



PROTECT

ממשק ניהול מרכזי מבוסס ענן
מאפשר לכם לצפות, לנהל ולקבל החלטות בזמן אמת על
מערך האבטחה עבור כל מערכות ההפעלה

CYBERSECURITY
EXPERTS ON YOUR SIDE

מה זה ממשק ניהול בענן לאבטחת תחנות הקצה?

למה יש צורך בממשק ניהול לאבטחת תחנות קצה?

שקיפות ונראות

מתקפות Zero Day, מתקפות Advanced APT (persistent threat), מתקפות ממוקדות ובוטנטים מעוררים דאגה בכל התעשיות ברחבי העולם. שקיפות מול האיומים האלה בזמן-אמת היא חשובה מאוד, שכן היא מאפשרת לצוות ה-IT להגיב במהירות ולנטרל כל סיכון שעשוי להתפתח. מכיוון שבזמן האחרון חברות נדרשות לאפשר לעובדים לעבוד מרחוק, יש צורך בשקיפות גם מול מכשירים שאינם נמצאים פיזית במקום העבודה.

ESET PROTECT מספק מידע עדכני שנועד לדווח לצוות ה-IT על המצב של כל תחנות הקצה - בין אם הן נמצאות במקום העבודה עצמו ובין אם הן נמצאות מחוצה לו. הוא גם מספק שקיפות לכל מערכות ההפעלה בהן החברה עשויה להשתמש, ולא רק לחלק מהן. ברוב המקרים, ישנה רמת נראות משופרת המאפשרת לראות מידע ברמת המכשיר, כמו סוגי החומרה והתוכנה הנמצאים בו, במטרה לוודא כי צוותי ה-IT מודעים למצב הרשת באופן מלא.

ניהול וביצוע פעולות בזמן אמת

מרחב אבטחת הסייבר של ימינו מתפתח באופן קבוע, ולעיתים קרובות ניתן לראות שיטות התקפה חדשות או איומים חדשים שעדיין לא נראו בעבר. לאחר התרחשות מתקפה או הדלפת מידע, רוב הארגונים מופתעים מכך שמערך האבטחה שלהם כשל או שהם כלל אינם מודעים לכך שהמתקפה קרתה. לאחר גילוי מתקפה, סביר להניח שהארגון ירצה לבצע כמה פעולות על כל אחד מהמכשירים המחוברים אליו, כמו סריקה לאיתור נזקקות. מתקפה כזו עשויה לגרום לארגונים לשנות לגמרי את מדיניות ההגדרות שלהם כדי להתגונן בצורה טובה יותר מפני מתקפה עתידית.

ESET PROTECT מגיע עם כמה מערכי הגדרות מדיניות חזקים וחכמים שהוגדרו מראש, אך מאפשר לארגונים להתאים את המדיניות וההגדרות של מוצרי האבטחה לתחנות הקצה בכל רגע נתון. בנוסף, ניתן להגדיר אוטומציה של המשימות, וכך לחסוך למנהלי ה-IT את הזמן היקר הנדרש לביצוען על כל אחד מהמחשבים בנפרד.

דוחות מותאמים אישית

לחלק מהארגונים ישנן דרישות פנימיות הנוגעות לדיווח, בנוסף לדרישות הנובעות מחובת הציות לתקנות הגנת המידע. בכל ארגון שהוא יהיו דוחות אותם יש להפיק במרווחי זמן קבועים ולהעביר לנזפים רלוונטיים אחרים או לאחסן אותם למועד מאוחר יותר.

ESET PROTECT מאפשר יצירת דוחות במרווחי זמן קבועים ולשמור אותם בתיקייה ספציפית או לשלוח אותם ישירות למי שמבקש אותם. ישנן עשרות תבניות מוכנות מראש לדוחות, וניתן להשתמש בהן כמו שהן או להתאים אותן אישית כך שישפיקו את הנתונים הנדרשים לגוף שמבקש אותם. התהליך הזה חוסך זמן רב למנהלי ה-IT בעבודה התובענית הקשורה לאותו דיווח מתמשך.

“היתרון העיקרי של ESET הוא שכל המשתמשים מרוכזים לתוך ממשק ניהול מרכזי אחד, וכך ניתן לנהל אותם ולסקור את מצב האבטחה שלהם בקלות.”

יוס סאוולקול, מנהל צוות טכנולוגיית מידע ותקשורת (ICT), בית החולים Zuyderland, הולנד, מעל 10,000 תחנות קצה

אתם עדיין לא משתמשים בממשק ניהול בענן? נעזור לכם להחליט.

