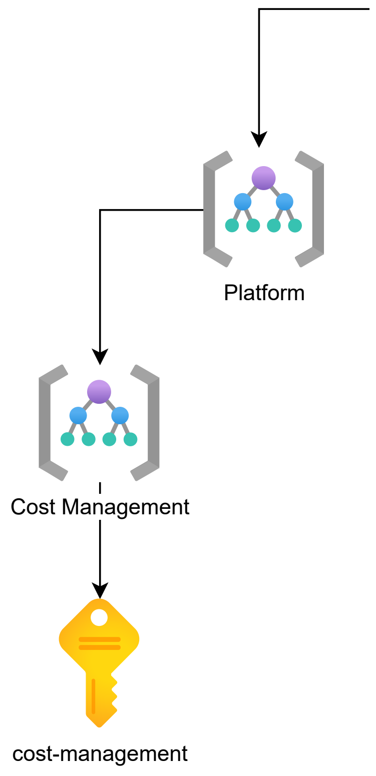
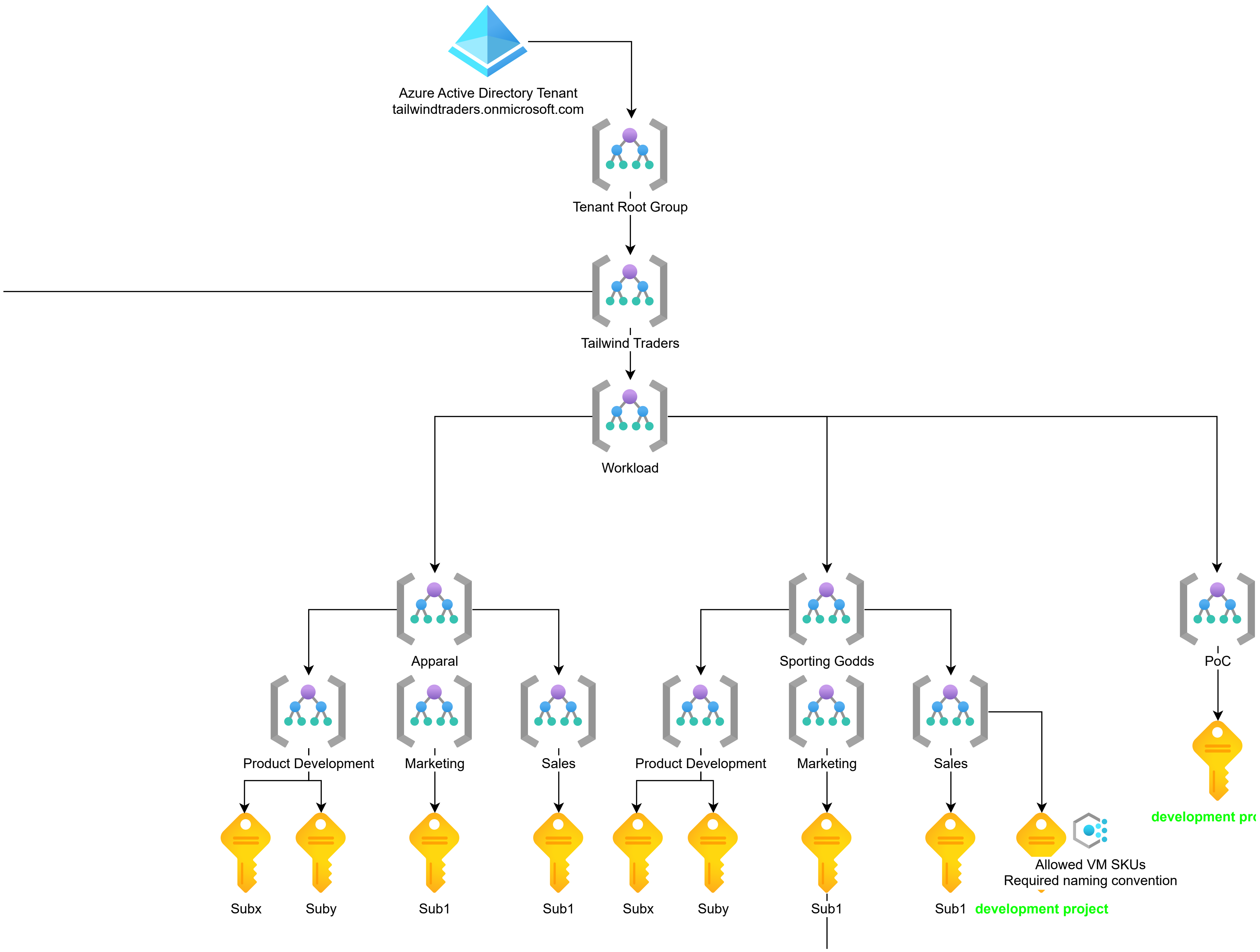
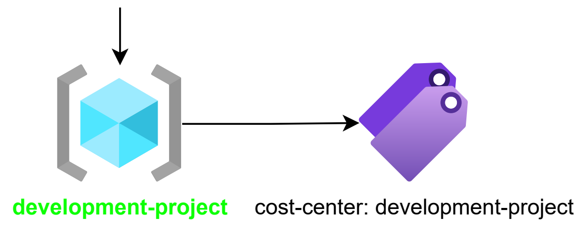
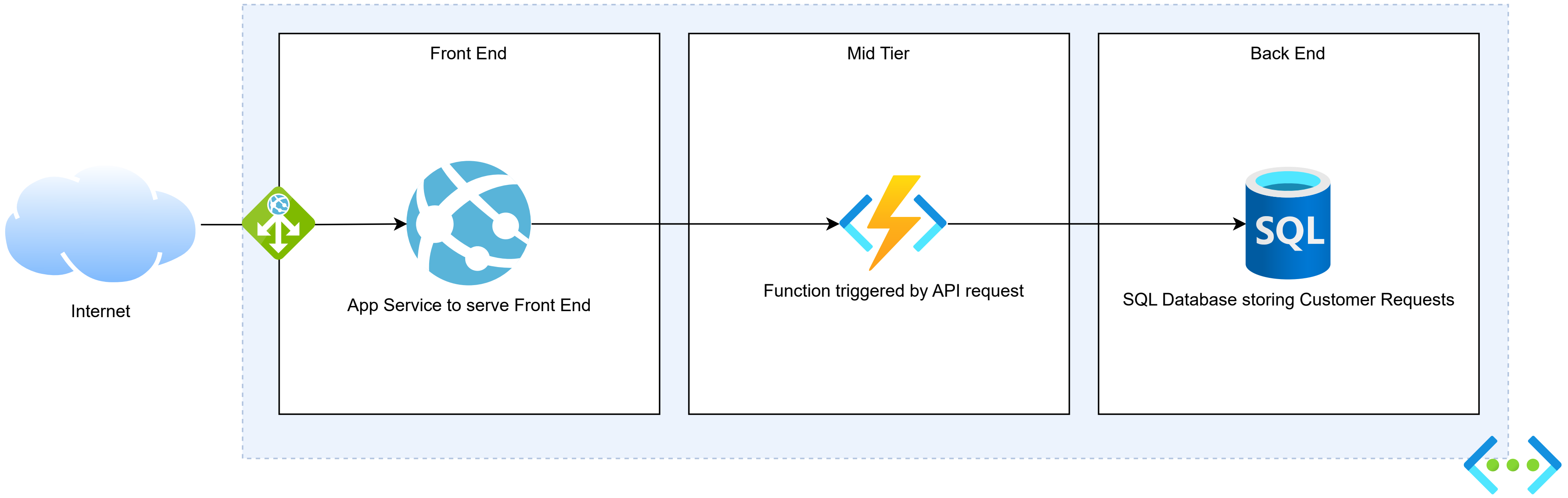

