הגנה רב שכבתית והטכנולוגיה שתומכת בה

ENJOY SAFER TECHNOLOGY™

האם העסק שלך מוגן מפני מתקפות סייבר וכופר?

כל ארגון זקוק להגנה מקיפה על תחנות הקצה והשרתים. ככל שיש יותר מעגלי אבטחה, כך הסיכוי לטפל ולמנוע מתקפות סייבר וכופר הולך וגדל.

מתקפות סייבר בכלל ומתקפות כופר בפרט ממשיכות להיות האיום הגדול ביותר על ארגונים. עבריינות הרשת המשתכללת והמתפתחת, הפכה להיות תעשייה המגלגלת מיליארדי דולרים ומטרתה האחת היא - להרוויח כמה שיותר.

כל שיטת הגנה הנשענת על טכנולוגיה אחת בלבד לא מספיקה - נדרשת הגנה רב שכבתית של מודולים רבים המשלימים את ההגנה לארגון.

הייחודיות של ESET היא בגישת ההגנה הרב שכבתית שנועדה לחסום מתקפות סייבר באמצעות טכנולוגיה פרו אקטיבית (מודולים במעגלי אבטחה).

ישנם 3 מודולים שפועלים ברקע בכל המוצרים של ESET ומטרתם לבצע ניטור ובקרה בזמן אמת:

1 | הגנה מפני חדירת קוד זדוני למערכות הפעלה (HIPS: HOST INTRUSION PREVENTION SYSTEM)

מערכת המנטרת את מערכת ההפעלה ומשתמשת בסט חוקים מובנים על מנת לזהות התנהגות חשודה במחשב.
כאשר מזוהה פעילות זדונית על גבי קבצים, תהליכים, שירותים, רשומות REGISTRY וכו', מערכת ההגנה העצמית של HIPS עוצרת את התוכנה או את התהליך הזדוני ומונעת ממנו מלבצע שינויים במערכת ההפעלה.

