

**ממר”ם**

**מסמך מענה הגנה  
רשת דביר**

**גרסה 1.0**

08/09/2025

**ספקית העננים הצה״לית**

ענף סייבר

מדור ארכיטקטורה ומו"פ

– מוגבל –

כל המוסר תוכן מסמך זה כולו או מקצתו, לידיעת אנשים שאינם מוסמכים לכך, עובר על חוקי בטחון המדינה. כל המוצא מסמך זה נדרש למסרו לתחנה הקרובה של משטרת ישראל או המשטרה הצבאית.

**מסמך מענה הגנה – שם**

**מהדורה** 1.0

**תאריך כתיבה:** 00/00/2025

**סביבה:**

**כתבו:** יועצים - דור הוברמן, אופק מאיירשטיין

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **מס'** | **תאריך** | **כתבו** | **אישר** | **פרטי עדכון** |
| 1.0 | 08/09/2025 |  |  | גרסה 1.0 |

**עדכונים:**

**תוכן עניינים**

[1. הקדמה 3](#_Toc178901135)

[2. הנחות יסוד 4](#_Toc1728478977)

[3. עקרונות הגנה מנחים 5](#_Toc2013326332)

[4. ארכיטקטורה 6](#_Toc695094429)

[5. זהויות והרשאות 8](#_Toc1401802412)

[6. אבטחת מידע 12](#_Toc263167305)

[7. שגרת הגנה 14](#_Toc1077217712)

# הקדמה

1. כחלק מפרויקט נימבוס, הוחלט על הקמת סביבות צה"ליות מטכ"לית בתשתית הענן של חברת גוגל – Google Cloud Platform (GCP), ושל חברת אמאזון – Amazon Web Services (AWS).
2. הסביבות הינן באחריות תפעולית והגנתית של יחידת ממר"ם.
3. כחלק ממלחמת "חרבות ברזל" הועלה הצורך להעלות פרויקטים בעלי Impact Level מנהלתי לסביבת הענן הציבורי (Terra AWS).
4. כמו כן, עלה הצורך להנגיש אפליקציות בסיווג עד שמור מנהלתי לתפקידנים במרחב זה על בסיס תשתית מוקשחת מנוטרת ומוגנת.
5. מסמך זה יתאר את עקרונות וארכיטקטורת ההגנה עבור רשת המשתמשים של סביבת TERRA.
6. רשת המשתמשים במרחב TERRA תשרת לקוחות בסביבה המעוניינים לחשוף אפליקציות בסיווג עד שמור מנהלתי שרצות במרחב TERRA בסביבות AWS ו- GCP למשתמשי קצה.
7. בפרויקט זה קיימת חלוקת עבודה בין ספקית התשתית (סלקום) ליחידת ממר״ם (פלטפורמה/סייבר ציבורי).
8. מסמך זה יאפיין את תהליכי ואמצעי שגרת ההגנה שיש לייצר עבור הפרויקט.
9. עקרונות אלו מוכוונים למול הצורך המבצעי עבור עמדות קצה נייחות בלבד, ככל שיעלה צורך שתצורה שורה מנייחת נדרש לקבל הנחיות ייעודיות.

