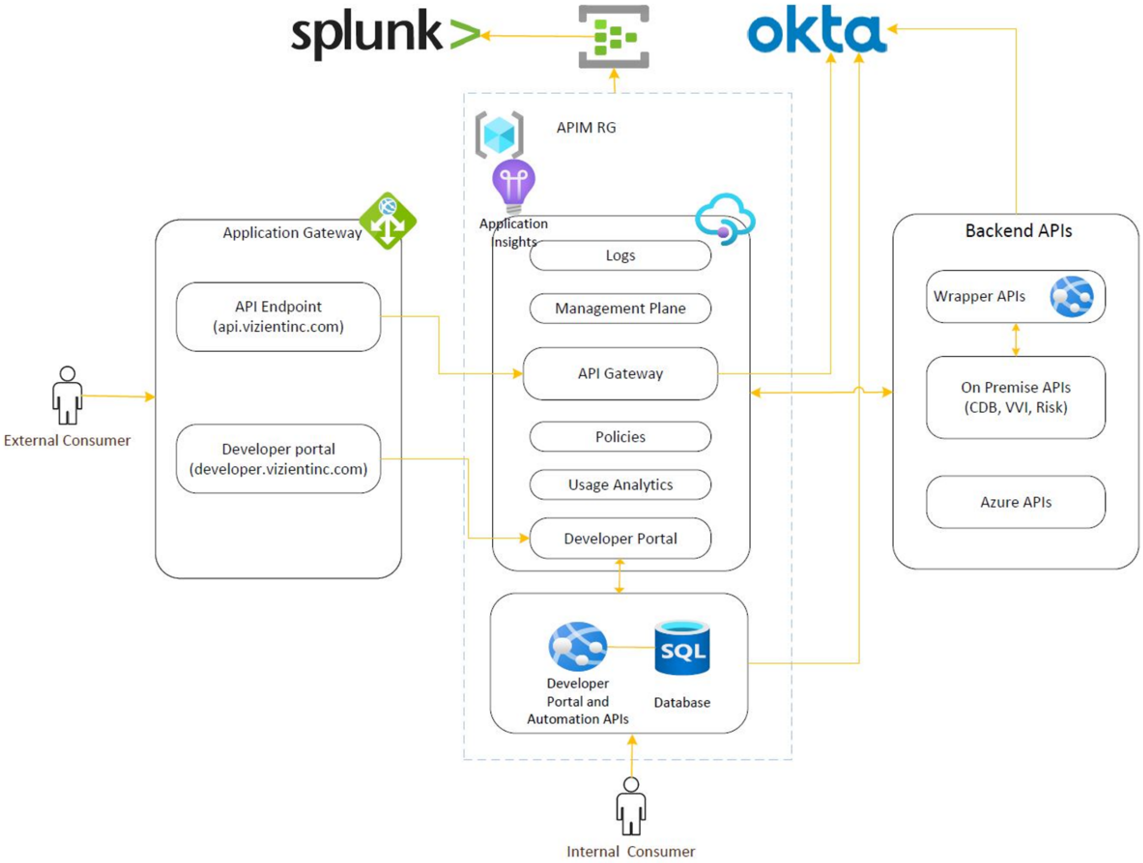
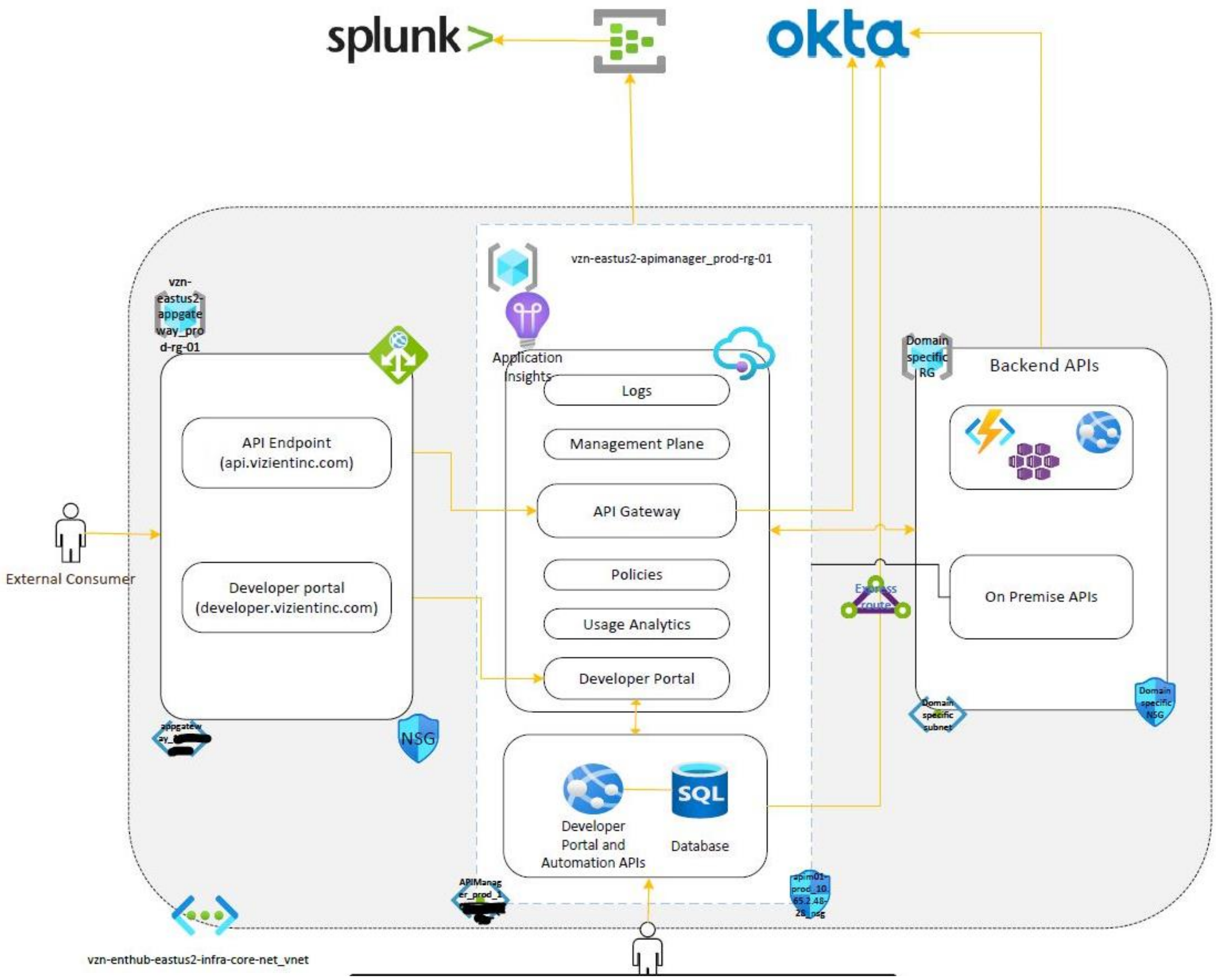