Platform
Cost Management
cost-management


Azure Active Directory Tenant
tailwindtraders.onmicrosoft.com
Tenant Root Group
Tailwind Traders
Workload
Apparal
Sporting Godds
PoC
Product Development
Marketing
Sales
Product Development
Marketing
Sales
Subx
Suby
Sub1
Sub1
Subx
Suby
Sub1
Sub1
development project
Allowed VM SKUs
Required naming convention
development pro

Allowed VM SKUs
Required naming convention

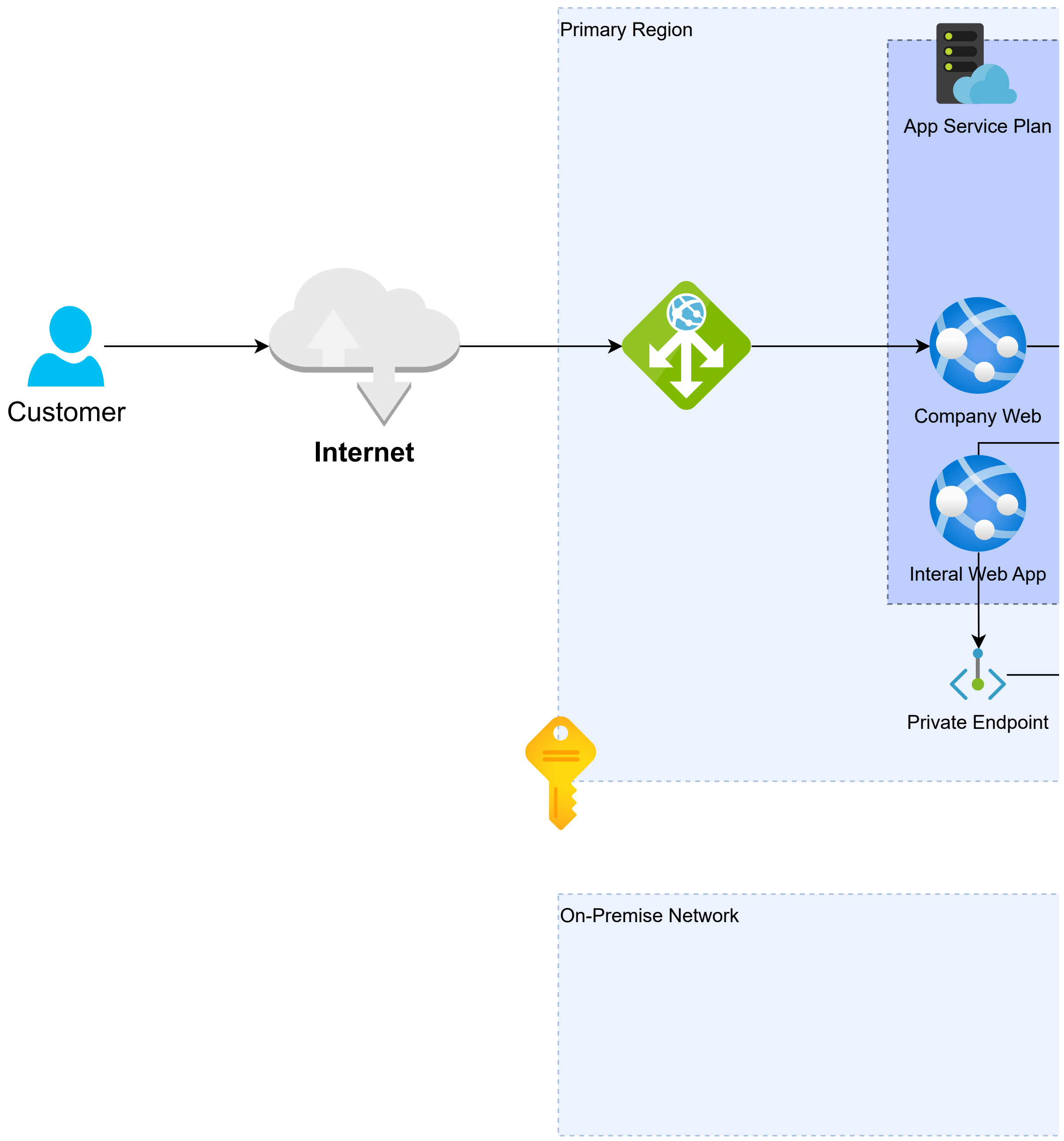
oject

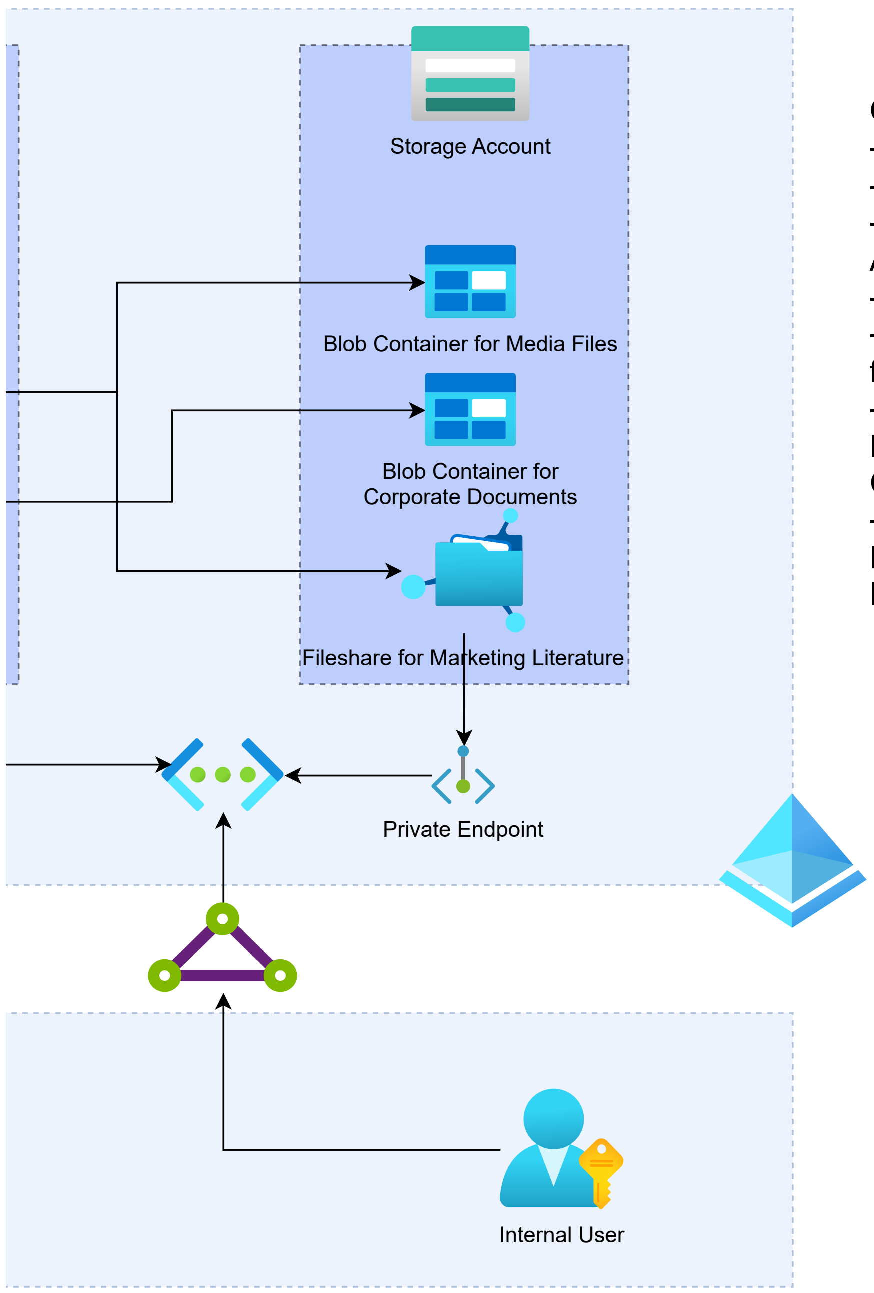

development-project
cost-center: development-project


Internet
Front End
App Service to serve Front End
Mid Tier
Function triggered by API request
Back End
SQL
SQL Database storing Customer Requests

Reasoning:
- .Net App lication can be hosted in App Service
