אל: ועדת המכרזים

משרד:	רשות המסים בישראל – אגף המכס והמע"מ
יחידה מזמינה:	טד"מ
תאריך:	30.7.2026

הנדון: <u>חוות דעת מקצועית במסגרת כוונה להתקשר עם ספק יחיד/ ספק חוץ</u>

הבקשה מסתמכת על תקנה ☒ 3(29) / ☐ 3(31) (סמן את התקנה המתאימה) לתקנות חובת מכרזים ועל הוראות תכ"ם, "פטור מחובת המכרז", מס' 7.8.1 והוראת תכ"ם, "בחינת קיומם של ספקים ומיזמים", מס' 7.8.2.

תיאור מהות ההתקשרות (רקע ופירוט התכונות של הטובין/השירות/העבודה)
הסדרת רכש, חידוש והרחבת רישיונות קיימים עבור קבוצת מוצרי חברת **Manage Engine**, המהווים נדבך קריטי ומרכזי במערך אבטחת המידע, ניהול תחנות הקצה (**UEM**) והעמידה ברגולציית מס"ל והנחיות הגנת הסייבר באגף המכס והמע"מ. ההתקשרות מתוכננת מול חברת "מאגרי תוכנה בע"מ", המשמשת כמפיצה הבלעדית של היצרן בישראל.

האם קיים בנושא זה מכרז מרכזי של החשב הכללי או גורם ממשלתי מוסמך אחר? ☐ כן ☒ לא

סוג ההתקשרות: (סמן **X** במקום המתאים)

☐ טובין ☒ שירותים ☐ ביצוע עבודה

שם הספק:	מאגרי תוכנה (מ.ת.) בע"מ	
מספר הספק (ח.פ/ח.צ/ע.מ/מספר עמותה)	513442442	
ספק זה הנו:	☒ספק יחיד	☐ספק חוץ
אומדן / שווי ההתקשרות:	300,000 ₪ לשנה כולל מע"מ (לכל התקופה כ- 900,000 ₪ כולל מע"מ)	
תקופת ההתקשרות:	שנה עם אופציה לשנתיים נוספות	

1. האמצעים שבהם נערכו בדיקות לאיתור ספקים נוספים והכנת חוות דעת

נערך מחקר שוק מקיף וסקירה טכנולוגית של פתרונות ניהול והגנת תחנות קצה (**UEM/Endpoint Security**) הפועלים במודל **On-Premises** מלא (תנאי סף הכרחי לפעילות ברשתות המאובטחות והסגורות של אגף המכס). בין היתר נבחנו פתרונות מבוססים כגון: **HCL BigFix, Microsoft MCM/SCCM, Ivanti EPM**, ו- **Trellix ePO**. הבחינה בוצעה באמצעות השוואת קטלוגים טכניים, ניתוח ארכיטקטורת רשת ומענה לדרישות הרגולטוריות הספציפיות של מערך הסייבר הלאומי.
בנוסף לנתונים הטכניים, בוצעו **POC** ל **MANAGE ENGINE**, **BIG FIX** ו**SCCM**

2. ממצאי הבדיקה

נערכה השוואה בין חמישה מוצרים כמפורט להלן:

