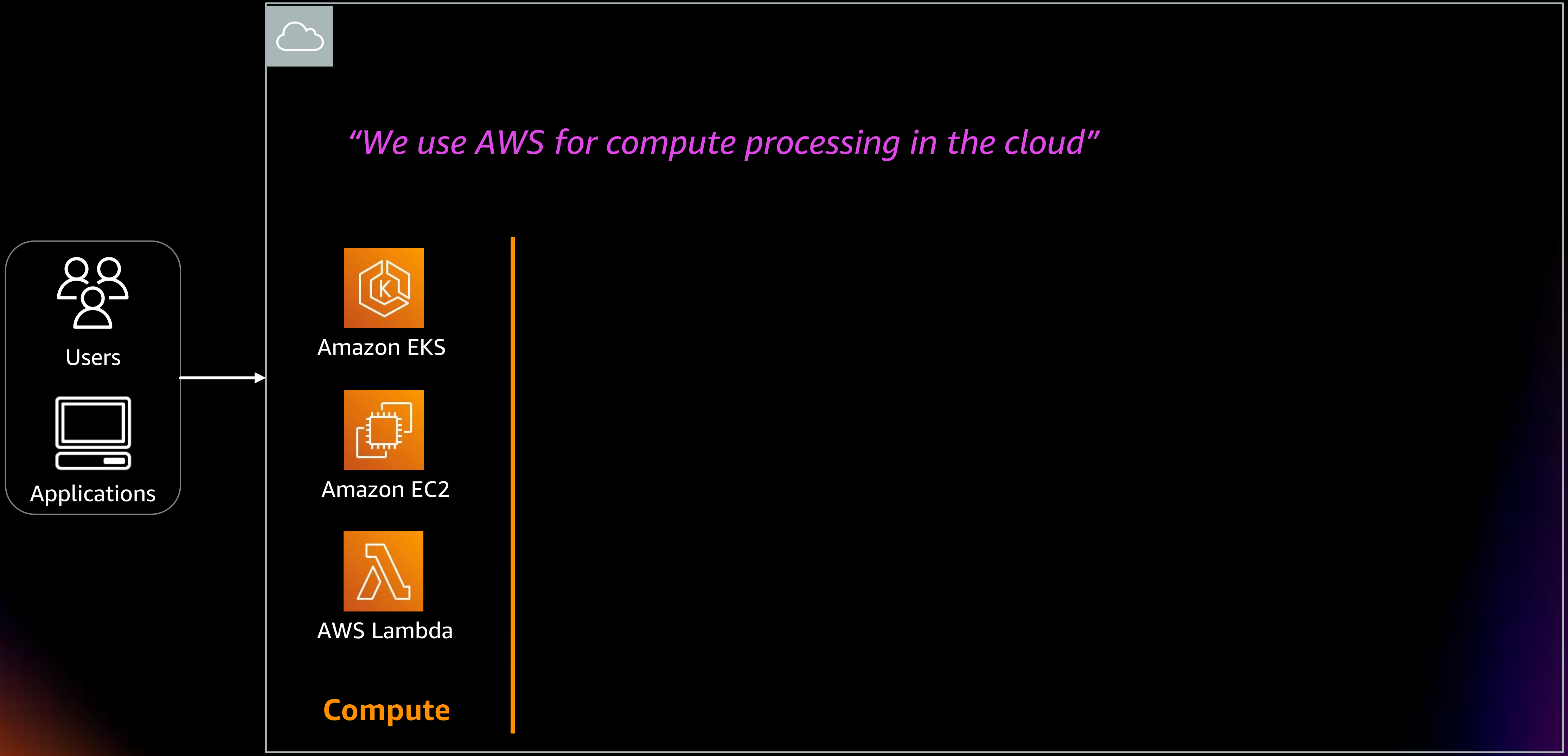
Principal Solutions Architect – Security
Amazon Web Services

Agenda

- Fundamentals of data protection on AWS
- Which AWS services to use with your workloads
- Deeper dive into service capabilities
- Recap and summary
- Next steps

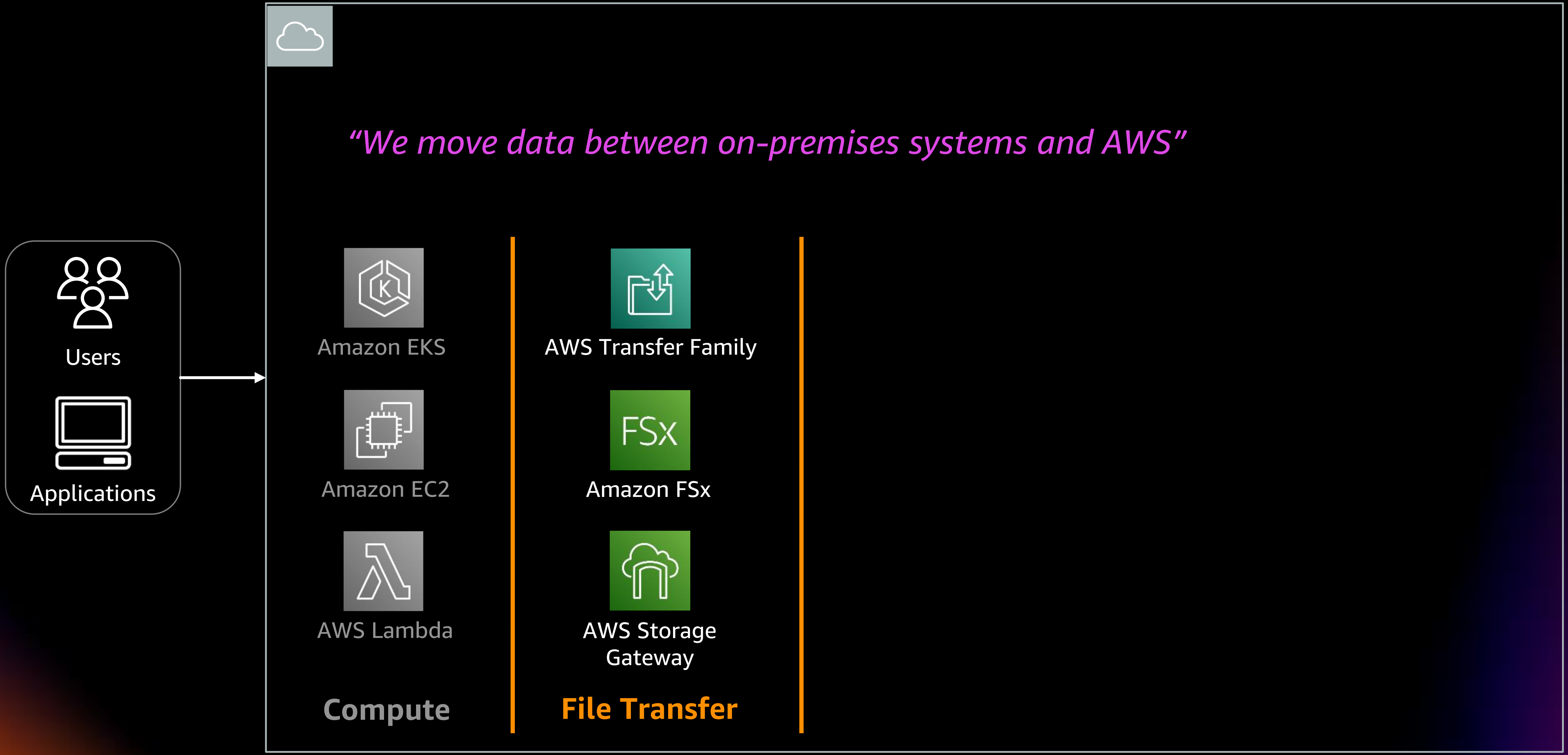
What are the fundamentals of data protection on AWS?