- App Service supports automatic scaling
- Use Application Insights for detailed Application Monitoring same for Front End and Mid Tier
- Middle Tier Business Logic can be hosted using Azure Function which is triggered by REST API Call from Front End
- Mid Tier Logic can directly store data in SQL Database
- *Consider Application Gateway for extra protection

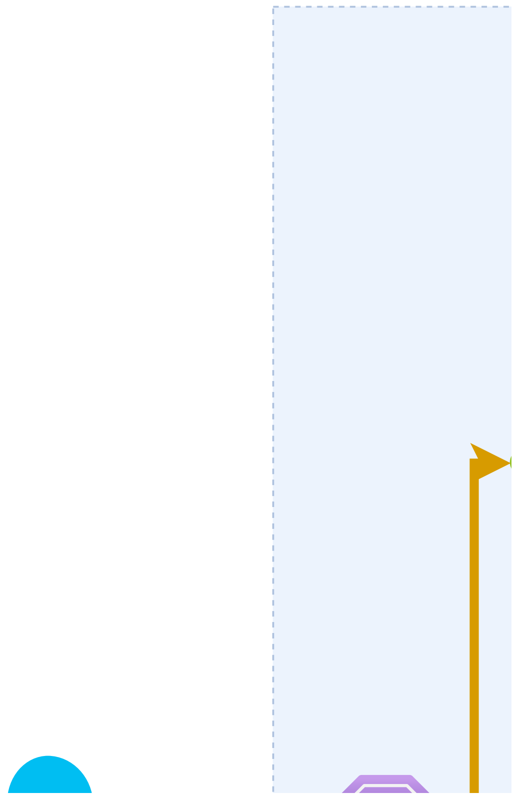
Alternatives:
- VMSS instead of App Service
    -> Would bring big management overhead
    -> Would have negative impact on cost efficiency
    -> Slow spin up times for additional nodes
- API Management instead of Function
    -> Overkill for this small application
    -> Could be considered if service would be transitioned to Microservice architecture to a later point in time