תכונה / דרישה	Endpoint Central (On-Prem)	HCL BigFix	Microsoft MCM (SCCM)	Ivanti Endpoint Manager (EPM)	Trellix ePO (On-Prem)
(כן/לא) ON PREM	כן מלא. התקנה מקומית עצמאית לחלוטין.	כן מלא. מבוסס שרת מקומי וארכיטקטורת Relays.	כן מלא. פתרון On-Premises קלאסי המבוסס על תשתית ארגונית.	כן מלא. שרת ניהול מקומי (Core Server).	כן מלא. שרת ePO מקומי מנוהל עצמאית.
DLP (Data Loss Prevention)	כן. רכיב DLP ייעודי (כחלק מחבילת ה-Security) - חסימת דליפת מידע דרך דוא"ל, ענן, הדפסות וכו'.	חלקי מאוד. דורש אינטגרציות חיצוניות או פיתוח Fixlets מורכבים למניעת תהליכים.	לא מובנה. בעבר התבסס על Windows EDP, כיום מיקרוסופט מפנה ל- Purview בענן.	חלקי. כולל הגנות בסיסיות על קבצים אך לא DLP ארגוני מלא ועמוק.	כן. אחד מפתרונות ה-DLP החזקים והמובילים בשוק (DLP Trellix) המשולב ב-ePO.
APPLICATION CONTROL	כן. מאפשר יצירת רשימות לבנות/שחורות (Whitelisting/Blacklisting), ניהול הרשאות והסדרת יישומים מורשים.	כן. באמצעות מודול BigFix Relevance או חוקי Protection קשיחים לחסימת הרצת קבצים ביניהם.	כן. אינטגרציה מובנית עם Windows WDAC (Windows AppLocker או Defender Application Control).	כן. כולל מנגנון Application Control מובנה כחלק מחבילת ה-Endpoint Security.	כן. מנגנון Application Control עוצמתי (המבוסס על רכישת Solidcore) הכולל הגנה מפני שינויים (Whitelisting דינמי).
DISK ENCRYPTION	כן. ניהול מרכזי של BitLocker (Windows) ו-FileVault (Mac), כולל גיבוי מפתחות שחזור (Recovery Keys).	כן. מודול ניהול הצפנות מובנה לניהול מפתחות BitLocker ו-FileVault מרחוק.	כן. ניהול BitLocker מקיף ביותר דרך MBAM המובנה בתוך ה-Console.	כן. מודול ייעודי לניהול ואכיפת הצפנת דיסקים מקומית ומפתחות שחזור.	כן. ניהול מקיף של BitLocker/FileVault וכן מנגנון הצפנה עצמאי של Trellix (לשעבר McAfee Drive Encryption).
PATCH MANAGEMENT	כן. תמיכה אוטומטית מלאה ב-Windows, Mac, Linux ומעל 850 אפליקציות צד שלישי ללא תלות באינטרנט.	כן. הפצת טלאים מהירה במיוחד (Fixlets), תמיכה רחבה מאוד בשרתים, מערכות הפעלה רבות וצד שלישי.	כן. מעולה ל-Windows. תמיכה בצד שלישי אפשרית אך דורשת רישוי נוסף (כמו Patch My PC) או הגדרות מורכבות.	כן. מנוע Patch ותיק (Shavlik) התומך במגוון עצום של מערכות הפעלה ואפליקציות.	חלקי. תומך בעיקר בעדכוני רכיבי אבטחה ומוצרי Trellix. פחות מתאים ככלי להפצת טלאים כלל-ארגוני למערכות הפעלה.
VULNERABILITY SCAN	כן. סורק מובנה (Vulnerability Manager) המזהה חולשות אבטחה, הגדרות שגויות (Misconfigurations) ונכסים חשופים.	כן. מודול BigFix Insights for Vulnerability Remediation המסתנכרן עם סורקים כמו Tenable/Qualys ומבצע תיקון אוטומטי.	חלקי. מציג חוסרי עדכונים, אך לא סורק חולשות CVE מקיף בפני עצמו (מפנה ל-Defender for Endpoint).	כן. כולל סורק חולשות מובנה שמצליב מידע ומאפשר הפצת טלאים ישירה לחולשות שהתגלו.	כן. כולל סורק חולשות מובנה ומנגנוני הגנה אקטיביים המבוססים על מודיעין איומים בזמן אמת.
ניהול מדיניות (Policy Management)	כן. ניהול מבוסס קונפיגורציות (Configurations) המאפשר אכיפת הגדרות, חסימת פיצ'רים ב-OS, והחלת חוקים קבועים.	כן. ניהול באמצעות Baseline ו-Fixlets המבטיחים שהתחנה תישאר תמיד במצב המדיניות המוגדר (Desired State).	כן. מנגנון Compliance Settings ו-Baselines עמוק המאפשר הרצת סקריפטים ואכיפת הגדרות קשיחה.	כן. מערכת הגדרת Agent Policies קפדנית המאפשרת החלת פרופילים שונים לפי קבוצות או מיקומים.	כן. מערכת ניהול המדיניות (Policy Catalog) של ePO היא מהמפורטות והחזקות ביותר בתעשייה ברמת האבטחה.
התחברות מרחוק (Remote Control)	כן. שליטה מרחוק מתקדמת (HTML5) הכוללת הקלטת מפגשים, העברת קבצים, צ'אט וניהול פגישות ללא רישוי נוסף.	חלקי. כולל כלי בסיסי, אך לרוב נדרש מודול ייעודי או תוכנה חיצונית בארגונים גדולים.	כן. כלי Remote Control ותיק ומהיר המופעל ישירות בתוך הרשת המקומית.	כן. כולל את Ivanti Remote Control המאפשר שליטה מהירה, העברת קבצים וצ'אט.	לא. ePO הוא כלי ניהול ואבטחה, הוא אינו כולל רכיב השתלטות מרחוק ותמיכה במשתמשים.
