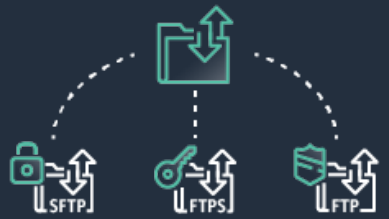
AWS Transfer Family

Simply and seamlessly set up secure file transfers to Amazon S3 over SFTP and other protocols



Smitha Sriram, Product Manager, AWS
Jeff Bartley, Data Transfer Solutions Architect, AWS

Agenda

- AWS Transfer Family overview
- Use cases & benefits
- Recent launches
- Demo
- Recap
- Q&A

Where are file transfers used?

Third party file transfers

Data distribution

Internal Applications for Data Lakes

Integrate with your vendors, suppliers, research organizations, end customers, or internal legacy applications for access to data lakes in AWS

aws

Challenges with self-managed file transfer systems

Managing servers & storage

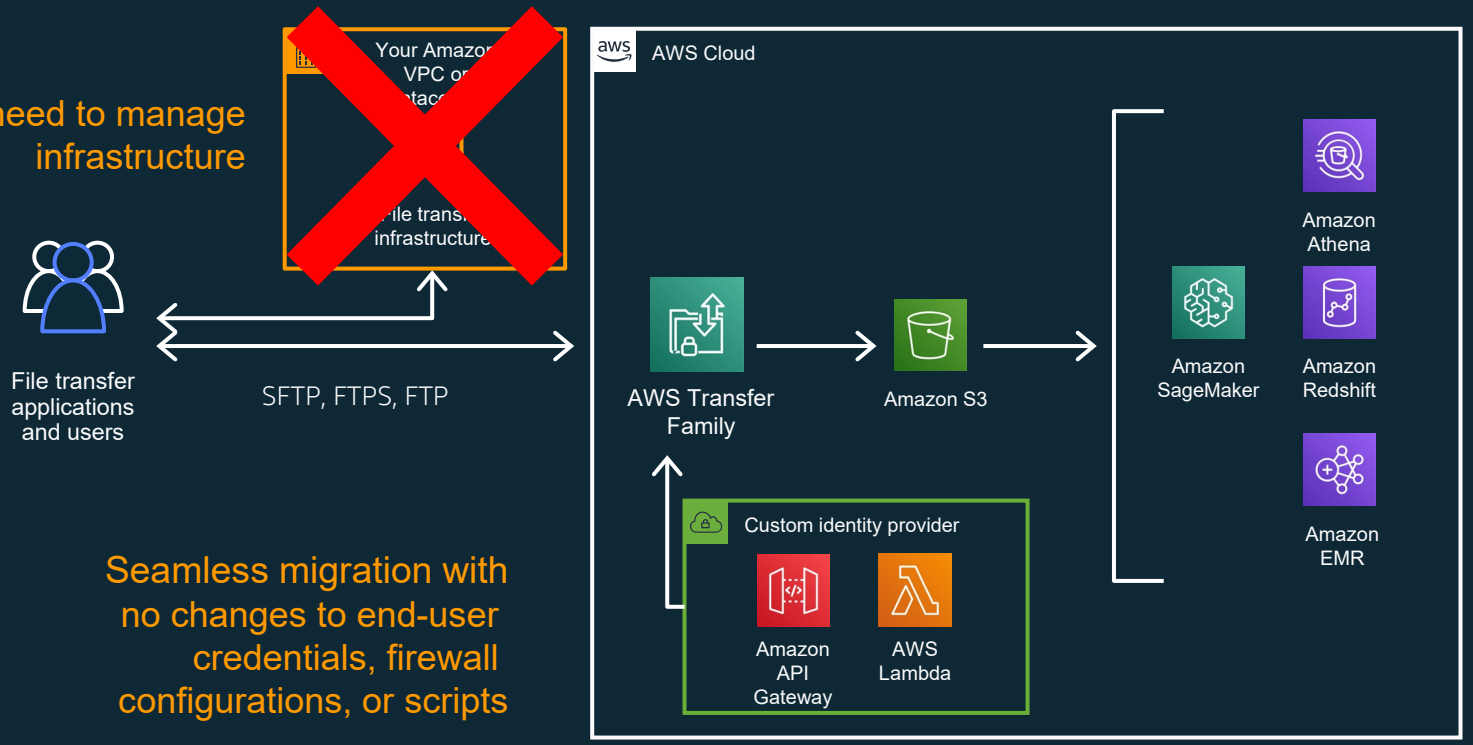
Scalability & reliability

Security & maintenance

aws

AWS Transfer Family

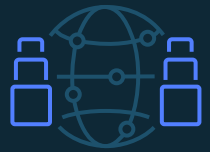
No need to manage infrastructure