Typical AWS service data use cases

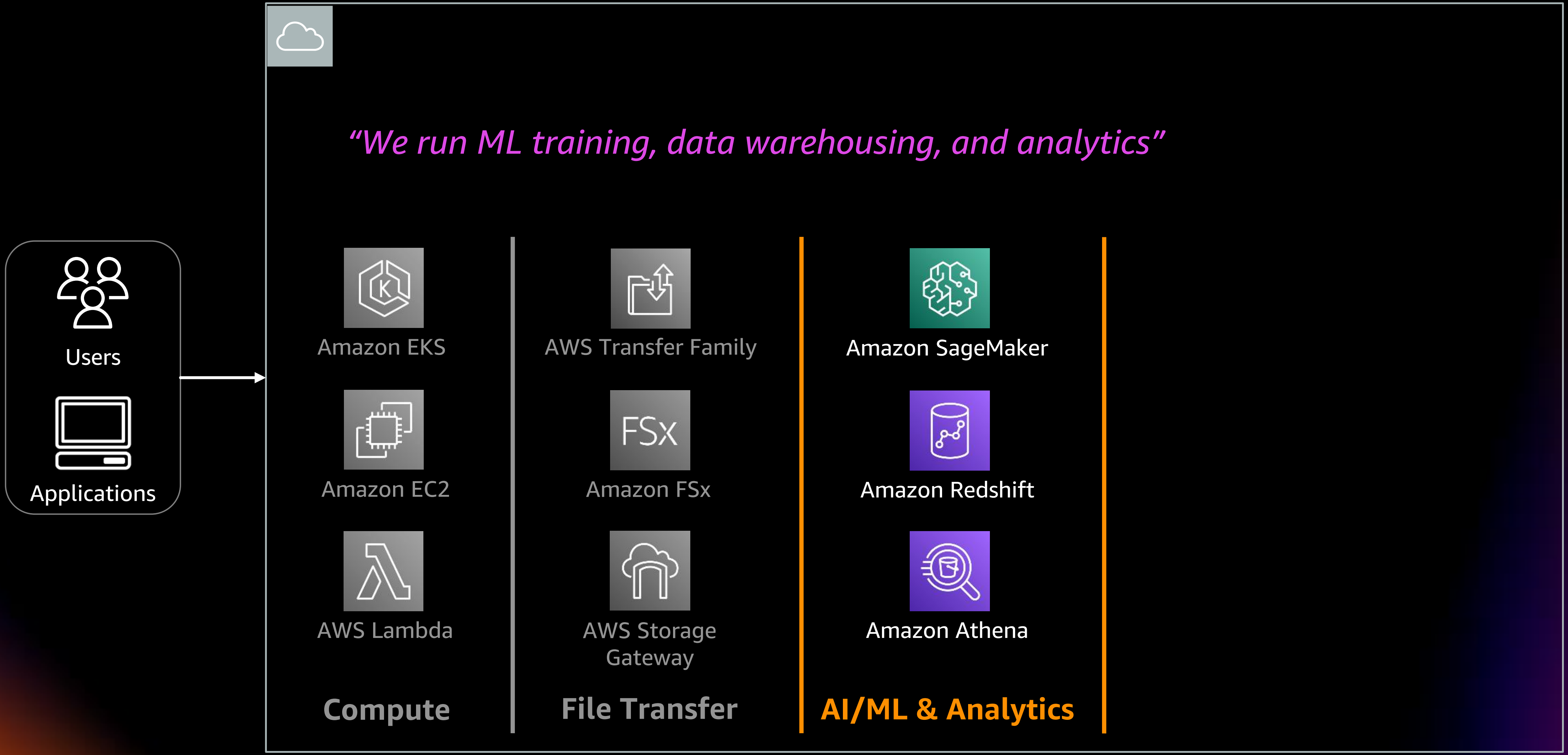


“We use AWS for compute processing in the cloud”

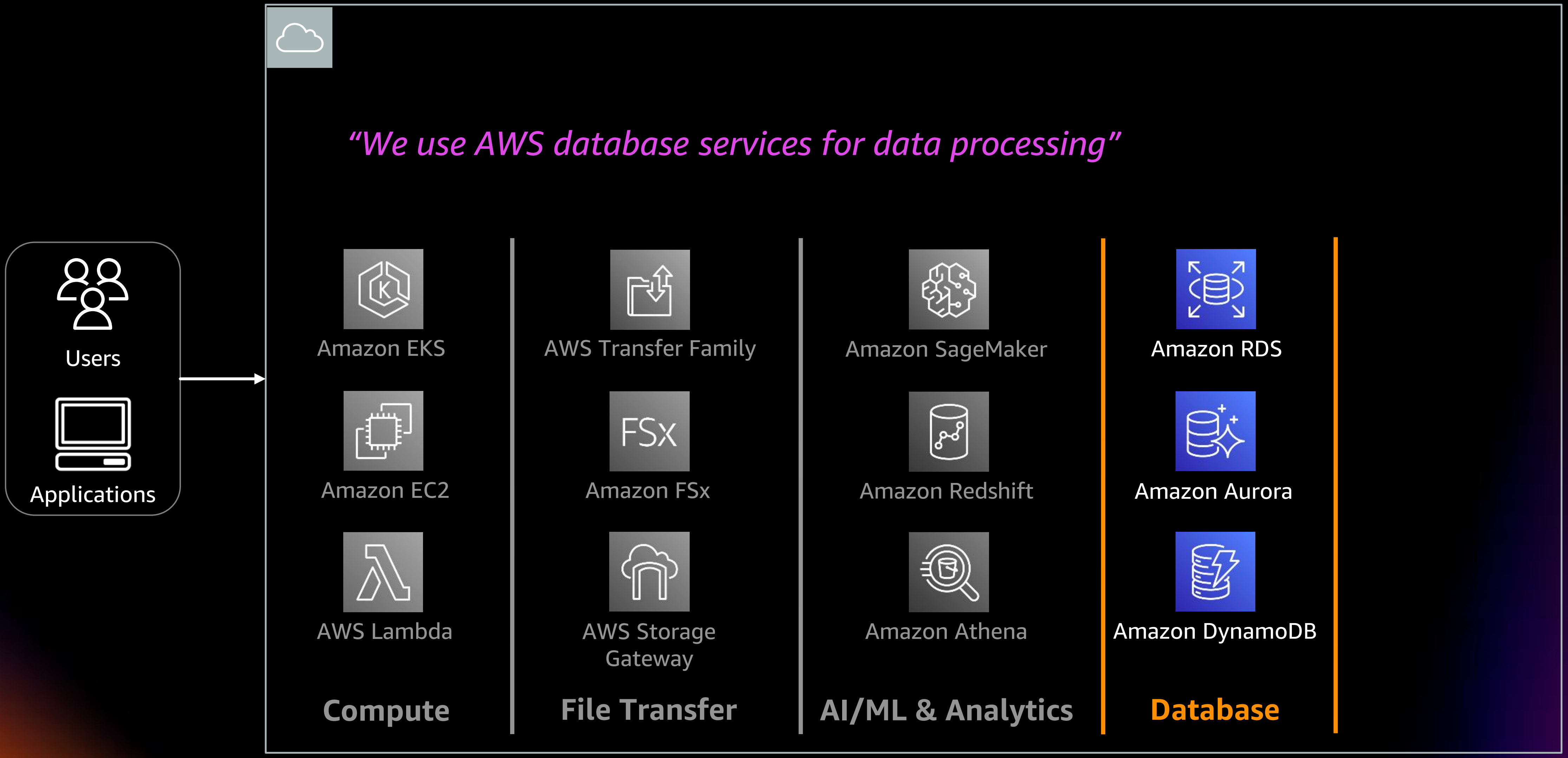
Typical AWS service data use cases



Typical AWS service data use cases



Typical AWS service data use cases



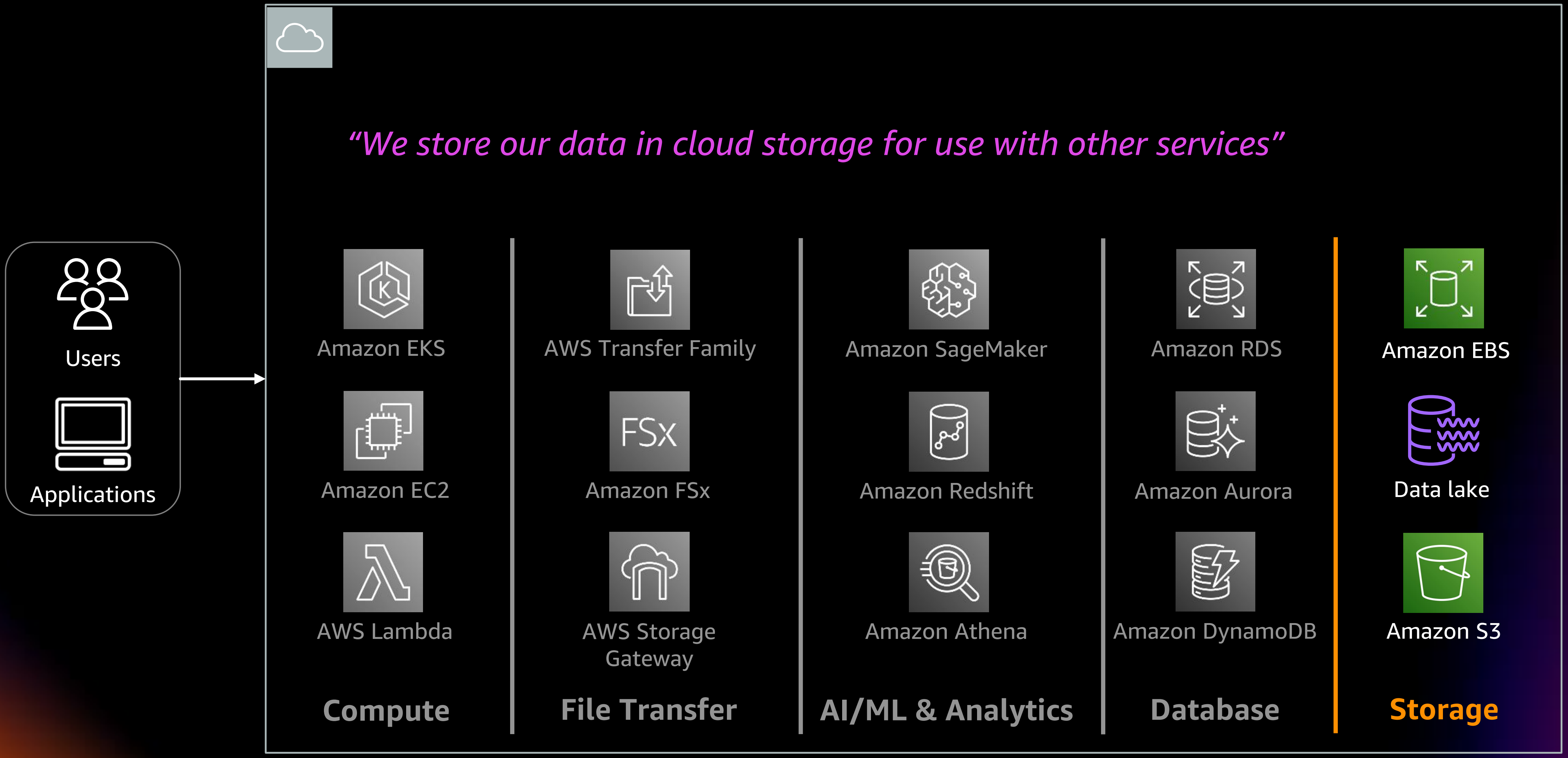
“We use AWS database services for data processing”

