Case study scenario summary: Securing apps and data

About the organization

- Fabrikam Inc. is a U.S.-based e-commerce company with a global customer base
- Offers online marketplace with personalization, loyalty programs, promotions
- Operates fully in the cloud using Microsoft Azure and AWS
- Platform architecture
  - Microservices on Azure Kubernetes Service (AKS) and Amazon EKS
  - Web and backend apps containerized and distributed across both clouds
  - Uses OpenID Connect and OAuth 2.0 for authentication
- Data storage & governance
  - Critical data is in Azure: Azure SQL Database for transactions; Cosmos DB for profiles, metadata, and personalization
  - Enables consistent governance, compliance, and audit controls

Scenario & challenges

Data protection & access

Scenario

- Transparent Data Encryption (TDE) in Azure SQL data
- App-layer data masking before display/logging
- TLS 1.3 enforced for all backend traffic over public endpoints
- Kubernetes secrets store credentials; accessed via environment variables/volumes
- Long-lived tokens manually rotated during maintenance

Challenges

- Manual token rotation increases risk of operational delays and secret exposure

CI/CD & DevOps

Scenario

- GitHub Actions handles CI/CD with private repositories
- Automatic deployments follow successful builds and tests

Challenges

- Runtime environment misconfigurations can bypass pre-deployment checks and impact production stability

Security Incidents

- A failed deployment due to a misconfigured Kubernetes admission policy, later detected by Azure Policy.
- An overly permissive role was added via an IaC template
  - Discovered post-deployment during a security review
  - Required manual tracing by security and development teams

Open source & container security

Scenario

- Open-source packages used; vulnerabilities tracked via community feeds
- Azure Container Registry (ACR) hosts base images, rebuilt to patch vulnerabilities

Challenges:

- Risk detection and secret scanning depend on developer diligence and custom CI/CD scripts.
- Security insights are handled within projects using project-specific tooling

Monitoring & alerts

Scenario

- Azure Monitor collects app telemetry
- Microsoft Sentinel receives data via Azure Activity and Defender for Cloud
- Custom rules detect anomalous sign-ins and elevated OAuth permission grants
- Alerts routed to internal ops dashboard accessed by DevOps engineers, Security ops, App support
- Telemetry is used for performance tuning, exception tracing, and diagnostics

Challenges:

- Alert triage and response workflows vary across teams, limiting coordinated incident handling

Your role as a security architect

Analyze Fabrikam Inc.'s current security posture and design a resilient Zero Trust architecture that:

- Secures apps and data
- Improves visibility and response
- Reduces DevOps configuration risks
- Maintains operational continuity across Azure and AWS