Store data in S3 and modernize workflows using cloud native services

Seamless migration with no changes to end-user credentials, firewall configurations, or scripts

AWS Transfer Family benefits



Fully Managed

- Highly available across up to 3 AZs
- Scales on demand
- Supports thousands of concurrent users

Seamless Migration

- Import host keys
- Use your own IP addresses and hostnames
- Use existing authentication systems

Secure & Compliant

- IP address filtering
- Support for VPC endpoints
- SOC, PCI, HIPAA, FISMA compliance

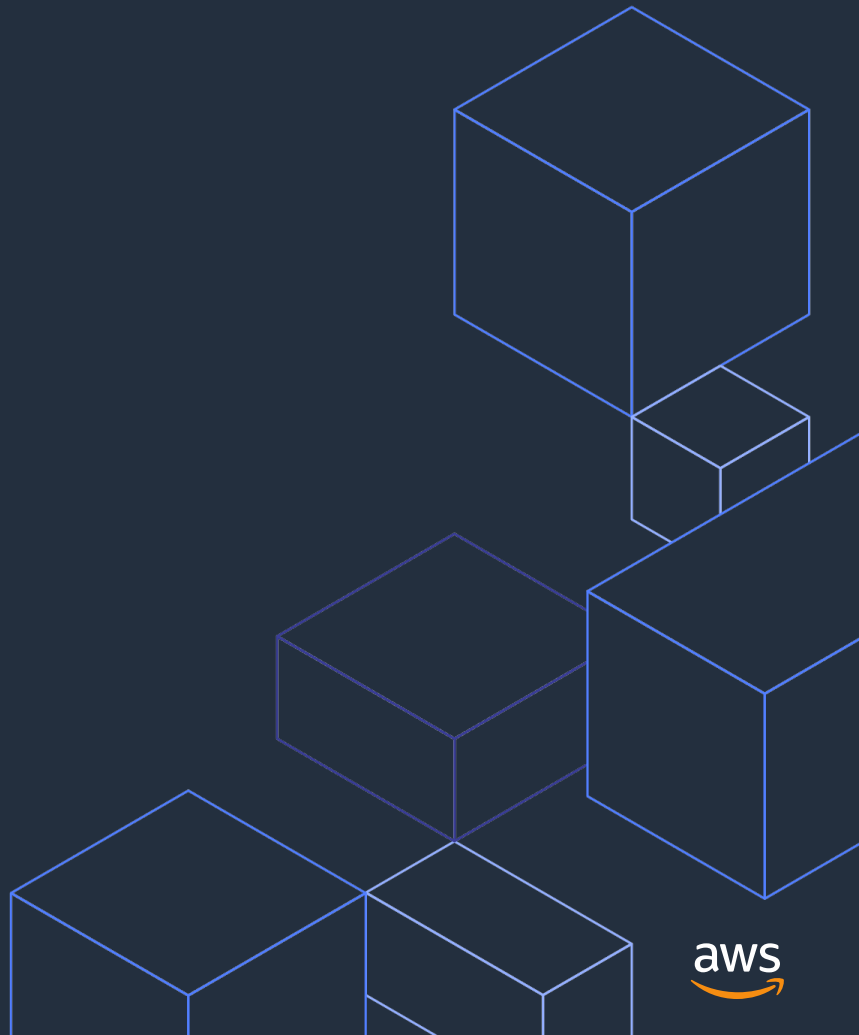
AWS Integrated

- Store data in S3 and access using AWS services
- Log to CloudTrail and CloudWatch
- Custom authentication using API Gateway and Lambda

AWS Transfer Family customers

aws

Recent Launches



AWS Transfer Family Launches YTD

FTPS & FTP

Source IP as a factor for authorization

Enhanced traceability in logs and events

Expanded username support NEW!

