



LIVEGUARD ADVANCED

הגנה פרו-אקטיבית מפני מתקפות כופר
ואיומי Zero day

Progress. Protected.

מה זה Live Guard ?Advanced

טכנולוגיה פרו-אקטיבית מבוססת-ענן שעושה שימוש בסריקה מתקדמת, Machine Learning, Sandbox וניתוח התנהגותי מעמיק כדי למנוע מתקפות ממוקדות, מתקפות כופר ואיומי Zero day.

ESET LiveGuard Advanced מספק שכבת אבטחה נוספת למוצרי ESET כמו הגנה על תיבות הדוא"ל, הגנה על תחנות הקצה והגנה על יישומי Microsoft365.

הטכנולוגיה מבוססת-הענן המתקדמת של ESET מורכבת מסוגים שונים של חיישנים שיוצרים אנליזה סטטית מלאה של הקוד, ניתוח מעמיק של הקוד באמצעות Machine Learning, בחינת זיכרון התוכנה וזיהוי מבוסס התנהגות.

מדוע להשתמש בהגנה פרו-אקטיבית מבוססת-ענן?

מתקפות כופר

משנת 2013 עם הופעתה של Cryptorlocker, מתקפות כופר מהוות גורם קבוע לדאגה בקרב תעשיות שונות בעולם. למרות שכופרות היו קיימות זמן רב לפני כן, הן לא היוו איום משמעותי שארגונים חששו ממנו. כיום, לעומת זאת, מקרה בודד של מתקפת כופר יכול להשבית ארגון שלם על ידי הצפנת קבצים חשובים או נחוצים. כאשר ארגון חווה מתקפת כופר, מנהליו ובעליו יבינו במהרה שהגיבויים שברשותם עלולים להיות לא עדכניים מספיק, ולכן ירגישו שהם מוכרחים לשלם את הכופר.

פתרון פרו-אקטיבי ומבוסס-ענן לזיהוי איומים מספק שכבת הגנה נוספת מחוץ לרשת החברה שמונעת הרצה של כופרות ונוזקות בסביבת העבודה.

מתקפות ממוקדות והדלפות מידע

מרחב אבטחת הסייבר של ימינו מתפתח באופן קבוע, ולעיתים קרובות ניתן לראות שיטות התקפה חדשות או איומים שטרם נצפו 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 המתקפה, ארגונים יטמיעו מנגנוני הגנה נוספים כדי למנוע התרחשות של מתקפה כזו. אך צעדים אלה לא יגנו עליהם בהכרח מפני המתקפה הבאה, שעשויה להשתמש בווקטור תקיפה חדש לחלוטין.

הגישה של Sandbox בענן לצרכי אבטחה היא הרבה יותר אפקטיבית מכיוון שהפתרון בוחן בצורה מעמיקה את האיום ורואה מה האיום הפוטנציאלי מבצע. כך, קל יותר להגיע למסקנה חד-משמעית כשקובעים האם מדובר המתקפה ממוקדת, איום מתמשך או קובץ תמים.

Sandbox בענן
שנמצא מחוץ לרשת הארגון
יכול לראות מה האיום
הפוטנציאלי עושה באמת,
במקום לנתח רק את הקוד שלו.

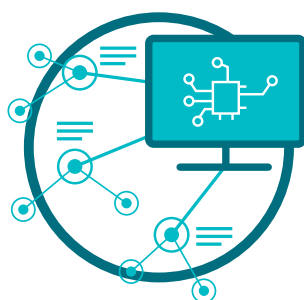
ניתוח קוד סטטי ודינמי
מתבצעים באמצעות
מערך אלגוריתמים
של Machine Learning,
המשתמשים בטכנולוגיות
כמו Deep Learning

המוצרים והטכנולוגיות שלנו מתבססים על 3 עמודי תווך



ESET LiveGrid®

בכל מקרה בו מזהה מתקפת Zero day למשל כופרה, הקובץ נשלח למערכת מבוססת מוניטין בענן שלנו, ESET LiveGrid®, שבה מתבצעת הרצה וניטור של הקובץ. תוצאות הבדיקה של מערכת זו נשלחות לכל תחנות הקצה בעולם ללא צורך בביצוע עדכון כלשהו.