ניהול מערכות לינוקס	כן. תמיכה בהתקנת סוכנים על מגוון הפצות Ubuntu, RedHat, CentOS, Debian, SUSE וכו') וניהול נכסים.	כן. תמיכה עמוקה ביותר בלינוקס (כולל שרתי Enterprise גדולים) וניהול קונפיגורציות.	כן. מיקרוסופט הסירה חלק ניכר מהתמיכה הישירה ב-Linux בגרסאות האחרונות של MCM.	כן. תמיכה בניהול ומלאי של הפצות לינוקס נפוצות בארגון.	כן. תמיכה מלאה בהתקנת סוכן (McAfee Agent) על לינוקס לצורכי אבטחה ומלאי.
הפצת עדכונים ללינוקס	כן. הפצה וניהול אוטומטי של טלאי אבטחה ועדכוני מערכת להפצות לינוקס הנתמכות.	כן. תמיכה ברמת ה-Kernel והאפליקציות בצורה המקצועית ביותר בשוק עבור שרתי לינוקס.	לא. לא נתמך/לא מומלץ. דורש מעקפים מורכבים ולא מיועד לכך בגרסאות המודרניות.	כן. תמיכה מובנית בהפצת עדכוני אבטחה וטלאים עבור RedHat, Ubuntu וכד'.	חלקי. עדכוני רכיבי אבטחה של Trellix בלבד, לא משמש כשרת עדכוני OS ללינוקס.
DEVICE CONTROL	כן. חסימה וניהול של התקני USB, מדיה ניידת, Wi-Fi, Bluetooth ומתן הרשאות זמניות לפי משתמש/מחשב.	כן. מודול ייעודי לבקרת התקנים וחסימת פורטים פיזיים.	כן. ניהול חוקי חסימת USB דרך הגדרות קונפיגורציה או אינטגרציה עם Defender.	כן. פתרון Device Control חזק מאוד (המבוסס על רכישת חברת Sanctuary/Lumension בעבר).	כן. רכיב Trellix Device Control נחשב למוצר Enterprise קלאסי וקשוח לחסימת התקנים.
שיוך חולשות (CVE) לתיקון (Patch) בלחיצה אחת	כן. תחת ממשק אחד רואים את החולשה שנסרקה ומבצעים ישירות 'Remediate' שמוריד את ה-Patch הנכון.	חלקי. דורש אינטגרציה מורכבת עם סורק חיצוני (Tenable/Qualys) וסנכרון ידני באמצעות מודול Insights.	לא. דורש הגדרה של Defender for Endpoint בענן וסנכרון מורכב, לא מציע תיקון מובנה ישיר לחולשות צד ג'.	חלקי. סורק חולשות עצמאי חביב, אך לא מציע קישור אוטומטי ומלא לקטלוג צד שלישי רחב כמו של ME.	לא. מסוגל לזהות חולשות אבטחה, אך אינו משמש ככלי הפצת עדכונים למערכות הפעלה ואפליקציות צד ג'.
ניהול דפדפנים מקיף (Browser Management) מובנה	כן. ניהול תוספים (Extensions), חסימת תוספים זדוניים, ניתוב תעבורה ארגונית מאובטחת, ואכיפת הגדרות אבטחה ב-Edge, Chrome.	לא. דורש כתיבת חוקי רג'יסטרי (Registry) מורכבים או סקריפטים לכל דפדפן בנפרד.	חלקי. מתבצע דרך הגדרות קונפיגורציה/GPO, אך אין קונסולה ייעודית גרפית לניהול תוספים וניטור סיכוני דפדפנים.	לא. אין רכיב ניהול דפדפנים ייעודי מובנה ברמת ה-Endpoint.	לא. מתמקד בהגנת סייבר רשתית ואנטי-וירוס, לא בניהול תצורת דפדפן ותוספים ברמת ה-IT והחלת חוקים.
מנגנון השבתת שירותים (Anti-Ransomware) בהתנהגות	כן. כולל מנגנון ייחודי המזהה הצפנת זדונית בזמן אמת, חוסם את התהליך ומגבה את הקבצים המקוריים מקומית.	לא. נשען על חוקי חסימה בסיסיים, אין מנגנון זיהוי והתאוששות ייעודי מ-Ransomware מובנה בסוכן.	חלקי. דורש הפעלת רכיבים של Microsoft Defender הארגוני, לא פיצ'ר ייעודי פנימי בתוך קונסולת ה-MCM.	חלקי. כולל הגנות אבטחה בסיסיות על קבצים אך לא מנגנון רולבק (Rollback) ייעודי והגנת קבצים קריטיים בהתנהגות.	כן. מנגנון חזק מאוד (Trellix ENS) הכולל הגנת אקטיבית והתנהגותית, אך דורש רישוי והתקנה מורכבים בנפרד.
אינטגרציה טבעית למערכת Helpdesk (מאותו יצרן)	כן. אינטגרציה 'מהקופסה' (Out of the box) למוצרים כמו ServiceDesk Plus. פתיחת קריאה, השתלטות והפצת Patch ישירות מתוך	לא. אין לחברה פתרון Helpdesk מוביל משלה, דורש פתוח API מול מערכות צד שלישי (כמו ServiceNow).	חלקי. אינטגרציה קיימת מול מערכת SCSM של מיקרוסופט (מוצר כבד וכמעט נטוש) או כלי ענן.	כן. אינטגרציה טובה מאוד למוצרי ה-Service Desk של Ivanti, אך אלו מערכות Enterprise מורכבות ויקרות משמעותית.	לא. חברת אבטחה טהורה ללא כלי IT וניהול קריאות שירות (ITSM).