Security Policies for encryption algorithms NEW!

FIPS endpoints NEW!

April 2020	June 2020	July 2020	August 2020

Available in 16 AWS commercial Regions

aws

FTP & FTPS

FTP

Use case: Non-sensitive/publicly accessible data or data that's encrypted on the client side

- Only supported within VPC – no public or Internet-facing access
- Requires custom authentication (*for now*)
- Passive mode only
- Best practice: use different passwords between FTP and FTPS/SFTP

FTPS

Use case: Data that needs encryption, customer CRM/ERP applications that can't use SFTP today

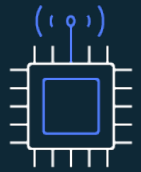
- Supported on Internet-facing and VPC-only endpoints
- Requires custom authentication (*for now*)
- Passive mode only
- BYO ACM certificate
- Explicit FTPS only

SFTP, FTP, and FTPS all supported on the same server (if endpoint requirements are met)

Sample FTPS/FTP industry applications

Automotive
Dealer management platforms

M&E
Content management platforms



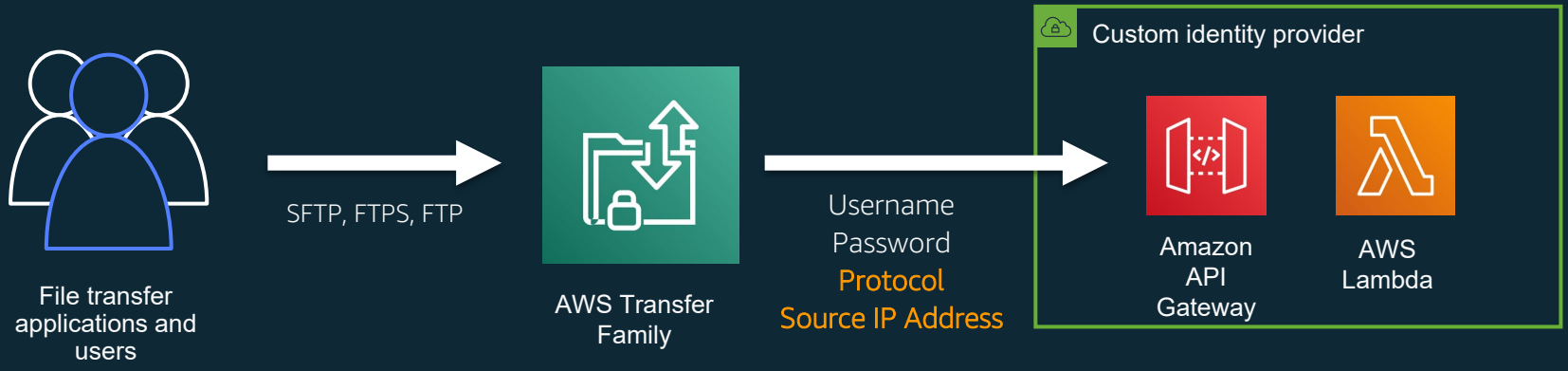
Manufacturing
Device integrations

Utility
Supply chain platforms

Financial Services
Data acquisition and distribution, payment solutions

aws

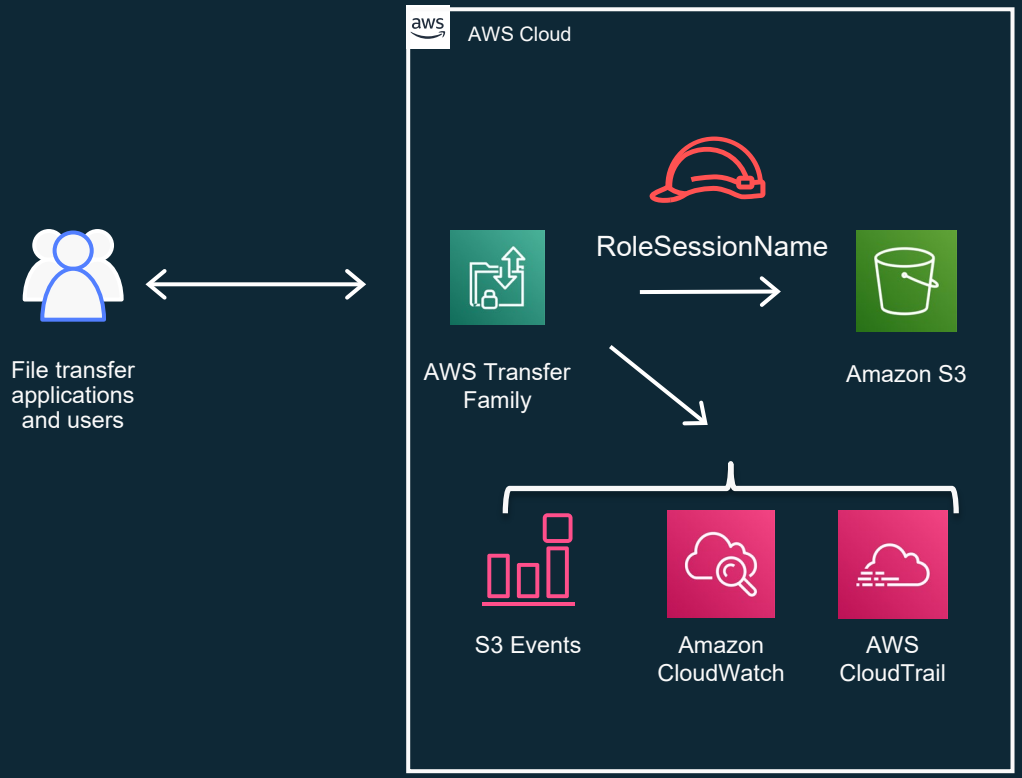
Source IP authentication



Benefits

- Additional authentication mechanism
- Scale IP address allow/deny beyond security group limits

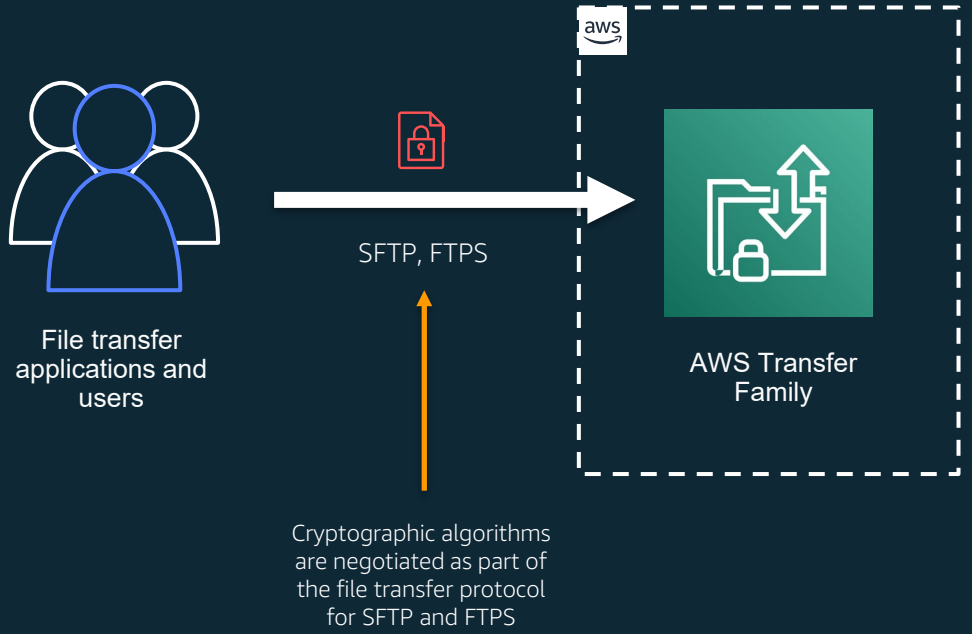
Enhanced Traceability in logs and events



