Cloud Infrastructure for Multisoftware Enterprise – Analytical Report





Εικόνα που περιέχει γραμματοσειρά, γραφικά, λογότυπο, Μπελ ηλεκτρίκ

Το περιεχόμενο που δημιουργείται από τεχνολογία AI ενδέχεται να είναι εσφαλμένο.



# Table of contents

[Table of contents 2](#_Toc197105571)

[Table of Figures 3](#_Toc197105572)

[1. Executive Summary 3](#_Toc197105573)

[2. Project Overview 4](#_Toc197105574)

[3. Functional Requirements 5](#_Toc197105575)

[4. Service Selection and Justification 6](#_Toc197105576)

[5. Detailed Resource Configuration 7](#_Toc197105577)

[6. System Architecture and Diagrams 9](#_Toc197105578)

[7. Security and Compliance Strategy 12](#_Toc197105579)

[8. Monitoring and Cost Visibility 13](#_Toc197105580)

[9. Billing Estimate & On-premises Comparison 13](#_Toc197105581)

[10. Team Collaboration & Project Management 13](#_Toc197105582)

[11. Challenges and Resolutions 14](#_Toc197105583)

[12. Future Improvements & Scalability 14](#_Toc197105584)

[13. Conclusions 14](#_Toc197105585)

[14. References / Appendices 14](#_Toc197105586)

# Table of Figures

[Εικόνα 1 11](#_Toc197105047)

# 1. Executive Summary

Η παρούσα αναφορά περιγράφει τον σχεδιασμό και την υλοποίηση μιας πλήρως cloud-native υποδομής για τη MultiSoftware Enterprise, μια πολυεθνική εταιρεία ανάπτυξης λογισμικού με έδρα την Αθήνα, Ελλάδα. Το έργο ευθυγραμμίζεται με τη στρατηγική απόφαση της εταιρείας να υιοθετήσει μια προσέγγιση cloud-first, δημιουργώντας την υποδομή της εξ ολοκλήρου στο Microsoft Azure, χωρίς εξάρτηση από παλαιότερα συστήματα ή εγκαταστάσεις εντός της επιχείρησης.

Οι βασικοί στόχοι του έργου είναι η διασφάλιση υψηλής διαθεσιμότητας, επεκτασιμότητας, ασφάλειας και αποδοτικότητας κόστους για όλα τα τμήματα της επιχείρησης. Η προτεινόμενη λύση περιλαμβάνει κεντρική διαχείριση ταυτότητας και πρόσβασης, ασφαλή αποθήκευση δομημένων και αδόμητων δεδομένων, φιλοξενία του εταιρικού ιστοτόπου και API, καθώς και αξιόπιστη παρακολούθηση με ενσωματωμένες δυνατότητες συμμόρφωσης.

Στην παρούσα αναφορά παρουσιάζεται η επιλογή και παραμετροποίηση των κατάλληλων υπηρεσιών Azure, υποστηριζόμενη από αρχιτεκτονικά διαγράμματα, εκτιμήσεις κόστους και συγκρίσεις με παραδοσιακές λύσεις ιδιόκτητου υπολογιστικού νέφους (private cloud). Επιπλέον, περιγράφεται η συνεργατική προσέγγιση της ομάδας, οι προκλήσεις που αντιμετωπίστηκαν και προτάσεις για μελλοντική βελτίωση.

Το έργο αυτό λειτουργεί ως οδηγός για κάθε επιχείρηση που στοχεύει στην υιοθέτηση μιας σύγχρονης, επεκτάσιμης και ασφαλούς υποδομής cloud, αξιοποιώντας τις τεχνολογίες της Azure.

# 2. Project Overview

Η υποδομή cloud πρέπει να καλύπτει ένα σύνολο λειτουργικών απαιτήσεων ώστε να υποστηρίζει τις επιχειρησιακές ανάγκες της MultiSoftware Enterprise. Οι απαιτήσεις αυτές εστιάζουν στη διαχείριση ταυτότητας, την αποθήκευση δεδομένων, τη φιλοξενία εφαρμογών, την παρακολούθηση και τη συμμόρφωση.