Machine Learning

שימוש בכוח המשולב של Machine Learning ואלגוריתמים שנבחרו באופן ידני כדי לתייג את הדגימות המגיעות למערכת כנקיות, לא רצויות או זדוניות באופן מדויק.



מומחיות אנושית

חוקרי אבטחה ברמה עולמית החולקים ידע טכני ומוזיעיני איכותי כדי להבטיח את המודיעין הטוב ביותר בכל רגע נתון.



היתרון של ESET

הגנה רב-שכבתית

ESET LiveGuard Advanced הוא פתרון מבוסס ענן להגנה מפני איומים ששולח את כל הדגימות החשודות לסביבת בדיקה מבודדת מבוססת-ענן של ESET. הדגימות החשודות מנותחות על ידי הפתרון באמצעות כלים למודיעין איומים, אנליזה דינמית וסטטית, נתוני מוניטין וכלים נוספים לזיהוי איומי Zero-day. ל-ESET LiveGuard Advanced יש ארבע שכבות הגנה שונות המשמשות לניתוח הדגימות וניתן להפעיל אותן באופן דינמי על פי התוצאות העולות מהבדיקה. ESET LiveGuard Advanced משלב את כל התוצאות משכבות הזיהוי ומעריך את סטטוס הדגימה. התוצאות נשלחות תחילה למוצר האבטחה של ESET במחשב המשתמש ולתשתית החברה בה הוא נמצא.

שקיפות מלאה

ניתן לצפות בתוצאות של כל דגימה שנותחה, בממשק הניהול ESET PROTECT. בנוסף, לקוחות עם רישיון הכולל יותר מ-100 תחנות יקבלו דו"ח התנהגות מפורט ופשוט להבנה הכולל מידע מפורט על הדגימות ועל ההתנהגויות שנצפו במהלך הניתוח ב-Sandbox בענן. אנחנו מציגים לא רק דגימות שנשלחו ל-ESET LiveGuard Advanced, אלא גם את כל מה שנשלח למערכת ההגנה מבוססת מוניטין בענן של ESET LiveGrid® - ESET.

ניידות

כיום, העובדים נעים כל הזמן ולא תמיד פיזית במשרדי הארגון, ESET LiveGuard Advanced מסוגל לנתח קבצים ללא תלות במיקום הפיזי של המשתמשים או התחנות. היתרון המשמעותי הוא שבמקרה של זיהוי נזוקה, הארגון כולו מוגן מפני האיום באופן מיידי.

פרטיות

ESET מתייחסת לפרטיות ולעמידה בתקנות ברצינות רבה. באמצעות הגדרה פשוטה, המשתמש יכול להגדיר מחיקת דגימות אוטומטית מיד לאחר הניתוח.

מהירות ללא תחרות

כל דקה חשובה. ESET LiveGuard Advanced מסוגל לנתח את מרבית הדגימות בפחות מ-5 דקות. אם הדגימה כבר עברה ניתוח בעבר, כל הארגון יהיה מוגן תוך מספר שניות.

מוכח ואמין

חברת ESET נמצאת בתעשיית האבטחה כבר למעלה מ-30 שנים, וממשיכה לפתח את הטכנולוגיה כדי להיות צעד אחד לפני האיומים החדשים ביותר. זו הסיבה לכך שמעל מיליארד משתמשים בעולם מוגנים על ידי ESET. הטכנולוגיה שלנו עוברת ביקורת ותיקוף באופן קבוע על ידי גופים חיצוניים עצמאיים שמוכיחים פעם אחר פעם עד כמה הגישה שלנו מועילה בעצירת איומים חדשים.

הגנה פרו-אקטיבית

אם הדגימה נמצאה כחשודה, הפעלתה תיחסם עד שהניתוח שלה יסתיים ע"י ESET LiveGuard Advanced.

כך אנו מונעים מהאיומים הפוטנציאליים ליצור נזק במערכת של המשתמש. בנוסף, בסיום הניתוח, אם אותר איום בתחנת קצה אחת, המידע הזה מועבר תוך דקות לכל תחנת קצה ברשת הארגון, מה שמגן באופן מיידי על כל משתמש שעשוי להיות בסכנה.

מקרים לשימוש

כופרות

הגנה מותאמת אישית לתפקידים שונים בחברה

מקרה לדוגמה

לכל תפקיד בחברה נדרשת רמת אבטחה שונה. מגבלות האבטחה שיש להציב על מפתחים או אנשי IT שונה מאמצעי האבטחה שיש להציב על מנהל משרד או מנכ"ל.

