



סקירה

PROTECT

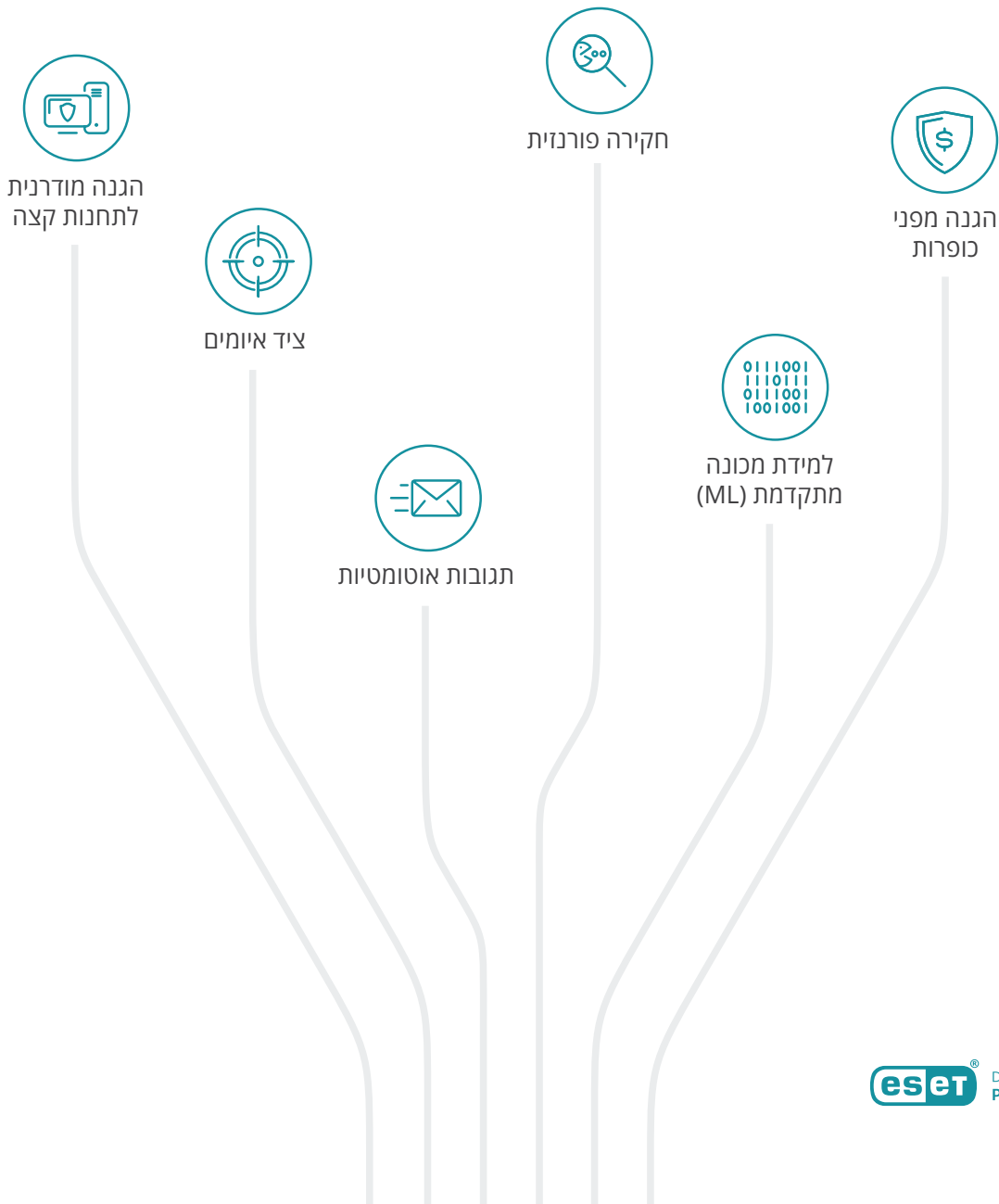
ממשק ניהול מרכזי המאפשר שקיפות
מקסימלית לרשת הארגונית

Progress. Protected.

מה זה ממשק ניהול לאבטחת תחנות הקצה?

