CONSIST
Business Information Technology

NAGIX AI
Powered by CONSIST

NAGIX AI:
ארכיטקטורת המערכת

גרסה 1.5

Zero Project
For a world with zero barriers

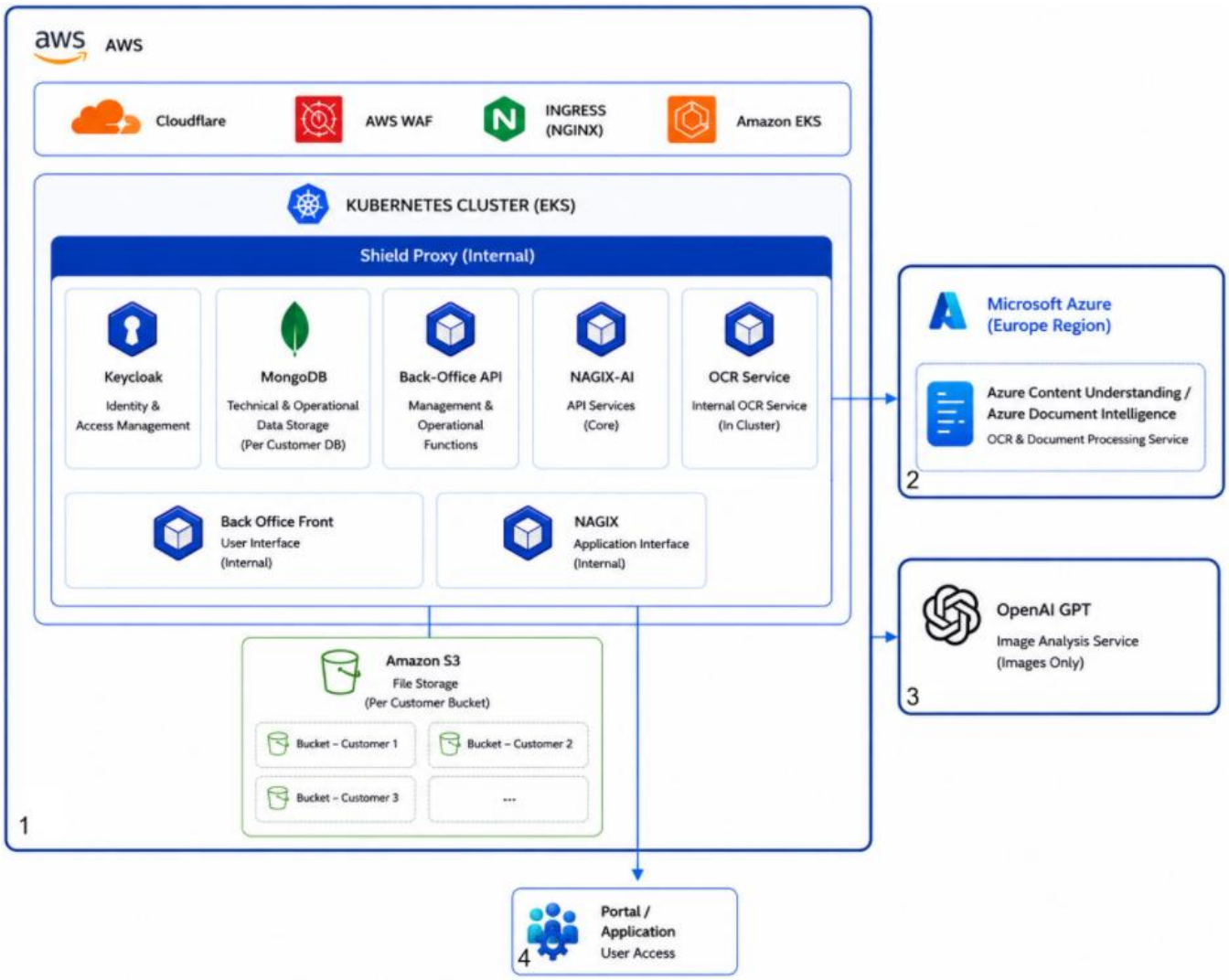
Valuable 500

www.nagix-ua.com

ארכיטקטורת מערכת NAGIX AI בענן

NAGIX AI היא מערכת SaaS (Software as a Service) שיושבת ב- AWS שנועדה להפקת מסמכים מונגשים ע"ב בינה מלאכותית. המערכת נועדה להמיר מסמכים בודדים, ארוכים ומורכבים ככל שיהיו, באופן אוטומטי ומיידי למסמכי PDF/UA נגישים לחלוטין.