**Διαχείριση Ταυτότητας και Πρόσβασης**

Όλοι οι υπάλληλοι πρέπει να αυθεντικοποιούνται μέσω του Microsoft Entra ID, με ενεργοποιημένο τον Έλεγχο Ταυτότητας Δύο Παραγόντων (MFA) για πρόσβαση εκτός γραφείων και υποχρεωτικά για διαχειριστές. Οι φορητοί υπολογιστές της εταιρείας πρέπει να υποστηρίζουν είσοδο με τα διαπιστευτήρια Office 365. Ο έλεγχος πρόσβασης πρέπει να βασίζεται σε ρόλους: οι developers να χρησιμοποιούν υπάρχοντες πόρους και οι administrators να μπορούν και να δημιουργούν. Όλο το σύστημα πρέπει να συμμορφώνεται με κανονισμούς προστασίας δεδομένων.

**Φιλοξενία Εφαρμογών**

Ο κύριος ιστότοπος της εταιρείας, ανεπτυγμένος σε ASP.NET Core, πρέπει να φιλοξενείται σε Azure App Service και να δέχεται περίπου 1.000 επισκέψεις ημερησίως.

**Αποθήκευση Δεδομένων**

Δομημένα δεδομένα: σε Azure SQL Database ή Cosmos DB, ανάλογα με την περίπτωση χρήσης (~2.000 αναγνώσεις και 500 εγγραφές ημερησίως).

Αδόμητα δεδομένα (π.χ. έγγραφα, εικόνες): σε Azure Blob Storage, με αυτόματο backup και κρυπτογράφηση κατά την αποθήκευση.

**Φιλοξενία Δημόσιου API**

Το δημόσιο API πρέπει να εξυπηρετεί περίπου 5.000 αιτήματα ημερησίως, με μέσο όρο 5 KB ανά αίτημα.

**Serverless Υλοποιήσεις**

Stateless λειτουργίες πρέπει να υλοποιούνται με serverless υπηρεσίες Azure για επεκτασιμότητα και οικονομία.

**Αποθήκευση Μέσων**

Δημόσιο περιεχόμενο εικόνων και βίντεο (~250 GB συνολικά) πρέπει να αποθηκεύεται και να εξυπηρετείται μέσω cloud, με ~100.000 αναγνώσεις και ~10.000 εγγραφές το μήνα.

**Αρχειοθέτηση Καταγραφών (Logs)**

Τα logs των servers πρέπει να αποθηκεύονται για λόγους συμμόρφωσης, συνολικής χωρητικότητας έως 5 TB, με μηνιαία αύξηση 50 GB. Πρόσβαση γίνεται μόνο σε εξαιρετικές περιπτώσεις.

**Παρακολούθηση και Ειδοποιήσεις**

Πρέπει να ενεργοποιηθούν Azure Monitor, Application Insights και Log Analytics. Κρίσιμες ειδοποιήσεις (π.χ. χρήση CPU, αποτυχίες εφαρμογών, καθυστέρηση βάσεων) πρέπει να ρυθμιστούν. Τα logs διατηρούνται για τουλάχιστον 90 ημέρες ή όσο απαιτεί η συμμόρφωση.

**Διαφάνεια Κόστους**

Το κόστος cloud που σχετίζεται με το project πρέπει να διαχωρίζεται από το γενικό IT στις χρεώσεις του Azure.

# 3. Functional Requirements

Η υποδομή cloud που σχεδιάζεται για τη MultiSoftware Enterprise πρέπει να καλύπτει ένα σύνολο κρίσιμων λειτουργικών απαιτήσεων που εξασφαλίζουν την ασφάλεια, τη διαθεσιμότητα, την επεκτασιμότητα και τη συμμόρφωση του οργανισμού με τις σύγχρονες τεχνολογικές ανάγκες.