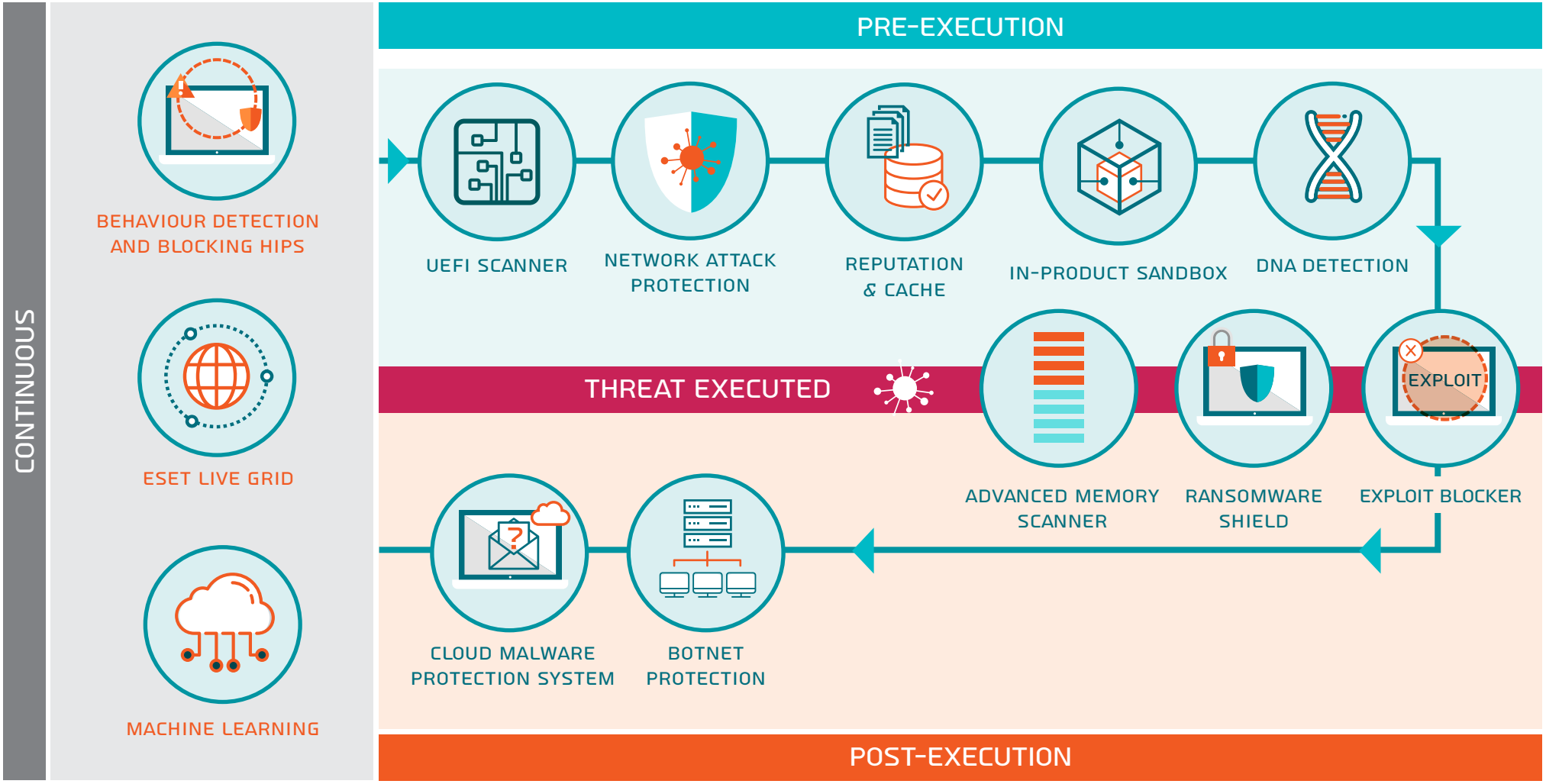
2 | LIVE GRID

מאגר מידע בענן של ESET המתעדכן באופן מיידי ובודק בזמן אמת מוניטין של קבצים במחשב.
המאגר מאפשר ביצועים משופרים ושיתוף מידע מהיר על נוזקות בקרב יותר מ-110 מיליון משתמשי ESET - זמן תגובה מהיר של עד 20 דקות מרגע זיהוי איום חדש ולא מוכר, עד שהתחנות מוגנות מפניו באמצעות המאגר בענן.

3 | שימוש ב- MACHINE LEARNING

המידע שנאסף ב-LIVEGRID מתוך מודולים אחרים, זיהויים קודמים ודגימות, מנותח בצורה מעמיקה יותר בסביבת SANDBOX בענן, באמצעות טכניקות ואלגוריתמים מתקדמים.

המודולים השונים במוצרי ESET על פי שלבי ההפעלה של נוזקות



מספקים הגנה מתמשכת	הגנה בטרם הפעלת הנוזקה	הגנה בעת הפעלת הנוזקה	הגנה לאחר הפעלת הנוזקה
HIPS	UEFI SCANNER	ADVANCED MEMORY SCANNER	CLOUD MALWARE PROTECTION SYSTEM
LIVE GRID	NETWORK ATTACK PROTECTION	RANSOMWARE SHIELD	BOTNET PROTECTION
MACHINE LEARNING	REPUTATION AND CACHE	EXPLOIT BLOCKER	
	IN-PRODUCT SANDBOX		
	DNA DETECTION		

הגנה בטרם הפעלת הנוזקה

הגנה על החומרה במחשב (UEFI SCANNER)

הגנה ייעודית מפני השתלטות וירוסים, טרם עליית מערכת ההפעלה של המחשב (מניעת הדבקת BIOS)
הסורק מבצע בדיקה ואכיפת אבטחה בסביבת האתחול המקדים. הסורק תוכנן כדי לנטר את הרכיב וזהותו ובמקרה שמתגלה בו שינוי כלשהו, הסורק מתריע על כך למשתמש.

