



# FILE SECURITY

הגנה על שרתים באמצעות הגנה רב-שכבתית  
עוצמתית ואמינה

CYBERSECURITY  
EXPERTS ON YOUR SIDE

# מהו פתרון לאבטחת קבצים?

מוצר אבטחת קבצים נועד להגן על השרתים המרכזיים מפני איומים. יש להתקין את המוצר על כל שרת שאינו בעל תפקיד ייעודי כדי להבטיח שמשאבי הארגון אינם מודבקים בנוזקות. כיום, חברות מסכנות את הארגון שלהן בכך שהן מאפשרות לעובדיהן לשמור קבצים על שרת משותף של החברה, מבלי להגן עליו כראוי מפני קבצים זדוניים. משתמש בודד ששומר קובץ זדוני בכונן רשת עלול להביא למצב בו כל קבצי הארגון אינם נגישים יותר.

**ESET File Security** מספק הגנה מתקדמת לכל השרתים הכלליים, שרתי האחסון ברשת והשרתים הרב-תכליתיים. הוא נותן תשומת לב מיוחדת להבטחת יציבות השרתים ומניעת קונפליקטים, וכך מצמצם את חלונות הזמן של התחזוקה והפעלות מחדש למינימום האפשרי, כדי להבטיח המשכיות עסקית.

# למה יש צורך בפתרונות אבטחת קבצים?

## מתקפות כופרה

החל בשנת 2013, עם הופעתה של Cryptolocker, כופרות החלו לעורר דאגה באופן קבוע בתעשיות שונות בכל העולם. למרות שכופרות היו קיימות זמן רב לפני כן, הן לא היו איום משמעותי שארגונים חששו ממנו. כיום, לעומת זאת, מקרה בודד של מתקפת כופרה יכול להשבית ארגון שלם על ידי הצפנת קבצים חשובים או נחוצים. כאשר עסק חווה מתקפת כופרה, מנהליו ובעליו יבינו במהרה שהגיבויים שברשותם אינם עדכניים מספיק, ולכן ירגישו שהם מוכרחים לשלם את הכופר.

אם ישנם שרתים בתמונה, הנוק העלול להיגרם מנוזקות גדל משמעותית, שכן משתמשים מסוגלים לשמור קבצי נוזקה בכונן רשת. פתרונות ההגנה לתחנות הקצה של ESET מספקים שכבות הגנה שלא רק מונעות הגעת כופרות, אלא גם בודקות האם הקובץ היה קיים אי פעם בארגון. חשוב לזהות ולמנוע מתקפות כופרה, מכיוון שבכל פעם שתשלום כופר נשלח לעבריינים, הם מבינים שכדאי להם להמשיך להשתמש בשיטת ההתקפה הזו.

## מתקפות ממוקדות והדלפות מידע

מרחב אבטחת הסייבר של ימינו מתפתח באופן קבוע, ולעיתים קרובות ניתן לראות שיטות התקפה חדשות או איומים שעדיין לא נראו. 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, ארגונים יטמיעו שיטות שונות כדי למנוע התרחשות של מתקפה דומה. אך צעדים אלה לא יגנו עליהם מפני המתקפה הבאה, שעשויה להשתמש בשיטת תקיפה חדשה לחלוטין.

פתרונות ההגנה לתחנות הקצה של ESET משתמשים במידע על איומים מ-Threat Intelligence, המתבסס על מידת התפוצה שלהם בעולם, כדי ליצור סדר עדיפויות ולחסום את האיומים החדשים ביותר באופן אפקטיבי, לפני שיופצו למקומות אחרים בעולם. שרתים הם מטרה נפוצה יותר, שכן ברוב המקרים הם מכילים מידע רגיש או מסווג. כדי להתגונן מפני איומים אלה בצורה טובה יותר, פתרונות ESET File Security כוללים אפשרות התעדכנות מבוססת-ענן כדי להגיב במהירות לזיהוי שהוחמץ מבלי להמתין לעדכון שגרתי

## מתקפות נטולות קבצים

איומים חדשים יותר, הנקראים נוזקות נטולות-קבצים (Fileless), פועלות רק בזיכרון המחשב, ולכן אינן יכולות להתגלות על ידי הגנות המתבססות על סריקת קבצים. בנוסף, חלק מהמתקפות נטולות הקבצים ינצלו תוכנות קיימות שמובנות במערכת ההפעלה כדי שיהיה קשה אף יותר לזהות את הקוד הזדוני שבהן. לדוגמה, רבות מהמתקפות האלה מנצלות את PowerShell.