ESET PROTECT הוא ממשק (Unified Endpoint Management) UEM - ניהול מאוחד של תחנות קצה) גמיש שמאפשר גישה לפלטפורמת ESET PROTECT העוצמתית. ניתן להטמיע אותו באופן מקומי או בענן, והוא מאפשר שקיפות בזמן אמת לתחנות הקצה המקומיות והמרוחקות, יחד עם ניהול אבטחה וקבלת דיווחים באופן מלא עבור כל מערכות ההפעלה.

זהו ממשק מרכזי המנהל את כל פתרונות האבטחה של ESET שהוטמעו ברשת. הוא שולט על שכבות המניעה, הזיהוי והתגובה בכל הפלטפורמות - תחנות קצה, שרתים, מכונות וירטואליות ואפילו מכשירים ניידים מנוהלים.



היתרונות של ESET

ממניעה לתגובה

ESET PROTECT מאפשר לנהל כמה פתרונות אבטחה של ESET מתוך ממשק ניהול מרכזי. החל ממניעת איומים ועד לזיהוי ותגובה, הפתרון מכסה את הארגון כולו באופן רב-שכבתי במטרה לספק את רמת האבטחה הגבוהה ביותר.

טיפול באירועי אבטחה בלחיצת כפתור

מנהל IT יכול להעריך במהירות את המצב הנוכחי ולהגיב לבעיות שונות מתוך מסך הניהול הראשי. ניתן לבצע פעולות כמו יצירת כלל החרגה, שליחת קבצים לניתוח מתקדם או ביצוע סריקה נגד נזקות בלחיצת כפתור. ניתן ליצור כללי החרגה הפועלים לפי שם האיום, URL, גיבוב (hash) או שילוב בין כל אחד מהם.

מערכת אימות והרשאות מתקדמת

ממשק הניהול מצויד במערכת RBAC (ניהול גישה מבוסס-תפקיד), המתחיל בהגנת הגישה אליה באמצעות מנגנון אימות רב-שלבי. ניתן לקבוע מי מהמנהלים והמשתמשים בממשק הניהול יוכל לגשת למערכות או קבוצות שונות, וכן ניתן להגדיר מערכי הרשאות באופן פרטני יותר מאי פעם לדוגמה צפיה בלבד, גישה מלאה או חלקית ברמת פירוט גבוה.

מוכנות ל-MSP

אם אתם ספק שירות מנוהל (MSP) המטפל ברשתות של הלקוחות שלכם, ודאי תעריכו את התמיכה המלאה של ESET PROTECT עם כל הלקוחות בממשק ניהול מאוחד רישיונות MSP מזוהים באופן אוטומטי ומסונכרנים עם שרת הרישוי, וממשק הניהול מאפשר לכם לבצע פעולות מתקדמות כמו התקנת או הסרת תוכנות צד שלישי, הרצת סקריפטים, הפעלת פקודות מרחוק, הפקת רשימה של התהליכים הפועלים, הגדרת חומרה ועוד.

מוכח ואמין

חברת ESET נמצאת בתעשיית האבטחה במשך יותר מ-30 שנים ואנו ממשיכים לפתח את הטכנולוגיה שלנו כדי שנוכל להיות ביתרון מול האיומים החדשים ביותר. מסיבה זו, ישנם יותר מ-110 מיליון משתמשים ברחבי העולם שסומכים על שירותינו. הטכנולוגיה שלנו עוברת ביקורות ואימותים באופן קבוע ע"י גורמי צד-שלישי שמוכיחים עד כמה הגישה שלנו עוזרת בעצירת האיומים החדשים ביותר.

דיווח דינמי ומותאם אישית

ESET PROTECT מספקת יותר מ-170 דו"חות המובנים במערכת, ומאפשרת לכם להפיק דו"חות מותאמים אישית המכילים מידע מיותר מ-1,000 מקורות שונים. זה מאפשר לארגונים להפיק דו"חות שייראו ויגישו לפי רצונם. לאחר הפקת הדו"חות, ניתן להגדיר שליחה אוטומטית שלהם בפרקי זמן קבועים.