splunk>
okta
APIM RG
Application Insights
Application Gateway
API Endpoint (api.vizientinc.com)
Developer portal (developer.vizientinc.com)
External Consumer
Logs
Management Plane
API Gateway
Policies
Usage Analytics
Developer Portal
Developer Portal and Automation APIs
SQL
Database
Internal Consumer
Backend APIs
Wrapper APIs
On Premise APIs (CDB, VVI, Risk)
Azure APIs


splunk>
okta
vzn-eastus2-apimanager_prod-rg-01
vzn-eastus2-appgateway_prod-rg-01
Application Insights
Logs
Management Plane
API Gateway
Policies
Usage Analytics
Developer Portal
API Endpoint (api.vizientinc.com)
Developer portal (developer.vizientinc.com)
External Consumer
appgateway_[redacted]
NSG
Developer Portal and Automation APIs
Database
SQL
APIManager_prod_1[redacted]
apim01-prod_10.65.2.48-28_nsg
vzn-enthub-eastus2-infra-core-net_vnet
Domain specific RG
Backend APIs
On Premise APIs
Express route
Domain specific subnet
Domain specific NSG

Questions

Networking

1. In the diagram that you shared looks like APIM instance and SQL databases are present in the same VNet. Is this correct?

    Reference

2. How do internal Consumers access these APIM endpoints?

    Reference

    ○ Are they using private endpoint for your API Management instance. By using private endpoints, network traffic between a client on your private network and APIM traverses over the Vnet and a private link on the Microsoft backbone network, eliminating exposure from the public internet. [Set up inbound private endpoint for Azure API Management | Microsoft Learn]

3. Are you all using same instance of APIM to expose endpoints to internal and external consumers ?

    Reference - Deploy a Web Application Firewall (WAF) in front of API Management to protect against common web application exploits and vulnerabilities. Azure Application Gateway includes a built-in Web Application Firewall (WAF) feature. The WAF helps protect web applications from common web-based attacks and vulnerabilities. It provides an additional layer of security by inspecting incoming traffic and blocking malicious requests. The WAF feature in Azure Application Gateway offers customizable rule sets and provides protection against OWASP (Open Web Application Security Project) top 10 vulnerabilities, such as SQL injection, cross-site scripting (XSS), and more.

- Use API Management in a virtual network with Azure Application Gateway - Azure API Management | Microsoft Learn

4. Is there a plan for multi region deployment?

   Reference

   - Use front door in this scenario instead of Application Gateway - Network topology and connectivity considerations for Azure API Management - Cloud Adoption Framework | Microsoft Learn
   - https://learn.microsoft.com/en-us/azure/frontdoor/front-door-overview

5. What is your strategy to consume APIM endpoint across multiple different VNets ?

   Reference - VNet peering supports high performance in a region but has a scalability limit of 500 networks. If you require more workloads to be connected, use a hub spoke architecture or Private Endpoint.

