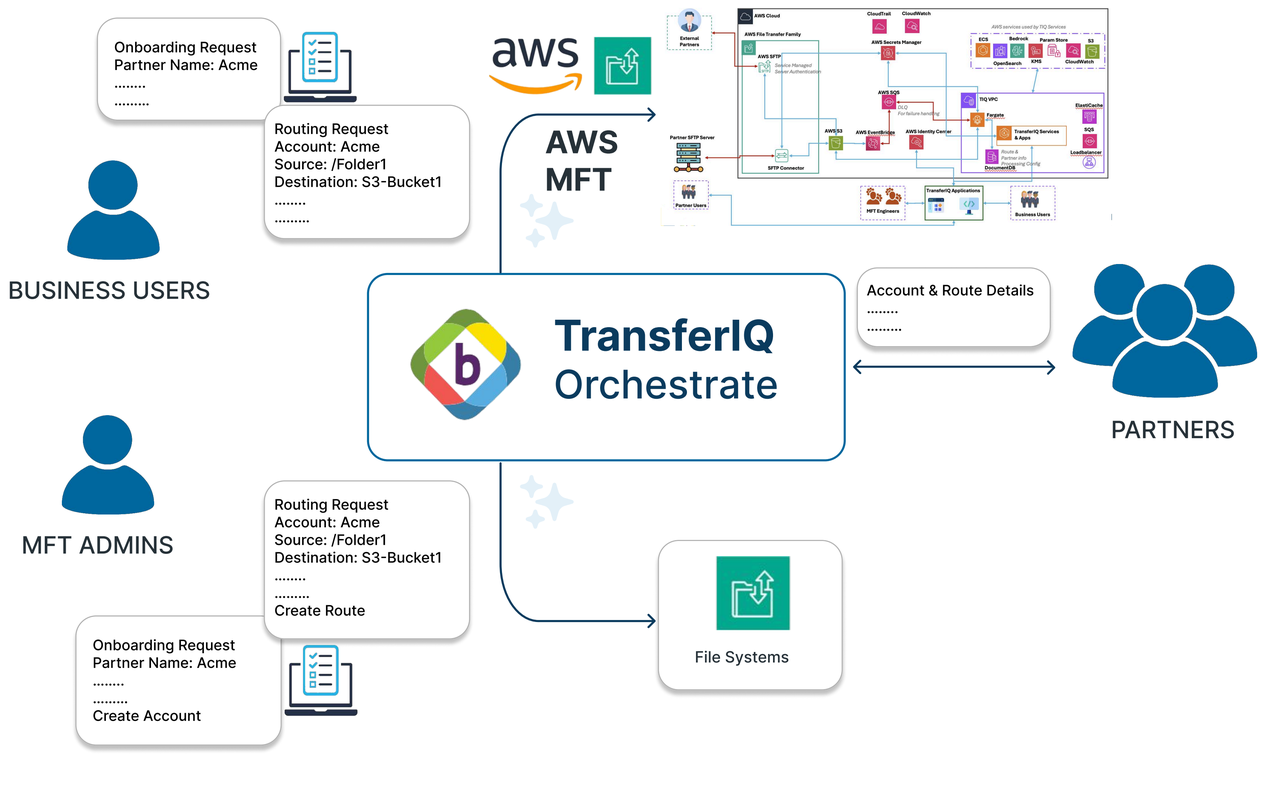
TransferIQ Orchestrate for AWS - Deployment Overview.

This document provides an overview of the deployment process for TransferIQ Orchestrate for AWS Managed File Transfer (MFT) in a Bring-Your-Own-Cloud (BYOC) model, as part of the AWS Marketplace submission review. It details how the application is deployed, including the delivery mechanism, infrastructure setup, and security considerations. A placeholder for the network architecture diagram is included to illustrate the deployment topology. This collateral ensures compliance with AWS Marketplace guidelines for Software-as-a-Service (SaaS) products, focusing on secure, scalable, and customer-managed deployment.



Product Overview

TransferIQ Orchestrate is a secure, scalable MFT solution delivered via the AWS Marketplace, designed to simplify file transfers with multi-protocol support (SFTP, FTPS, HTTPS, AS2, EDI) and automated infrastructure setup. In the BYOC model, the application is deployed in the customer's AWS account, leveraging AWS Transfer Family, S3, and EKS/ECS for scalability and security. The application includes Admin pages for launching CloudFormation or Terraform scripts to configure the MFT infrastructure, ensuring least-privilege access and compliance with HIPAA, PCI DSS, and GDPR standards.

Deployment Process

TransferIQ Orchestrate is delivered as a container-based SaaS product, deployable via Amazon Elastic Container Service (ECS) or Elastic Kubernetes Service (EKS), aligning with AWS Marketplace guidelines for SaaS products. The container delivery method was chosen for its portability, native Kubernetes integration, and simplified updates, as outlined in the AMI vs. container options evaluation. Below is the step-by-step deployment process:

Subscription via AWS Marketplace

- Customers subscribe to TransferIQ Orchestrate through the AWS Marketplace, selecting the Bring-Your-Own-License (BYOL) pricing model.
- The subscription process is initiated in the AWS Marketplace Management Portal, where customers agree to the End User License Agreement (EULA).