אוטומציה לעבודה נוחה ויעילה

קבוצות דינמיות מסוגלות למיין מחשבים על פי המצב הנוכחי שלו או על פי קריטריון מוגדר אחר. לאחר המיין ניתן להגדיר משימות אוטומטיות שיפעילו פעולות כמו סריקה, שינוי מדיניות והתקנה או הסרה של תוכנות כאשר מחשב מסוים עובר מקבוצה דינמית אחת לאחרת.

תמיכה ב-VDI הכוללת אוטומציה מלאה

מנגנון מתקדם לאיתור חומרה, מסייע לקבוע את זהות המכשיר על פי רכיבי החומרה שבו. כך ניתן לפרוס מחדש Image או להעתיק Image של סביבות חומרה לא-קבועות. התמיכה של ESET ב-VDI אינה דורשת מגע יד אדם והיא אוטומטית לחלוטין.

מערכת התראות בעלת אפשרות להתאמה אישית

מערכת ההתראות כוללת עורך בשיטת "מה שרואים הוא מה שמקבלים" (WYSIWYG), בו תוכלו להגדיר באופן מלא מהם האירועים שעבורם אתם רוצים לקבל התראות ואיזה מידע הן יכללו.

מאפיינים טכניים

דשבורד עם תצוגה מרכזית

ניתן לנהל את כל מוצרי האבטחה לתחנות קצה של ESET באמצעות ממשק הניהול של ESET PROTECT - תחנות עבודה, מכשירים ניידים, שרתים ומכונות וירטואליות המשתמשים במערכות ההפעלה הבאות: Windows, macOS, Linux ו-Android.

תמיכה ב-XDR

כדי לשפר עוד יותר את המודעות למצב ולספק שקיפות לרשת כולה, ESET PROTECT עובד עם ESET Inspect, הרכיב של פלטפורמת ESET PROTECT שמאפשר ESET Inspect XDR. תומך בפלטפורמות מרובות (Windows, macOS ו-Linux), מאפשר ציד של איומים (threat hunting) והחזרה לשגרה לאחר פגיעה, ויכול להתחבר באופן חלק עם מרכז הגנת הסייבר (SOC) שלכם.

הצפנה של כוננים בשלמותם

ESET Full Disk Encryption הוא חלק בלתי נפרד מ-ESET PROTECT, המנהל את ההצפנה של תחנות קצה המשתמשות במערכת ההפעלה Windows ו-macOS (באמצעות FileVault), משפר את ביטחון המידע ומסייע לארגונים לפתור בעיות הנוגעות לציוד לתקנות אבטחת המידע.

הגנה מתקדמת מפני איומים

התמיכה בהגנה מתקדמת מפני איומים משפרת במידה רבה את הזיהוי של איומי Zero-day כמו כופרות, באמצעות ניתוח זריז של קבצים חשודים ב-sandbox בענן של ESET. בנוסף, הוא מפעיל מספר גדול של בדיקות נוזקה מקיפות, שביניהן הרצה של הקובץ החשוד בסביבת ענן.