Security

1. How do you secure your front end APIs

   Reference

   - Protect API in API Management using OAuth 2.0 and Azure Active Directory - Azure API Management | Microsoft Learn

2. How to you manage access to the developer portal?

   Reference

   - Authorize developer accounts by using Azure Active Directory B2C - Azure API Management | Microsoft Learn

3. How do you manage constant string values and secrets across all API configurations and policies?

   Reference

   - Named values can be used for that purpose. It’s a global name-value collection. Value can be plain string or can be a secret. Using key vault secrets is recommended because it helps improve API Management security. How to use named values in Azure API Management policies | Microsoft Learn

Management

1. How about Scaling the APIM instance?

   Reference

   - Be aware of maximum throughput - https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits#api-management-limits

- ○ Be aware of maximum number of scale units per APIM service tier. https://azure.microsoft.com/pricing/details/api-management/
- ○ Be aware of time required to scale out/ deploy to another region, or convert to a different service tier. APIM doesn't scale out automatically, you need additional configurations for that - https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-autoscale

3. What usage analytics you capture ?

Reference

- ○ Use API analytics in Azure API Management | Microsoft Learn
- ○ Integration with App Insights - Integrate Azure API Management with Azure Application Insights - Azure API Management | Microsoft Learn

4. Do you measure performance impact of Application Insights logging and the number of inbound and outbound policies?

References

- ○ Based on internal load tests, enabling the logging feature caused a 40%-50% reduction in throughput when request rate exceeded 1,000 requests per second.Integrate Azure API Management with Azure Application Insights - Azure API Management | Microsoft Learn
- ○ When multiple policies are applied, each policy adds processing overhead, which can affect the overall performance of the API Management instance. It is important to carefully evaluate and optimize the policies to strike a balance between functionality and performance. Reducing the number of policies or optimizing their execution can help improve the overall performance of Azure API Management.

5. Do you use Built-in cache?

Reference

- ○ APIs and operations in API Management can be configured with response caching. Response caching can significantly reduce latency for API callers and backend load for API providers. Add caching to improve performance in Azure API Management | Microsoft Learn

6. What is your strategy for APIM Backup and BCDR(Business Continuity & Disaster Recovery)?
7. Have you already determined RTO and RPO?

Reference

- ○ This article shows how to automate backup and restore operations of your API Management instance using an external storage account.
  - Backup and restore your Azure API Management instance for disaster recovery - Azure API Management | Microsoft Learn

    ★ Each backup expires after 30 days. If you attempt to restore a backup after the 30-day expiration period has expired, the restore will fail with a ***Cannot restore: backup expired*** message.
- ○ What is not backed up? Backup and restore your Azure API Management instance for disaster recovery - Azure API Management | Microsoft Learn

- ○ In case of outage, you may want to consider the feasibility for deploying fresh instances or having a hot/ cold standby.
- ○ Failover can be automated - Multizone is automatic whereas multi-region deployment required a DNS-based load balancer such as Traffic Manager.

        - https://learn.microsoft.com/en-us/azure/api-management/zone-redundancy
        - Deploy Azure API Management instance to multiple Azure regions - Azure API Management | Microsoft Learn

Governance

1. Are you using any inbuilt Azure Policies for API Management?

    Reference

    - Azure Policy helps to enforce organizational standards and to assess compliance at-scale.
        - Overview of Azure Policy - Azure Policy | Microsoft Learn
        - In-built APIM policies - Built-in policy definitions for Azure API Management | Microsoft Learn
            - API Management calls to API backends should be authenticated.
            - API Management direct management endpoint should not be enabled
            - API Management secret named values should be stored in Azure Key Vault
            - API Management subscriptions should not be scoped to all APIs

2. How do you monitor published APIs?

    Reference

    - API Management emits metrics every minute, giving you near real-time visibility into the state and health of your APIs. Two most importants metrics are as follows:
        - Capacity - helps you make decisions about upgrading/downgrading your API Management services. The metric is emitted per minute and reflects the estimated gateway capacity at the time of reporting. The metric ranges from 0-100 calculated based on gateway resources such as CPU and memory utilization.
        - Requests - helps you analyze API traffic going through your API Management services. The metric is emitted per minute and reports the number of gateway requests with dimensions. Filter requests by response codes, location, hostname, and errors.
        - https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-use-azure-monitor
        - You can set up alerts based on metrics and activity log:
            - Send an email notification
            - Call a webhook
            - Invoke an Azure Logic App

3. Have you all implemented Error Handling in APIM policies?

    Reference

    - https://learn.microsoft.com/en-us/azure/api-management/api-management-error-handling-policies

1. Are you all using ApiOps?

    Reference

    - APIOps applies the concepts of GitOps and DevOps to API deployment. By using practices from these two methodologies, APIOps can enable everyone involved in the lifecycle of API design, development, and deployment with self-service and automated tools to ensure the quality of the specifications and APIs that they’re building.
        - https://github.com/azure/apiops