פתרון

✓ הגדירו מדיניות ייחודית לכל מחשב או לכל שרת באמצעות ESET LiveGuard Advanced

✓ החילו מדיניות שונה באופן אוטומטי על בסיס קבוצות משתמשים סטטיות או על בסיס קבוצות Active Directory.

✓ שנו את ההגדרות באופן אוטומטי על ידי הזנת המשתמש מקבוצה אחת לקבוצה אחרת.

מקרה לדוגמה

ברוב המקרים כופרות חוזרות לארגון באמצעות תיבת הדוא"ל של המשתמשים.

פתרון

✓ ESET Mail Security מעביר את הקבצים המצורפים החשודים באופן אוטומטי ל-ESET LiveGuard Advanced.

✓ ESET LiveGuard Advanced מנתח את הדגימה, ומחזיר את תוצאות הבדיקה ל-Mail Security לאחר 5 דקות במרבית המקרים.

✓ ESET Mail Security מזהה את הקבצים המצורפים שמכילים תוכן זדוני ומנטרל אותם באופן אוטומטי.

✓ הקובץ המצורף הזדוני לא מגיע לנמען אף פעם.



VERY SUSPICIOUS

SHA-1: 1872A482C41DC305DF80A95CCD9811B4E82AFD2C
Category: Executable

ADVANCED SCANNING ENGINES

Advanced Unpacking And Scanning

The sample undergoes static analysis and state-of-the-art unpacking and is then matched against an enriched threat database.
Sample is malicious

Advanced Machine Learning Detection

Static and dynamic analysis is performed by an array of machine learning algorithms, including deep learning.
Sample is clean

BEHAVIORAL ANALYSIS SANDBOX

Experimental Detection Engine

A sample is executed in "sandboxes on steroids" that closely resemble full-scale user devices and that are subsequently monitored for any sign of malicious behavior.
Sample is suspicious

In-Depth Behavioral Analysis

The memory dumps produced by previous ETD layers are subject to an in-depth behavioral analysis that identifies known malicious patterns and chains of actions.
Sample is malicious

ANALYZED BEHAVIORS

Anti-Debug Trick

Sample tries to detect if it is debugged or run in a controlled environment.
Malicious causes: A lot of malware does this to hide its presence or make life of an analyst harder.
Benign causes: Used by packers and protectors.

✗ Anti-Debug Trick	Behaviour not detected
✗ Anti-Debug Trick	Behaviour not detected
✗ Anti-Debug Trick	Behaviour not detected

קבצים לא ידועים או חשודים מקרה לדוגמה

במקרים מסוימים, העובדים בחברה או אנשי ה-IT שלה ירצו לבדוק פעם נוספת האם הקובץ בטוח.

פתרון

✓ כל משתמש יכול לשלוח דגימה לבדיקה באופן ישיר מכל אחד ממוצרי ESET.

✓ הדגימה מנותחת במהירות על ידי ESET LiveGuard Advanced.

✓ אם הדגימה התגלתה כזדונית, כל תחנות הקצה בארגון מוגנות מפניו.

✓ מנהל ה-IT יכול לדעת באופן שקוף לחלוטין מי המשתמש ששלח את הדגימה והאם הקובץ התגלה כתקין או כזדוני.



מאפיינים טכניים של ESET LiveGuard Advanced

שליחת דגימה ידנית

כל משתמש או מנהל רשת יכול לשלוח דגימה לניתוח באמצעות מוצר תואם של ESET ולקבל את התוצאות המלאות, בכל זמן נתון. מנהלי הרשת יראו מי שלח מה ואת תוצאות הניתוח בממשק הניהול ESET PROTECT.

הגנה על תיבת הדוא"ל

ESET LiveGuard Advanced עובד לא רק עם קבצים על המחשב, אלא גם יחד עם ESET Mail Security, כדי לוודא שהודעות דוא"ל וזדוניות לא מגיעות לארגון. כדי להבטיח את המשך הפעילות התקינה של הארגון, רק הודעות שמגיעות מחוץ לארגון יכולות להישלח ל-ESET LiveGuard Advanced לבדיקה.