Η αυθεντικοποίηση των χρηστών θα υλοποιείται μέσω του Azure Entra ID σε πλήρη ενσωμάτωση με τους λογαριασμούς Office 365, ώστε όλοι οι εργαζόμενοι να έχουν πρόσβαση με ενιαίο τρόπο στις υπηρεσίες της εταιρείας. Παράλληλα, θα εφαρμόζεται υποχρεωτικός έλεγχος ταυτότητας δύο παραγόντων (Multi-Factor Authentication - MFA) για όλους τους διαχειριστές, αλλά και για οποιονδήποτε χρήστη επιχειρεί πρόσβαση από εξωτερικό δίκτυο, με στόχο την ενίσχυση της ασφάλειας.

Η ιστοσελίδα της εταιρείας, η οποία έχει αναπτυχθεί σε ASP.NET Core, θα φιλοξενείται στο Azure App Service και προβλέπεται να εξυπηρετεί περίπου 1.000 επισκέπτες την ημέρα. Επιπλέον, το δημόσιο API της εταιρείας θα φιλοξενείται επίσης στο cloud, με αναμενόμενο όγκο περίπου 5.000 αιτημάτων ημερησίως. Οι υπηρεσίες αυτές θα σχεδιαστούν ώστε να παρέχουν υψηλή διαθεσιμότητα και απόδοση, ακόμη και σε περιόδους αυξημένης ζήτησης.

Όσον αφορά την αποθήκευση δεδομένων, τα δομημένα δεδομένα θα αποθηκεύονται είτε σε Azure SQL Database είτε σε Azure Cosmos DB, ανάλογα με τις απαιτήσεις κάθε εφαρμογής. Για τα αδόμητα δεδομένα, όπως έγγραφα, εικόνες και βίντεο, θα χρησιμοποιηθεί το Azure Blob Storage, με εκτιμώμενο συνολικό όγκο γύρω στα 250 GB. Όλα τα δεδομένα θα προστατεύονται μέσω κρυπτογράφησης κατά την αποθήκευση και θα υποστηρίζονται από αυτοματοποιημένα αντίγραφα ασφαλείας.

Οι λειτουργίες που είναι stateless θα υλοποιούνται με serverless τεχνολογίες, και συγκεκριμένα με Azure Functions, επιτυγχάνοντας έτσι υψηλή επεκτασιμότητα και χαμηλό λειτουργικό κόστος, χωρίς την ανάγκη για συνεχή διαχείριση υποδομής.

Για την παρακολούθηση της κατάστασης του συστήματος και την άμεση ειδοποίηση σε περίπτωση προβλημάτων, θα ενεργοποιηθούν οι υπηρεσίες Azure Monitor, Application Insights και Log Analytics. Θα οριστούν κανόνες ειδοποιήσεων για κρίσιμες παραμέτρους, όπως η χρήση επεξεργαστή (CPU), η καθυστέρηση στη βάση δεδομένων και οι αστοχίες εφαρμογών. Τα αρχεία καταγραφής (logs) θα διατηρούνται για τουλάχιστον 90 ημέρες, ή και περισσότερο όπου αυτό απαιτείται από κανονισμούς συμμόρφωσης.

Τέλος, θα υπάρχει σαφής διαχωρισμός του κόστους που σχετίζεται με το έργο από τις υπόλοιπες εσωτερικές λειτουργίες της εταιρείας. Μέσω εργαλείων παρακολούθησης κόστους του Azure, θα είναι δυνατή η καταγραφή και ανάλυση των χρεώσεων ανά χρήση, διασφαλίζοντας πλήρη διαφάνεια και έλεγχο στον οικονομικό προγραμματισμό του οργανισμού.

# 4. Service Selection and Justification

Η επιλογή των υπηρεσιών Azure βασίστηκε στις λειτουργικές απαιτήσεις του οργανισμού, στη στρατηγική cloud-first προσέγγιση της εταιρείας και στις βέλτιστες πρακτικές της αγοράς για ασφάλεια, επεκτασιμότητα και κόστος. Κάθε υπηρεσία που επιλέχθηκε αξιολογήθηκε σε σύγκριση με εναλλακτικές λύσεις, τόσο εντός του Azure όσο και σε σχέση με παραδοσιακές on-premises υποδομές.