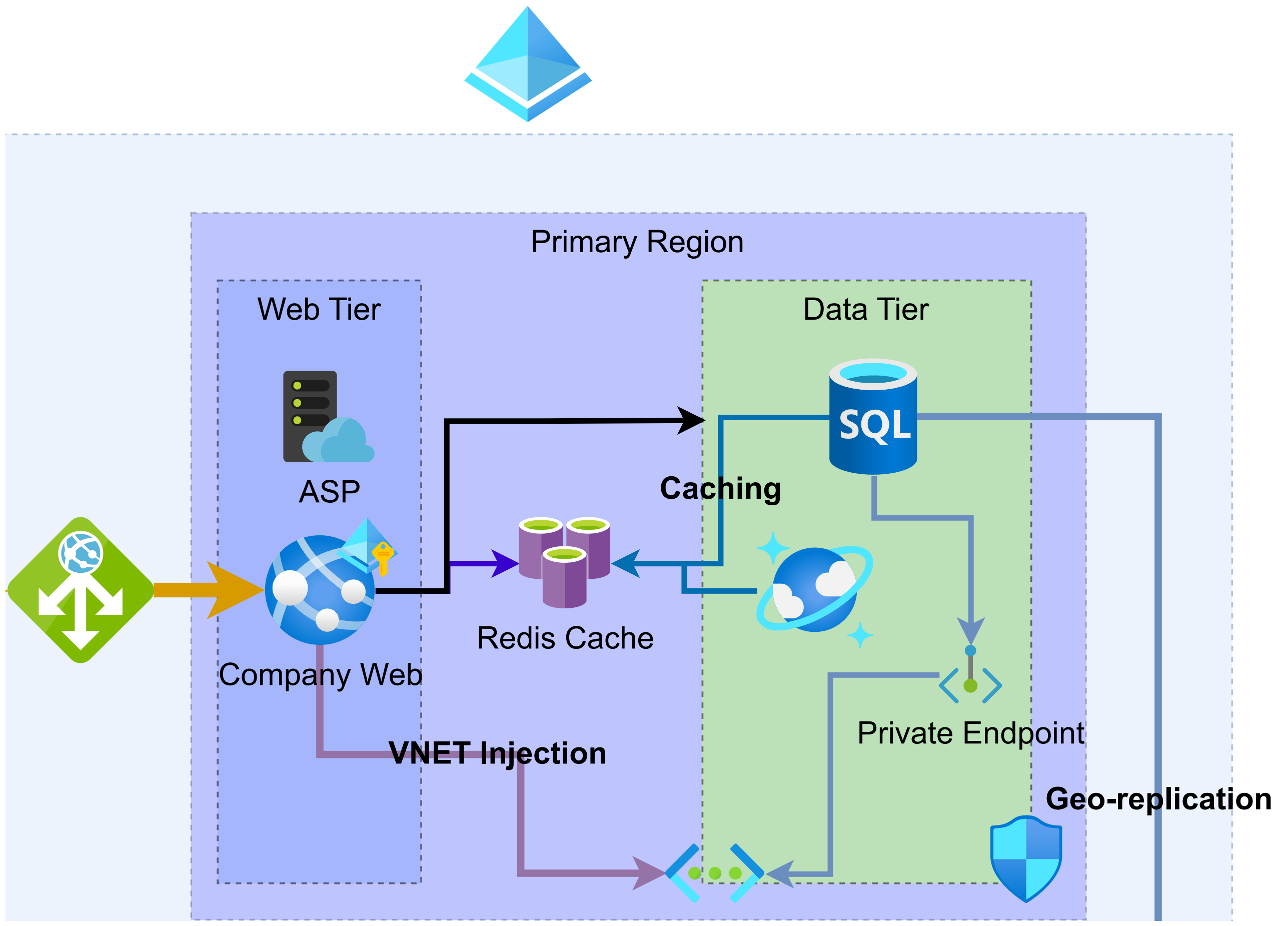

Primary Region
App Service Plan
Customer
Internet
Company Web
Interal Web App
Private Endpoint
On-Premise Network


Storage Account
Blob Container for Media Files
Blob Container for Corporate Documents
Fileshare for Marketing Literature
Private Endpoint
Internal User

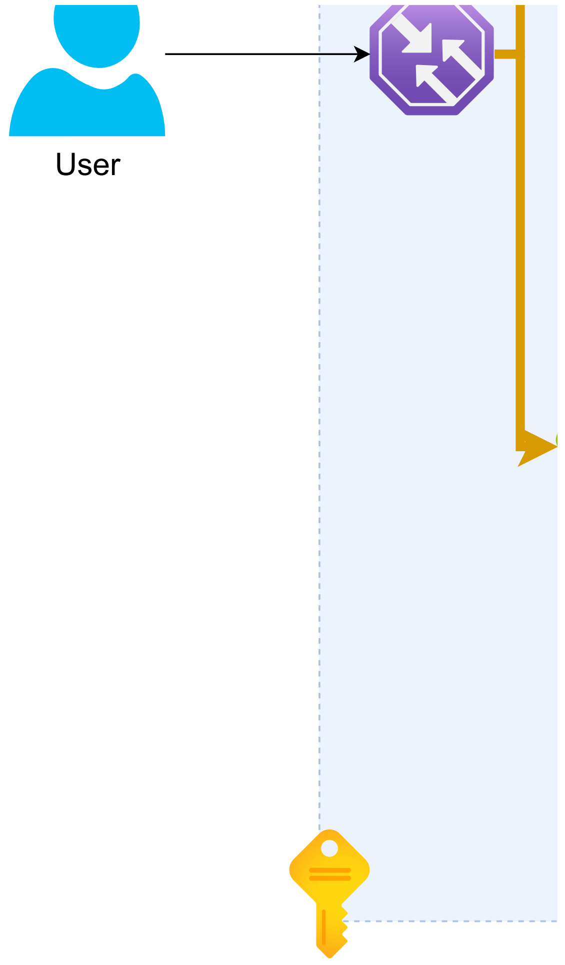
Considerations:
- All data is non-relational
- Default Access Tier: Hot
- Use Lifecycle Policy to move Blobs from Hot to Cold or Archive after 1 year
- Use Legal Hold for Investigated Data
- Recommend Zone redundant storage, Geo-redundant for if mission-critical
- Use Private Endpoints for Secure access for Marketing Literature Fileshare and Internal Web App to access Corporate Documents
- Azure File Sync could be used instead of Private Endpoint Integration to simplify network. Public Path for Internal Web App would then also be required