תרשים ארכיטקטורה של המערכת



מודל הפריסה של ארכיטקטורת המערכת:

1. סימון 1: מנוהל בסביבת הספק. ניתן לפריסה בסביבת ה- EKS הארגונית של הלקוח.
2. סימונים 2-3: שירותים חיצוניים (Third-Party Services) המופעלים ומנוהלים בתשתית הספק בלבד ואינם מיועדים להתקנה בסביבת הלקוח.
3. סימון 4: ניתן להתקנה הן בסביבת הלקוח והן בסביבת הספק, בהתאם לארכיטקטורת היעד ולדרישות הפרויקט.

מפרט התרשים

רכיב ליבה:

NAGIX AI מהווה את שכבת השירות המרכזית של המערכת ומספק ממשקי API מאובטחים עבור צרכני המערכת והאינטגרציות השונות. השירות אחראי על קבלת הבקשות, ניהול ותיאום עיבוד הרכיבים השונים.

במסגרת פעילותו, השירות עושה שימוש במספר רכיבים. להלן תיאור:

- שירות OCR פנימי הפועל בתוך סביבת ה - Kubernetes Cluster לצורך עיבוד מסמכים וחילוץ מידע.
- **MongoDB** - המשמש לאחסון מידע טכני ותפעולי, כאשר לכל לקוח מוקצה מסד נתונים ייעודי ונפרד לצורך הבטחת בידוד מלא בין לקוחות.
- **Amazon S3** - המשמש לאחסון מסמכים וקבצים. לכל לקוח מוקצה Bucket ייעודי ונפרד, המאפשר הפרדה מלאה בין נתוני הלקוחות. הקבצים מאוחסנים באופן מוצפן ומנוהלים בהתאם למדיניות אבטחת המידע של הארגון
- **Keycloak** – מערכת המשמשת לניהול זהויות והרשאות (Identity & Access Management), ומספקת מנגנוני הזדהות מאובטחים המבוססים על תקני OpenID Connect (OIDC) ו- OAuth 2.0, כולל תמיכה ב-SSO ואינטגרציה עם מערכות זהויות ארגוניות.
- **Backoffice Front Application**
- **Backoffice API**

מסד נתונים (MongoDB):

המערכת עושה שימוש במסדי נתונים מסוג MongoDB, המנוהלים בסביבת הענן של AWS. לצורך הבטחת הפרדה מלאה בין לקוחות (Tenant Isolation), לכל לקוח מוקצה Instance ייעודי ונפרד של מסד הנתונים. המשמעות היא שכל הנתונים של לקוח נשמרים בסביבת נתונים מבודדת, ללא שיתוף או גישה בין מסדי הנתונים של לקוחות שונים.

מסד הנתונים משמש לאחסון מידע טכני ותפעולי בלבד, כגון:

- מזהי בקשות (Request IDs)
- זמני קליטה ועיבוד
- סטטוס עיבוד
- השירותים והרכיבים שהשתתפו בתהליך
- מידע לצורכי ניטור, תחקור ובקרה (Audit & Troubleshooting)

המערכת אינה שומרת במסד הנתונים את תוכן המסמכים עצמם, אלא מידע מטא-דאטה ותיעוד תפעולי הנדרש לניהול, ניטור ותחזוקת השירות. גישה למסדי הנתונים מבוקרת ומוגבלת בהתאם לעקרון ה- Least Privilege, תוך שימוש במנגנוני אבטחה והצפנה המקובלים בסביבות ענן ארגוניות.