Για τη διαχείριση ταυτότητας και πρόσβασης, επιλέχθηκε το Azure Entra ID (πρώην Azure Active Directory), καθώς προσφέρει πλήρη ενσωμάτωση με το Office 365, υποστήριξη για Single Sign-On, πολιτικές ασφαλείας με granular έλεγχο και υποχρεωτικό Multi-Factor Authentication (MFA). Παρέχει επίσης δυνατότητα σύνδεσης των εταιρικών φορητών υπολογιστών απευθείας με τους εταιρικούς λογαριασμούς, εξασφαλίζοντας συνεπή και ασφαλή πρόσβαση στα συστήματα.

Για τη φιλοξενία της ιστοσελίδας και του δημόσιου API, επιλέχθηκε το Azure App Service, το οποίο προσφέρει εύκολη ανάπτυξη εφαρμογών ASP.NET MVS, αυτόματη κλιμάκωση, υποστήριξη για deployment slots και απλοποιημένη διαχείριση. Η συγκεκριμένη λύση συγκρίνεται ευνοϊκά με τις παραδοσιακές λύσεις IaaS (όπως VMs), καθώς μειώνει το λειτουργικό κόστος και την ανάγκη για διαχείριση του υποκείμενου λειτουργικού συστήματος. Εναλλακτικά, για το API μπορεί να αξιοποιηθεί και το Azure API Management, σε περίπτωση που απαιτείται πολιτική throttling ή πρόσθετη ασφάλεια σε επίπεδο endpoints.

Όσον αφορά την αποθήκευση, τα δομημένα δεδομένα θα διαχειρίζονται μέσω Azure SQL Database, που παρέχει υψηλή διαθεσιμότητα, backup, scaling και υποστήριξη για T-SQL. Για πιο απαιτητικές εφαρμογές με ανάγκες παγκόσμιας διανομής ή NoSQL μοντέλου, επιλέγεται το Azure Cosmos DB. Τα αδόμητα δεδομένα, όπως έγγραφα, εικόνες και πολυμέσα, αποθηκεύονται στο Azure Blob Storage, το οποίο υποστηρίζει lifecycle management, encryption at rest και χαμηλό κόστος για cold/archival tiers.

Για τις stateless λειτουργίες, η χρήση του Azure Functions αποτελεί ιδανική λύση, προσφέροντας serverless περιβάλλον με δυνατότητα auto-scaling, πληρωμή ανά εκτέλεση και εύκολη ενσωμάτωση με άλλα Azure services μέσω Http event-driven triggers. Η συγκεκριμένη προσέγγιση είναι προτιμότερη από τη χρήση containers ή VMs για απλές ή περιοδικές λειτουργίες, καθώς μειώνει σημαντικά την πολυπλοκότητα και το κόστος.

Η παρακολούθηση και η παραμετροποίηση ειδοποιήσεων υλοποιείται με Azure Monitor, Application Insights και Log Analytics. Οι υπηρεσίες αυτές συνεργάζονται αρμονικά για τη συλλογή και ανάλυση τηλεμετρίας από εφαρμογές, υποδομές και βάσεις δεδομένων, επιτρέποντας την έγκαιρη ανίχνευση προβλημάτων και τη βελτιστοποίηση των επιδόσεων.

Τέλος, για την καταγραφή κόστους και τη διαχείριση πόρων, αξιοποιείται το Azure Cost Management, σε συνδυασμό με tags και management groups. Αυτό επιτρέπει τον διαχωρισμό των χρεώσεων ανά έργο ή περιβάλλον (π.χ. development, production), προσφέροντας ξεκάθαρη εικόνα και καλύτερη οικονομική διαχείριση.

Η συνολική επιλογή των υπηρεσιών βασίστηκε σε κριτήρια αξιοπιστίας, ασφάλειας, ευκολίας διαχείρισης και αποδοτικότητας κόστους, ενώ η χρήση PaaS και Serverless λύσεων έναντι IaaS παρέχει την απαιτούμενη ευελιξία και επεκτασιμότητα για τις μελλοντικές ανάγκες του οργανισμού.