Users

Applications

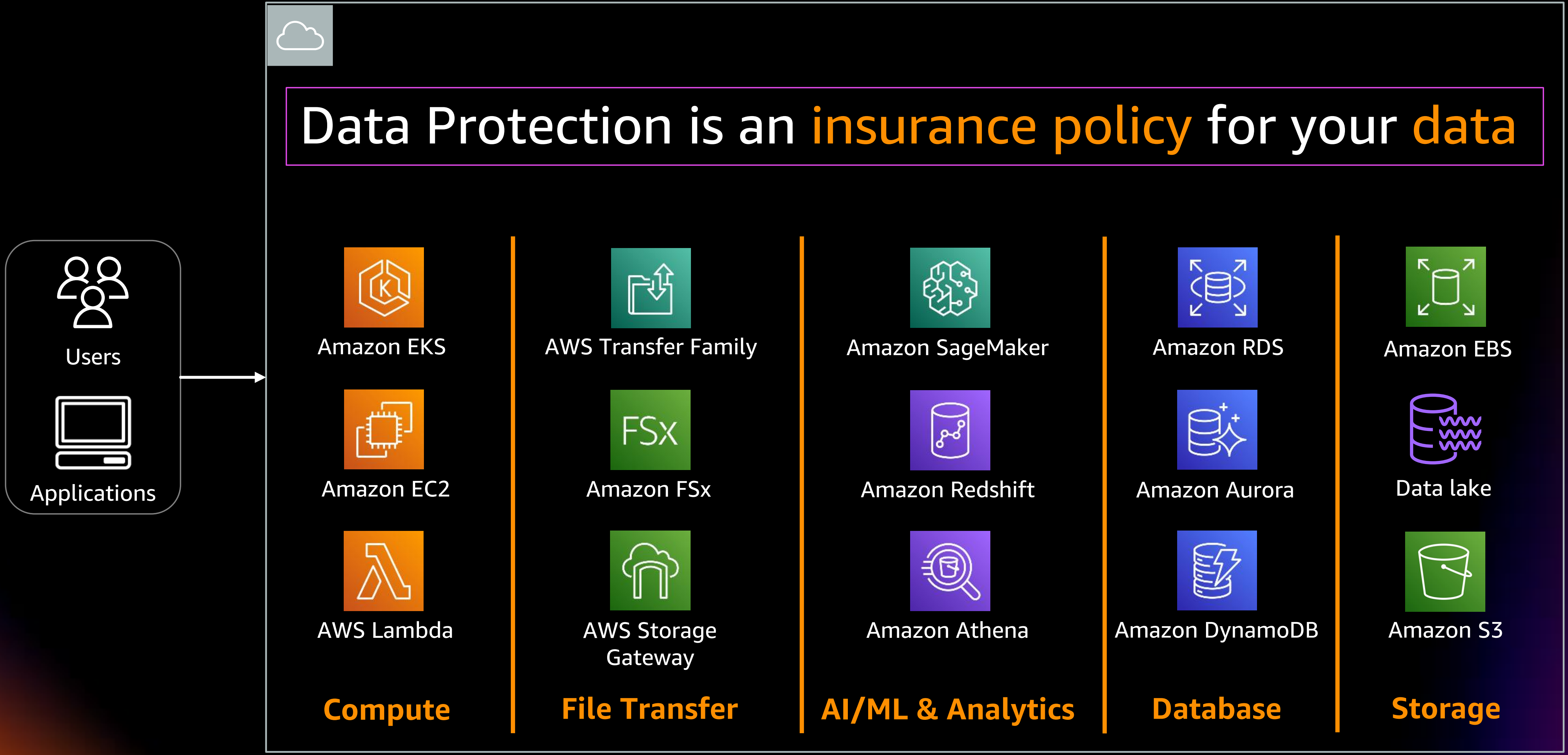
Compute	File Transfer	AI/ML & Analytics	Database
Amazon EKS	AWS Transfer Family	Amazon SageMaker	Amazon RDS
Amazon EC2	Amazon FSx	Amazon Redshift	Amazon Aurora
AWS Lambda	AWS Storage Gateway	Amazon Athena	Amazon DynamoDB

Typical AWS service data use cases



“We store our data in cloud storage for use with other services”

Data protection is important to all use cases



Data Protection is an insurance policy for your data

Users

Applications

Amazon EKS

Amazon EC2

AWS Lambda

Compute

AWS Transfer Family

Amazon FSx

AWS Storage Gateway

File Transfer

Amazon SageMaker

Amazon Redshift

Amazon Athena

AI/ML & Analytics

Amazon RDS

Amazon Aurora

Amazon DynamoDB

Database

Amazon EBS

Data lake

Amazon S3

Storage

Data protection drives better business outcomes

Protect intellectual property and trade secrets

Protect customer information and build a trusted brand

Automate tasks to save time and reduce risk

Scale with visibility and control as your business grows

Easily integrate with hundreds of AWS services

Inherit global security and compliance controls

Focus on key data protection tasks

Manage identity and authentication

Focus on key data protection tasks

Manage identity and authentication

Encrypt cloud storage and databases

Focus on key data protection tasks

Manage identity and authentication

Encrypt cloud storage and databases

Eliminate high-risk hardcoded secrets

Focus on key data protection tasks

Manage identity and authentication

Encrypt cloud storage and databases

Eliminate high-risk hardcoded secrets

Discover and classify sensitive data

Focus on key data protection tasks

Manage identity and authentication

Encrypt cloud storage and databases

Eliminate high-risk hardcoded secrets

Discover and classify sensitive data

Protect critical data stored in AWS services

Data protection on AWS

A suite of services designed to automate and simplify many security tasks ranging from identification and authorization, encryption, secrets management, sensitive data discovery, and backups

AWS Identity and Access Management (IAM)

Fine-grained access control across all of AWS

AWS Key Management Service (AWS KMS)

Easily create and control the keys used to encrypt

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials

Amazon Macie

Discover and protect your sensitive data at scale

AWS Backup

A cost-effective, fully managed, policy-based service that further simplifies data protection at scale

Identity and Access Management

Identity, access, and resource management

Who

Identity management

Name
Credentials
Metadata
Governance

Can access

Access management

Policies
Compliance
Governance

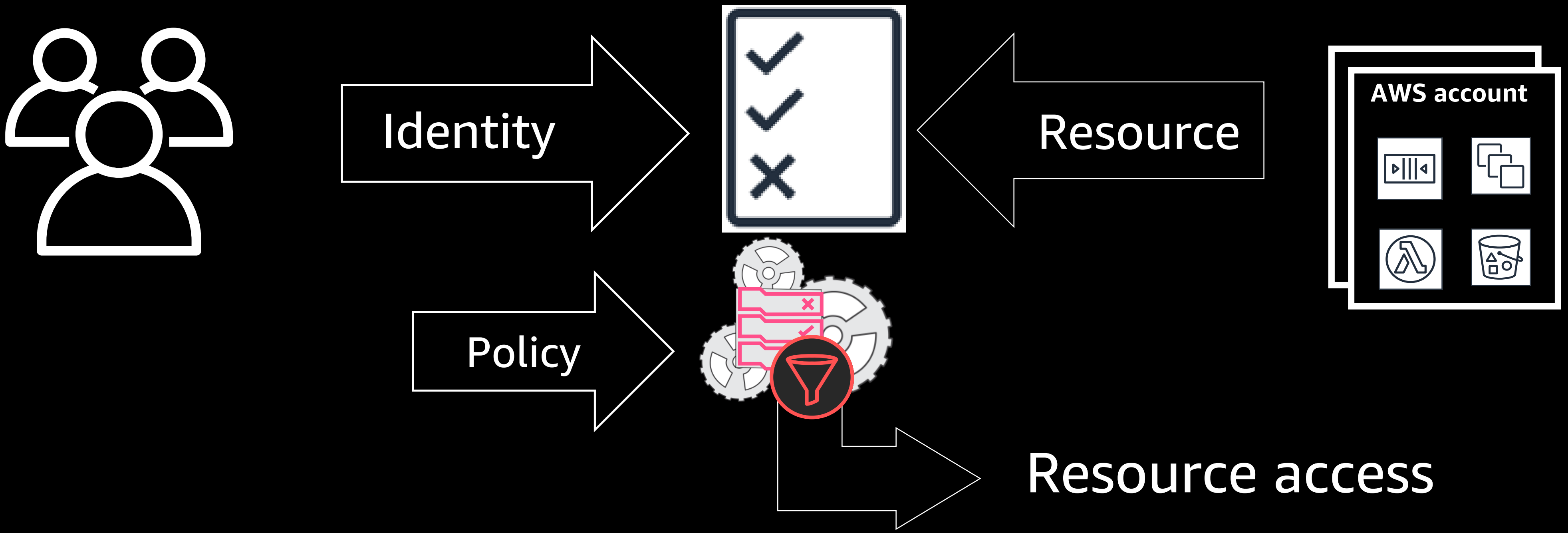
What

AWS account

Resource management

Isolation
Grouping
Tagging
Sharing
Governance

Identity, access, and resource management



Resource access

Simple: Access to an application

Complex: Resource-specific, fine-grained access

AWS Identity and Access Management

- Grant unique security credentials to users and groups to specify which AWS service APIs and resources they can access