התחברות מכל מקום, בכל זמן

כל מה שאתם זקוקים לו הוא דפדפן האינטרנט המועדף עליכם. אמנם מרבית ממשקי הניהול שמאוחסנים על שרתי החברה כבר מציעים אפשרות כזאת, אך הודות לממשק הניהול בענן, אין צורך להגדיר כללי החרגה בחומת האש או להגדיר VPN מסובך כדי לנגש אליו. תוכלו לסמוך על תשתית הענן החזקה שלנו שתספק לכם זמן פעולה תקינה (uptime) גבוה ככל האפשר.

פתרון בעיות במהירות

מומחי ESET יוכלו לספק תמיכה או פתרון בעיות אפקטיביים ביותר באמצעות ממשק הענן - זאת מכיוון שלא יהיה צורך לבזבז זמן על בדיקת גרסת התוכנה בה אתם משתמשים, מכיוון שתמיד תהיו בגרסה החדשה ביותר.

חיסכון בעלויות התחזוקה הכוללת

ההחלטה לעבור מממשק ניהול אבטחה הנמצא על שרתי החברה לממשק ניהול בענן עשויה להיראות בהתחלה כמו הוצאה גדולה. אך כדאי שתחשבו שוב - לא תצטרכו לדאוג שוב לתחזוקת השרת ולבזבז זמן על שדרוגים קבועים, התקנת עדכוני מערכת או הפעלות מחדש. באותו אופן, תוכלו לשכוח גם מרישוי לשרת וביצוע גיבויים, מה שהופך את השימוש בממשק ניהול בענן לעסקה משתלמת בתוך זמן קצר.

התקנה בתוך דקות

באמצעות ממשק ניהול בענן, משך הזמן הנדרש להגנה מלאה על הארגון מתקצר באופן משמעותי. אין צורך לבזבז זמן ומשאבים על המתנה להתקנת רכיבים או אפילו על קביעת תזמון ההתקנות בשרת. פשוט פתחו חשבון ב-ESET והוסיפו את כל תחנות הקצה עליהם אתם רוצים להגן - זה עד כדי כך פשוט.

תמיד בגרסה העדכנית ביותר

תנו לנו לדאוג לעדכון ממשק הניהול. אנחנו נעשה את זה ברקע, וכך אתם תמיד תחזיקו בגרסה העדכנית ביותר עם הרכיבים העדכניים ביותר. כך הארגון שלכם יוכל להנות מאפשרויות האבטחה העדכניות ביותר, ומנהלי הרשת יוכלו להנות משיפורים בחוויית המשתמש. עליהם אתם רוצים להגן - זה עד כדי כך פשוט.

למה ESET PROTECT?

ממניעה לתגובה

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

טיפול באירועים בלחיצת כפתור

מנהל הרשת 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 האיוס, URL, מחרוזת HASH או שילוב בין כל אחד מהם הנמצאים בו, במטרה לוודא כי צוותי ה-IT מודעים למצב הרשת באופן מלא.

מערכת התראות בהתאמה אישית

מערכת ההתראות כוללת עורך בשיטת "What you see is what you get", בו תוכלו להגדיר באופן מלא מהם האירועים שעבורם אתם רוצים לקבל התראות ואיזה מידע הן יכללו.

דיווח דינמי ומותאם אישית

PROTECT מספקת יותר מ-170 דוחות המובנים במערכת, ומאפשר להפיק דוחות מותאמים אישית המכילים מידע מיותר מ-1000 מקורות שונים. זה מאפשר לארגונים להפיק דוחות מותאמים לפי רצונם. לאחר הפקת הדוחות, ניתן להגדיר שליחה אוטומטית שלהם בפרקי זמן קבועים.

יכולות אוטומציה

קבוצות דינמיות מסוגלות למיין מחשבים על פי המצב הנוכחי שלם או על פי קריטריון מוגדר אחר. לאחר המיון ניתן להגדיר משימות 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 התערבות אנושית והיא אוטומטית לחלוטין.

מוכח ומובטח

חברת ESET נמצאת בתעשיית אבטחת המידע 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 ומבחנים באופן קבוע ע"י גורמי צד-שלישי שמוכיחים עד כמה הגישה שלנו עוזרת בעצירת האיומים החדשים ביותר.

מוכנות ל-MSP

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

“חברה יוצאת דופן, תמיכה טכנית מעולה, המספקת הגנה חזקה מפני

איומים ויכולת ניהול מרכזי.”

די"ב, מנהל IT, Deer Valley Unified School District, ארה"ב, מעל 15,500 תחנות קצה

מקרים לשימוש

מתקפות כופר

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

פתרון

✓ 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 Dynamic Threat Defense לאחר לחיצת כפתור נוספת.