פתרונות ההגנה לתחנות הקצה של ESET כוללים פתרונות לזיהוי אפליקציות שנפגעו או נפרצו, המגינים עליהן מפני מתקפות נטולות קבצים. חברות אחרות יצרו סורקים ייעודיים הבודקים באופן קבוע אם יש משהו חשוב בזיכרון המחשב. באמצעות שימוש בנישה רב-שכבתית זו, אנו יכולים להבטיח שאנחנו נמצאים צעד אחד לפני הנוזקות החדשות ביותר.

# למה ESET?

## הגנה רב-שכבתית

חברת ESET משלבת בין טכנולוגיה רב-שכבתית, למידת מכונה ומומחיות אנושית כדי לספק ללקוחותיה את רמת האבטחה הטובה ביותר. הטכנולוגיה שלנו משתנה ומותאמת באופן קבוע כדי ליצור איזון מושלם בין ביצועים, זיהויים מדויקים ומינימום זיהויים שגויים.

## ביצועים ללא תחרות

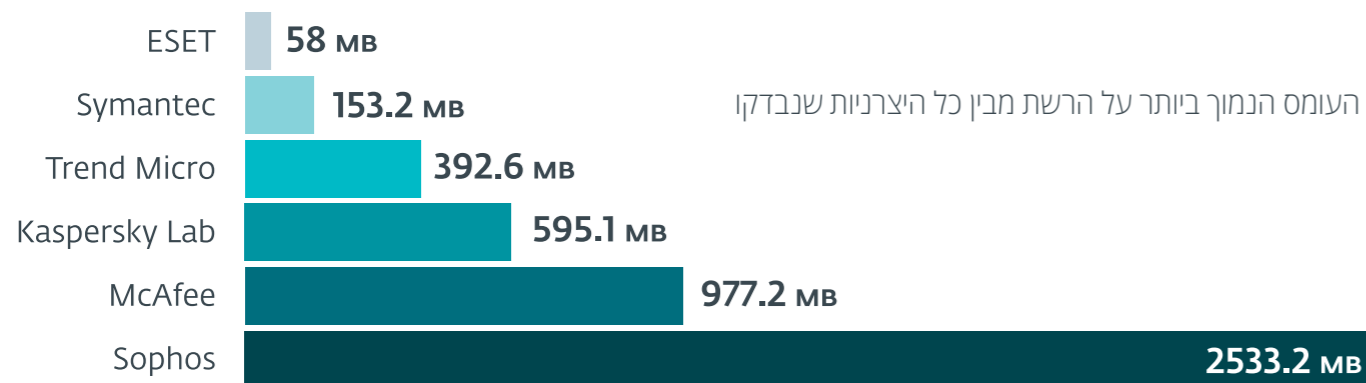
הדבר העיקרי שמדאיג ארגונים שמחפשים פתרון אבטחה לתחנות קצה הוא מידת ההשפעה על ביצועי המערכות. מוצרי ESET ממשיכים להצטיין בקטגוריית הביצועים וזוכים במבחנים של גופים חיצוניים הבוחנים את מידת ההשפעה של תוכנות תחנות הקצה שלנו על המערכות בארגון.

## תמיכה בפלטפורמות רבות

הפתרונות של ESET תומכים במספר רב של מערכות הפעלה ופלטפורמות, כגון Windows, Mac, Linux ו-iOS. ניתן לנהל את כל פתרונות מתוך ממשק ניהול אחד; גם הניהול מרחוק של מכשירי iOS ו-iOS הוא חלק בלתי נפרד מהפתרון.