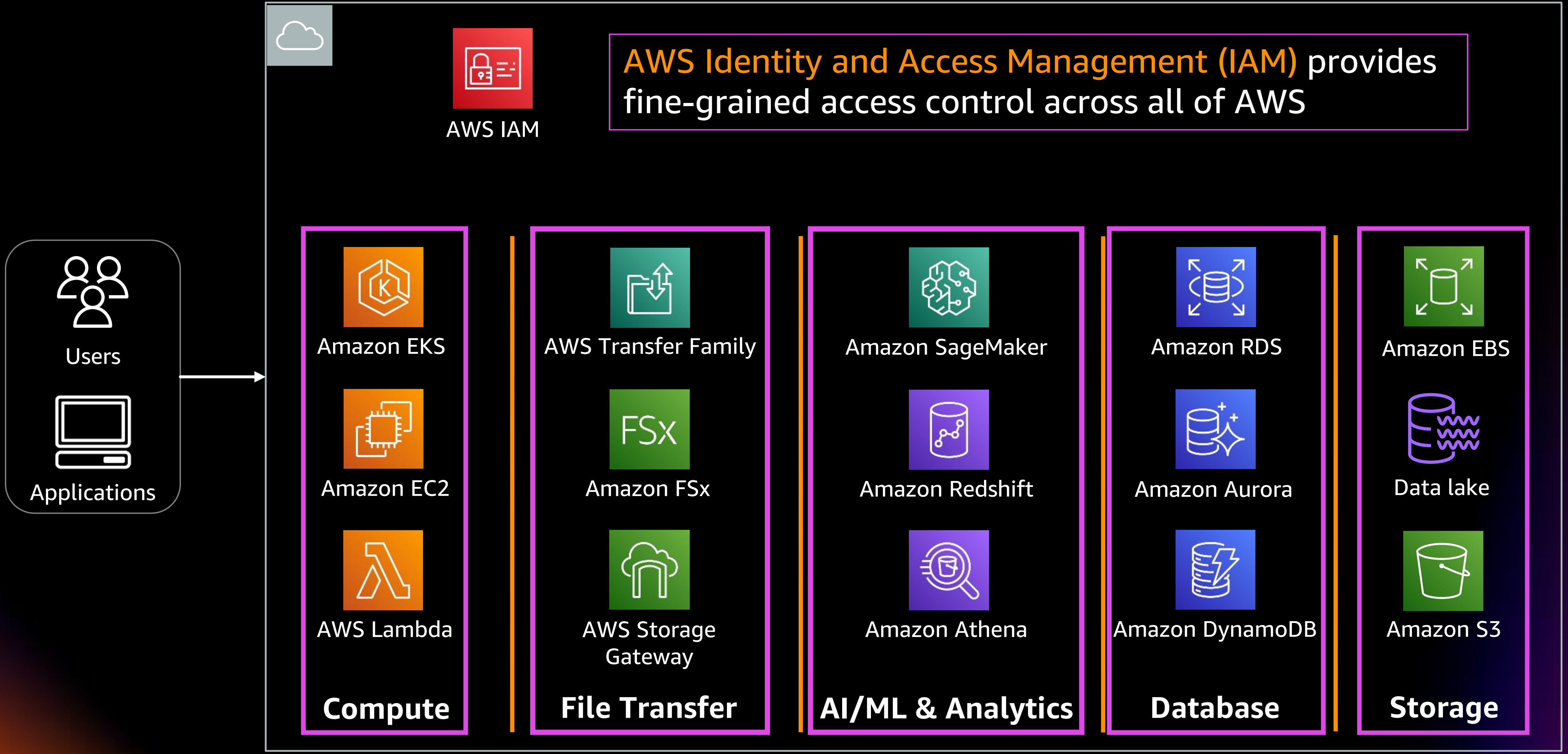
- IAM is secure by default; users have no access to AWS resources until permissions are explicitly granted

- IAM provides the granularity to control a user’s access to specific AWS services and resources using permissions

- Roles allow you to define a set of permissions and then let authenticated users or Amazon EC2 instances assume them, increasing your security posture by granting temporary access to the resources you define

- You can use IAM to support federation from corporate systems like Microsoft Active Directory as well as standards-based identity providers such as Okta, OneLogin and Ping

Where do I use AWS IAM?



Users

Applications

AWS IAM

AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS

Compute

- Amazon EKS
- Amazon EC2
- AWS Lambda

File Transfer

- AWS Transfer Family
- Amazon FSx
- AWS Storage Gateway

AI/ML & Analytics

- Amazon SageMaker
- Amazon Redshift
- Amazon Athena

Database

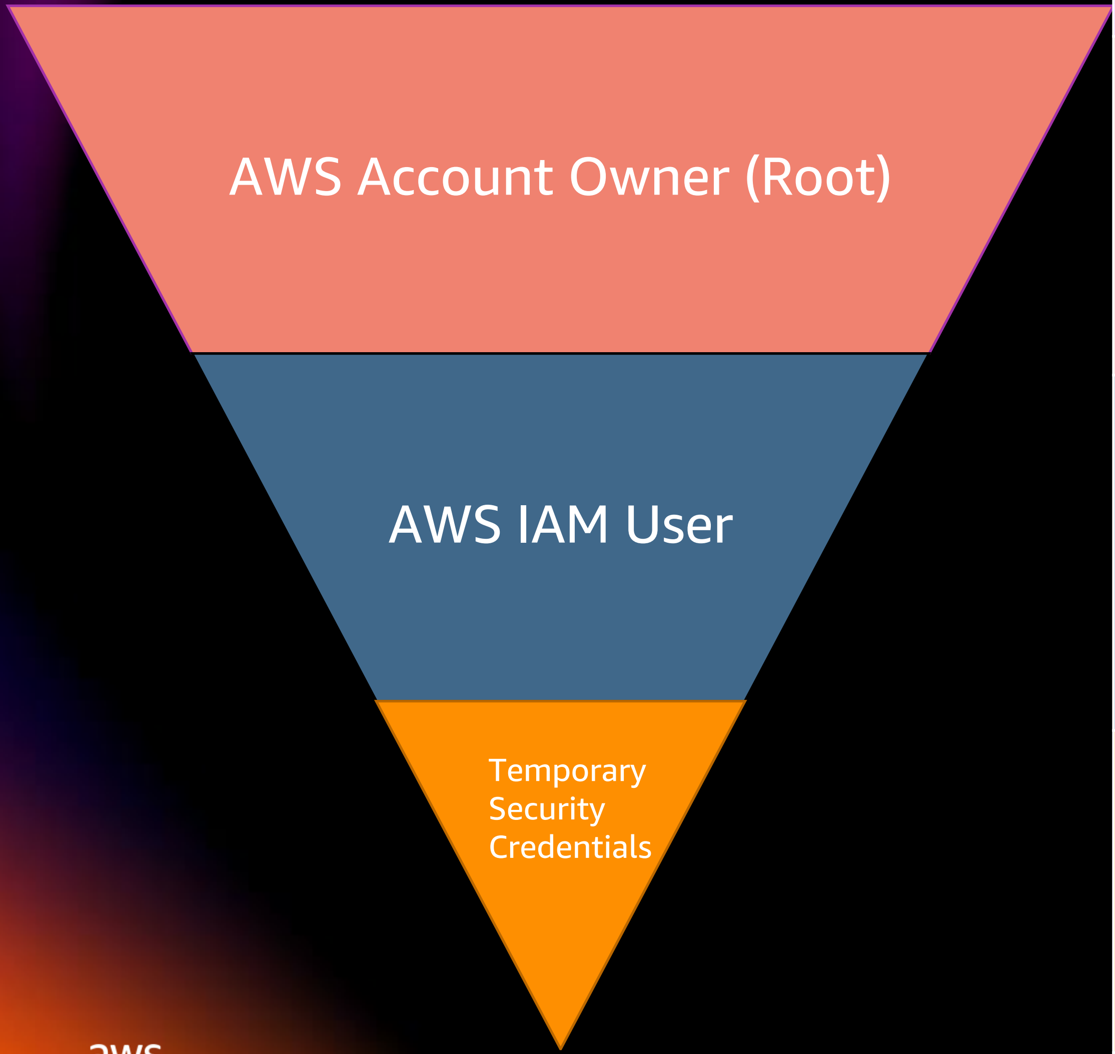
- Amazon RDS
- Amazon Aurora
- Amazon DynamoDB

Storage

- Amazon EBS
- Data lake
- Amazon S3

AWS IAM Hierarchy of Privileges

Enforce principle of least privilege with IAM users, groups, policies, and temporary credentials.