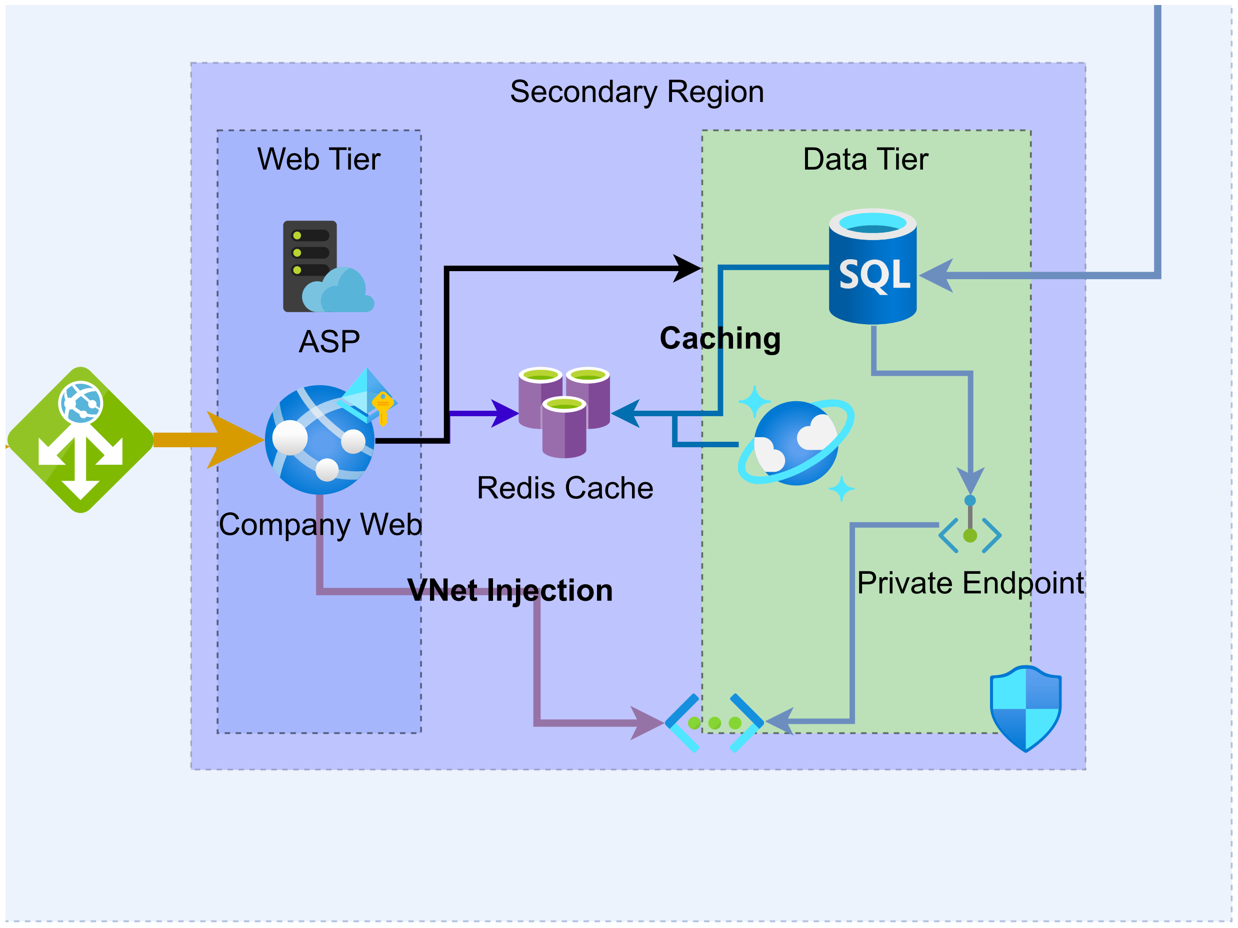
Considerations:
- Network Access: Disable Public Access and only Private Endpoints to access SQL database from App Service. Add NSG to filter traffic towards SQL Server Private Endpoint. Use VNet Injection for the App Service to be able to reach SQL.
- Authentication: Use AzureAD only authentication for SQL Server and leverage App Service Managed Identity to authenticate towards SQL Server
- **Pricing:** Azure SQL Database clearly more cost efficient than SQL MI or SQL VM. Incase of