## נוכחות בכל העולם

ל-ESET יש 22 משרדים ברחבי העולם, 13 מרכזי מחקר ופיתוח ונציגויות ביותר מ-200 מדינות וטריטוריות. זה עוזר לנו לקבל נתונים שיאיתרו נזקקות לפני שהן מתפשטות בעולם, וכן לתעדף פיתוח של טכנולוגיות חדשות על פי האיומים או שיטות ההתקפה החדשות שמתגלות.



Source: AV-Comparatives: Network Performance Test, Business Security Software

העומס הנמוך ביותר על הרשת מבין כל היצרניות שנבדקו

“... ההוכחה הטובה ביותר? הסטטיסטיקות של מוקד שירות הלקוחות שלנו: אחרי שהטמענו את פתרונות ESET, נציגי התמיכה שלנו לא מתעדים שיחות – הם לא צריכים להתעסק בבעיות הנוגעות לאנטי-וירוס או נזקקות!”

אדם הופמן, מנהל תשתיות IT, Mercury Engineering, אירלנד, 1,300 תחנות קצה



## פתרונות האבטחה של ESET File Server

ESET File Security for Microsoft Windows Server

ESET File Security for Linux / FreeBSD

ESET File Security for Microsoft Azure



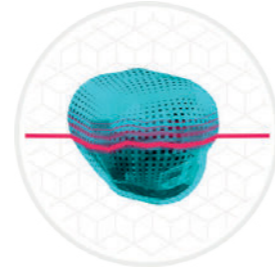
# הטכנולוגיה

המוצרים והטכנולוגיות שלנו מתבססים על 3 מרכיבים מרכזיים:



## למידת מכונה

כל מוצרי ההגנה לתחנות קצה של ESET משנת 1997 והלאה, השתמשו בלמידת מכונה, בנוסף לשכבות הגנה נוספות. כיום, חברת ESET משתמשת בלמידת מכונה ומשלבת אותה בכל שכבות ההגנה האחרות שלה. למידת המכונה מנוצלת להפקת פלט מאוחד וליצירת רשתות עצביות.



## סריקת זיכרון מחשב מתקדמת

מנטר את ההתנהגות של תהליכים זדוניים וסורק אותם ברגע שהם נחשפים בזיכרון המחשב. נוזקות נטולות-קבצים פועלות ללא רכיבים קבועים במערכת הקבצים, אותם ניתן לגלות בדרכים רגילות. רק סריקת זיכרון המחשב יכולה לגלות מתקפות זדוניות כמו אלה באופן מלא ולעצור אותן.



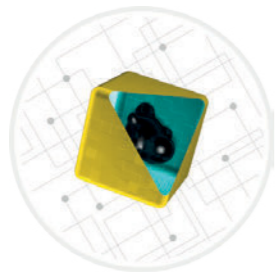
## מגן מפני כופרות

שכבה נוספת המגנה על משתמשים מפני כופרות. הטכנולוגיה מנטרת ובודקת את כל התוכנות המורצות על פי ההתנהגות והמוניטין שלהן. היא נועדה לזהות ולחסום תהליכים שהתנהגותם מזכירה התנהגות של כופרות.



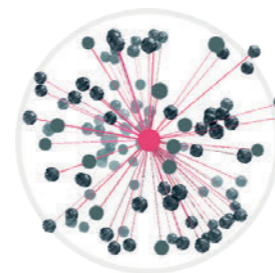
## חוסם פרצות אבטחה

מנטר אפליקציות שמתגלות בהן חולשות בדרך כלל (דפדפנים, קוראי מסמכים, תוכנות דוא"ל, Java, Flash ועוד), ובמקום התמקדות במזיהי CVA ספציפיים הוא מתמקד בטכניקות ניצול חולשות. מרגע שהרכיב הופעל, האיום נחסם באופן מיידי באותו המכשיר.



## Sandbox מובנה בפתרון

במקרים רבים, נוזקות מודרניות מסוות את עצמן ומנסות להימנע מזיהוי ככל האפשר. אנו משתמשים ב-Sandbox המובנה בפתרון האבטחה כדי לחשוף את ההתחמקות הזו ולגלות את ההתנהגות האמיתית המסתתרת מתחת לפני השטח. באמצעות טכנולוגיה זו, פתרונות ESET מדמים רכיבי חומרה ותוכנה שונים כדי להפעיל דגימה חשודה בסביבה וירטואלית מבודדת.