הגנה אוטומטית

לאחר הגדרת המוצר, המשתמש ומנהל הרשת לא צריכים לעשות עוד דבר. מוצר ההגנה לתחנת הקצה או לשרת מחליט באופן אוטומטי האם הדגימה נקייה, נגועה או לא מוכרת. אם הדגימה לא מוכרת, היא נשלחת ל-ESET LiveGuard Advanced לבדיקה. לאחר שהבדיקה מסתיימת, התוצאה משותפת לכל החברה ומוצרי הגנת תחנות הקצה מגיבים במידת הצורך.

התאמה אישית לצרכי הארגון

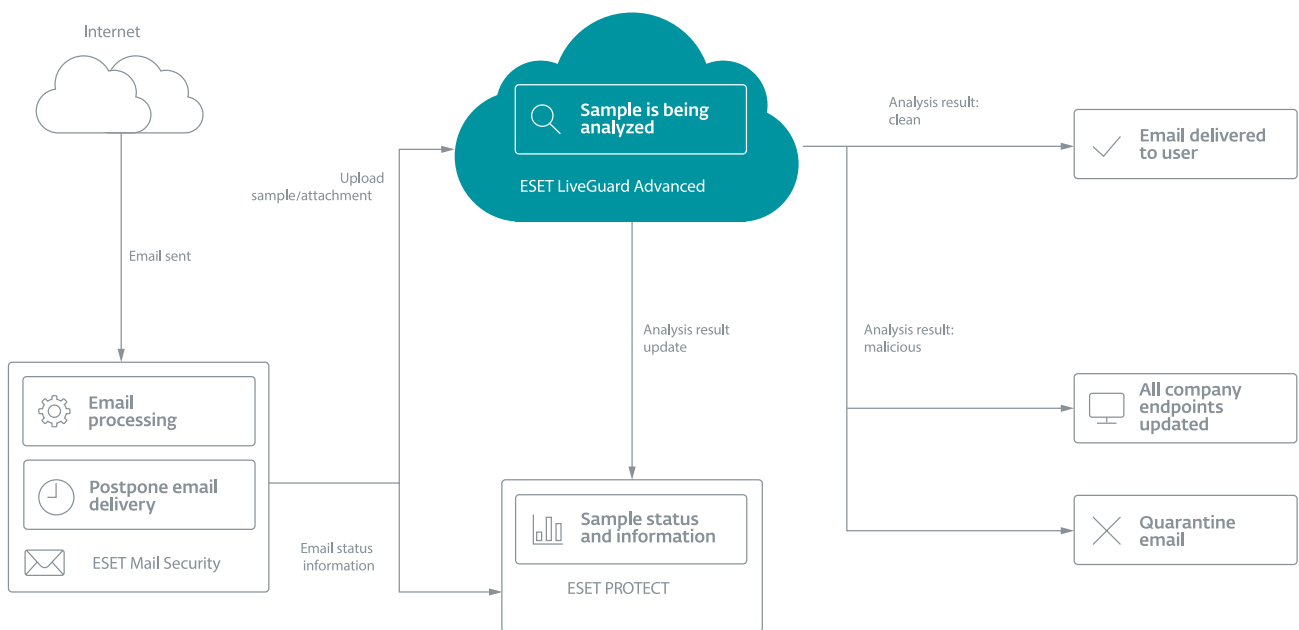
מוצרי ESET מאפשרים הגדרת מדיניות מפורטת לכל מחשב ומחשב ב-ESET LiveGuard Advanced כך שמנהל ה-ID יכול לשלוט במה שנשלח לבדיקה ובפעולות שצריכות להינקט לאחר שהתוצאה מגיעה.

FILE	STATUS	START	FIRST SENT ON	LAST PROCESSED ON	COMPUTER	CATEGORY	REASON	SENT TO	HASH	SIZE	USER
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	3A2C6A53760090883A6E711C...	198 KB	NT AUTHORITY\SYSTEM
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	CA12C3448911108A0F320012...	1 MB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	8F9846A5C652A502A000589F...	508 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	1076A03278A1983753009F...	870 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	1844488C7A68C278108F012F...	50 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	18329616420895780202783E...	15 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	3A017E5C20F4288940C1C2054E...	37 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	00A78D1778A75F0C8C80671...	6 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	4F532087F96600002323A2C8...	511 KB	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	4203982832000540141A199...	28 B	SYSTEM Administrator
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	9A04C02002A04020292A2...	5 MB	NT AUTHORITY\SYSTEM
K:\Users\..._13032714789F	Failed	2018 Mar 9 13:03:52	2018 Mar 9 13:03:51	2018 Mar 9 13:03:51	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	08157043107070815C18621...	403 KB	SYSTEM Administrator

שקיפות מלאה – ניתן לצפות בכל הדגימות שנשלחו ל-ESET LiveGrid®

כיצד ESET LiveGuard Advanced עובד?