RoleSessionName

- Stored in PrincipleId field
- RoleARN username.sessionid@server-id
- S3 Access & CloudTrail logs (object level logging)
- S3 Event notifications

Security policies for cryptographic algorithms



Security policies:

- Transfer-Security-Policy-2018-11 (Default)
- Transfer-Security-Policy-2020-06 (restrictive – No SHA1 policies)
- Transfer-FIPS-2020-06 (only FIPS compliant algorithms)

Expanded support for usernames

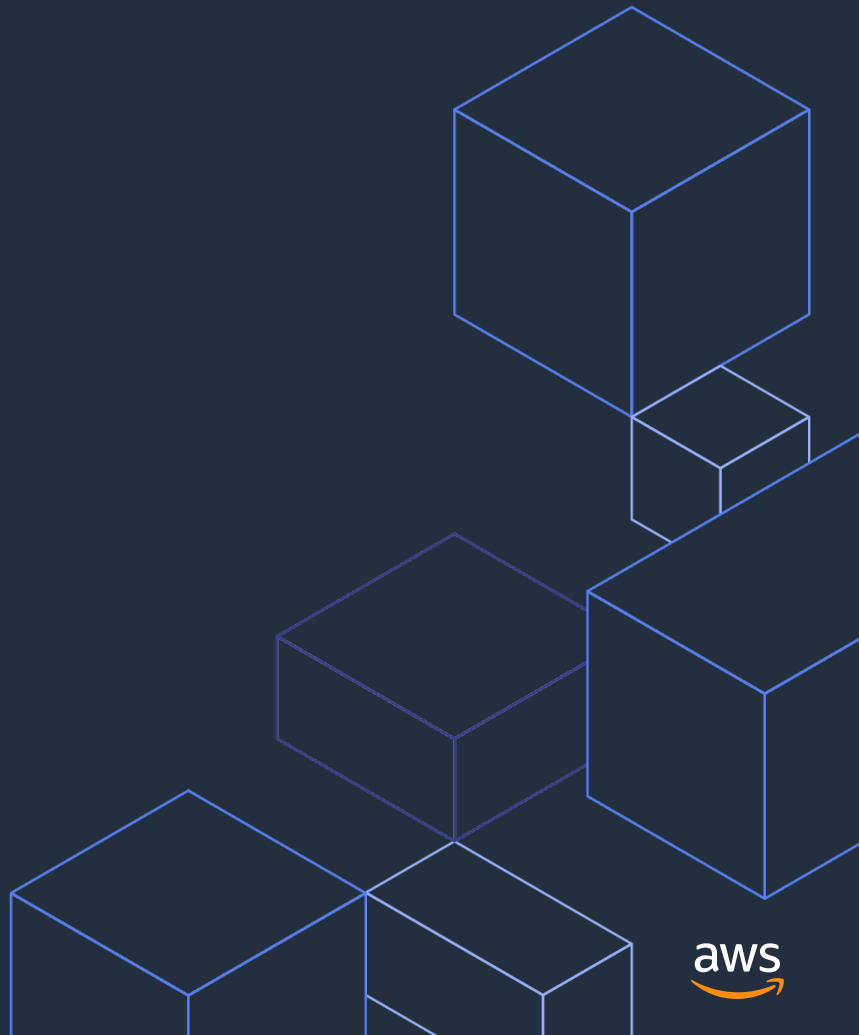
- Expanded supported character set to include @ and .
- Increased username limit from 32 to 100 characters