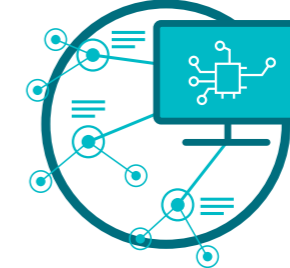
## הגנה מפני בוטנטים

מזהה תקשורות זדוניות המזוהות עם בוטנטים, תוך כדי שהוא מזהה את התהליכים המוציאים תקשורות אלה. כל תקשורת זדונית שמזוהה נחסמת ומדווחת למשתמש.



## ESET LiveGrid®

בכל מקרה בו מזהה מתקפת Zero Day, למשל כופרה, הקובץ נשלח למערכת מבוססת הענן שלנו, ESET LiveGrid®, שבה הקובץ מופעל ומנוטר. תוצאות הבדיקה של מערכת זו נשלחות לכל תחנות הקצה, ללא צורך בביצוע עדכון כלשהו.



## למידת מכונה (Machine Learning)

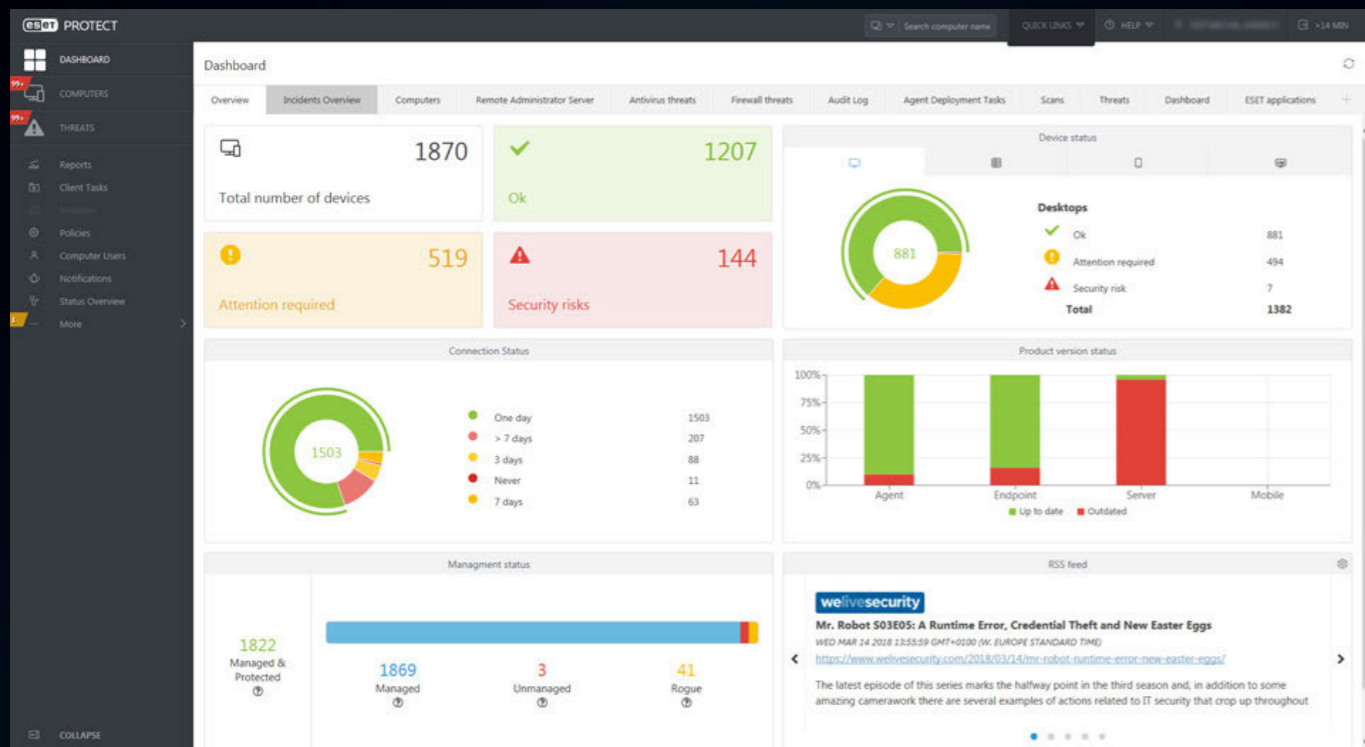
משתמש בעוצמה המשולבת של רשתות עצביות (למידה עמוקה וזיכרון לטווח הארוך ולטווח הקצר) ואלגוריתמים שנבחרו בקפידה כדי לייצר פלט מאוחד ולסייע בתיוג נכון של הדגימות הנכנסות כנקיות, כדגימות שעלולות להיות בלתי רצויות או כדגימות זדוניות.