עם ESET Mail Security DV



ESET LiveGuard Advanced תואם למוצרי ההגנה של ESET לתחנות הקצה, לשרתים וליישומי Microsoft 365 והוא משתלב באופן מלא עם ממשקי הניהול של ESET.

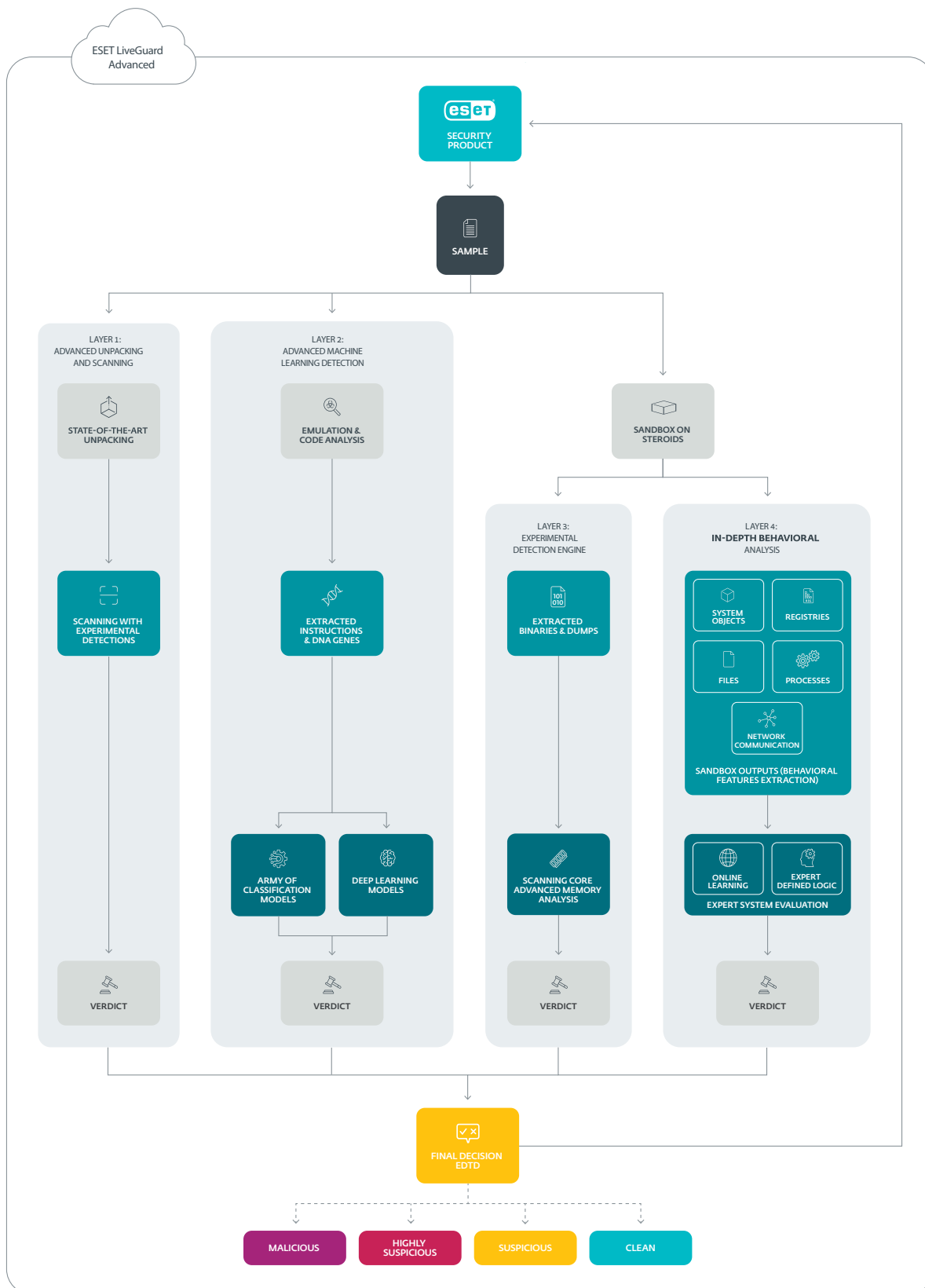
“מוצר מעולה”

מה אתה הכי אוהב בו?