Container Image Deployment

- **Upon subscription, customers access the container image (Docker-based) from the AWS Marketplace.**
- **The container is deployed to the customer's AWS account, targeting either ECS (Fargate for serverless) or EKS (for Kubernetes orchestration).**
- **Deployment is performed via the AWS Management Console, CLI, or Infrastructure-as-Code tools (e.g., CloudFormation, Terraform).**

License Activation

- Customers activate the application on container startup using a BYOL key provided during subscription.
- The activation process validates the license and initializes the application within the customer's VPC.

Infrastructure Configuration via Admin Pages

- Customers access the TransferIQ Orchestrate Admin pages, hosted within the deployed container, to configure the MFT infrastructure.
- Admin pages validate the AWS MFT Admin's credentials, requiring IAM permissions for:
- Managing VPCs, subnets, security groups, IAM roles, S3 buckets, EKS clusters, ECS tasks, ALB/NLB, and AWS Transfer Family endpoints.
- Accessing AWS KMS (encryption), CloudWatch (monitoring), CloudTrail (auditing), and S3 (file storage).
- The Admin pages launch predefined CloudFormation or Terraform scripts to provision:
  - **VPC Configuration:** Private subnets, NAT Gateways, and VPC endpoints for network isolation.
  - **IAM Roles:** Least-privilege roles for MFT operations, integrated with Kubernetes RBAC for EKS deployments.
  - **S3 Buckets:** Secure directory structures with bucket policies and prefixes for file exchanges.
  - **EKS/ECS Cluster:** Kubernetes-based scaling for high availability, with two container replicas across separate Availability Zones (AZs).
  - **Load Balancer:** Application Load Balancer (ALB) or Network Load Balancer (NLB) for failover.
  - **AWS Transfer Family:** Endpoints for secure file transfers.

Workflow and Route Setup

- Customers configure file exchange routes and partner accounts via the Admin pages, defining S3 directory access for business units or partners.
- Access controls are enforced through S3 bucket policies and IAM roles, ensuring data isolation

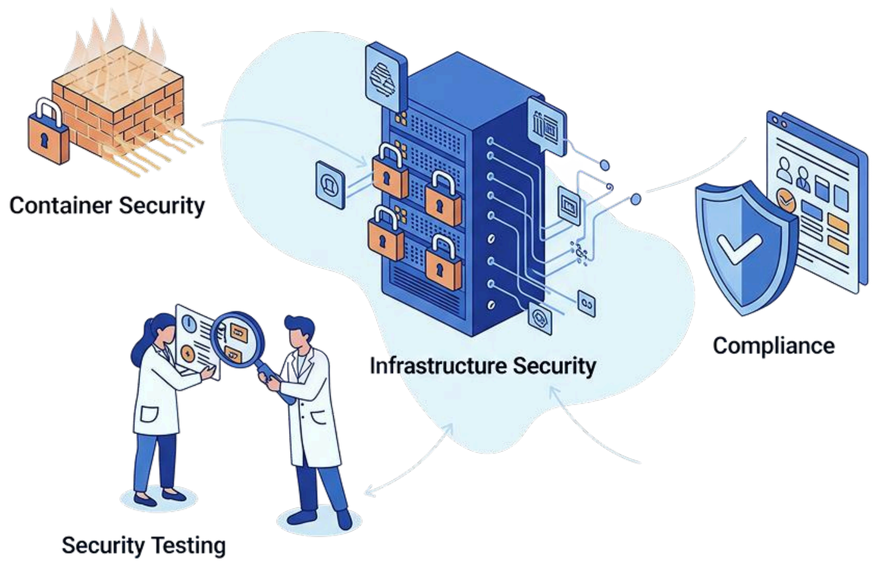
Monitoring and Support

- The deployment integrates with CloudWatch for monitoring, CloudTrail for auditing, and AWS KMS for end-to-end encryption.
- TransferIQ provides technical support for configuration, troubleshooting, and API integration, accessible via the AWS Marketplace support channel.