# הנחות יסוד

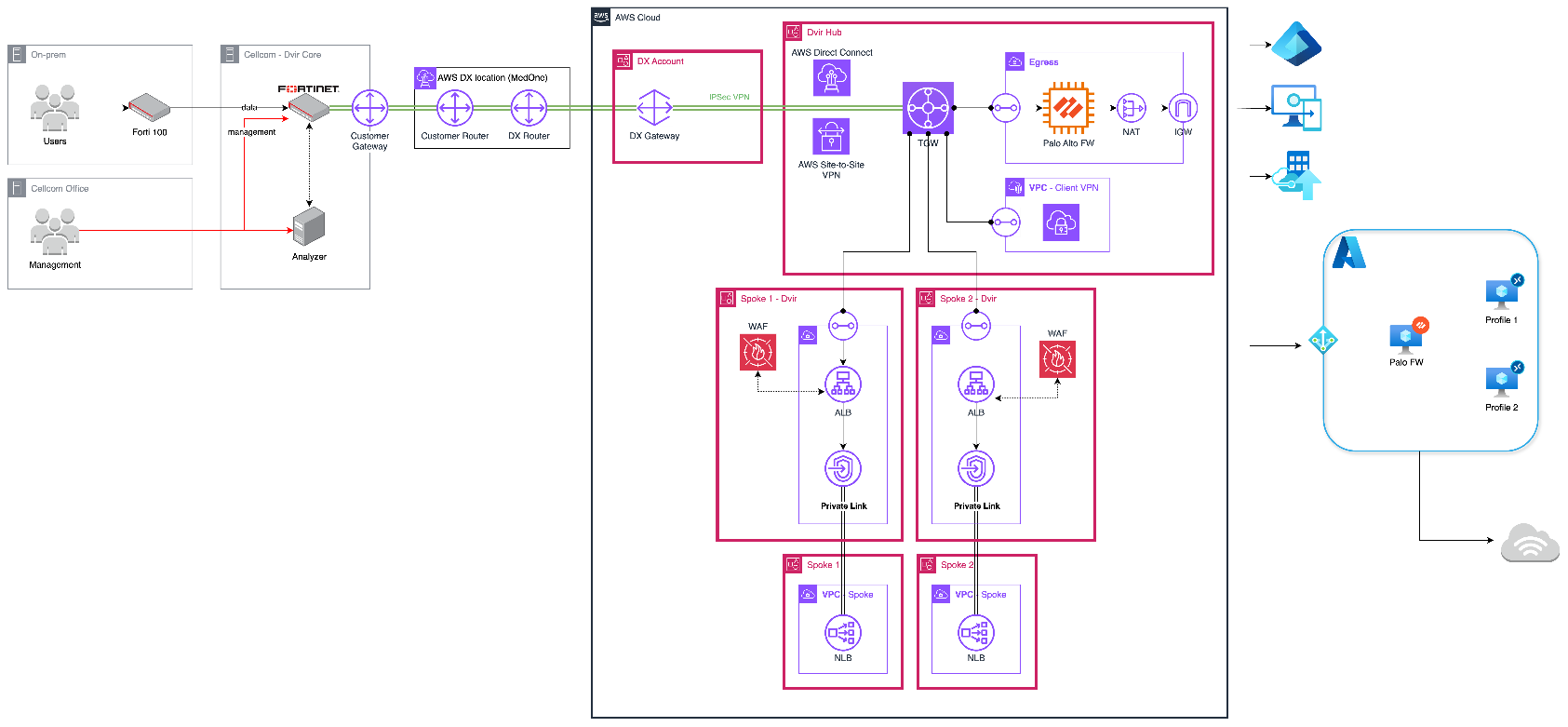
1. מסמך זה עוסק במענה הגנה עבור הקמת ותפעול רשת דביר, כפי שהיא מסופקת כשירות ללקוחות הענן הציבורי. לצרכי ניהול אפליקטיבי ותהליכים בסביבות הענן הציבורי המטכ"לית.
2. חשוב להבהיר כי המסמך אינו כולל התייחסות למקרים הבאים:
   1. פריצה או תקלה בתשתיות הענן של חברת סלקום עצמה (למשל – שרתים, מרכזי נתונים, ציוד פיזי).
   2. טעויות או זליגות מידע שמקורן מהמשתמשים השונים בצה״ל.
   3. תקלות או פגיעות ברכיבים חיצוניים שהשירות מסתמך עליהם, אשר לא בשליטת צה"ל.
3. מסמך זה אינו נותן מענה הגנה לאויב אשר משיג אחיזה על תשתית ספקית התשתית.
4. המסמך מתמקד בכל מה שנמצא בשליטת המשתמש הצה״לי – כגון:
5. ניהול שמות משתמשים וסיסמאות.
6. הרשאות גישה למידע ופעולות.
7. קביעת הגדרות האבטחה והגנה.
8. פירוט עקרונות הניטור בסביבה ושגרות הגנה וניטור פעולות חריגות אך לא יפרט את חוקי הניטור.
9. במודל האחריות המשותפת עם הספקית (Shared Responsibility Model), מסמך זה יטפל בגבולות האחריות של לקוח השירות (ממר״ם).
10. דרישות ההגנה במסמך זה מבטאות את המחקר והידע נכון ליום הפרסום וצפויות להשתנות בעתיד בהתאם לשינויים בעולם, שינויים ביכולות הספקית, שינויים ביכולות האויב, ובהתאם למחקרים נוספים.