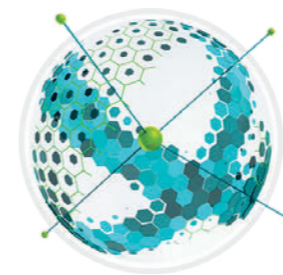
## מומחיות אנושית

חוקרי אבטחה ברמה עולמית החולקים ידע טכני ומודיעיני מובחר כדי להבטיח את המודיעין האיומים הטוב ביותר בכל רגע נתון.

שכבת הגנה אחת אינה מספיקה במרחב האיומים המתפתח באופן מתמיד. כל מוצרי ESET מסוגלים לזהות נוזקות לפני הרצתן, במהלך הרצתן ולאחר הרצתן. התמקדות בכל חלקי מחזור החיים של הנוזקה מאפשר לנו להגיע לרמת ההגנה הגבוהה ביותר.



כל הפתרונות לתחנות הקצה של ESET מנוהלים מתוך ממשק אחד, ESET PROTECT, המבטיח שקיפות ונראות מלאה על הרשת.



### הגנה ממתקפות רשת

הטכנולוגיה משפרת את הזיהוי של נקודות תורפה ידועות ברמת הרשת. היא יוצרת שכבת הגנה חשובה נוספת המגינה מפני הפצת נזקקות, מתקפות מבוססות רשת וניצול חולשות שעדיין לא תוקנו באמצעות טלאי.



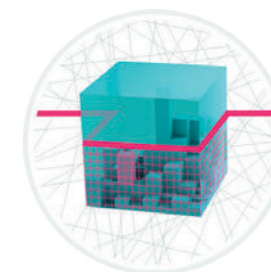
### דפדפן מאובטח

נועד להגן על נכסי החברה באמצעות שכבת הגנה מיוחדת המתמקדת בדפדפן, הכלי העיקרי המשמש לגישה לנתונים ברשת הפנימית ובענן. דפדפן מאובטח מספק הגנה משופרת על הזיכרון לתהליך הדפדפן והגנה על המקלדת, ומאפשר למנהלי הרשת להוסיף כתובות אינטרנט שיאובטחו ע"י רכיב זה.



### איתור וחסמה מבוססי התנהגות - HIPS

המערכת של ESET למניעת חדירות המבוססת על מארח (HIPS) מנסרת את פעילות המערכת ומשתמשת בקבוצת כללים מוגדרת מראש כדי לזהות התנהגות חשודה במערכת. כאשר פעילות מסוג כזה מזוהה, מנגנון מונע מהתהליך הפוגעני מלבצע פעילות שעלולה להיות מזיקה.



### סורק UEFI Scanner

ESET היא החברה הראשונה המספקת מוצר אבטחה לתחנות קצה שכוללת בפתרון האבטחה שלה שכבה ייחודית המגינה על ממשק הקושחה המורחב המאוחד (UEFI). סורק ה-UEFI בודק את סביבת טרום-ההפעלה ומיועד לנטר את שלמותה של הקושחה. אם אותר שינוי בקושחה, הרכיב מודיע למשתמש על שינוי זה.