“אני אוהב את קלות ההפצה לכל תחנות הקצה בארגון ואת המהירות בה המוצר מאבטח את הרשת הארגונית. מצאתי תוכנות לא-רצויות ואני מקבל הודעות דוא”ל שמעדכנות אותי על עצירת איומים. אני ישן טוב יותר בלילה כשאני יודע שהרשת שלי מוגנת ע”י ESET.”

מייקל פ. / מנהל רשת / (51-1,000 עובדים)

כיצד האנליזה והניתוח המתקדם שלנו עובד?



ESET LiveGuard Advanced משתמש בארבע שכבות זיהוי נפרדות כדי להבטיח את שיעור הזיהוי הגבוה ביותר. כל שכבה משתמשת בגישה אחרת ומספקת הכרעה בנוגע לדגימה. התוצאה הסופית מורכבת מכל המידע שהתקבל על הדגימה.

שכבה 1

הפצה וסריקה מתקדמים

הדגימות עוברות ניתוח קוד סטטי על ידי מנגנון מתוחכם, ולאחר מכן עוברות להשוואה מול בסיס מידע הנוגע לאיומים.

שכבה 2

זיהוי מתקדם באמצעות Machine Learning

ניתוח סטטי ודינמי מתבצעים באמצעות מערך אלגוריתמים של Machine Learning המשתמשים בטכנולוגיות כמו Deep Learning.

שכבה 3

מנוע זיהוי ניסיוני

הדגימות מנותחות ב-Sandbox מתקדם בענן המדמה סביבת משתמש אמיתית, ועוברות ניטור כדי לזהות כל סימן של התנהגות זדונית.

שכבה 4

ניתוח התנהגותי מעמיק

הממצאים של ה-Sandbox בענן מועברים לניתוח התנהגותי מעמיק שמזהה תבניות ודפוסי פעולה זדוניים מוכרים.

הפתרון משלב את כל התוצאות משכבות הזיהוי ומעריך את סטוס הדגימה. התוצאות נשלחות לתחנות הקצה באמצעות מוצרי האבטחה של ESET ולתשתית הארגון

מהירות ללא תחרות

ניתוח ב-Sandbox ייעודי בענן תוך 5 דקות



היתרון בזיהוי

ESET LiveGuard מופעל



ESET LiveGuard כבוי



יתרון ממוצע של

135 דקות

קצת על ESET

מבלי לעצור ותוך מינימום צריכת משאבים. בין לקוחותינו בישראל ניתן למנות משרדי ממשלה ועיריות, מוסדות חינוך ובריאות, חברות היי-טק ועסקים במגוון תחומים רחב.

www.eset.com/il

ESET היא חברת תוכנה בינלאומית ויצרנית אבטחת המידע מס' 1 באיחוד האירופי.

עם ניסיון של 30 שנים, אנחנו מפתחים פתרונות הגנה לתחנות קצה המצטיינים במניעה, זיהוי ותגובה לאירועי סייבר, ומאפשרים לארגונים להתמקד במטרותיהן

ESET במספרים

1 מיליארד
משתמשים
ברחבי העולם

400k+
לקוחות עסקיים

200+
נציגויות
בעולם

13
מרכזי מו"פ
עולמיים

בין לקוחותינו



מוגנת ע"י ESET
מאז 2017;
מעל 14,000 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 אבטחה מאז 2008;
למעלה מ-2 מיליון לקוחות

מחויבים לרמת האבטחה הגבוהה ביותר



ESET זכתה בחותמת איכות במבדק שבדק פתרונות עסקיים בדצמבר 2021 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



פתרונות ההגנה של ESET זוכים להכרה באופן עקבי על ידי גופים עצמאיים מובילים. לדוגמה בדו"ח של Forrester הבודק יכולות זיהוי ותגובה של איומי Zero-day לשנת 2021