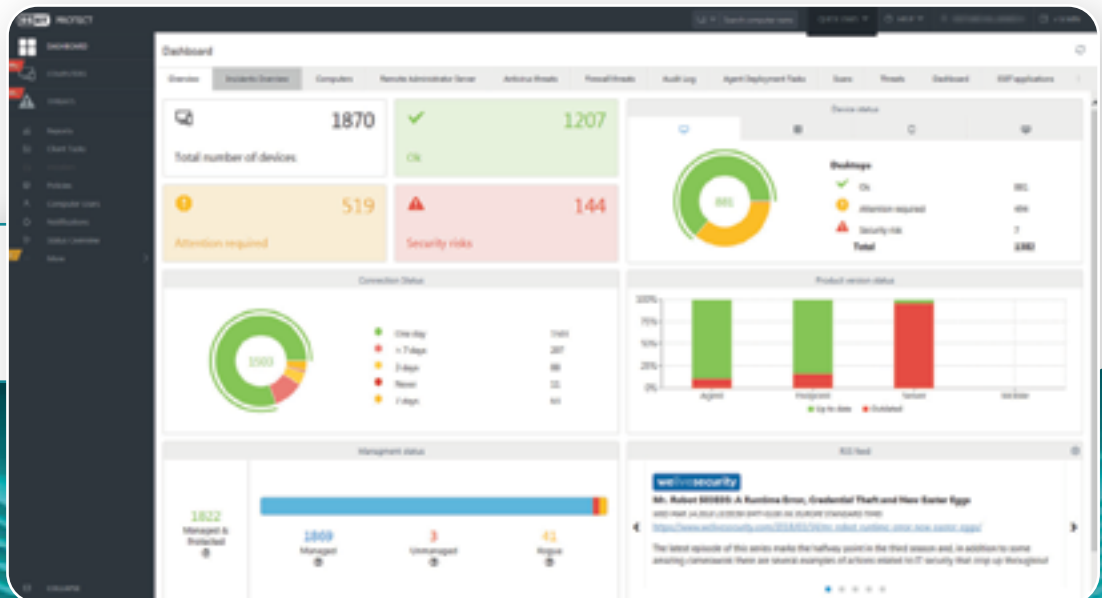
מצאי חומרה/תוכנה

ESET PROTECT לא מדווח רק על התוכנות המותקנות בכל אחד ממחשבי הארגון, אלא גם על רכיבי החומרה המותקנים בו.

תמיכה מלאה בניהול מאוחד

ניתן ליצור כמה קבוצות משתמשים וקבוצות הרשאות על מנת לספק גישה מוגבלת לממשק הניהול של ESET PROTECT. זה מאפשר להאציל סמכויות באופן מלא ופשוט בצוותי אבטחה גדולים. מאפיין זה מאפשר לכם לבצע מגוון רחב יותר של פעולות מאותו המיקום באמצעות יצירת קבוצות המחלקות מחשבים באופן דינמי על פי היצרן, הדגם, מערכת ההפעלה, המעבד, כמות זיכרון ה-RAM, כמות השטח הפנוי בכונן הקשיח ומאפיינים רבים אחרים.

המסך הראשי של
ESET PROTECT



ESET Vulnerability & Patch Management

ניטור של פרצות אבטחה במערכות הפעלה ובאפליקציות נפוצות באופן פעיל, והוספת האפשרות להתקנת תיקון (טלאי) אבטחה באופן אוטומטי בכל תחנות הקצה המנוהלות על ידי ESET PROTECT.

שליטה פרטנית במדיניות

ארגונים יכולים להגדיר מדיניות שונה עבור אותו מחשב או קבוצה, ויכולים ליצור תתי-מדיניות שיוכלו לרשת הרשאות ממדיניות-אב. בנוסף, ארגונים יכולים להגדיר את הגדרות המדיניות כהגדרות שמשתמש הקצה יוכל לשנות בעצמו, וכך תוכלו לקבוע למשתמשים אילו הגדרות הם יוכלו לשנות ואילו לא.

תמיכה ב-SIEM ו-SOC

ESET PROTECT תומך באופן מלא בכלי SIEM ויכול לייצא את כל הלוגים בפורמטי JSON או LEEF או CEF המקובלים בתעשייה, מה שמאפשר אינטגרציה עם מרכז פעולות האבטחה (SOC).

מקרים לדוגמה

הפצות VDI

הבעיה

ברוב המקרים, סביבות חומרה לא-עקביות דורשות טיפול אנושי של מחלקת ה-IT, מה שהופך את הדיווח והשקיפות מולן לסיטואציה של ממש.

הפתרון

✓ לאחר הפצת קובץ מאסטר (master image) למחשבים שכבר מוגנים על ידי ESET PROTECT, המחשבים ימשיכו לדווח למופע הקודם, על אף שהופצה תמונה חדשה לגמרי לאותה מערכת.

✓ המכונות שחוזרות למצב ההתחלתי שלהן בסוף המשמרת, לא יגרמו לכפילות מיותרת של מכונות אלא יותאמו לתיעוד אחד.

✓ בעת הפצה לא-עקביות של Image, תוכלו ליצור Image הכולל את הסוכן של ESET, כך שבכל פעם שבה נוצרת מכונה חדשה עם טביעת אצבע חומרית שונה, היא היא תופיע בממשק ניהול ESET PROTECT ותתקשר מולו באופן אוטומטי.