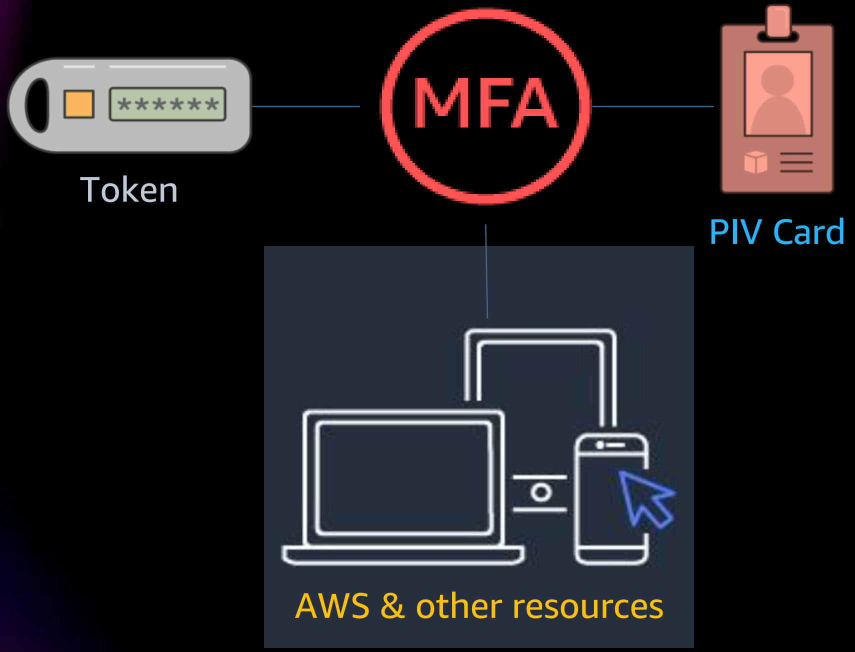
Permissions	Example

Unrestricted access to all enabled services and resources.	`Action: *`
	`Effect: Allow`
	`Resource: *`
	`(implicit)`

Access restricted by Group and User policies	`Action:`
	`[‘s3:*’,’sts:Get*’]`
	`Effect: Allow`
	`Resource: *`

Access restricted by generating identity and further by policies used to generate token	`Action: [ ‘s3:Get*’ ]`
	`Effect: Allow`
	`Resource:`
	`‘arn:aws:s3:::mybucket/*’`

Use multi-factor authentication (MFA)



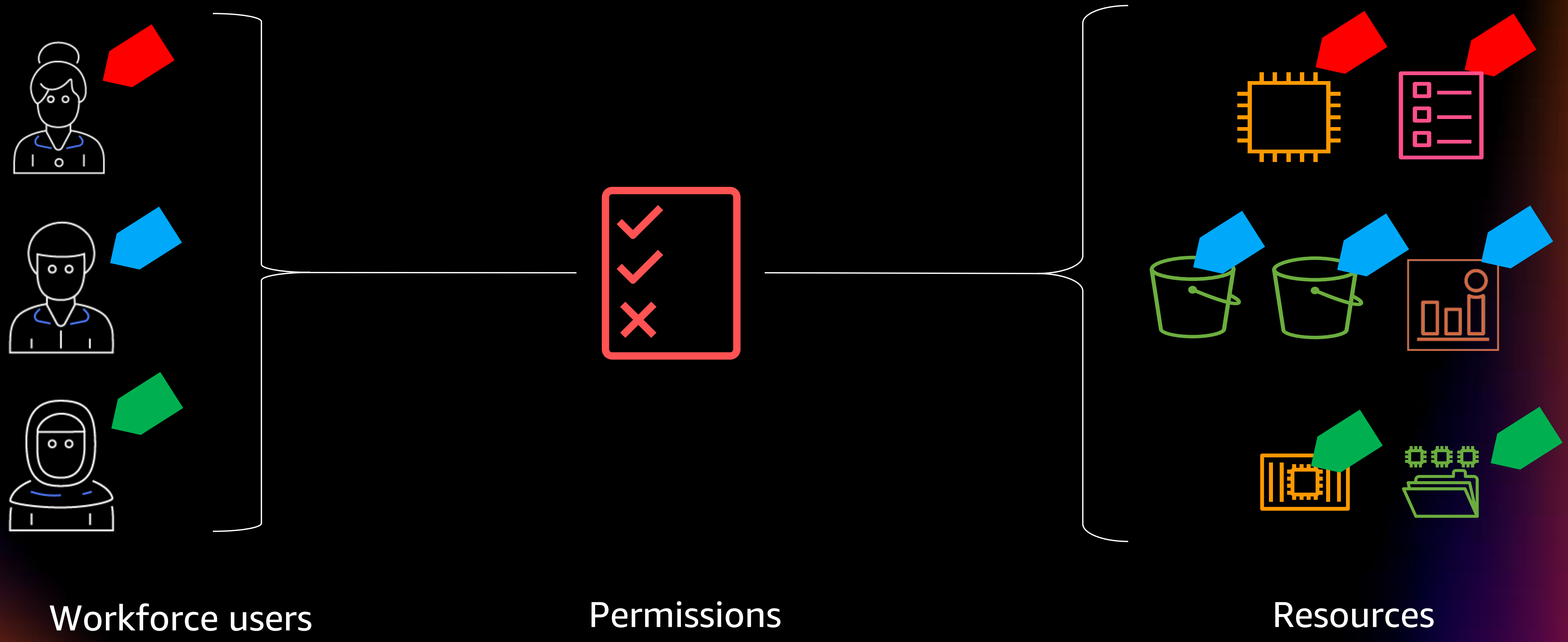
MFA adds an extra layer of protection on top of name and password for root, interactive IAM users

- Virtual MFA devices
- U2F security key
- Hardware MFA device

Identity federation changes the approach, but not the best practice

- Use MFA at your identity provider
- Also works with AWS Command Line Interface (AWS CLI) - version 2

A scalable permissions model based on attributes



AWS Key Management Service (AWS KMS)

What is AWS Key Management Service?

AWS Key Management Service (AWS KMS) makes it easy to create, manage, and securely store cryptographic keys

AWS KMS is incorporated in over 90 AWS services to encrypt sensitive data and create digital signatures

AWS Key Management Service (AWS KMS)

AWS KMS Benefits

Fully Managed Key Service

Secure, Centralized Key Management

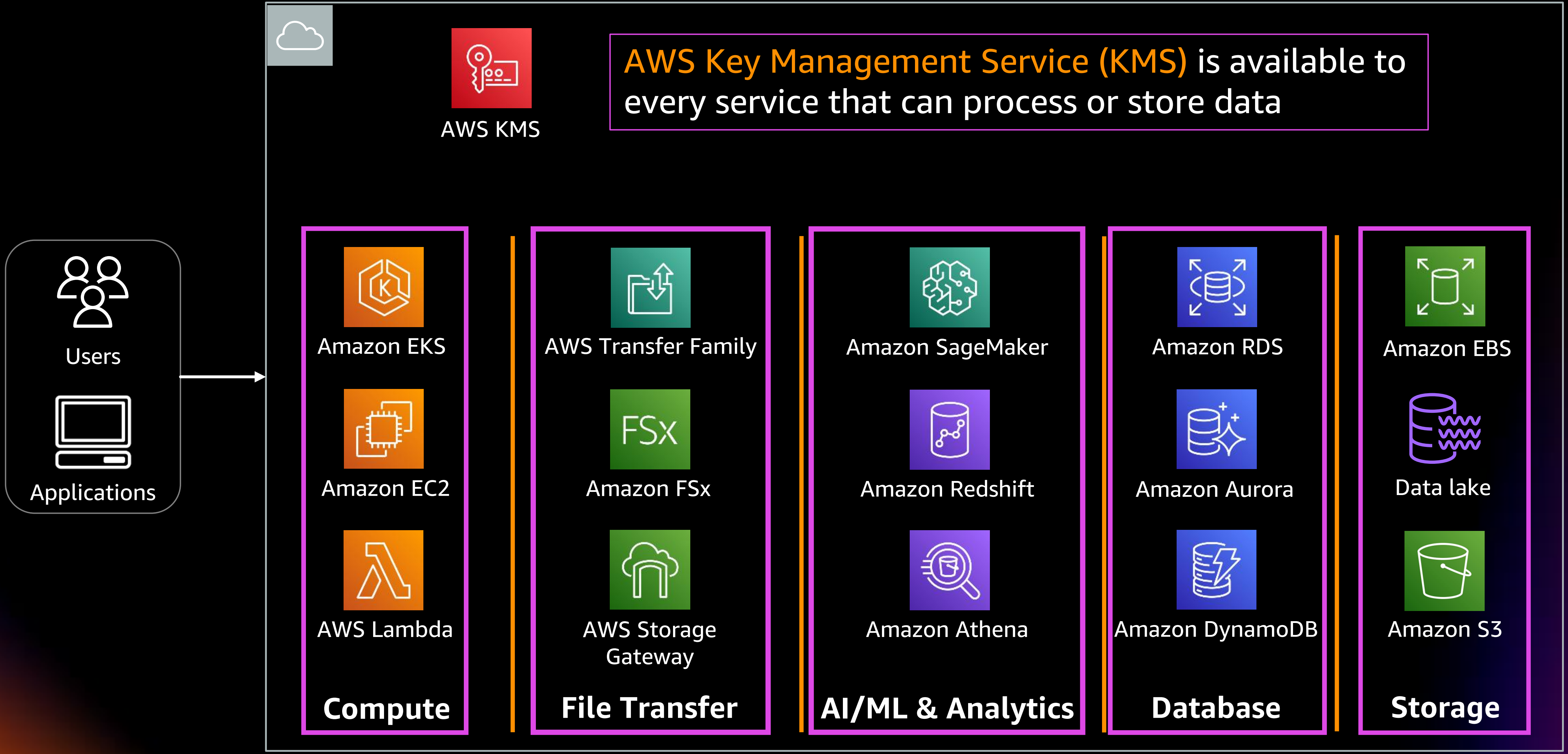
Encrypt Data in Your Applications

Native Integrations with AWS Services

Audit and Monitor Encryption Keys

Pay-as-You-Go Pricing

Where do I use AWS KMS?