*"מה שבולט במיוחד הוא היתרון הטכנולוגי שלו על פני מוצרים אחרים בשוק. ESET מציעה לנו אבטחה אמינה, וזה אומר שאני יכול לעבוד על כל פרויקט בכל זמן נתון, תוך כדי שאני יודעת שהמחשבים שלנו מוגנים לחלוטין."*

פיונה גרלנד, אנליסטית עסקים בקבוצת Mercury Engineering, IT, אירלנד, 1,300 תחנות קצה

# מקרים לשימוש

## נוזקות נטולות-קבצים

**מקרה לדוגמה:** נוזקה נטולת-קובץ היא איום חדש יחסית, ומכיוון שהיא פועלת רק בזיכרון המחשב יש להגן מפניהן בגישה אחרת לעומת נוזקות מבוססות-קבצים מסורתיות.

### פתרון

✓ סריקת זיכרון מתקדמת של ESET מגינה מפני איומים כאלה באמצעות ניטור התנהגות של תהליכים זדוניים וסריקתם מרגע הופעתם בזיכרון המחשב.

✓ אם ESET File Security אינו בטוח לגבי האיום הפוטנציאלי, הוא יכול להעביר את הקובץ המצורף ל-Sandbox בענן של ESET - ESET Dynamic Threat Defense, כדי לבחון באופן מקיף יותר אם אכן מדובר בקוד זדוני.

✓ אם אכן מדובר באיום, תוכלו להקטין את זמן איסוף הנתונים והחקירה באמצעות העלאת האיום למערכת ESET Threat Intelligence, שתוכל לספק מידע בנוגע לאופן הפעולה של אותו איום.

## איומי Zero Day

**מקרה לדוגמה:** איומי Zero Day הם אחד החששות הגדולים ביותר של עסקים מכיוון שהם אינם יודעים כיצד להתגונן מפני משהו שלא ראו מעולם.

### פתרון

✓ ESET Threat Intelligence מספק נתונים על האיומים והמגמות האחרונים ועל מתקפות ממוקדות כדי לסייע לעסקים לצפות לאיומים החדשים ביותר ולהתגונן מפניהם.

✓ הגנת תחנות הקצה של ESET משתמשים בזיהוי התנהגותי ולמידת מכונה כחלק מהגישה הרב-שכבתית שלנו כדי להגן מפני נוזקות חדשות שלא נראו מעולם.

✓ ESET LiveGrid® מגן באופן אוטומטי מפני איומים חדשים, מבלי לחכות לעדכון הבא של בסיס הנתונים לזיהוי.

## מתקפות כופרה

**מקרה לדוגמה:** ארגונים מעוניינים בהגנות נוספות שיבטיחו שהם יהיו מוגנים מפני מתקפות כופרה. בנוסף לכך, הם רוצים לוודא שכונני הרשת לא יוצפנו.

### פתרון

✓ חוסם פרצות האבטחה מונע את הדבקת המערכות בכופרות באמצעות עצירת פרצות אבטחה ברמת הרשת.

✓ Sandbox מובנה בפתרון המזהה נוזקה שמנסה להימנע מזיהוי באמצעות הסוואה.

✓ ESET LiveGrid® מגן באופן אוטומטי מפני איומים חדשים, מבלי לחכות לעדכון הבא של בסיס הנתונים לזיהוי.

✓ כל המוצרים כוללים הגנה לפני הרצה הנקראת Ransomware Shield שנועדה להגן על ארגונים מפני הצפנת קבצים זדונית.

✓ אם ESET File Security אינו בטוח לגבי האיום הפוטנציאלי, הוא יכול להעביר את הקובץ המצורף ל-Sandbox בענן של ESET - ESET Dynamic Threat Defense, כדי לבחון באופן מקיף יותר אם אכן מדובר בקוד זדוני.

“כשגילינו את ESET, ידענו שזו הייתה הבחירה הנכונה: טכנולוגיה אמינה, זיהוי מתוחכם, נציגות מקומית ותמיכה טכנית מצוינת – כל מה שהיינו צריכים.”

ארנסטו בונהוק, מנהל תשתיות IT, בית החולים Alemán, ארגנטינה, מעל 1,500 תחנות קצה

# 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

<b>13</b> מרכזי מחקר ופיתוח ברחבי העולם	<b>+200</b> נציגויות בעולם	<b>+400K</b> לקוחות עסקיים	<b>+110M</b> 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