3. נימוקים והערות נוספות - ממצאי הבדיקה וסיבות לאי-התאמת פתרונות מתחרים:

כיום מוטמעות ברשת המכס מספר מערכות של חברת **Manage Engine** המשלימות זו את זו. לא נמצא אף מוצר בשוק המסוגל להחליף את הפתרון הקיים או לספק פלטפורמה אחודה (**All-In-One**) העונה במקביל לכלל הדרישות הטכנולוגיות, הרגולטוריות והתפעוליות ברשת המקומית, מהנימוקים הבאים:
Endpoint Central (ניהול והגנת תחנות קצה):

א. הצדקה מקצועית: לאור ההשוואה שנערכה בין המוצרים הקיימים בשוק נמצא שמערכת **Endpoint Central** מספקת מענה מלא וייחודי תחת סוכן אחד לכלל הדרישות הרגולטוריות: הפצה אוטומטית של

תוכנות ועדכונים (כולל צד שלישי), הצפנת דיסקים קשיחים (**BitLocker/FileVault**), בקרת התקנים (**Device Control**), מניעת דליפת מידע (**DLP**) ושליטה מרחוק מבוססת **HTML5**.

ב. נחיתות מערכות מתחרות: מוצרים מתחרים כגון **Microsoft Intune** מחייבים חיבור ענן (בלתי אפשרי ברשת המקומית המאובטחת). מוצרים ותיקים כגון **Microsoft MCM (SCCM)** נטולי יכולות הגנת דפדפנים מובנות ויכולות **DLP** עצמאיות, ודורשים שילוב מוצרי צד-ג' מורכבים. **HCL BigFix** חסר רכיב **DLP** ואנטי-כופר מובנה,