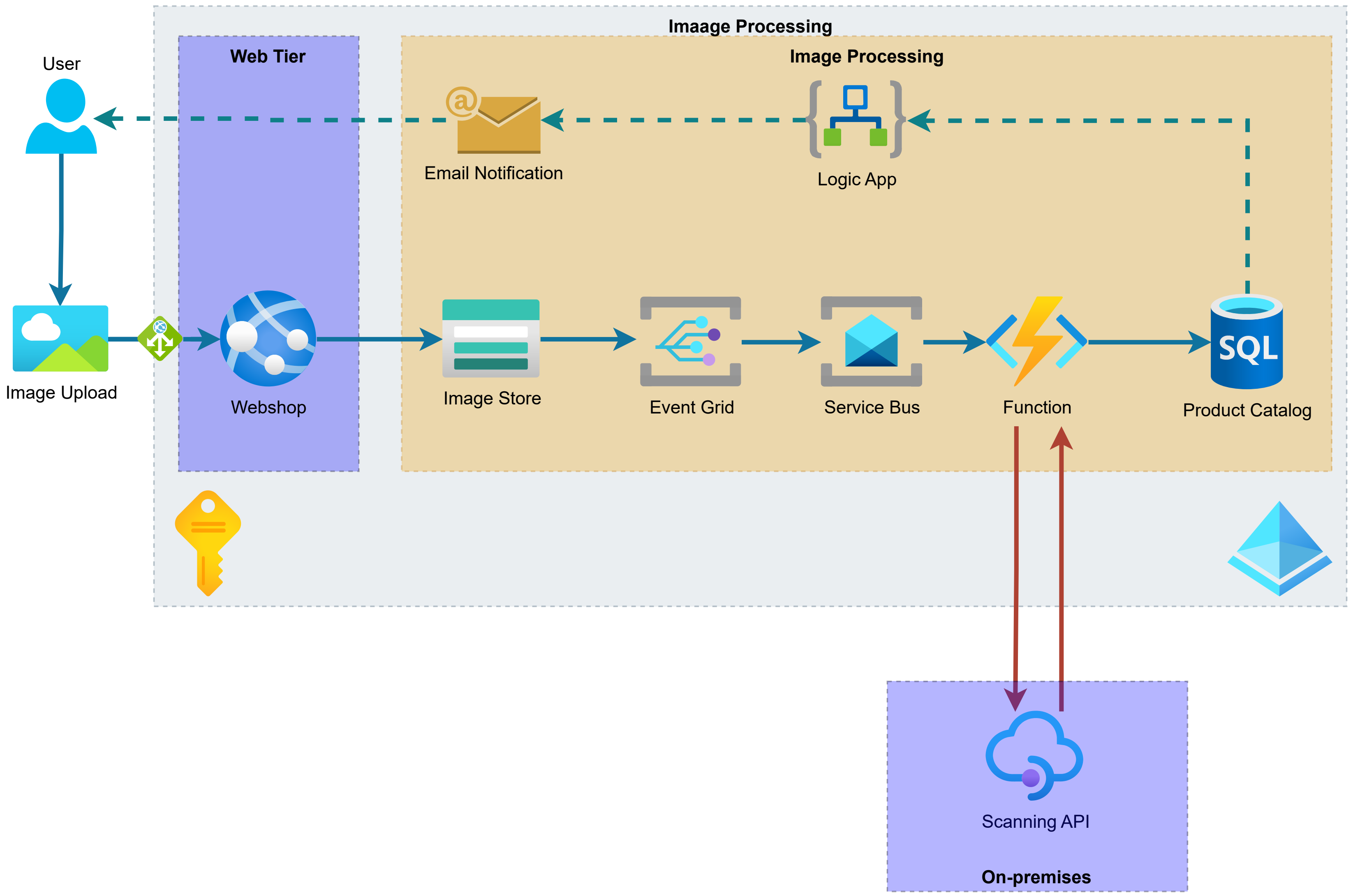


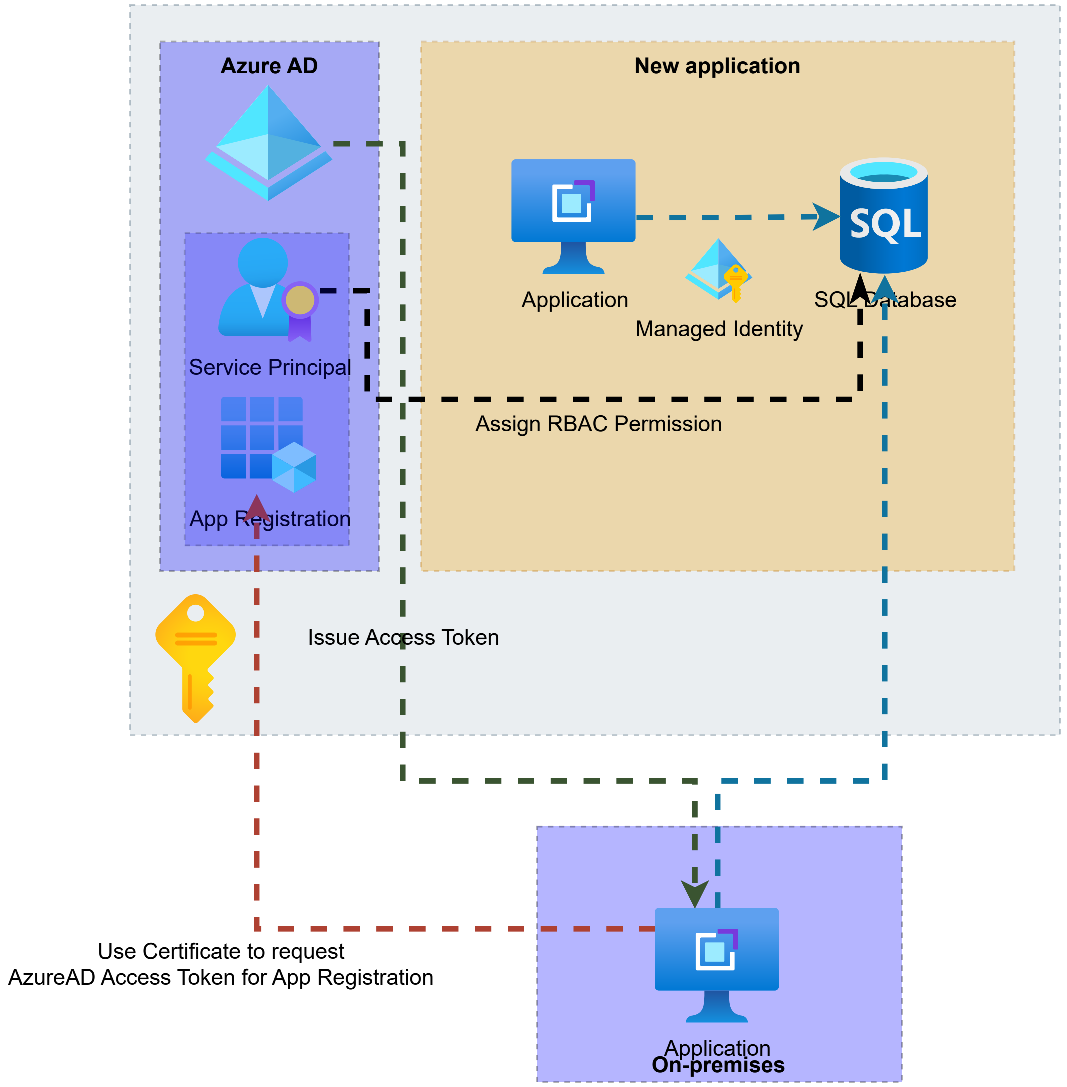

Primary Region
Web Tier
Data Tier
ASP
Caching
Company Web
Redis Cache
Private Endpoint
VNET Injection
Geo-replication