# 5. Detailed Resource Configuration

Για την επιτυχή υλοποίηση της υποδομής στο Microsoft Azure, απαιτείται η σωστή παραμετροποίηση των επιμέρους πόρων, σύμφωνα με τις απαιτήσεις της MultiSoftware Enterprise. Στην παρούσα ενότητα περιγράφεται λεπτομερώς η διαμόρφωση των υπηρεσιών, περιλαμβάνοντας ζητήματα όπως η ομαδοποίηση πόρων, τα επίπεδα υπηρεσιών, οι επιλογές ασφαλείας, οι ρυθμίσεις δικτύου και η πολιτική χρέωσης.

**Ομαδοποίηση Πόρων (Resource Groups):**

Οι πόροι οργανώνονται σε διακριτές ομάδες πόρων (resource groups) ανάλογα με τον σκοπό και το περιβάλλον τους (π.χ. παραγωγή, ανάπτυξη, δοκιμή). Η κατηγοριοποίηση αυτή διευκολύνει τη διαχείριση, την εφαρμογή πολιτικών (policies) και την παρακολούθηση κόστους.

**Δικτύωση και Ασφάλεια (Networking & Security):**

Δημιουργούνται εικονικά δίκτυα (Azure Virtual Networks) με κατάλληλες υποδικτυακές περιοχές (subnets), πίνακες δρομολόγησης (route tables) και ομάδες ασφάλειας δικτύου (NSGs), ώστε να εξασφαλίζεται ελεγχόμενη πρόσβαση μεταξύ των υπηρεσιών. Το Azure Firewall ή τα Service Endpoints χρησιμοποιούνται για την απομόνωση ευαίσθητων υπηρεσιών, όπως βάσεις δεδομένων. Η επικοινωνία μεταξύ των πόρων γίνεται με έμφαση στην ασφάλεια και την ελαχιστοποίηση της έκθεσης στο διαδίκτυο.

**Υπηρεσίες Αυθεντικοποίησης και Πρόσβασης:**

Το Azure Entra ID ρυθμίζεται για Single Sign-On και Role-Based Access Control (RBAC). Καθορίζονται πολιτικές MFA για όλους τους διαχειριστές και εξωτερικούς χρήστες. Οι φορητοί υπολογιστές της εταιρείας ενσωματώνονται στον Azure AD για έλεγχο ταυτότητας κατά την είσοδο στο σύστημα.

**Υποδομές Εφαρμογών (App Hosting):**

Η ιστοσελίδα και το API φιλοξενούνται στο Azure App Service, με ενεργοποίηση της αυτόματης κλιμάκωσης (autoscaling) βάσει φορτίου. Χρησιμοποιούνται deployment slots για την ασφαλή προώθηση νέων εκδόσεων. Το App Service ενσωματώνεται με το Application Insights για συνεχή παρακολούθηση.

**Αποθήκευση Δεδομένων:**

Οι δομημένες πληροφορίες αποθηκεύονται σε Azure SQL Database, με ενεργοποιημένα χαρακτηριστικά όπως geo-replication, encryption και performance tiers κατάλληλα για τις ανάγκες της κάθε εφαρμογής.

Τα αδόμητα δεδομένα (αρχεία, εικόνες, βίντεο) διαχειρίζονται μέσω Azure Blob Storage. Ορίζονται containers και lifecycle policies για τη βελτιστοποίηση κόστους, με δυνατότητα εναλλαγής μεταξύ hot, cool και archive tiers.

**Serverless Υλοποιήσεις:**

Οι Azure Functions διαχωρίζονται σε Function Apps ανάλογα με τον τύπο λειτουργιών. Ρυθμίζονται triggers (HTTP, blob, queue, timer) και διασυνδέονται με άλλες υπηρεσίες (π.χ. blob storage, databases). Εφαρμόζεται ελεγχόμενη πολιτική πρόσβασης (Managed Identity).

**Παρακολούθηση και Ειδοποιήσεις (Monitoring & Alerts):**

Οι υπηρεσίες Azure Monitor, Application Insights και Log Analytics ενεργοποιούνται σε όλους τους πόρους. Ορίζονται κανόνες ειδοποίησης για κρίσιμα KPIs όπως: CPU > 80%, αποτυχία εφαρμογών, κ.λπ. Τα δεδομένα παρακολούθησης αποθηκεύονται σε Log Analytics Workspace με retention τουλάχιστον 90 ημερών.