ג. הגנה על השקעה קיימת: לפני כשנתיים נרכשו **1,000** רישיונות בסכום של **100,000** ש"ח המוטמעים כיום על המחשבים הניידים בארגון. עקב גידול מצבת כוח האדם, נדרשת הרחבה מיידית של **500** רישיונות נוספים לניידים. בנוסף, כחלק מתוכנית העבודה לעמידה ברגולציית מערך הסייבר הלאומי (הצפנה, מניעת דליפה, חסימת אפליקציות), הוחלט להרחיב את פריסת המערכת גם לרשת הפנימית של הארגון – תוספת של כ-**2,000** רישיונות. החלפת היצרן בשלב זה תגרור הפסד תקציבי מוחלט של ההשקעה הקודמת ומאות שעות עבודה של כתיבת ארכיטקטורה מחדש ודורש עקומת למידה חדה.

ד. ממשק ותמיכה: המערכת מצטיינת בממשק ניהול גרפי אחוד ונוח, המאפשר שליטה קלה גם לגורמי תמיכה שאינם בעלי הכשרה מתקדמת, דבר החוסך עלויות הדרכה מורכבות. כמו כן, קיימת תמיכה מלאה בעברית וניסיון מוצלח של צוות המשרד בעבודה עם הכלי.

ה. בלעדיות מסחרית: חברת "מאגרי תוכנה (מ.ת.) בע"מ" היא המפיצה הבלעדית המורשת מטעם היצרן העולמי בישראל. כל ספק אחר בשוק שיוגש למכרז ייאלץ לרכוש את הרישוי ממאגרי תוכנה על מנת למכור ללקוחות, ולכן קיום מכרז פומבי אינו תחרותי ויגרור "כפל תיווך" המעלה את מחיר הרישוי למדינה. מצ"ב אישור מטעם היצרן בדבר "מאגרי תוכנה (מ.ת.) בע"מ" שהינה המפיצה הבלעדית המורשת מטעם היצרן העולמי בישראל.

4. סיכום והמלצה

לאור רמת ההטמעה הנוכחית, העמידה הייחודית של קבוצת מוצרי **Manage Engine** בדרישות הרגולטוריות של מערך הסייבר הלאומי בסביבת **On-Prem**, ובלעדיות ההפצה של חברת מאגרי תוכנה בישראל – פנייה למכרז פומבי אינה אפשרית, אינה כלכלית ותפגע קשות ברציפות אבטחת המידע של הארגון.

חוות דעתי זו ניתנת מתוקף היותי הסמכות המקצועית לנושא זה.

בכבוד רב,

פאולו אנקייר	מומחה טכנולוגיות הגנת הסייבר	
שם בעל הסמכות המקצועית	**תפקיד בעל הסמכות המקצועית**	**חתימה**

ZOHO CORPORATION PTE. LTD.
105, Cecil Street, 10-04 The Octagon, Singapore 069534

MANUFACTURER AUTHORIZATION FORM

Effective Date: 04 Sep 2025

To,
Israel Tax Authority
Jerusalem, Givat Shaul, Knafei Nesharim 66.

Reseller Name: Software Sources Ltd
Reseller Address: 141 Ahuza Street, 3rd FloorP.O. Box 639
Ra'anana Israel

Subject: Authorization letter to resell and support ManageEngine ADAudit Plus, ManageEngine ADManager Plus, ManageEngine ADSelfService Plus, ManageEngine Endpoint Central, ManageEngine Log360

Dear Sir/Madam,

This is to confirm that Software Sources Ltd is an exclusive reseller in Israel authorized to resell and support ManageEngine ADAudit Plus, ManageEngine ADManager Plus, ManageEngine ADSelfService Plus, ManageEngine Endpoint Central, ManageEngine Log360 in Israel in accordance with the applicable End User License Agreement.

We further confirm that Zoho Corporation Private Limited, having it's registered office at Estancia IT Park, Plot No.140,151, Vallancheri Village, Chengalpet, Kancheepuram, Tamilnadu, India - 603202, is the manufacturer of ManageEngine suite of software applications and has authorized it's fully owned subsidiary Zoho Corporation Pte. Ltd., to provide this letter. This Manufacturer Authorization Form shall be valid for a period of one (1) year from the Effective Date mentioned above.

For ZOHO CORPORATION PTE. LTD.,

Signature:

Name:Gibu Kurian Mathew

Title:VP & GM APAC