Use cases

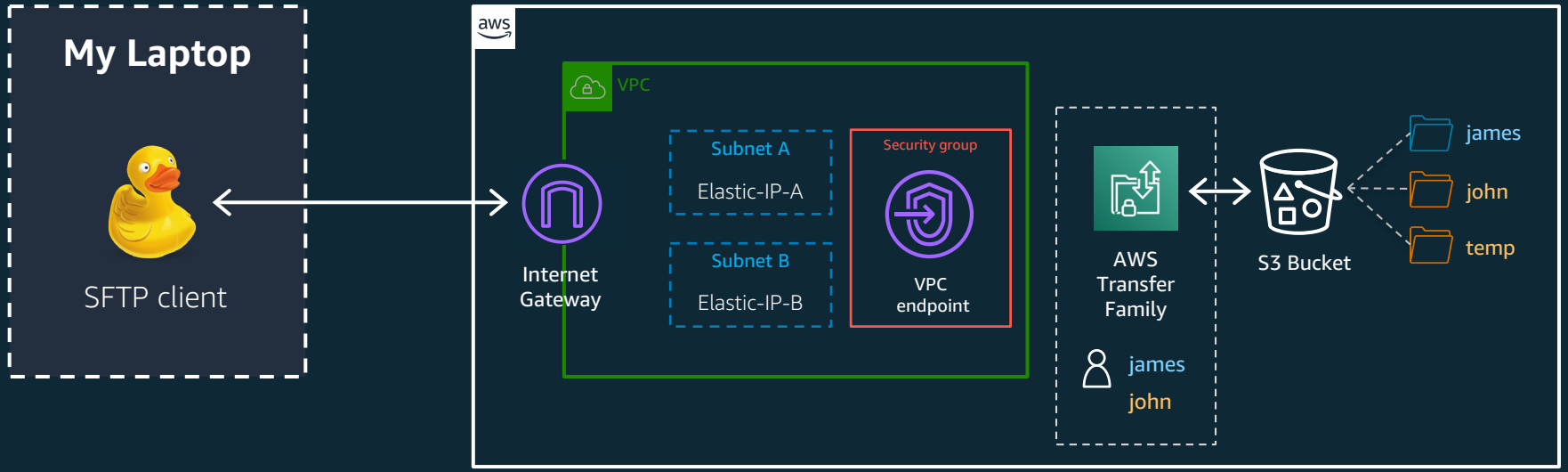
- Use email addresses as usernames for login (myname@emaildomain.com)
- Support directory domains to enable access controls based on domain (userID@DirectoryDomain.com)