**Συμμόρφωση και Αρχειοθέτηση:**

Οι καταγραφές (logs) των συστημάτων αποθηκεύονται σε dedicated storage accounts για λόγους συμμόρφωσης. Εφαρμόζονται κανόνες lifecycle ώστε τα δεδομένα να μεταβαίνουν αυτόματα σε archive tier. Υπολογίζεται συνολική χρήση άνω των 5 TB με μηνιαία αύξηση 50 GB.

**Χρέωση και Παρακολούθηση Κόστους:**

Οι πόροι επισημαίνονται με tags (π.χ. project name, environment, owner) και ομαδοποιούνται σε management groups ώστε να είναι δυνατή η λεπτομερής παρακολούθηση κόστους μέσω του Azure Cost Management. Οι αναφορές διαχωρίζουν το κόστος ανά υπηρεσία, περιβάλλον και υπεύθυνο τμήμα.

Η παραμετροποίηση των πόρων πραγματοποιείται με τη χρήση Bicep scripts, τα οποία εξασφαλίζουν επαναληψιμότητα, συνέπεια και εύκολη αναπαραγωγή της υποδομής.

# 6. System Architecture and Diagrams

Η αρχιτεκτονική του συστήματος σχεδιάστηκε με γνώμονα την ασφάλεια, την επεκτασιμότητα, την αποδοτική διαχείριση των πόρων και την ευκολία συντήρησης. Η υποδομή ακολουθεί ένα πλήρως cloud-native μοντέλο βασισμένο σε υπηρεσίες PaaS και Serverless του Microsoft Azure, εξαλείφοντας την ανάγκη για φυσικούς servers ή παραδοσιακές λύσεις IaaS.

Το σύστημα διαχωρίζεται σε λογικές περιοχές (logical layers) που περιλαμβάνουν:

**Επίπεδο Πρόσβασης και Αυθεντικοποίησης**:

Όλοι οι χρήστες αυθεντικοποιούνται μέσω του Azure Entra ID, ενώ η πρόσβαση στις εφαρμογές και τους πόρους ελέγχεται με Role-Based Access Control (RBAC). Η Multi-Factor Authentication είναι ενεργοποιημένη για ευαίσθητες λειτουργίες και διαχειριστικούς ρόλους.

**Επίπεδο Εφαρμογών (Application Layer)**:

Η ιστοσελίδα της εταιρείας και το δημόσιο API φιλοξενούνται σε Azure App Service, με δυνατότητα οριζόντιας κλιμάκωσης. Το API είναι διαθέσιμο μέσω HTTPS, με προστασία από DDoS και δυνατότητα σύνδεσης με Azure API Management για πρόσθετη ασφάλεια και παρακολούθηση.

**Επίπεδο Δεδομένων (Data Layer)**:

Τα δομημένα δεδομένα αποθηκεύονται σε Azure SQL Database ή Cosmos DB, ανάλογα με τις απαιτήσεις εφαρμογής (σχέσεις, ανάγκες παγκόσμιας διανομής). Τα αδόμητα δεδομένα αποθηκεύονται σε Azure Blob Storage με διαχωρισμό σε containers και χρήση διαφορετικών επιπέδων αποθήκευσης (tiers) βάσει της συχνότητας πρόσβασης.

**Επίπεδο Λειτουργιών (Serverless Layer)**:

Οι επαναλαμβανόμενες και stateless λειτουργίες υλοποιούνται μέσω Azure Functions, οι οποίες ενεργοποιούνται από events (π.χ. HTTP requests, μεταφόρτωση αρχείων σε storage ή χρονοπρογραμματισμένες εργασίες).