אחסון מסמכים וקבצים (Amazon S3):

המערכת עושה שימוש בשירות Amazon S3 (Simple Storage Service) לצורך אחסון מאובטח של מסמכים וקבצים. תקופת השמירה המוגדרת בברירת מחדל היא עד 30 יום, כאשר ניתן להתאים את משך השמירה בהתאם לדרישות הלקוח. אמין וסקיילבילי של מסמכים וקבצים. לכל לקוח מוקצה Bucket ייעודי ונפרד, המאפשר הפרדה מלאה בין נתוני לקוחות ומבטיח שלא קיימת גישה או חשיפה של מידע בין סביבות שונות. בנוסף, במידת הצורך ניתן להגדיר את המערכת כך שתעבוד ישירות מול סביבת ה- S3 של הלקוח, ללא צורך באחסון הקבצים בסביבת האחסון שלנו.

בתוך סביבת האחסון קיימת גם הפרדה לוגית בין השירותים השונים במערכת, כך שכל שירות מקבל גישה רק למידע הנדרש לצורך ביצוע תפקידו, בהתאם לעקרון ה- Least Privilege. מנגנון זה מסייע במניעת חשיפה לא נחוצה של מידע ומקטין את משטח התקיפה הפוטנציאלי.

כל הקבצים המאוחסנים ב- S3 מוגנים באמצעות הצפנה אוטומטית במנוחה (Encryption at Rest) המסופקת על ידי AWS ומועברים בתקשורת מוצפנת באמצעות HTTPS/TLS.

Keycloak:

רכיב ניהול הזהויות והגישה (IAM) של מערכת ה-Backoffice. הוא אחראי על אימות משתמשים (Authentication), ניהול הרשאות (Authorization), תפקידים וקבוצות משתמשים. בפריסה אצל לקוח ניתן לשלב את Keycloak מול ה- Active Directory או Microsoft Entra ID הארגוני, ולאפשר הזדהות באמצעות מנגנון ה- SSO של הארגון. כך ניהול המשתמשים, מדיניות הסיסמאות, ה- MFA ותהליכי מחזור חיי המשתמש נשארים בשליטת הלקוח ובהתאם למדיניות האבטחה הארגונית שלו.

Backoffice Front Application:

אפליקציית Web המבוססת על Angular, המשמשת כממשק הניהול של המערכת. האפליקציה יכולה להיות מותקנת בסביבת הספק או בסביבת הלקוח, בהתאם לארכיטקטורת ההטמעה שנבחרה.

באמצעות הממשק ניתן לנהל חברות, משתמשים מורשים, תפקידים והרשאות גישה למערכת, וכן לבצע פעולות אדמיניסטרטיביות ותפעוליות שונות. האפליקציה מתקשרת באופן מאובטח עם שירותי ה-Backend באמצעות APIs, ומאפשרת שליטה מרכזית בניהול המשתמשים והארגונים במערכת.

הגישה לאפליקציה מוגבלת למשתמשים מורשים בלבד, ומנוהלת באמצעות מנגנוני הזדהות והרשאות, כך שכל משתמש נחשף אך ורק למידע ולפעולות המותרים לו בהתאם לתפקידו בארגון.

Backoffice API:

שירות המהווה את שכבת השרת (Backend) של מערכת הניהול. השירות מספק ממשקי API מאובטחים עבור אפליקציית ה- Backoffice ומאפשר ניהול חברות, משתמשים, תפקידים והרשאות במערכת. בנוסף, השירות אחראי על עיבוד בקשות, אכיפת הרשאות גישה, ביצוע אימות נתונים, שמירה ועדכון המידע במאגרי הנתונים של המערכת. הגישה לשירות מתבצעת באמצעות מנגנוני הזדהות והרשאות בהתאם למדיניות האבטחה שהוגדרה.

NAGIX-AI Portal (Frontend Application):

מהווה את שכבת הגישה של המשתמשים למערכת. הממשק יכול לפעול על גבי שרת הממוקם בסביבת הלקוח או בסביבה המנוהלת על ידי הספק. הרכיב מתקשר עם שירותי המערכת באמצעות APIs מאובטחים. דרך הממשק ניתן ליצור ולנהל תהליכים עסקיים, לצפות במסמכים שהונגשו ועובדו, לקבל רשימות מסמכים, לבצע פעולות ניהול ובקרה ולעקוב אחר תהליכי העבודה במערכת. הגישה למידע ולפונקציונליות השונות נשלטת באמצעות מנגנוני הזדהות והרשאות, כך שכל משתמש נחשף רק למידע ולפעולות המותרים לו בהתאם לתפקידו.