aws

Demo

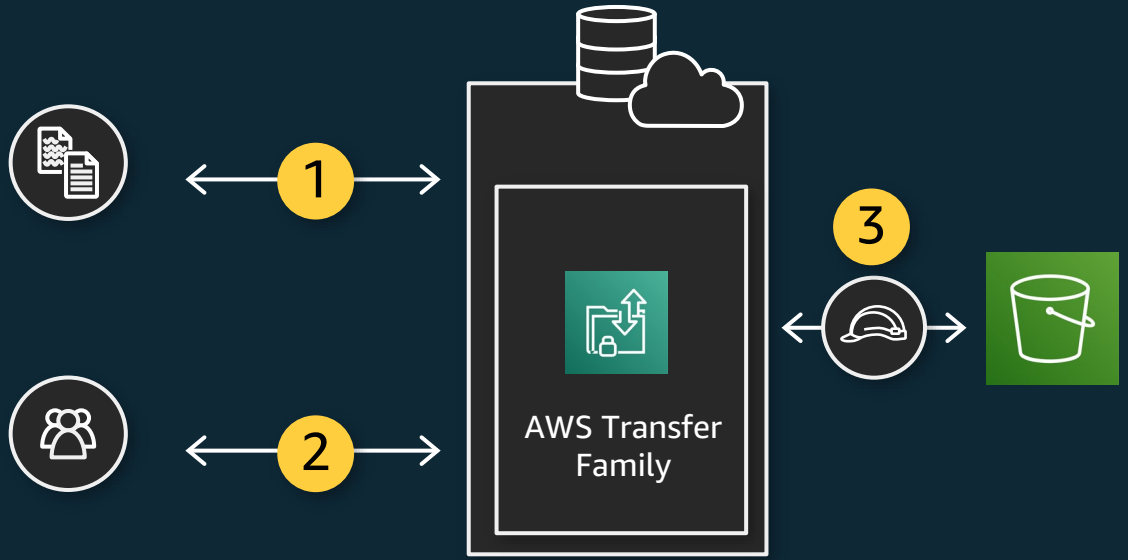


Demo architecture



Service managed authentication

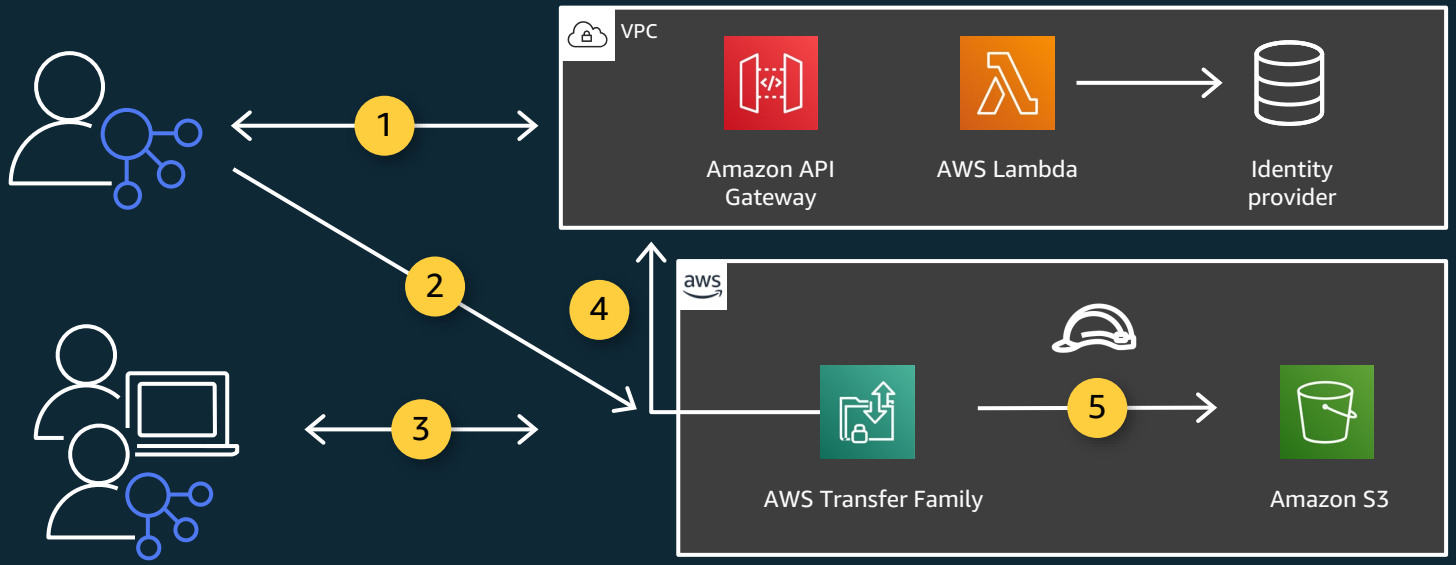
Store and manage user identities and keys inside the service



1. Configure your users' credentials and keys using the AWS Console
2. Users serviced using their existing clients and credentials
3. Amazon S3 accessed using AWS IAM during file transfers