טיפול בתוכנות

הבעיה

ארגונים צריכים לדעת אילו תוכנות לא-מורשות הותקנו ולטפל בהן לאחר שהותקנו.

הפתרון

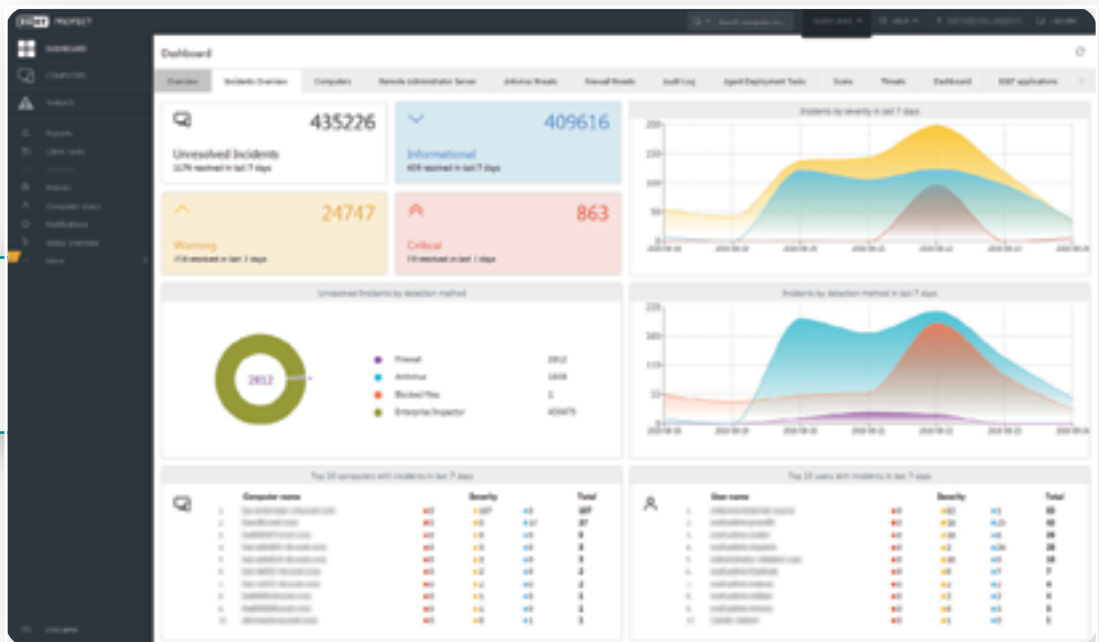
✓ הגדירו קבוצה דינמית בתוך ESET PROTECT שתחפש תוכנות לא-רצויות ספציפיות.

✓ צרו התראה שתודיע למחלקת ה-IT כשמחשב מסוים עונה לאותו הקריטריון.

✓ הגדירו מטלת הסרת תוכנה בממשק הניהול של ESET PROTECT שתופעל אוטומטית כאשר מחשב מסוים עונה לקריטריון של הקבוצה הדינמית.

✓ הגדירו התראה למשתמש שתופיע באופן אוטומטי על המסך שלו ותודיע לו שהוא עבר על תקנות התקנת התוכנה בכך שהתקין את התוכנה הנ"ל.

ממשק הניהול של ESET PROTECT - תצוגת תקריות



כופרות

הבעיה

משתמש פותח הודעת דוא"ל זדונית המכילה כופרה מסוג חדש.

הפתרון

✓ מחלקת ה-IT מקבלת התראה באמצעות הדוא"ל וה-SIEM על זיהוי איום חדש במחשב כלשהו.

✓ סריקה של המחשב הנגוע מתחילה להתבצע בלחיצת כפתור.

✓ הקובץ מועבר לבדיקה ב-ESET LiveGuard Advanced לאחר לחיצת כפתור נוספת.

✓ לאחר שהאיום הוכל, ההתראות ב-ESET PROTECT נעלמות באופן אוטומטי.

מפתחי קוד

הבעיה

מפתחים היוצרים קודי תוכנה במחשבי העבודה נוטים ליצור זיהויים שגויים באמצעות תוכנות ההידור.