המערכת צורכת שירותי צד ג :

- Azure Content Understanding & Azure Document Intelligence
- Open AI

שירותי OCR וניתוח מסמכים (Azure Content Understanding & Azure Document Intelligence):

המערכת עושה שימוש בשירותי Azure Content Understanding ו-Azure Document Intelligence של Microsoft Azure לצורך ביצוע OCR (זיהוי טקסט אופטי), ניתוח מסמכים וחילוץ מידע מובנה ברמת דיוק גבוהה. שירותים אלו מאפשרים עיבוד של מסמכים בפורמטים שונים והפקת נתונים באופן אוטומטי לצורך המשך עיבוד במערכת. התקשורת בין תשתית AWS לבין שירותי Azure מתבצעת באמצעות HTTPS/TLS, תוך שימוש בהצפנה מקצה לקצה במהלך העברת הנתונים.

לצורך חיזוק אבטחת המידע והקטנת החשיפה לרשת הציבורית, הגישה לשירותים מתבצעת באמצעות Private Endpoint ו-Private Channel כך שהשירותים אינם חשופים לאינטרנט הציבורי ונגישים רק מכתובות ורשתות מורשות שהוגדרו מראש.

במהלך העיבוד, המסמכים נשמרים באופן זמני בלבד בסביבת השירות של Microsoft Azure ב Region: West Europe. הנתונים מוצפנים בזמן האחסון והעיבוד בהתאם למנגנוני האבטחה של Azure, ולאחר השלמת תהליך העיבוד הם נמחקים בהתאם למדיניות השירות. שירותי ה- AI של Microsoft משמשים לעיבוד המסמכים בלבד. Microsoft אינה שומרת את המסמכים לאחר סיום העיבוד ואינה משתמשת בתוכן המועבר לשירות לצורך אימון, שיפור או התאמה של מודלי הבינה המלאכותית שלה.

הזדהות המערכת מול שירותי Azure מתבצעת באמצעות מנגנון ניהול סודות מאובטח, כאשר פרטי ההזדהות וההרשאות נשמרים ומנוהלים באמצעות AWS Secrets Manager, בהתאם למדיניות ניהול הזהויות והסודות של הארגון.

שירות Open AI לניתוח תמונות:

המערכת עושה שימוש בשירות Open AI לצורך ניתוח תמונות בלבד. במסגרת תהליך זה, מועברות לשירות רק התמונות הנדרשות לעיבוד, ללא העברת המסמך המלא או מידע שאינו נדרש לצורך הניתוח.

הפרדה זו מאפשרת לצמצם את היקף המידע המועבר לשירות החיצוני ולפעול בהתאם לעקרון Data Minimization, שלפיו מועבר רק המידע ההכרחי לביצוע הפעולה הנדרשת.

שירות ה- Open AI משמש לזיהוי, ניתוח והפקת תובנות מתוך תמונות, כחלק מתהליך עיבוד המסמך הכולל במערכת. הנתונים המועברים לשירות משמשים לצורך העיבוד בלבד ואינם כוללים את כלל תוכן המסמך או מידע נוסף מעבר לתמונה הרלוונטית.

מנגנוני הגנה ובקרה

- Secrets Management
- ניטור, בקרה ואחריות תפעולית

Secrets Management:

המערכת עושה שימוש במנגנון מאובטח לניהול Secrets, הכוללים בין היתר מפתחות גישה, טוקנים, פרטי הזדהות לשירותים חיצוניים והרשאות גישה למשאבי ענן.

כיום, ה- Secrets הנדרשים להפעלת המערכת מנוהלים בסביבת Kubernetes, תוך הקפדה על הגבלת גישה לרכיבים ולשירותים המורשים בלבד. בנוסף, קיימת תמיכה בניהול Secrets באמצעות AWS Secrets Manager, המאפשר אחסון מאובטח, ניהול הרשאות ובקרה מרכזית על השימוש במידע רגיש.