# עקרונות הגנה מנחים

מסמך זה נשען על עקרונות הגנה, אשר ייושמו בתשתית:

1. הזדהות חזקה וניהול הרשאות בתצורת Least Privilege.
2. צמצום משטח התקיפה ככל הניתן.
3. מימוש עקרונות Zero Trust בכדי לצמצם Blast Radius במקרה של אירוע.
4. נראות מלאה של הפעולות אשר מתבצעות במערכת עבור מימוש שגרת הגנה, לרבות הפעלת מנגנוני ניטור ותיעוד.

# ארכיטקטורה

****

1. לרשת המשתמשים יחוברו עמדות 'דביר' בלבד.
2. העמדה תחובר באתר קצה של רשת 'קליקנט' ל- VRF ייעודי לסביבת המשתמשים של מרחב TERRA – VRF דביר.
3. יוקם HUB ייעודי בסיבות AWS TERRA בשם Users Hub עבור קליטת המשתמשים אשר ישרת בשלב א׳ את AWS ובשלב ב׳ GCP עבור הקישוריות למול שירותי מייקרוסופט.
4. יוקם S2S על גבי קווי נל"ן ייעודיים (DIRECT CONNECT) בין ליבת סלקום ל- - AWS ו- GCP.
5. העמדה תקבל הגדרות רשת משירות DHCP בניהול סלקום
6. העמדה תעשה שימוש בשירות DNS בניהול פלטפורמה, יש לממש DNS FW
7. ב- Users Hub יוגדר transit gateway שיאפשר את הגישות הבאות בלבד:
   1. גישה מעמדות ברשת דביר לאזורי קליטה אפליקטיביים בסביבות הענן השונות של TERRA בשלב א׳ AWS בלבד.
   2. גישה מעמדות ברשת דביר לשירותים האינטרנטיים הנדרשים להזדהות וניהול העמדה דרך NextGen FW .
   3. גישה מעמדות ברשת דביר לשירותי ההזדהות של ENTRA ID.
   4. גישה מעמדות ברשת דביר לכתובות הנדרשות לצורך עדכוני מערכת הפעלה של Windows.
   5. גישה מעמדות ברשת דביר לכתובות הנדרשות לצורך ניהול העמדה ע"י INTUNE.
   6. גישה מעמדות ברשת דביר לכתובות הנדרשות לצורך פעילות תקינה של Defender for Endpoint.
   7. צריכת שירותי אינטרנט באופן 'מרוחק' ע"ב פתרון AVD מצומצם (edge בלבד).
   8. הקמת יכולת NextGen fw , TLS INSPECTION יש לממש באמצעות HEADER INSERTION יכולות TENANT RESTRICTION v2 של AZURE.
   9. כל חוק נוסף הנדרש לטובת פעילות תקינה של הפרויקט המשתמש בתשתית תאושר על ידי מדור ארכיקטורה ומו״פ בענף סייבר ממר״ם.
8. עבור כל מערכת ב- AWS יוגדר ב- Users Hub אזור קליטה אפליקטיבי:
9. אזור הקליטה יוקם בחשבון ייעודי כ-SPOKE של Users Hub.
10. חשיפת האפליקציה תתבצע באמצעות רכיב ALB.
11. רכיב ה- ALB יבצע TLS Termination עבור האפליקציה.
12. ה- ENDPOINT יקושר ל- ENDPOINT SERVICE שחושף NLB בחשבון האפליקטיבי.
13. רכיב ה- ALB יחיל פוליסות WAF שמטרתן לצמצם את היכולת להשמיש פגיעויות אפליקטיביות
14. ככלל, רכיב ה- ALB יממש ויאכוף את תהליך ההזדהות למול Entra ID.