AWS Key Management Service (KMS) is available to every service that can process or store data

AWS KMS helps you focus on what matters

- You control access to encrypted data with IAM policy and AWS KMS key policy

- AWS manages the underlying infrastructure - hardware security modules, key management APIs, and service integrations

- AWS KMS enforces the permissions you define in key policy and handles the durability and physical security of KMS keys

AWS KMS provides an additional layer of security

- Resources protected by AWS KMS require additional authorization

- Even with Amazon S3 full access, accessing objects backed by SSE-KMS requires authorization to use the AWS KMS key

- Amazon RDS separation of duties – separate access to instances and snapshots from access to secrets and credentials

AWS Secrets Manager

AWS Secrets Manager

AWS Secrets Manager enables customers to manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their lifecycle

- Prevent people from viewing or sharing secrets
- Stop secret sprawl
- Visibility into who uses which secrets and when
- Enable flexibility without waiting on other teams to provision secrets
- Roll-out secrets safely
- Rotate secrets safely with no downtime

AWS Secrets Manager benefits

Secure secrets storage

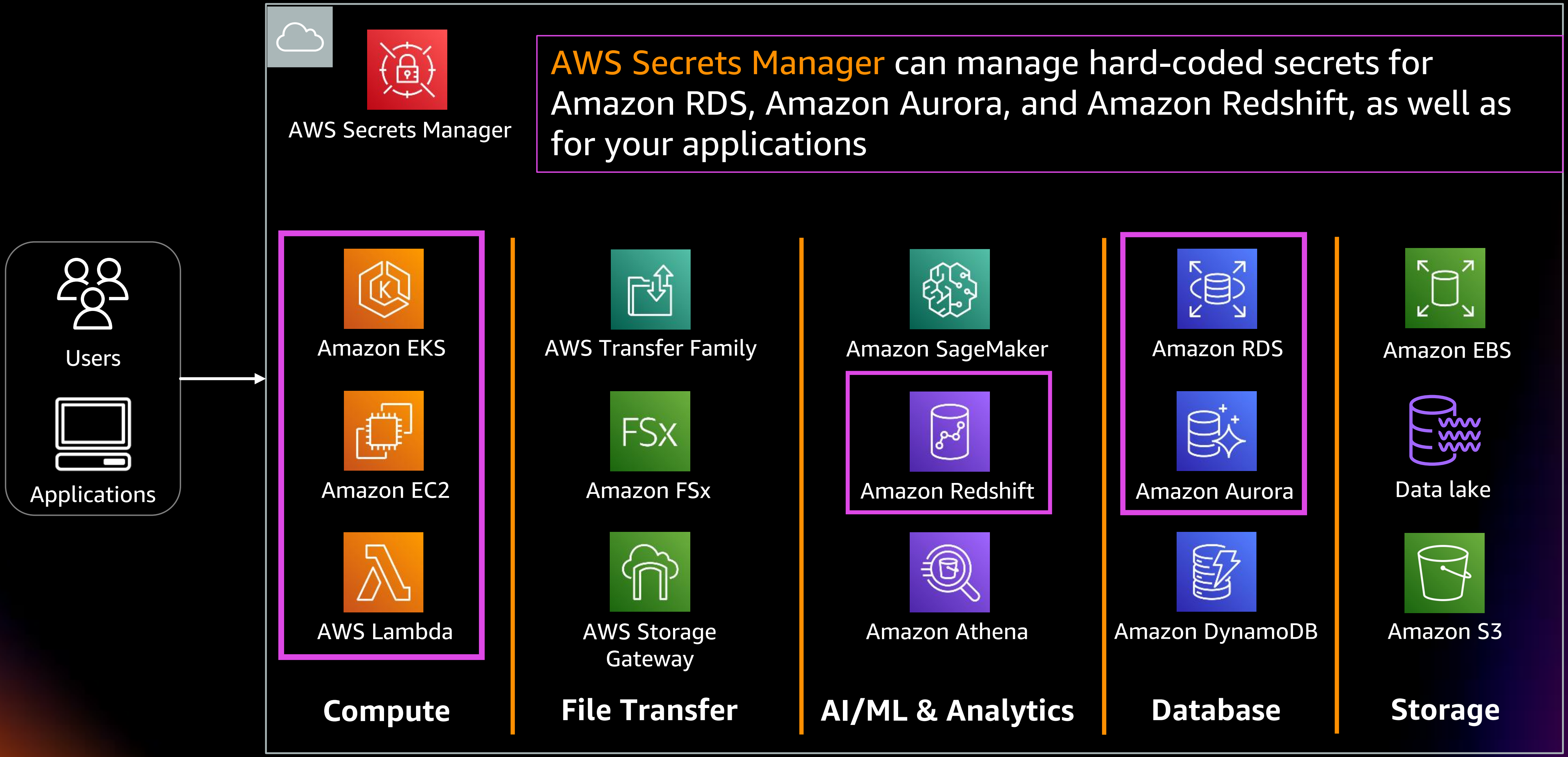
Fine-grained access control

Rotate secrets safely

Auditing and monitoring

Pay-as-you-go pricing

Where do I use AWS Secrets Manager?



AWS Secrets Manager can manage hard-coded secrets for Amazon RDS, Amazon Aurora, and Amazon Redshift, as well as for your applications

Fine-grained access control policies

- Use AWS IAM policies to manage access to your secrets for IAM users, roles, and groups to control access to individual secrets
- Use resource-based policies to access secrets across AWS accounts
- Assign tag-based policies for more granular access to your secrets with attribute-based access control (ABAC) using AWS IAM

Amazon Macie

What is Amazon Macie?

Amazon Macie enables you to discover and protect your sensitive data at scale.

Amazon Macie

Gain visibility and evaluate

- Bucket inventory
- Bucket policies

Discover sensitive data

- Inspection jobs
- Flexible scope

Centrally manage at scale

- AWS Organizations
- Managed & custom data detections

Gain visibility and evaluate

- Provides customers visibility into Amazon S3 bucket inventory
  - Number of buckets
  - Storage size
  - Object count
- Monitors changes to Amazon S3 bucket policies
  - Publicly accessible
  - Unencrypted
  - Shared outside of the account
  - Replicated to external accounts

Works across multiple accounts and automatically includes new buckets

Discover sensitive data

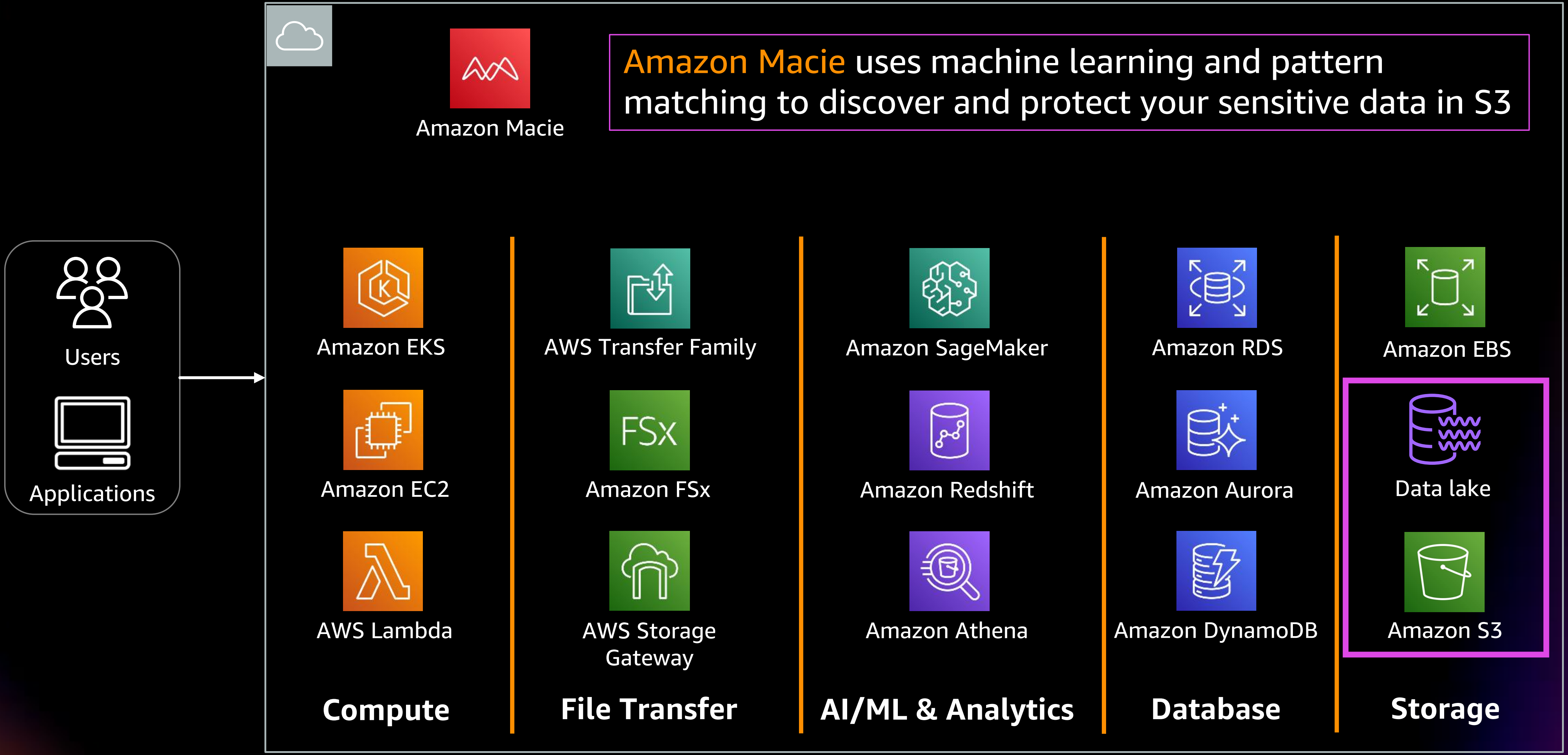
- Ongoing evaluation of your Amazon S3 environment and data