הפתרון

✓ מחלקת ה-IT מקבלת התראה באמצעות הדוא"ל וה-SIEM על זיהוי איום חדש במחשב כלשהו.

✓ ההתראה מראה שהאיום הגיע ממחשב של מפתח.

✓ בלחיצת כפתור, הקובץ נשלח ל-ESET LiveGuard Advanced כדי לוודא שהקובץ אינו זדוני.

✓ מחלקת ה-IT יכולה ליצור כלל החרגה בלחיצת כפתור שיחריג את הקבצים בתיקיה הזו מאנליזה בענן.

מצאי חומרה ותוכנה

הבעיה

ארגונים צריכים לדעת אילו תוכנות מותקנות בכל אחד מהמחשבים ואת גילם של כל אחד מהמחשבים.

הפתרון

✓ צפו בכל תוכנה שהותקנה על המחשב, כולל הגרסה המותקנת, בתיעוד המחשב.

✓ צפו בנתוני החומרה של כל אחד מהמחשבים, כולל סוג המכשיר, יצרן, דגם, מספר סידורי, מעבד, זיכרון RAM, מקום פנוי בכונן הקשיח ועוד.

✓ הפיקו דוחות שיספקו תצוגה הוליסטית יותר של הארגון ויסייעו לקבל החלטות תקציביות על שדרוגי חומרה בשנים הבאות על פי דגמי המכשירים הנמצאים כרגע במצאי.

התחילו בתקופת ניסיון של 30 ימים עכשיו

נצלו את תקופת הניסיון החינמית בת 30 הימים כדי לבחון את הפתרון המלא, הכולל הגנה על תחנות קצה.

כיצד לרכוש:

תוכלו לרכוש כל אחד מהפתרונות העסקיים שלנו באופן פשוט [מאתר האינטרנט שלנו](#).

אודות ESET

כשאלה משולבים עם חקר ומודיעין האימונים הטובים בעולם, מוצרי ESET מציעים את האיזון המושלם בין יכולות מניעה, זיהוי ותגובה. קלות השימוש והמהירות חסרת התחרות מוכיחות שיש לנו מטרה אחת – להגן על ההתקדמות של לקוחותינו באמצעות מתן ההגנה הטובה ביותר האפשרית. www.eset.com/il

ESET בעלת ניסיון של יותר מ-30 שנים של חדשנות טכנולוגית ומספקת את פתרונות הגנת הסייבר המתקדמים ביותר בשוק. ההגנה המודרנית שלנו לתחנות הקצה מתבססת על טכנולוגיות האבטחה הרב-שכבתיות של ESET LiveSense, יחד עם שימוש מתמשך ב-Machine Learning ובמחשוב ענן.

ESET במספרים

1 מיליארד
משתמשים
ברחבי העולם

400k+
לקוחות
עסקיים

195
נציגויות
בעולם

13
מרכזי מו"פ
עולמיים

בין לקוחותינו



מוגנת ע"י ESET
מאז 2017,
מעל 9,000 תחנות קצה



מוגנת ע"י ESET
מאז 2016,
מעל 4,000 תיבות דוא"ל



מוגנת ע"י ESET
מאז 2016,
מעל 32,000 תחנות קצה



ספק שירותי אינטרנט,
שותף מאז 2008, למעלה
מ-2 מיליון לקוחות

מחויבים לרמת האבטחה הגבוהה ביותר



ESET זכתה בחותמת איכות במבדק שבדק פתרונות עסקיים בדצמבר 2022 על פתרון ההגנה שלה לארגונים.



ESET באופן עקבי מדורגת במיקומים גבוהים בביקורות של פלטפורמת G2 הבינלאומית והפתרונות של ESET מוערכים על ידי משתמשים מכל העולם



ESET זכתה להכרה כ"Top Player" בשנה הרביעית ברציפות בדו"ח לשנת 2023

קומסקיור בע"מ - הנציגה הבלעדית של ESET בישראל

1 מיליון משתמשים בישראל



מערך מומחים טכני בעברית
המספק שירות ללקוחות פרטיים
ועסקיים