הגנה מפני התקפות ברשת (NETWORK ATTACK PROTECTION) רק במוצרי SECURITY

מהווה רכיב חשוב בחומת האש האישית. שכבת אבטחה חשובה כנגד נוזקות, המפיצות את עצמן באמצעות פירצות אבטחה שעדיין לא יצא עבורן עדכון ומתפשטות ברחבי האינטרנט והרשת הפנים ארגונית.
במתקפה הנרחבת של נוזקת הכופר WANNACRY נחסמה ההתקפה ידי חסימת הפירצה שאותרה באמצעות המודול הזה. הקוד הזדוני נחסם עוד לפני שהריץ את עצמו.

לצפייה בסרטון על המודול >>

מוניטין ומטמון (REPUTATION AND CACHE)

כל אובייקט (קובץ, קישורים לאתרים זדוניים כמו אתרי פישינג) נבדק ברכיב ה-LOCAL CACHE עוד בטרם מתבצעת סריקה. פעולה זו משפרת את הביצועים על ידי חסכון במשאבי הסריקה.
מערכת ה-LIVE GRID (מערכת ענן לדירוג מוניטין קבצים) בודקת האם האובייקט סווג כזדוני בקרב 110 מיליון המשתמשים. המערכת מאפשרת הפצת ושיתוף מידע אודות נוזקות בקרב משתמשים במהירות רבה.

לצפייה בסרטון על המודול >>

SANDBOX מובנה במוצר (IN-PRODUCT SANDBOX)

שכבה נוספת ומשלימה לזיהוי על פי DNA. מנגנון זה בוחן את טיב הנוזקות החשודות והתנהגותן, שכן היום נהוג להשתמש בטכניקות הסוואה כדי לחמוק מגילוי.

זיהוי על פי DNA (DNA DETECTION)

קוד זדוני ניתן לשינוי על ידי האקרים, אך ההתנהגות שלו לא משתנה. עקרון זה יושם בזיהוי על-פי DNA אשר קיים במוצרים שלנו:
לכן מתבצע ניתוח התנהגותי מעמיק של הקוד, כדי לאתר התנהגות חשודה או חריגה. כל קוד שאינו מאומת, נחשב כזדוני ונבדק לעומק.
הזיהוי מתבצע כדי לזהות לא רק דגימות של נוזקות מוכרות, אלא גם נוזקות שלא נראו מעולם (IN THE WILD) המכילות קוד עם התנהגות זדונית.

לצפייה בסרטון על המודול >>

הגנה בעת הפעלת הנוזקה

סריקת זיכרון מחשב מתקדמת (ADVANCED MEMORY SCANNER)

טכנולוגיה ייחודית, המציעה פתרון אפקטיבי לבעיה רווחת בעידן הנוזקות המודרני: נוזקות המסוות עצמן או עוברות הצפנה בכדי לחמוק מזיהוי.
בעבר, הטכניקות הקבועות לטפל בנוזקות מוסוות היו להריץ ולבדוק את התנהגותן בתוך סביבה וירטואלית מבודדת (SANDBOX), אך זה לא מספיק משום שבדיקה כזו מתבצעת באופן חד פעמי ונוזקות יודעות להסוות את עצמן. טכנולוגיה זו בודקת ומנטרת את ההתנהגות של תהליכים, לאחר שכבר הופעלו ונטענו לזיכרון המחשב.

לצפייה בסרטון על המודול >>

הגנה מפני נוזקות כופר (RANSOMWARE SHIELD)

טכנולוגיה ייעודית המנטרת ומזהה נוזקות כופר על פי התנהגות ומוניטין, כמו למשל ניסיון לבצע שינויים בלתי רצויים בקבצים קיימים, תהליכים, שירותים ורשומות רג'יסטרי. הגנה זו בשילוב כלל מודולי ההגנה של ESET, מאפשרים זיהוי ברמת דיוק גבוהה.