**Επίπεδο Δικτύου και Ασφαλείας (Networking & Security)**:

Οι πόροι διασυνδέονται μέσω Azure Virtual Networks, με χρήση υποδικτύων, Network Security Groups (NSGs) και Route Tables για ελεγχόμενη ροή δεδομένων. Εφαρμόζονται Service Endpoints και Private Links για ασφαλή πρόσβαση σε βάσεις δεδομένων και αποθηκευτικά μέσα.

**Επίπεδο Παρακολούθησης και Συμμόρφωσης (Monitoring & Compliance)**:

Όλοι οι πόροι παρακολουθούνται μέσω Azure Monitor, Application Insights και Log Analytics. Οι κρίσιμες λειτουργίες (ιστοσελίδα, API, βάση δεδομένων) διαθέτουν ρυθμισμένες ειδοποιήσεις σε περίπτωση υπέρβασης κατωφλίων (thresholds). Τα logs διατηρούνται για τουλάχιστον 90 ημέρες, ενώ τα αρχειοθετημένα δεδομένα καταγραφής αποθηκεύονται σε Azure Blob Storage.

**Αρχιτεκτονικά Διαγράμματα**

Τα διαγράμματα αρχιτεκτονικής έχουν σχεδιαστεί χρησιμοποιώντας εργαλεία όπως το draw.io ή Microsoft Visio και περιλαμβάνουν όλα τα βασικά υποσυστήματα και τις μεταξύ τους συνδέσεις. Τα σύμβολα των Azure υπηρεσιών προέρχονται από την επίσημη συλλογή εικονιδίων της Microsoft (https://code.benco.io/icon-collection/azure-icons/) για συνέπεια και αναγνωρισιμότητα.

Τα διαγράμματα περιλαμβάνουν:

* Τη γενική αρχιτεκτονική υποδομής και τα κύρια components
* Τη ροή δεδομένων μεταξύ χρηστών, εφαρμογών, βάσεων και storage
* Τη ρύθμιση των δικτύων, firewalls και κανόνων ασφαλείας
* Την ενσωμάτωση των εργαλείων παρακολούθησης και ειδοποίησης
* Η αρχιτεκτονική έχει σχεδιαστεί ώστε να είναι επεκτάσιμη, modular και συμβατή με μελλοντική χρήση containerization (π.χ. Azure Kubernetes Service), εφόσον χρειαστεί.

A screen shot of a computer

AI-generated content may be incorrect.

# 7. Security and Compliance Strategy

Η ασφάλεια και η συμμόρφωση αποτελούν θεμελιώδεις πυλώνες της αρχιτεκτονικής του έργου, καθώς η MultiSoftware Enterprise διαχειρίζεται επιχειρηματικά κρίσιμα δεδομένα και προσωπικές πληροφορίες υπαλλήλων. Η προτεινόμενη στρατηγική βασίζεται σε ένα μοντέλο “zero trust” με έμφαση στον έλεγχο ταυτότητας, την προστασία δεδομένων, τον περιορισμό πρόσβασης και τη διαφάνεια των ενεργειών εντός της υποδομής.

**Αυθεντικοποίηση και Έλεγχος Πρόσβασης:**

Όλοι οι χρήστες αυθεντικοποιούνται μέσω του Azure Entra ID, ενώ εφαρμόζονται πολιτικές Role-Based Access Control (RBAC) για τον διαχωρισμό δικαιωμάτων ανάλογα με τον ρόλο. Για όλους τους διαχειριστές, αλλά και για κάθε πρόσβαση από εξωτερικά δίκτυα, εφαρμόζεται υποχρεωτικά Multi-Factor Authentication (MFA). Η πρόσβαση στους εταιρικούς πόρους γίνεται αποκλειστικά από εξουσιοδοτημένες συσκευές και λογαριασμούς.

**Κρυπτογράφηση και Προστασία Δεδομένων:**

Όλα τα δεδομένα, είτε δομημένα είτε αδόμητα, αποθηκεύονται με ενεργή κρυπτογράφηση κατά την αποθήκευση (encryption at rest) και κατά τη μεταφορά (encryption in transit). Για τις βάσεις δεδομένων χρησιμοποιούνται Azure-managed keys, ενώ σε κρίσιμα συστήματα ενεργοποιείται η χρήση πελατειακών κλειδιών (customer-managed keys) μέσω Azure Key Vault.