- Select target for data discovery
- Create and schedule jobs

- Define the scope
- Scheduled frequency (one-time, daily, weekly, monthly)
- Object criteria (Tags, modified time, extension type, size)

- Review status (complete, cancelled, idle)
- Take actions (Cancel, copy)

Where do I use Amazon Macie?



Amazon Macie uses machine learning and pattern matching to discover and protect your sensitive data in S3

Centrally manage at scale

Primary/Member setup

- Multi-accounts with up to 1,000 member accounts
- AWS Organizations support up to 5,000 accounts
- Macie primary account can create jobs on behalf of members
- One-click deployment with no upfront data source integration

Centrally Manage at Scale – Managed data types

Amazon Macie maintains a growing list of sensitive data types that include common personally identifiable information (PII) and other sensitive data types as defined by data privacy regulations.

File formats

.txt .json .xml Avro
.csv .tsv
.doc .docx .xls .xlsx
.pdf
.tar .zip .gzip
Parquet

Data types

- *Financial (card, bank account numbers…)*
- *Personal (names, address, contact…)*
- *National (passport, ID, driver license…)*
- *Medical (healthcare, drug agency …)*
- *Credentials & secrets*

Centrally manage at scale – Custom data types

Amazon Macie provides you the ability to add custom-defined data types using regular expressions to enable Macie to discover proprietary or unique sensitive data for your business.

- *Regular expression that defines a pattern to match*
- *Keywords that define specific text to match*
- *Ignore words that define specific text to exclude*

Automate and take actions – Finding types

Finding types

- Bucket policy findings
- Sensitive data discovery findings

Findings categorised by

- By bucket
- By type
- By job

Detailed and actionable security and sensitive data discovery findings

- Findings sent to Amazon CloudWatch Events
- Bucket policy findings sent to Security Hub

AWS Backup

Cloud-native backup challenges

Backup operations siloed across AWS services

Complexity

- Custom scripts needed to automate & manage backups
- Lack of centralized monitoring
- Auditing distributed logs is time consuming
- Data protection sprawl with too many tools

Compliance

- Difficult reporting for audit and compliance
- Lack of automated policy enforcement for data protection
- Per-service IAM roles are difficult to manage

Cost

- Time and resources allocated to building, maintaining and supporting data protection tools
- Potential for non-compliance penalties
- Exposure resulting from inefficient DR and retention policies

AWS Backup – meeting the challenges

Backup operations unified across AWS services

Complexity

- Policy- and tag-based backup solution
- Automated backup scheduling

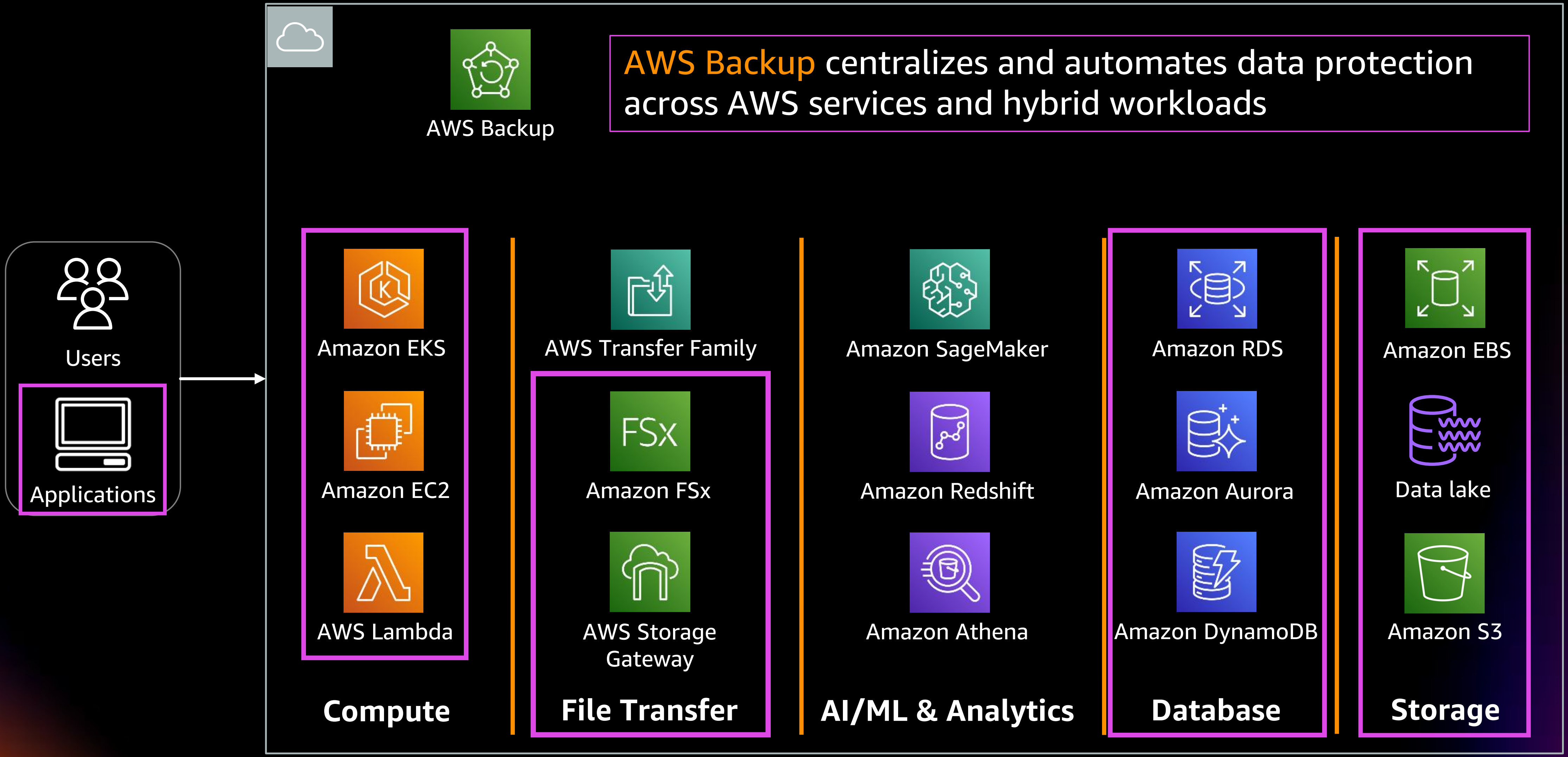
Compliance

- Centralized backup activity monitoring and logs
- Backup encryption
- Backup access policies

Cost

- Automated backup retention management
- No added cost for orchestration

Where do I use AWS Backup?



AWS Backup centralizes and automates data protection across AWS services and hybrid workloads

