Γραφείο Σταδιοδρομίας και Απασχολησιμότητας

A white background with blue text

Description automatically generated

**TEAM 1**

**Selection of Services and Justifications**

Services Best Suited for the Company:

1. Azure Entra ID

Why : Azure Entra ID supports single sign-on and multi-factor authentication, which is critical for ensuring secure access to resources, especially for users accessing services from outside the office or administrators who should always be challenged for MFA. Furthermore, employees can sign into their laptops using Office 365 credentials making identity management way more efficient. Finally, Role-Based Access Control ensures that developers have limited access (read-only), while admins can manage and create resources. The alternative which is an Active Directory on-premises requires significant infrastructure and complex configuration for remote access while Azure Entra ID offers a cloud solution that integrates easily with Azure services and Office 365, providing scalability, built-in security, and ease of administration.

1. Azure App Service

Why : Azure App Service allows hosting of the company's ASP.NET Core website and public API without managing the underlying infrastructure, it supports auto-scaling based on traffic, which is ideal for handling the anticipated website (1000 visitors/day) and API traffic (5000 requests/day) and finally it can easily integrate with Azure Functions for stateless operations. The alternative is hosting them on Virtual Machines which require configuring, maintaining, and scaling the VM manually, which adds complexity. Azure App Service offers scaling, monitoring, and built-in integration with Azure AD, which reduces complexity, especially when compared to VM based hosting solutions.

1. Azure Blob Storage

Why : Azure Blob Storage is optimized for handling large volumes of unstructured data, which is ideal for the 250GB of image/video content and 5TB of logs while also supporting Shared Access Signatures for secure access to public content. Moreover it can automatically move infrequently accessed logs to cold or archival storage, optimizing cost. The alternative file storage systems like Azure Files or on-premises Network Attached Storage don’t scale as efficiently or economically for the expected data growth while Blob storage’s flexibility, cost-effectiveness, and ability to support massive amounts of unstructured data make it the best fit for both media content and logs.

1. Azure SQL Database

Why : Azure SQL Database provides a fully managed relational database service for storing internal databases that offers automatic backups, patching, scaling, and high availability. It also supports encryption at rest and in transit, and integrates with Azure Entra ID for secure access. Alternatively, Azure Cosmos DB is ideal for globally distributed applications with NoSQL needs, but for a relational database structure with predictable transaction loads, which the company requires making Azure SQL Database more appropriate.

1. Azure Functions

Why: Azure Functions supports stateless event-driven tasks such as processing API requests or automating operational workflows while it automatically scales based on the number of incoming requests, making it perfect for handling the unpredictable workloads. The other alternative is manually managing functions on VMs or App Service, an option that would require handling infrastructure scaling which is unnecessary for lightweight, stateless operations. Azure Functions abstracts away infrastructure management and provides a cost-efficient, scalable way to handle microservices or event-driven tasks.

1. Azure Monitor

Why: Azure Monitor provides detailed logging and monitoring services across all Azure resources, ensuring visibility for the compliance logs stored in Blob storage while it also supports long-term retention, and integration with Azure Blob Storage to store large logs cost-effectively. Alternatively, Using third-party tools or setting up logging on self-managed servers would require additional infrastructure and complexity while Azure Monitor provides connection with other Azure services and offers built-in capabilities for monitoring, which is essential for compliance.

1. Azure Virtual Networks

Why: Azure Virtual Networks enables secure communication between services, such as the database, App Service, and other internal resources, through service endpoints and Network Security Groups while intergrating with Azure Firewall ensures security at both the network and application levels. On-premises networking requires expensive hardware, physical setup, and manual configuration for security layers like firewalls and VPNs. On the other hand, Azure VNET provides networking options with better security and flexibility, and eliminates the need for hardware intensive on-premises solutions.

Advantages Against On-Premises Configuration:

* Cost Efficiency

On-premises infrastructure requires significant capital expenditure (CAPEX) for purchasing hardware, maintaining servers, networking, and storage devices, as well as managing the power, cooling, and physical space for data centers. In contrast, Azure offers a pay-as-you-go model, which transforms the cost structure into operational expenditure (OPEX), allowing the company to only pay for what is used.

* Scalability

Scaling on-premises infrastructure involves purchasing and deploying additional hardware, which is both time-consuming and costly. In Azure, scaling can be done automatically and dynamically based on demand, enabling rapid response to changing traffic loads with autoscaling features.

* Maintenance and Management

On-premises solutions require regular updates, patching, and hardware replacement cycles, all of which involve significant labor costs and downtime. Azure services, especially Platforms As A Service, handle these tasks automatically, reducing the burden on IT staff and minimizing service disruptions.

* Disaster Recovery and High Availability

Implementing disaster recovery and high availability solutions on-premises requires redundant hardware, complex configurations, and regular testing. Azure offers built-in redundancy, automatic backups, and global availability zones, ensuring high uptime and quicker disaster recovery without the need for additional infrastructure.

* Security and Compliance

Azure provides end-to-end encryption, identity management, and compliance certifications ensuring better data protection and regulatory support compared to manually managing security on-premises.

Benefits of Using PAAS Over IAAS:

* Simplified Management

Azure App Service (PAAS) abstracts away the underlying infrastructure management (OS updates, patches, and hardware failures), allowing the development team to focus solely on the application logic while IAAS, like hosting applications on Virtual Machines would require setting up, maintaining, and scaling the VMs, adding significant management overhead.

* Elasticity and Scalability

With PAAS, scaling is dynamic, and capacity can be adjusted instantly without downtime while IAAS require manual scaling which is slower and resource intensive.

* Costs

PAAS services like Azure App Service and Azure Functions offer a consumption based model, where you only pay for what you use whereas IAAS cost even when idle. Furthermore, PAAS automatically optimizes resource allocation based on usage while IAAS might result in paying for more resources than needed.

* Security

PAAS services have built-in security features such as patch management, SSL certificates, and DDoS protection reducing the workload for the security team. With IAAS, all security updates and compliance checks must be managed internally adding complexity and increasing the risk of vulnerabilities if not properly maintained.