**Δίκτυα και Απομόνωση Πόρων:**

Οι υπηρεσίες προστατεύονται μέσω Network Security Groups (NSGs), ενώ οι ευαίσθητοι πόροι (όπως βάσεις δεδομένων και αποθηκευτικά μέσα) είναι προσβάσιμοι μόνο μέσω εσωτερικών endpoints ή private links. Το Azure Firewall και τα service endpoints συμβάλλουν στην αποτροπή μη εξουσιοδοτημένης εξωτερικής πρόσβασης. Η χρήση Azure DDoS Protection προστατεύει τις δημόσια εκτεθειμένες εφαρμογές από κακόβουλες επιθέσεις.

**Καταγραφή Δραστηριότητας και Παρακολούθηση:**

Ενεργοποιούνται όλες οι δυνατότητες του Azure Monitor, Log Analytics και Activity Logs, επιτρέποντας την πλήρη ιχνηλασιμότητα (traceability) των ενεργειών χρηστών και υπηρεσιών. Οι ειδοποιήσεις (alerts) σε περίπτωση αποτυχιών ή ύποπτων ενεργειών ενεργοποιούνται άμεσα και συνδέονται με πολιτικές απόκρισης.

**Συμμόρφωση με Κανονισμούς:**

Η υποδομή είναι σχεδιασμένη ώστε να συμμορφώνεται με ευρωπαϊκούς και διεθνείς κανονισμούς, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR). Τα δεδομένα παραμένουν εντός ευρωπαϊκών data centers του Azure, και τα logs διατηρούνται για τουλάχιστον 90 ημέρες, ενώ τα αρχειοθετημένα δεδομένα συμμορφώνονται με τις απαιτήσεις διατήρησης για νομικούς ή λογιστικούς σκοπούς.

**Αυτοματισμοί και Πολιτικές Ασφαλείας:**

Μέσω Azure Policy και Azure Blueprints εφαρμόζονται αυτόματα κανόνες ασφάλειας, όπως η απαίτηση για encryption, η αποφυγή δημόσιων IP σε κρίσιμους πόρους και η επιβολή συγκεκριμένων tags για λόγους ανιχνευσιμότητας και κόστους. Παράλληλα, η χρήση Infrastructure-as-Code (Bicep) εξασφαλίζει ότι οι πολιτικές ασφαλείας τηρούνται ομοιόμορφα και επαναλαμβανόμενα σε όλα τα περιβάλλοντα.

Η παραπάνω στρατηγική εξασφαλίζει ένα ισχυρό, αξιόπιστο και διαχειρίσιμο πλαίσιο ασφάλειας, περιορίζοντας τους κινδύνους παραβίασης δεδομένων και υποστηρίζοντας τη συμμόρφωση με τα πρότυπα του κλάδου.

# 8. Monitoring and Cost Visibility

* Ενεργοποίηση Azure Monitor, Log Analytics, Application Insights.
* Alerting rules και visibility του κόστους ανά πόρο.

# 9. Billing Estimate & On-premises Comparison

* Ανάλυση κόστους Azure (με πίνακες/Excel).
* Σύγκριση με ιδιόκτητη λύση (κόστος hardware, συντήρησης, κ.λπ.).

# 10. Team Collaboration & Project Management

* Χρήση MS Teams, GitHub, κατανομή ρόλων, συντονισμός εργασιών.
* Παρακολούθηση milestone.

# 11. Challenges and Resolutions

* Δυσκολίες που αντιμετωπίστηκαν (π.χ., επιλογή database, networking).
* Λύσεις που εφαρμόστηκαν.

# 12. Future Improvements & Scalability

* Πώς μπορεί να εξελιχθεί η υποδομή (π.χ., Kubernetes, AI integration, global CDN).

# 13. Conclusions

* Τι πετύχατε, γενικά συμπεράσματα για την υλοποίηση και τα οφέλη.

# 14. References / Appendices

* Πηγές, συνδέσεις σε scripts, templates, αρχεία διαγραμμάτων.