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

מפתחי קוד

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

פתרון

✓ 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 Dynamic Threat Defense כדי לוודא שהקובץ אינו זדוני.

✓ מחלקת ה-IT יכולה ליצור כלל החרגה בלחיצת כפתור שימנע הצגת זיהויים שגויים נוספים על קבצים בתיקה הזו.

טיפול בתוכנות

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

פתרון

✓ 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.

הפצות VDI

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

פתרון

✓ לאחר הפצת Master Image למחשבים שכבר מוגנים ע"י ESET PROTECT, המחשבים ימשיכו לדווח לרשומה המקורית, על אף Image חדש שהופץ לאותה מערכת.

✓ המכונות שחוזרות למצב ההתחלתי שלהן בסוף המשמרת לא יגרמו לכפילות מיותרת של מכונות אלא יותאמו לרשומה אחת.

✓ בעת הפצה של Image לא-עקביות, תוכלו ליצור Image הכוללת את הסוכן, כך שבכל פעם שבה נוצרת מכונה חדשה עם טביעת אצבע חומרית שונה, היא תיצור רשומת חדשה ב-ESET PROTECT באופן אוטומטי.

מידע על חומרה ותוכנה

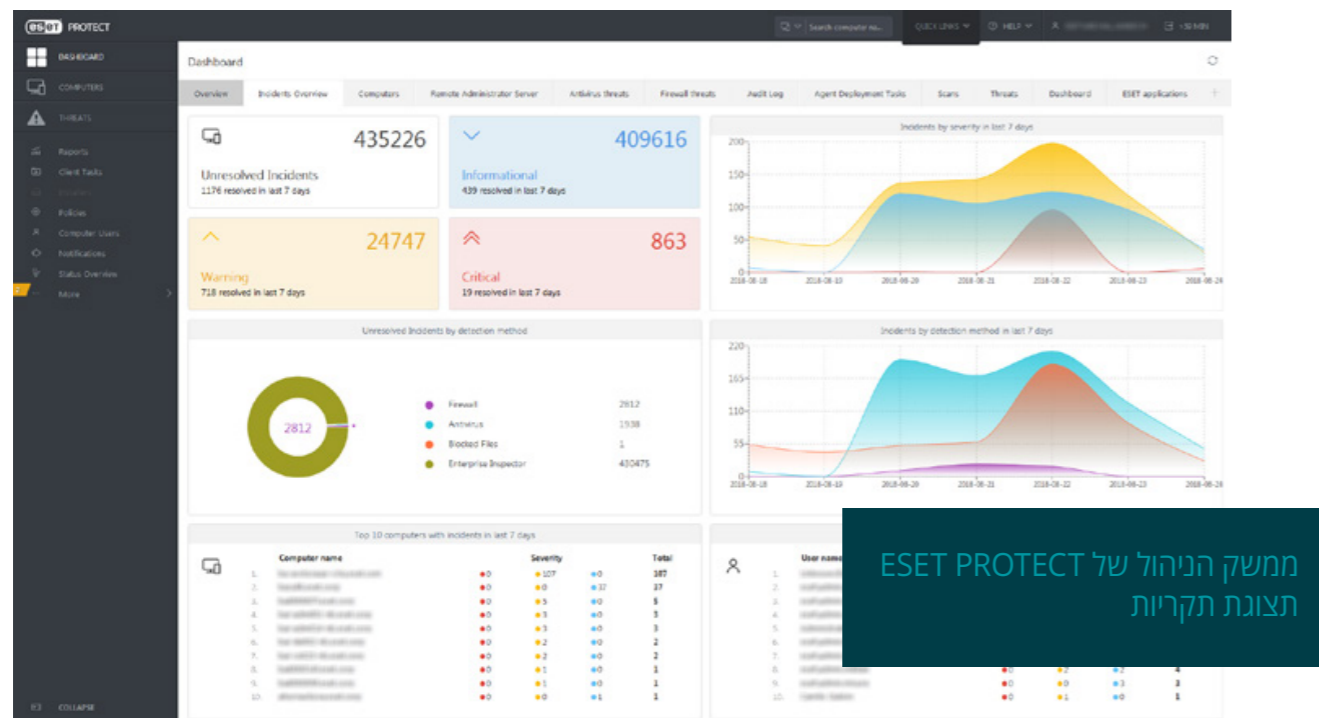
ארגונים צריכים לדעת אילו תוכנות וחומרות מותקנות בכל אחד מהמחשבים ואת גילם של כל אחד מהמחשבים.