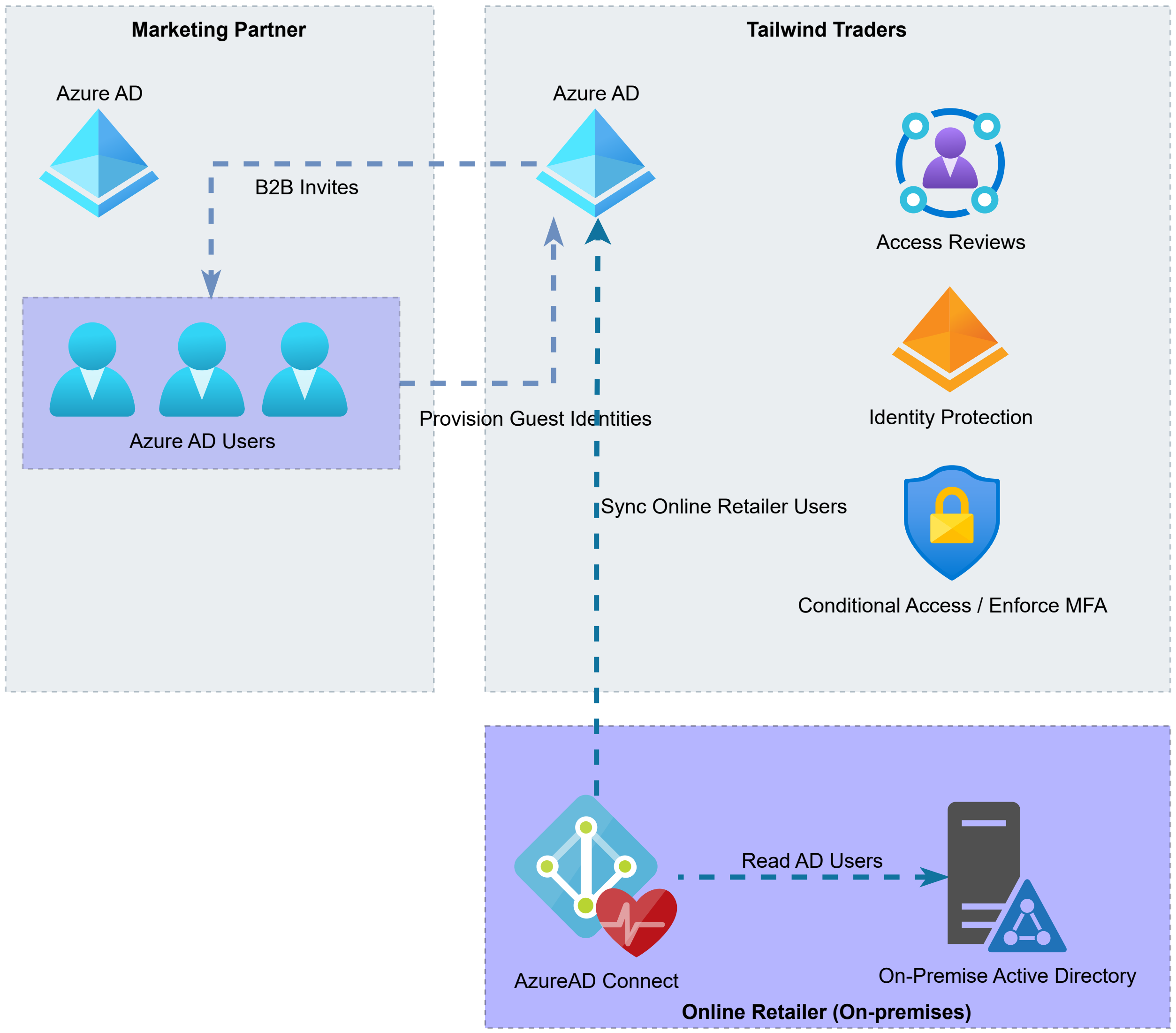
efficient than SQL MI or SQL VM. Incase of compatibility issue SQL MI or SQL VM should be used.
- Performance: Azure SQL Database with sufficient resources may already solve all issues. However moving the product catalog to NoSQL CosmosDB which allows sharding / partitioning would provide much faster response times. Major code refactoring might be required. The usage of Redis Cache for Database transactions will also increase performance.
- **High Availability:** Business Critical Pricing Tier recommend for SQL Database. Latency of read operations optimized by using read-only replicas accross different regions.