הארכיטקטורה תומכת בהפרדה ברורה בין Secrets השייכים לסביבת הלקוח לבין Secrets השייכים לספק השירות:

- Secrets הקשורים למשאבי הלקוח (בגון מערכות פנימיות, שירותי ענן, ממשקים ארגוניים או מקורות מידע בבעלות הלקוח) יכולים להישאר בניהול ובשליטה מלאה של הלקוח.
- Secrets הקשורים לשירותי המערכת ולרכיבים המנוהלים על ידי הספק נשמרים ומנוהלים בסביבה המאובטחת של הספק.

בנוסף, עבור שירותים חיצוניים כגון Azure Content Understanding ו- Open AI, פרטי ההזדהות והגישה מנוהלים באמצעות מנגנוני ניהול סודות מאובטחים, בהתאם למדיניות האבטחה של הספק.

הפתרון מאפשר גם אינטגרציה עם מערכות Secret Management ארגוניות של הלקוח, כך שניתן לצרוך Secrets ישירות ממערכות הארגון ללא צורך בשכפול או העתקת מידע רגיש.

במסגרת תהליך ההטמעה, מתבצע מיפוי של כלל סוגי ה- Secrets במערכת והגדרת מודל בעלות (Ownership Model) על מנת לקבוע אילו סודות נמצאים באחריות הלקוח ואילו נמצאים באחריות הספק. גישה זו מאפשרת עמידה בדרישות אבטחת מידע, ממשל תאגידי ורגולציה הנהוגות בארגונים פיננסיים ובנקאיים.

ניטור, בקרה ואחריות תפעולית:

המערכת כוללת יכולות ניטור, בקרה והתראות (Monitoring & Alerting) המאפשרות מעקב רציף אחר זמינות השירותים, ביצועי המערכת, תקינות תהליכי העיבוד ואירועי מערכת חריגים.

מודל האחריות התפעולית נקבע בהתאם לאופן פריסת המערכת:

1. סביבת SaaS מנוהלת על ידי הספק:

כאשר המערכת פועלת בסביבת הענן המנוהלת על ידי הספק, האחריות לניטור, תחזוקה שוטפת, טיפול בתקלות, ניהול התראות ובקרת זמינות השירותים נמצאת באחריות הספק. צוותי התפעול מבצעים מעקב שוטף אחר רכיבי המערכת ופועלים לזיהוי ולטיפול מהיר בתקלות או חריגות.

2. סביבת לקוח (Customer Hosted):

כאשר המערכת מותקנת ומופעלת על גבי תשתיות הלקוח, האחריות לניטור התשתיות, השירותים והמשאבים נמצאת בידי הלקוח. במודל זה הלקוח מנהל את כלי הניטור, ההתראות והבקרה התפעולית בהתאם לנהלים ולמערכות הארגוניות שלו. במידת הצורך ניתן להגדיר מנגנוני שיתוף מידע, התראות או גישה מבוקרת לצורכי תמיכה ותחקור, בהתאם למדיניות אבטחת המידע של הארגון. מודל זה מאפשר חלוקת אחריות ברורה בין הצדדים ותמיכה בדרישות הממשל התאגידי והרגולציה המקובלות בארגונים.

על NAGIX AI

NAGIX - AI היא תשתית SaaS מתקדמת המבוססת על טכנולוגיות בינה מלאכותית ומאפשרת המרה אוטומטית של מסמכים לפורמטים נגישים העומדים בדרישות התקנים והרגולציות המקובלות, כגון PDF/UA ו- WCAG. המערכת תומכת במגוון רחב של סוגי קבצים, לרבות PDF, Word, PowerPoint ו- Excel ומספקת יכולות עיבוד מתקדמות לזיהוי מבנה המסמך, כותרות, טבלאות, תמונות, סדר קריאה ואלמנטים נוספים הנדרשים לצורך נגישות מלאה. הפתרון מיועד לארגונים המעוניינים להנגיש כמויות גדולות של מסמכים באופן מהיר, מדויק ויעיל, תוך צמצום התלות בתהליכים ידניים ושיפור העמידה בדרישות רגולטוריות ותקני נגישות בינלאומיים.