# זהויות והרשאות

1. **מאפייני עמדה**
   1. עמדת קצה ייעודית המרשתת את משתמשי מרחב TERRA
   2. העמדה תשרת אפליקציות שרצות בסביבת AWS ובסיבת GCP במרחב TERRA
   3. העמדה תנוהל באמצעות כלי הניהול הניתנים כחלק מתשתית AZURE (INTUNE,DEFENDER FOR ENDPOIT))
   4. תהליך ההזדהות לעמדה יתבצע באמצעות משתמשים ייעודיים המנוהלים ב- Entra ID כמפורט בפרק זהויות והרשאות
   5. יש לחסום באמצעות HFW כל תקשורת Inbound לעמדה.
   6. יש להגדיר את העמדה בתצורת 'קיוסק' כמפורט להלן:  
      א. יש להגדיר פוליסת Application Control המונעת הרצת אפליקציות שאינן דפדפן Edge ופתרון הגלישה  
      יש להגדיר פרופילי גלישה על פי כתובות URLים מאושרים בתצורת WL, יש לממשם גם ברמת העמדה.  
      יש להגדיר פוליסה על הדפדפן המונעת גלישה במצב In-Private .  
      יש להגדיר פוליסה על הדפדפן המונעת הורדה/העלאת קבצים והעתקה/הדבקה של תוכן מ/אל הדפדפן  
      יש להגדיר פוליסה על הדפדפן המונעת גישה DevTools
   7. למשתמשי העמדה לא יהיוי הרשאות Local Admin
   8. יש לחסום את האפשרות לשנות הגדרות רשת על העמדה (ובכלל זה הגדרות PROXY)
   9. יש להגדיר פוליסת Device Control המונעת חיבור של התקנים לעמדה.
   10. על אובייקט המחשב של העמדה ב- Entra יוגדר Extention attribute ייעודי המאפיין את סוג העמדה.
2. **הזדהות למערכת**
3. בסביבת TERRA קיימים משתמשים עבור מפתחים DEV ו- PROD אליהם יצטרף סוג משתמש חדש עבור משתמשי קצה ברשת 'דביר'.
4. הזדהות למערכת תתבצע בעזרת המשתמשים הצה"ליים של IDP Terra בלבד ('משתמשי דביר׳ תחת Azure Entra AD).
5. הזדהות משתמשים צה"ליים לסביבה תתבצע באמצעות שם משתמש וסיסמה, כאשר תידרש סיסמה חזקה (אכיפה באמצעות Strong Password Policy בהגדרות השירות) בתוספת MFA על בסיס Microsoft Authenticator.
6. הזדהות לסביבה, תבוצע רק מעמדות דביר, אכיפה באמצעות CA.
7. עבור משתמשי הקצה האישיים תוגדר קונבנציה חדש:

dvr.palmoni789@idf.il

First name – ploni  
Last name – Almoni

ID - 123456789

1. כלל האפליקציות ב-TERRA יממשו הזדהות אפליקטיבית אישית, לרבות בעמדות חמ"ל.
2. **הרשאות**
3. הרשאות יסופקו בתצורת Least Privilege, תוך כדי מתן הרשאות לצרכים נוכחיים, וצרכים פוטנציאליים של התפקידן בעמדת דביר.
4. הרשאות יסופקו ברמת כלל הארגון, ענף, או פרויקט.