חוסם פרצות אבטחה (EXPLOIT BLOCKER)

שכבת אבטחה ייחודית המיועדת לטפל בפרצות אבטחה.
חוסם הפרצות מנטר דרך קבע אפליקציות שבדרך כלל מתגלות בהן פרצות (דפדפנים, קוראי מסמכים, תוכנות לדואר אלקטרוני ועוד), הוא סורק תהליכים המנסים לנצל את אותן פירצות ומאתר אותם.
תהליכים הנחשדים כזדוניים נחסמים מיידית והמידע מועבר לענן (ESET LIVE GRID) במטרה לבחון אותו לעומק.
מידע זה מאפשר יעילות גבוהה בהתמודדות עם איומים לא מוכרים שזה עתה התפרצו (ZERO DAY ATTACKS).

לצפייה בסרטון על המודול >>

הגנה לאחר הפעלת הנוזקה

מערכת זיהוי מבוססת-ענן (CLOUD MALWARE PROTECTION SYSTEM)

מערכת זו מקבלת דגימות חשודות דרך ה- ESET LIVE GRID הקיים בתחנה או בשרת. אותן דגימות עוברות תהליך סריקה אוטומטי באמצעות ניתוח התנהגותי, בשילוב תהליכי אמולציה (SANDBOX).
יכולת זו היא למעשה חלק ממנגנון ה-MACHINE LEARNING, המאפשר ניתוח על ידי אלגוריתמים חכמים יותר.
ה- LIVE GRID כולל מערכת מוניטין המאפשרת לכל משתמש לגלות בזמן אמת האם הקוד החשוד שנתגלה במחשב שלו, זוהה אצל אחד מבין יותר מ- 110 מיליון המשתמשים, הרבה לפני שעדכוני החתימות השוטפים מגיעים לכלל המשתמשים. לכן זוהי שכבת אבטחה קריטית בטיפול בהתפרצויות של נוזקות חדשות ולא מוכרות.

לצפייה בסרטון על המודול >>

הגנה מפני בוטנט (BOTNET PROTECTION) רק במוצרי ה- SECURITY

חלק מהנוזקות (כמו נוזקות כופר), תלויות בין השאר ביכולת של התוקפים לשדר להן פקודות מרחוק דרך שרת בקרה ושליטה.
רכיב ההגנה מפני בוטנטים פועל כדי לנטר ולזהות בהצלחה את התקשורת של בוטנטים עם שרת הבקרה והשליטה, וגם כדי לאתר את התהליך עצמו שאחראי על התקשורת.
מכאן החשיבות הכפולה של רכיב זה: הוא מאפשר באופן ייחודי לאתר חולשות ברשת או ערכות פריצה קיימות, אשר באמצעותן מתבצעת התקשורת. כמו כן הוא מאפשר לזהות במדויק את התהליכים הזדוניים.

לצפייה בסרטון על המודול >>

ENJOY SAFER TECHNOLOGY™

ESET היא חברת אבטחת המידע הרביעית בגודלה בעולם הנחשבת לחלוצת תחום האנטי וירוס, עם יותר מ-110 מיליון משתמשים מוגנים ופריסה במעל ל-200 מדינות ברחבי העולם.

ESET מפתחת ומייצרת פתרונות הגנה המצטיינים בזיהוי איומים ומיועדים למגזר הפרטי והעסקי כאחד וכוללים הגנה מפני ווירוסים, מתקפות מקוונות, גניבת זהויות, הגנה על תשלומים ברשת, הצפנת מידע עסקי, הקשחת תהליכי התחברות לרשת ועוד.

בין לקוחותינו ניתן למנות את משרדי ממשלה ועיריות, מוסדות חינוך ובריאות, חברות היי-טק ועסקים במגוון תחומים רחב. פתרונות האנטי וירוס של ESET הם הנמכרים ביותר בישראל בשוק הפרטי.

ESET
ENJOY SAFER TECHNOLOGY™