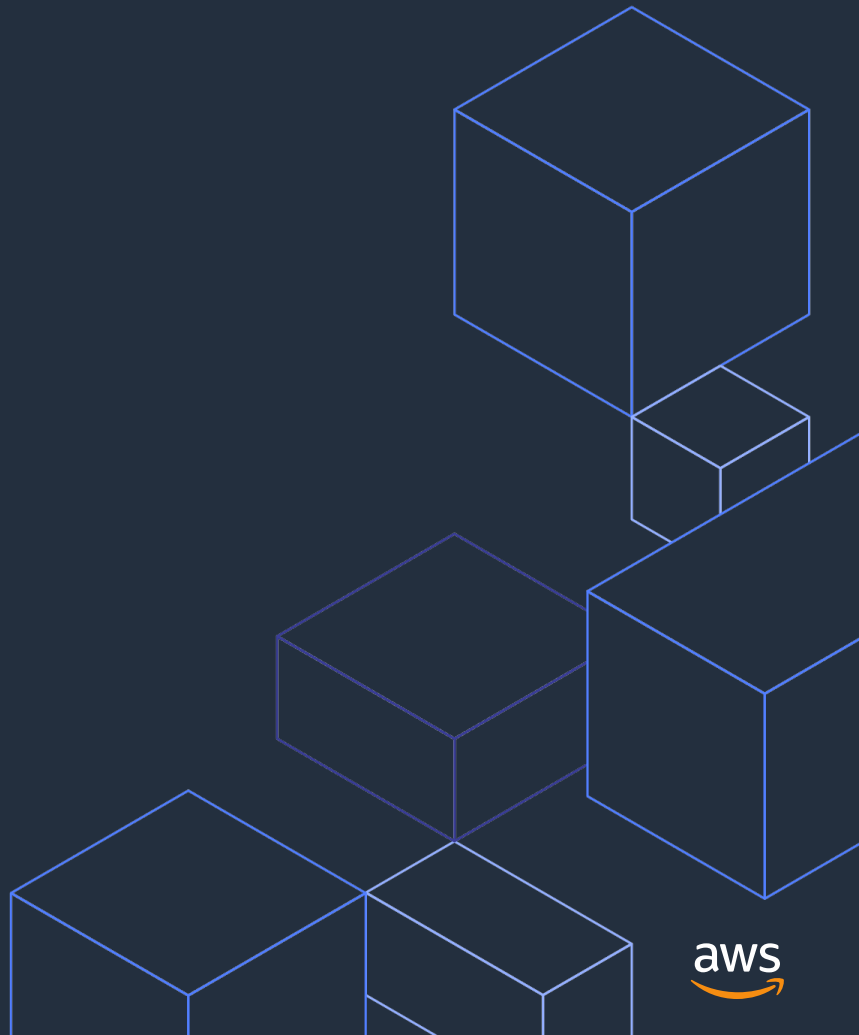
“Bring Your Own” (Custom) authentication

Integrate an existing identity provider



Set up an API Gateway and Lambda for Identity Provider access → API Gateway URL supplied during SFTP server creation → End users login using SFTP client and credentials → API Gateway and Lambda are invoked to authenticate → Response from API Gateway used to authorize S3 access

Recap



Migration recap

Seamlessly migrate users from existing systems

✓ Same Protocols	→	Enable SFTP, FTPS, & FTP
✓ Same credentials	→	Use existing identity management systems
✓ Same firewall configurations	→	Elastic IP support
✓ Same scripts	→	Logical directory mappings
✓ Same identity files	→	BYO host key (SFTP) and TLS certificate (FTPS)

aws

Resources

Blogs

- AWS Transfer for FTP and FTPS, in addition to existing SFTP
- Using Okta with multi-factor authentication for AWS Transfer for SFTP
- Use IP whitelisting to secure your AWS Transfer for SFTP servers
- Centralize data access using AWS Transfer Family and AWS Storage Gateway
- How Liberty Mutual uses AWS Transfer Family to manage financial data

Workshops

- Access data in Amazon S3 using AWS Transfer Family and AWS Storage Gateway
- Using IP whitelisting to secure your AWS Transfer for SFTP servers

Videos

- Transfer Family Overview
- Transfer family Demo

aws

Thank you!