פתרון

✓ 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 במצא,



ממשק הניהול של ESET PROTECT תצוגת תקריות

מאפיינים טכניים

ממשק ניהול אחד

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

הצפנת דיסק מלאה

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

Sandbox בענן

התמיכה ב-Sandbox בענן משפרת משמעותית את יכולת הזיהוי של איומי Zero Day כמו כופרות באמצעות ניתוח זריז של קבצים חשודים ב-Sandbox חיצוני של ESET שנמצא בענן.

מידע על חומרה/תוכנה

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

תמיכה במספר חשבונות

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 היצור, הדגם, מערכת ההפעלה, המעבד, כמות זיכרון ה-RAM, כמות השטח הפנוי בכונן הקשיח ומאפיינים רבים אחרים.

שליטה פרטנית במדיניות

ארגונים יכולים להגדיר מדיניות שונות עבור אותו מחשב או קבוצה, ויכולים ליצור תתי-מדיניות שיוכלו לרשת הרשאות ממדיניות-אב. בנוסף, ארגונים יכולים להגדיר את הגדרות המדיניות כהגדרות שמשמשות הקצה ויכל 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 המידע ביומנים בפורמט JSON או LEAF המקובלים בתעשייה, מה שמאפשר אינטגרציה עם מרכז פעולות האבטחה (SOC).

רוצים להשתמש בממשק ניהול מקומי?

בחלק מהארגונים קיימת דרישה לאכסון כל התוכנות באופן פנים-ארגוני, הנובעת מסיבות פנימיות או חוקיות שונות. ESET PROTECT זמין לא רק כממשק בענן אלא גם כפתרון פנים-ארגוני הניתן להתקין מקומית, ללא התפשרות על אף אחד מהמאפיינים, עבור הטמעת פתרון מקומי מלא.

התקנה גמישה

ניתן להתקין את ESET PROTECT על מערכות Windows או Linux, או להפיץ אותו על מכונה וירטואלית. לאחר ההתקנה, כל הניהול מתבצע באמצעות ממשק אינטרנטי, המאפשר גישה וניהול פשוטים מכל מכשיר או מערכת הפעלה.

תמיכה ב-EDR*

כדי לשפר אף יותר את המודעות למצב האבטחה ולהשיג שקיפות ונראות גבוהה יותר על הרשת, ESET PROTECT תומכת בפתרון ה-EDR (זיהוי ותגובה לתחנות קצה) שלנו, ESET Enterprise Inspector. ESET Enterprise Inspector תומך בכמה פלטפורמות (Windows ו-macOS), מאפשרת איתור מתקדם של איומים וטיפול בהם, ויכולה להשתלב ללא הפרעה במרכז מערך האבטחה שלכם.

*התמיכה ב-EDR אפשרית רק בממשק הניהול המקומי ESET PROTECT

איך מתחילים?

מעבר מממשק ניהול מקומי של ESET

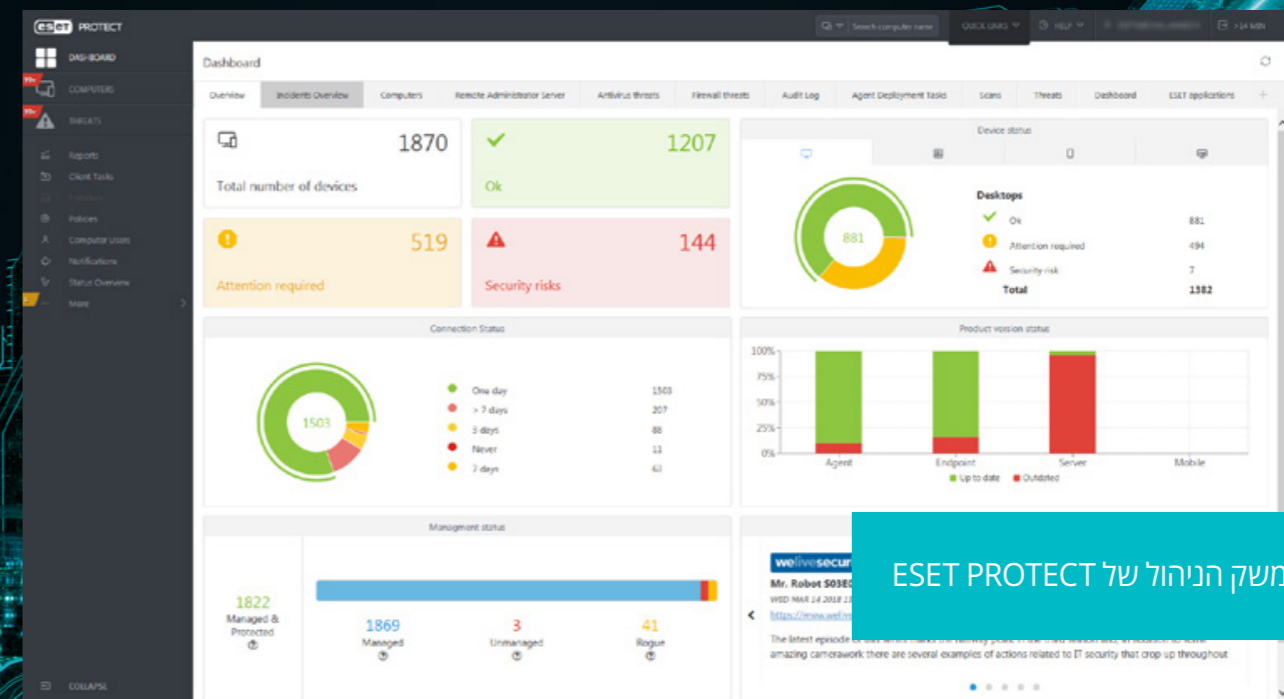
משתמשים כיום בממשק ניהול מקומי של ESET? צרו איתנו קשר ונסייע לכם עם המעבר לממשק ניהול בענן.