Security and Compliance

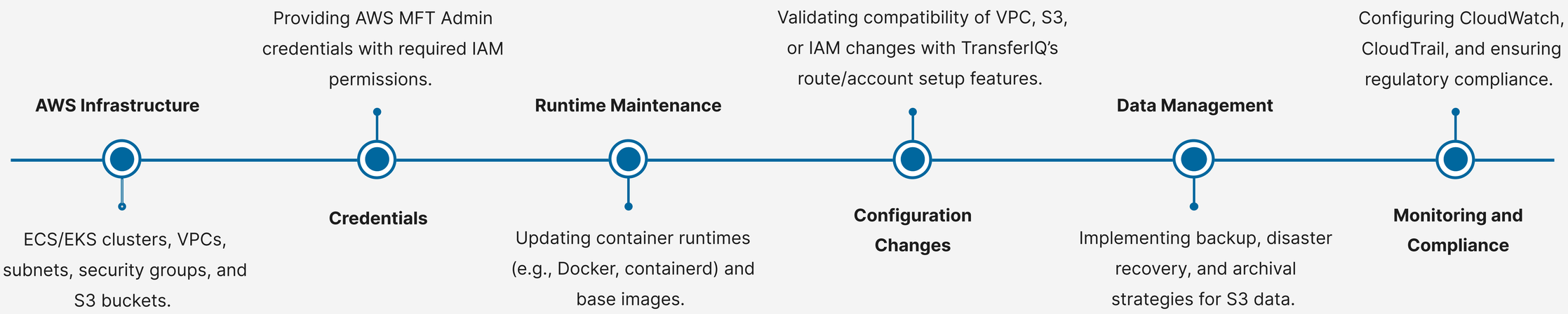
TransferIQ Orchestrate adheres to AWS Marketplace security guidelines, ensuring a secure deployment environment:

- **Container Security:**
  - The container image is built with a minimal base layer, scanned for vulnerabilities using Docker Scout or Trivy before publication.
  - Images are free of default credentials, with root login disabled and only Sudo access accounts permitted.
  - Software Composition Analysis (SCA) via OWASP Dependency-Check ensures no vulnerable third-party libraries.
- **Infrastructure Security:**
  - CloudFormation/Terraform scripts enforce private subnets, least-privilege IAM roles, and VPC endpoints.
  - Administrative access is restricted to AWS Systems Manager Session Manager or Kubernetes APIs, with outbound traffic routed via NAT Gateway.
- **Security Testing:**
  - Static Application Security Testing (SAST) with SonarQube analyzes source code.
  - Dynamic Application Security Testing (DAST) with OWASP ZAP identifies runtime vulnerabilities.
  - Quarterly manual penetration testing by certified ethical hackers ensures robustness.
  - CI/CD pipelines (Jenkins, AWS CodePipeline) integrate SAST, SCA, and container scanning to block releases with critical issues.
- **Compliance:**
  - The application supports compliance with HIPAA, PCI DSS, and GDPR through customizable scripts and secure configurations.
  - Customers are advised to perform periodic penetration testing in their environments to validate modified configurations.



Customer Responsibilities

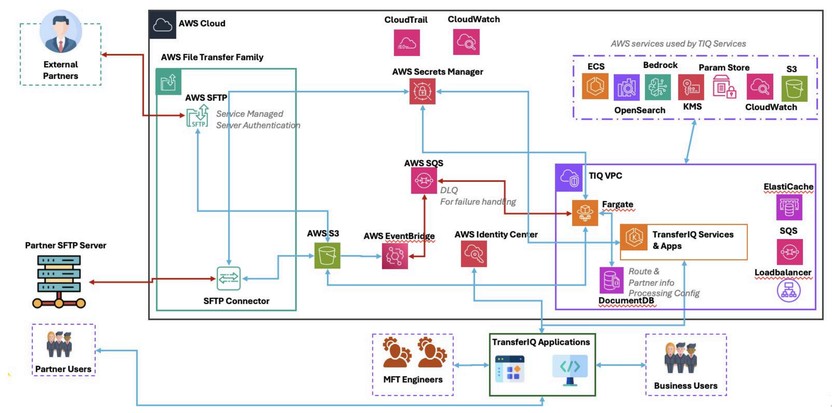
Under the BYOC model, customers manage the following:



Network Architecture Diagram

- **Components:** EKS/ECS cluster, ALB/NLB, private subnets, NAT Gateway, VPC endpoints, S3 buckets, AWS Transfer Family endpoints, and Admin pages.
- **Connectivity:** Traffic flow between containers, load balancer, S3, and external partners via Transfer Family endpoints.
- **Security Boundaries:** Private subnets, IAM roles, Kubernetes RBAC, and encryption layers.
- **Deployment Scope:** Customer's AWS account, with two container replicas across AZs for high availability.

The diagram groups components into application plane (TransferIQ Orchestrate application, Admin pages) and control plane (EKS/ECS orchestration, IAM, S3), adhering to AWS Marketplace architecture diagram requirements. All components run entirely on AWS, qualifying for the "Deployed on AWS" designation.



AWS Marketplace Submission Compliance

The deployment process aligns with AWS Marketplace SaaS product guidelines:

- **Hosting:** The application and control planes run entirely on AWS infrastructure in the customer's account, meeting the "Deployed on AWS" criteria.
- **Security:** Resources are provisioned securely using AWS IAM and STS, with least-privilege principles.
- **Architecture Diagram:** A detailed diagram labeling application and control plane components will be submitted via the AWS Marketplace Management Portal.
- **Product Load Form (PLF):** The submission includes a completed PLF, uploaded via the Assets tab, detailing product description, pricing (BYOL), and deployment instructions.
- **Testing:** The container image is scanned for vulnerabilities, and the deployment process is tested in a staging environment to ensure usability.
- **Documentation:** Customers receive clear instructions for deployment, including IAM policy requirements and CloudFormation/Terraform script usage, as part of the Admin pages.