4. **מחזור חיים של Sessions**

1. יוגדר אורך סשן מינימלי - כשעה, ובכל אופן יתאפשר לדעת בכל זמן נתון מי עבד על העמדה.  
   **משתמשי חירום (Break Glass)**
2. משתמש Break Glass, הינו משתמש אשר אינו מקושר אל מול ה-IDP של Terra, ואינו משויך למשתמש אנושי. מטרתו לאפשר גישה למערכת בתרחישי **חירום בלבד** – כאשר לא ניתן להשתמש באמצעי הזדהות.
3. משתמש ה-Break Glass ינוהל על ידי יחידת ממר"ם.
4. על ה-Break Glass User להיות בעל סיסמה חזקה מאוד (18 תווים, לפחות אות אחת גדולה, אחת קטנה, מספר ותו מיוחד), ולהיות שמורה ב-Key Vault ברשתות המבודלות של צה"ל.
5. יש לנטר כל פעילות הנוגעת למשתמש הBreak Glass.
6. **מחזור חיים של משתמשים**
7. אחת לחודש, יש לבצע הסרה של משתמשים אשר אינם דורשים שימוש בשירות.
8. יש להסיר משתמשים אשר לא התחברו למערכת למעלה מחודשיים.
9. יש לקיים סקירה רבעונית של כלל משתמשי ה-Administrator - על ידי גורם הגנה.
10. על כל יוזר ינוהל מחזור חיים שלם:  
     א. סדיר (לרבות אע"צ ויועצים בחצרות צה"ל) – עד שחרור/סיום פעילות  
     ב. מילואים – לשנה (ואישור מתחדש על פי צורך)  
     ג. שרשרת אספקה (מחוץ לחצרות צה"ל) – לשלושה חודשים (ואישור מתחדש על פי צורך).

# אבטחת מידע

1. איום ייחוס – בהלימה לאיומים שחלים בסביבת TERRA, קרי אויב ראשי (מדינתי ותת מדינתי), גורמי פשיעה, תעמולה ו-NGO, איום פנימי (לרבות בשרשרת האספקה) ואיומים הנשקפים לפרויקט מתקיפת שרשרת האספקה
2. סיכונים:  
   1) דלף מידע מסווג או ערכי מ:  
    א. רכיבי הרשת – ליבת, רשת הניהול , תקשורת, ציוד תקשורת ועמדות קצה.  
    ב. מסביבות סוד בהן פרוסה הרשת ויחידות הקצה, באמצעות מרכיבים משדרים  
    ברשת (רמקול, מיקרופון, מצלמה).  
    ג. חיבור בין רשתות ובדגש על רשת בסיווג נמוך יותר (אינטרנט, קליק-נט)  
    ד. חיבור ציוד לא מורשה לרשת BYOD,USB , מדפסת, מקרן וכו'.  
    ה. גישת משתמשים לא מורשים  
    ו. אובדן או גניבה של תחנת קצה
3. 2) פגיעה בזמינות ואמינות הרשת, הסביבה העננית, המידע והתהליכים בפרויקטים  
    השונים.
4. יעדי הסתרה:  
   1) יעדי ההסתרה של צה"ל בפרויקטים השונים – סד"כ, נתוני משרתים ומשטחי תקיפה   
    אודותם, פעילות מבצעית וסימנים מעידים, מודיעין, אמל"ח, תשתיות ופערים.  
   2) הצורך המבצעי- עצם קיום ופירוט על תהליכים המשרתים פעילות צה"ל רגישה   
    ומסווגת בתשתיות ענן ציבורי – סביבות, שירותים, לקוחות ופיתוחים ייעודיים,  
    שרשרת אספקה וכו'.  
   3) כושר ההפעלה והשליטה בתשתיות ובמערכות – גורמים מעורבים, תפיסת ההפעלה,   
    מרחבים. ספקיות, שירותים, ארכיטקטורה, מזהים טכנולוגיים ומשטחי תקיפה  
    (שמות סביבות, דומיינים, IP וכו'.), ממשקים לרשתות נוספים, פערים וכו'.  
   4) מרכיבי הבטחון וההגנה – עצם אחסון, עיבוד ושינוע מידע העולה על סיווג בלמ"ס,   
    מרחב ניהול הסיכונים, מרכיבי ההגנה, הניטור וההערכות לאירוע, תהליכי האישורים  
    בצה"ל ומרכיבי בדיקות חדירות טרם מבצעי פרויקט, פערים וספקי שירותי ביטחון  
    והגנה.  
   5) שרשרת האספקה – מידע אודות חברות אזרחיות, בדגש על גורמים שאינם מזוהים ישירות עם הספקיות של 'נימבוס' המשמשים כשרשרת אספקה בתהליכים השונים.  
   6) יישום NAC לשם הפרדה חזקה בין VLANים יוטמע בהמשך הפרויקט ועד אז  
    תיהיה הפרדת מתגים בין 'קליקנט' ל-'דביר'.  
   7) ניהול רכיבי הרשת (מתגים, נתבים, FW) – יתבצע מרשת ניהול בסטנדרט   
    המתאים לרשת בסיווג 'שמור מנהלתי', כולל התאמות ברשת הקיימת   
    המשתמשת לניהול רשת 'קליקנט' ככל שידרשו בהתאם למענה הגנה והביטחון  
    שיוגדר.  
   8) ללא שירותי SaaS ברשת , לרבות שירותי קולבורציה Office 365/.

