## השוואת תכונות מלאה: Velociraptor לעומת Trellix Endpoint Security HX (לסביבה מקומית)

### 🔧 פריסה והתקנה

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| תמיכה בסביבה מקומית | ✅ נתמך באופן מלא | ✅ נתמך באופן מלא | שני הכלים יכולים לפעול בסביבה מקומית לחלוטין ללא צורך בענן. |
| מתאים לרשת מנותקת (Air-Gap) | ✅ כן, לא דורש אינטרנט | ✅ כן, אך דורש עדכונים ידניים | Velociraptor מאפשר הפעלה מלאה ללא אינטרנט, בעוד Trellix דורש טעינה ידנית של חתימות ועדכונים. |
| סוכן נדרש | ✅ סוכן קל משקל | ✅ סוכן HX | שני הכלים דורשים התקנת סוכן אך הסוכן של Velociraptor קל בהרבה. |
| משאבי מערכת | 🟢 מאוד קל | 🔴 צורך גבוה במשאבים | Velociraptor משתמש בפחות זיכרון ומשאבים ולכן מתאים גם לעמדות חלשות. Trellix מכיל מנוע EDR שלם ולכן כבד יותר. |
| מורכבות התקנת השרת | ⚠️ בינונית | ⚠️ בינונית-גבוהה | Trellix כולל ממשק ePO, שרתים ומסדי נתונים בעוד Velociraptor פשוט יותר אך דורש קונפיגורציה ידנית. |
| תמיכה במערכות הפעלה | Windows, Linux, macOS | בעיקר Windows, תמיכה חלקית ב-Linux | Velociraptor תומך במערכות הפעלה רבות. Trellix ממוקד בעיקר ב-Windows ולכן פחות מתאים לסביבות מעורבות. |
| עדכונים אוטומטיים | ❌ לא, רק ידני | ✅ כן (עם ePO או קבצים ידניים) | Velociraptor דורש סקריפטים או הפעלה ידנית לעדכון, בעוד Trellix משתלב במערכות עדכון של Trellix. |
| תמיכה בריבוי לקוחות | ⚠️ בעייתי | ✅ נתמך מובנה | Trellix מאפשר הפרדה בין לקוחות (multi-tenancy) כחלק מהמערכת. ב-Velociraptor נדרש פתרון מותאם. |
| אינטגרציה עם Active Directory | ⚠️ ידנית | ✅ מלאה דרך ePO/HX Server | Trellix כולל אינטגרציה מלאה עם AD לניהול תחנות. Velociraptor דורש חיבור ידני או סקריפטים. |
| ניהול הרשאות משתמשים | ✅ כן | ✅ כן | לשני הכלים יש תמיכה ב-RBAC. ב-Trellix הניהול פשוט יותר דרך הממשק. |
| הגנה עצמית של הסוכן | ❌ לא | ✅ כן | הסוכן של Velociraptor ניתן להריגה על ידי משתמשים, לעומת סוכן Trellix שמוגן ברמת מערכת ההפעלה. |

### 🔍 גילוי וציד איומים

| תכונה | Velociraptor | Trellix Endpoint Security HX | הסבר |
| --- | --- | --- | --- |
| מנוע ציד איומים | ✅ שפת VQL מותאמת | ✅ שפת שאילתות HX | שני הכלים מציעים שפות חקירה מתקדמות. VQL גמיש ומיועד לאנשי DFIR. |
| זיהוי IOC בזמן אמת | ✅ ידני (IOC/YARA) | ✅ כן, כולל חוקים פנימיים | Trellix סורק את המערכת כל הזמן לפי חתימות. Velociraptor מבצע זאת רק לפי דרישה. |
| זיהוי התנהגותי | ❌ אין, רק ידני | ✅ כן (EDR מובנה) | Trellix כולל מנוע לזיהוי פעילות חשודה (כגון ביצוע מ-PowerShell), Velociraptor מבוסס חקירה ידנית בלבד. |
| זיהוי תקיפות ללא קבצים | ⚠️ אפשרי עם סקריפטים | ✅ כן | Velociraptor תומך רק אם כתבת חוקים ייעודיים. Trellix מזהה תבניות של fileless כמו PowerShell. |
| מיפוי למטריצת MITRE | ⚠️ דורש הגדרה ידנית | ✅ כן | ב-Trellix יש חיבור מובנה למיפוי ATT&CK. ב-Velociraptor יש צורך לבנות חיבורים מותאמים. |
| אינטגרציה עם מודיעין איומים | ❌ לא | ✅ כן, דורש עדכון ידני | Trellix תומך בטעינת feeds (מקומיים או מהענן). Velociraptor לא כולל זאת אך ניתן לבנות בתצורה מותאמת. |
| תמיכה ב-YARA | ✅ כן | ⚠️ חלקית | Velociraptor מאפשר חיפוש לפי YARA באופן מלא. Trellix מגביל בשימוש בחוקים. |
| תמיכה ב-IOC מותאם | ✅ כן (קבצים, דומיינים וכו’) | ✅ כן (רשימות או חוקים) | שני הכלים תומכים ב-IOC ידניים, אך ב-Trellix השילוב קל יותר דרך UI. |
| בניית ציר זמן | ✅ כן (אירועים, לוגים, prefetch וכו’) | ⚠️ חלקי | Velociraptor מציג ציר זמן של כל artefact שנאסף. ב-Trellix הנתונים אינם מרוכזים כך. |
| ניתוח לוגים | ✅ כן | ⚠️ מוגבל | Velociraptor מאפשר שאילתות בלוגים חיים (כגון Security.evtx). Trellix אינו ממוקד בכך. |

### 🧪 תגובה וחקירה

(כבר מופיעים הסברים טכניים במקטע זה — אין צורך לשנות.)