ליצירת קשר <

קבלו גרסת ניסיון ל-30 ימים

נצלו את תקופת הניסיון החינמית ל-30 ימים כדי לבחון את הפתרון המלא, הכולל הגנה על תחנות קצה.

לקבלת גרסת ניסיון <



ממשק הניהול של ESET PROTECT

קצת על ESET

ESET עומדת בתקן ISO/IEC 27001:2013, תקן בעל הכרה בינלאומית הנחשב כתקן בטיחות ישים להטמעת וניהול הגנה על מידע. האישור ניתן ע"י גוף התקינה החיצוני SGS, שהוא גוף תקינה בעל מוניטין רב, מה שמראה על העמידה של ESET בתקנים החדשניים ביותר של התעשייה באופן מלא.



השירות ללקוחות מבחינתנו הוא מעל הכול ועל כן מומחי השירות שלנו בישראל עומדים לרשותכם בעברית ובשעות הנוחות לכם. בין לקוחותינו בישראל ניתן למנות משרדי ממשלה ועיריות, מוסדות חינוך ובריאות, חברות היי-טק ועסקים במגוון תחומים רחב.

במשך יותר מ-30 שנים, ESET מפתחת פתרונות הגנה לתחנות קצה המצטיינים במניעה, זיהוי ותגובה לאירועי סייבר, ומאפשרים לארגונים להתמקד במטרותיהן מבלי לעצור ותוך מינימום צריכת משאבים.

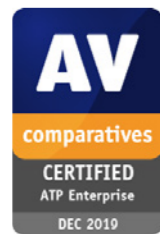
ESET היא אחת התורמות הגדולות ל-Mitre ATT&CK. מוכיחה את עמידתה בהבטחתה – לספק הגנה מיטבית לקהילה וללקוחותינו – באמצעות היותה אחת מספקיות שירותי האבטחה שתרמו נתונים בהיקף הגדול ביותר ל-Mitre ATT&CK.



ESET במספרים

13 מרכזי מחקר ופיתוח ברחבי העולם	+200 נציגויות בעולם	+400K לקוחות עסקיים	+110M משתמשים בכל העולם
---	-------------------------------	-------------------------------	-----------------------------------

פרטי ESET



בין לקוחותינו



מוגנת ע"י ESET מאז 2017;
מעל 14,000 תחנות קצה



מוגנת ע"י ESET מאז 2016;
מעל 9,000 תחנות קצה

הכרה מתעשיית אבטחת המידע



חברת ESET היא היחידה שזכתה לתואר Challenger במבדק Gartner Magic Quadrant for Endpoint Protection Platforms של שנת 2019, וזו השנה השנייה ברציפות.



חברת ESET זכתה לתואר "Strong Performer" בדוח של Forrester Wave™ לרבעון השלישי של 2019, המדרג ערכות אבטחה למוצרי קצה.



חברת ESET דורגה כ-"Top Player" בשנת 2019 בדוח שוק אבטחת נקודות הקצה של Radicati על פי שני קריטריונים עיקריים: פונקציונליות וחזון אסטרטגי.



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



פק שירותי אינטרנט, שותף אבטחה מאז 2008; למעלה מ-2 מיליון לקוחות