# שגרת הגנה

1. **הזרמת לוגים בסביבה**
2. נראות הינה חלק בלתי נפרד מתפיסת ההגנה ואפשור שגרת הגנה על השירות ועל המידע המאוחסן בו.
3. יש להזרים את הלוגים האפליקטיבים של השירות ל-SIEM הארגוני ול-Datalake הארגוני.
4. הזרמת ואיסוף לוגים יתבצעו על ידי ממר"ם.
5. **ניטור המערכת**
6. על הניטור להיות Near Real Time אשר קרוב ככל הניתן ל-Real Time.
7. הניטור יתבצע על ידי SOC ייעודי של סביבות הענן הצה"ליות 24/7.
8. יש לנטר כל חריגה אל מול המנגנונים לזיהוי:
   1. כשלון בהזדהות Conditional Access (זהות + עמדה + רשת)
   2. חריגה מהרשאות וניסיון גישה לפרויקטים אחרים (ALB)
   3. גישה לכתובות שאינן מאושרות (Palo Alto NGFW)
   4. שינויי קונפיגורציה ברשת הניהול של סלקום
   5. שינויי ארכיטקטורה/קונפיגורציה בליבת הענן
   6. שינויים ברמת העמדה.
9. **מתאר איומים:**

במסגרת ניתוח הגנה ארכיטקטוני, נדרשת בחינה מקדימה של משטחי התקיפה וה איומים המרכזיים על שימוש בתשתית. להלן מתאר האיומים אשר יש לקחת בחשבון בתכנון ההגנה ובהגדרת יכולות הניטור:

1. **הדלפת מידע ואיסוף מודיעין -** הדלפת מידע של הארגון בדרכים הבאות:
   1. ניסיון ניצול חולשות בממשק האפליקטיבי שמפותח על ידי הגורם המבצעי לטובת חדירה לאזורים רגישים והבנת הארכיטקטורה.
2. **שיבוש תהליכים בענן וניהול מבצע-** שיבוש תהליכים מבצעיים של הארגון בדרכים הבאות:
   1. הבנת התהליך המבצעי והשפעה עליו, הסיכון גדל כתלות בפיצ׳רים שיפותחו בעתיד לטובת מנהל המערכת.
3. **זיוף מידע -** שיבוש מידע בדרכים הבאות:
   1. יצירת התראות שווא/השפעה על מי נמעני ההתראה.

המידע שבסעיף זה מהווה בסיס לבניית חוקים ותהליכי ניטור ייעודיים ע״י צוותי SOC וזו״ס, ואינו מחליף את אפיון חוקי הניטור עצמם.

1. **תהליך עדכון מענה ההגנה**

מענה ההגנה ייבדק אחת לחצי שנה או לאחר שינויים מהותיים בפלטפורמה בהתאם למענה שהוגדר. כל שינוי ייבחן ויאושר ע״י ארכיטקט הגנה.

**פערים להשלמה**

ניהול jwks

גישה לgcp