Use AWS Backup Vault

Cloud-native Backups

Protect your critical data across AWS services

Vault level protection

Compliance

Business & regulatory compliance

WORM storage

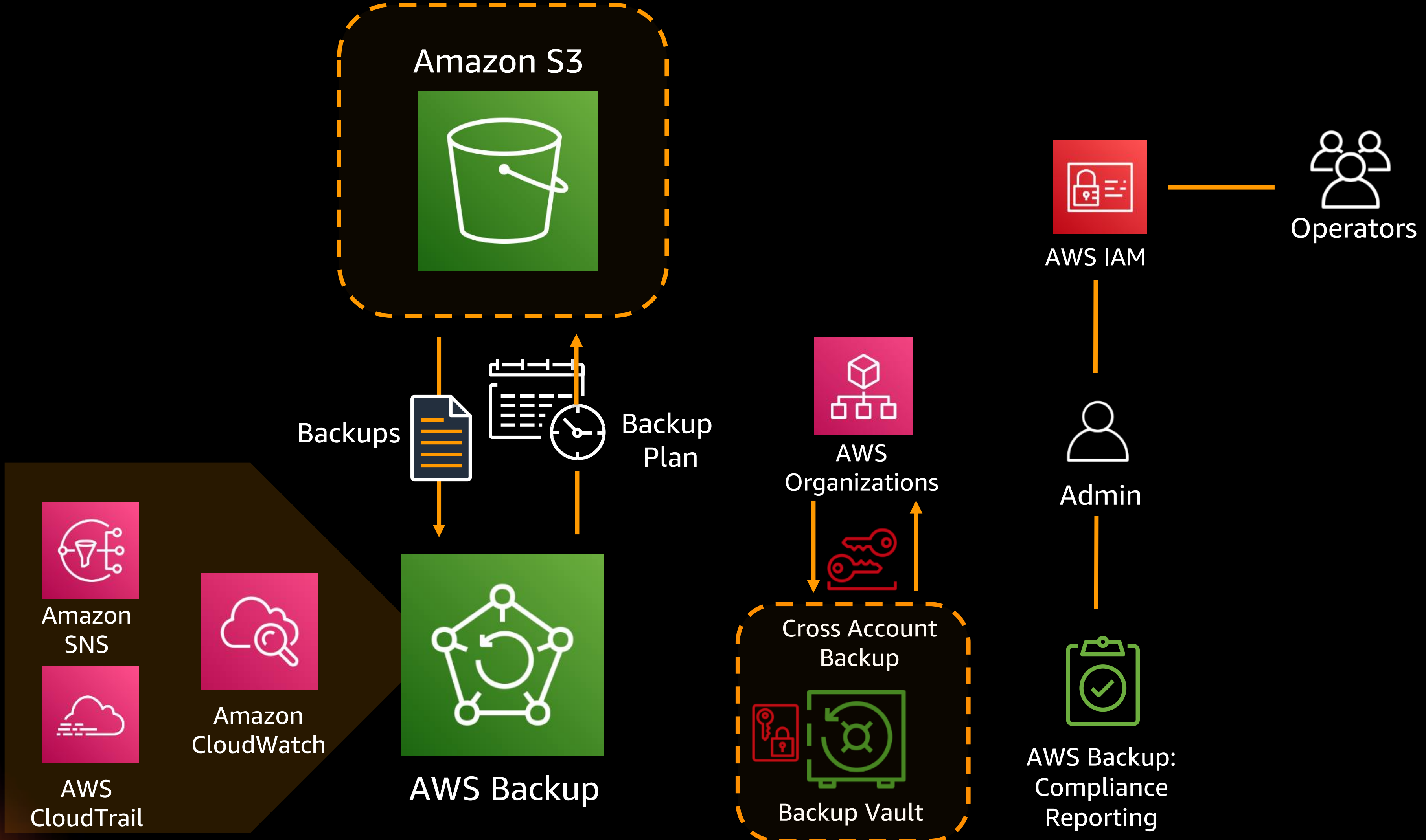
Disaster Recovery

Reduce risk of downtime and build foundation for business continuity

Malicious or accidental actions

AWS Backup for Amazon Simple Storage Service (Amazon S3)

CREATE AUTOMATED CONTINUOUS OR PERIODIC BACKUPS USING A CENTRAL BACKUP PLAN



AWS Backup protects in-cloud and hybrid application data

AWS Backup

Policy-based, centralized data protection and management

Hybrid Workloads

AWS Storage Gateway

vmware

AWS Storage Services

- Amazon EBS
- Amazon FSx
- Amazon EFS
- Amazon S3

VMs and Applications

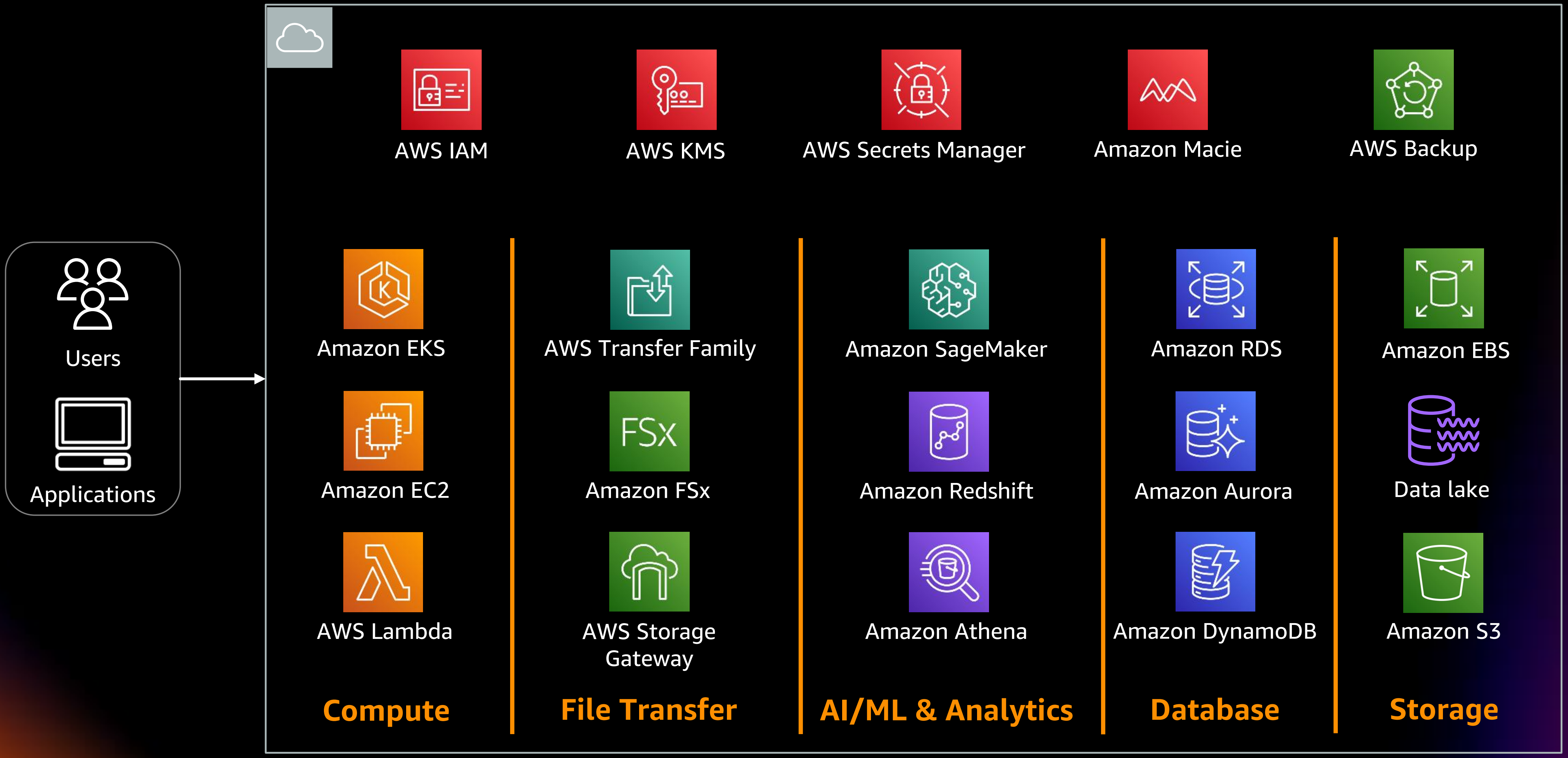
- Amazon EC2
- Windows
- SQL Server

Managed Databases

- Amazon RDS
- Amazon Aurora
- Amazon DynamoDB
- Amazon Neptune
- Amazon DocumentDB (with MongoDB compatibility)

Wrap up and summary

Use the foundational services to protect data



Users

Applications

AWS IAM

AWS KMS

AWS Secrets Manager

Amazon Macie

AWS Backup

Compute

Amazon EKS

Amazon EC2

AWS Lambda

File Transfer

AWS Transfer Family

Amazon FSx

AWS Storage Gateway

AI/ML & Analytics

Amazon SageMaker

Amazon Redshift

Amazon Athena

Database

Amazon RDS

Amazon Aurora

Amazon DynamoDB

Storage

Amazon EBS

Data lake

Amazon S3

AWS has data protection resources to help organisations at any stage of their cloud journey

Use data protection services to achieve granular control over access and policy enforcement

Reduce operational risk through automation and increased visibility

Engage with the AWS network of security and consulting partners

Visit the AWS Data resource hub

A modern data strategy can help you manage, act on, and react to your data so you can make better decisions, respond faster, and uncover new opportunities. Dive deeper with these resources today.

- Harness data to reinvent your organization
- In unpredictable times, a data strategy is key
- Make data a strategic asset
- Rewiring your culture to be data-driven
- Put your data to work with a modern analytics approach
- … and more!

https://tinyurl.com/data-hub-aws

Visit resource hub

AWS Training and Certification for Data and Analytics

AWS Data & Analytics FREE Training Resources

Discover how to harness data, one of the world's most valuable resources, and innovate at scale.

https://bit.ly/3Ntlhy7

AWS Data Analytics Learning Plan

This learning plan expose you to the fastest way to get answers from all your data to all your users. It can also help prepare you for the AWS Certified Data Analytics - Specialty certification exam.

https://bit.ly/3wBVjD1

AWS Certified Data Analytics - Specialty

Earning AWS Certified Data Analytics – Specialty validates expertise in using AWS data lakes and analytics services.

https://go.aws/3lwF0RR

Thank you for attending AWS Innovate – Data Edition

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.

- aws-apj-marketing@amazon.com
- twitter.com/AWSCloud
- facebook.com/AmazonWebServices
- youtube.com/user/AmazonWebServices
- slideshare.net/AmazonWebServices
- twitch.tv/aws

Thank you!