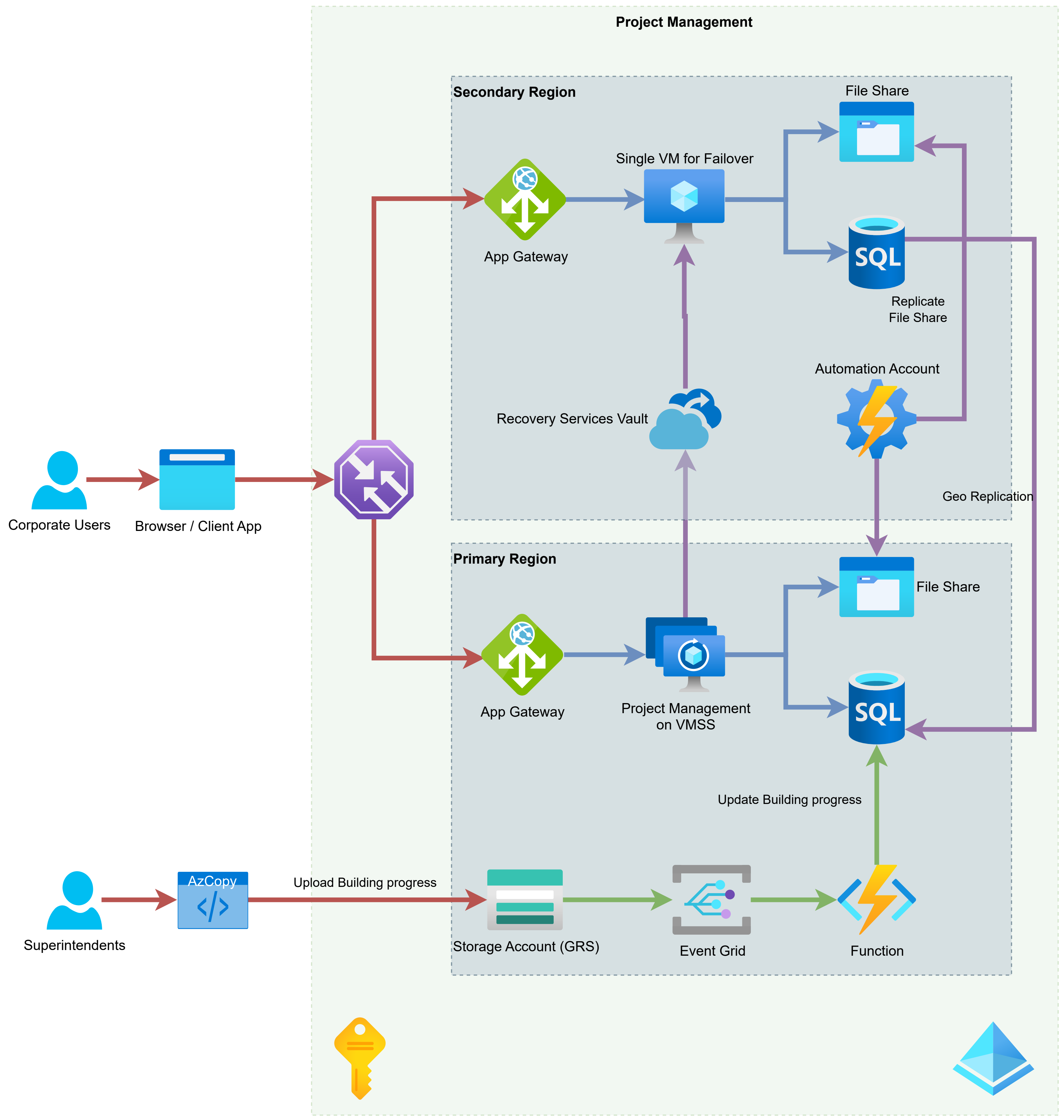



Secondary Region
Web Tier
ASP
Company Web
Data Tier
SQL
Caching
Redis Cache
Private Endpoint
VNet Injection


Imaage Processing
Web Tier
Image Processing
User
Email Notification
Logic App
Image Upload
Webshop
Image Store
Event Grid
Service Bus
Function
Product Catalog
Scanning API
On-premises

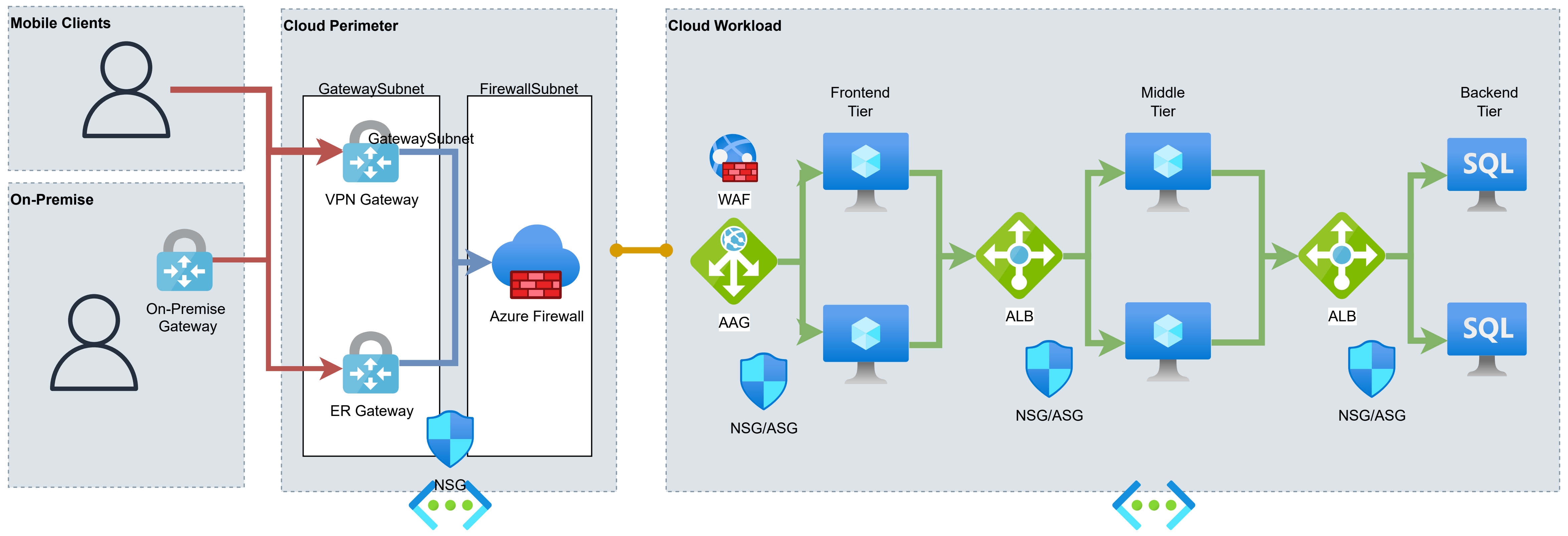

Azure AD
New application
Service Principal
App Registration
Application
Managed Identity
SQL Database
Assign RBAC Permission
Issue Access Token
Use Certificate to request
AzureAD Access Token for App Registration
Application
On-premises


Marketing Partner
Azure AD
B2B Invites
Azure AD Users
Provision Guest Identities
Tailwind Traders
Azure AD
Access Reviews
Identity Protection
Sync Online Retailer Users
Conditional Access / Enforce MFA
Read AD Users
AzureAD Connect
On-Premise Active Directory
Online Retailer (On-premises)



Considerations:

- Use VMSS for Primary Region as migration to PaaS Service would require support from third party vendor. Use Azure Site Recovery to replicate VM to Secondary Region for Failover in degraded state
- Use App Gateway for Load Balancing as users access using Browser
- Use Azure SQL Database in Business Critical Tier as Database
- Use Azure Files for the Applications File Share. Use Azure Automation Account to keep in sync with Secondary Region incase of Failover
- Replace FTP with Blob Storage and script with AzCopy
- Use Event Grid to continuously trigger Function which import the superintendents change file to the SQL Database
- Change File Import doesn't have to be region redundant as upload usually happens only once a day
- Consider Private Endpoints to improve Security



Mobile Clients
On-Premise
On-Premise Gateway
Cloud Perimeter
GatewaySubnet
FirewallSubnet
GatewaySubnet
VPN Gateway
ER Gateway
Azure Firewall
NSG
Cloud Workload
Frontend Tier
Middle Tier
Backend Tier
WAF
AAG
ALB
ALB
NSG/ASG
NSG/ASG
NSG/ASG
SQL
SQL