



# VULNERABILITY & PATCH MANAGEMENT

ממשק למעקב אחר פרצות ופגיעויות בכל תחנות  
הקצה ותיקון באופן פעיל

# מה זה ESET Vulnerability & Patch Management

פתרון ESET Vulnerability & Patch Management עוקב באופן פעיל אחרי חולשות ופרצות במערכות הפעלה ובאפליקציות נפוצות, ומאפשר התקנה אוטומטית של תיקון (טלאי) אבטחה בכל תחנות הקצה שמנוהלות על ידי ממשק הניהול שלנו

סריקה אוטומטית של התוכנות בתחנות הקצה בארגון ושל אפליקציות צד-שלישי, הכוללת דיווח מיידי לממשק הניהול, ומאפשרת שקיפות מיידית לחולשות. כדי להבטיח הגנה מתמשכת בארגון, ניתן להגדיר התקנה אוטומטית של תיקון אבטחה באמצעות בחירה באסטרטגיית עדכונים (עדכון כולל, עדכון חלקי, עדכון כולל עם החרגה) והגדרת זמנים ספציפיים בהם העדכון צריך להתרחש.



# תזמון התקנת תיקון אבטחה עבור מערכות ההפעלה והאפליקציות

בנוסף, נעשה שימוש בטכניקות תיעדוף מתקדמות וכלים לאוטומציה של תהליכי עבודה, על מנת לאפשר התאמה גבוהה ככל האפשר לצרכי התשתית של הארגון.

הפתרון הוא חלק מפלטפורמת ESET PROTECT, ולכן הוא לא רק מספק הערכה מתמשכת של פרצות הכוללת תיעדוף מבוסס-סיכון וצעדי טיפול, אלא גם מגן מפני איומים שאינם מוגדרים פרצות שמקורן בתוכנות. הפתרון מאפשר לכם הגנה ברמה ארגונית מפני נזקות מכל הסוגים, לרבות כופרות, וכן מניעה של איומי Zero-day בכל תחנות הקצה, השרתים ותיבות הדוא"ל – והכל מתוך ממשק ניהול מרכזי.

התקנה של תיקון אבטחה לטיפול בפרצות המתגלות במערכות ההפעלה ובאפליקציות היא בעלת חשיבות עליונה, וגם כיום היא עדיין אחת מהמשימות התובעניות ביותר של צוותי ה-IT.

ESET Vulnerability & Patch Management מספק שכבת הגנה נוספת לארגונים הזקוקים לכך שכל התוכנות שלהם יהיו מעודכנות, אך אין להם את משאבי ה-IT הנדרשים כדי לעמוד בדרישה הזו.

הפתרון מזהה פרצות ומטפל בהן או מונע ניצול שלהן באמצעות התקנת תיקוני האבטחה החדשים ביותר לאפליקציות ולמערכות ההפעלה, בכל תחנות הקצה.

## מאפיינים עיקריים

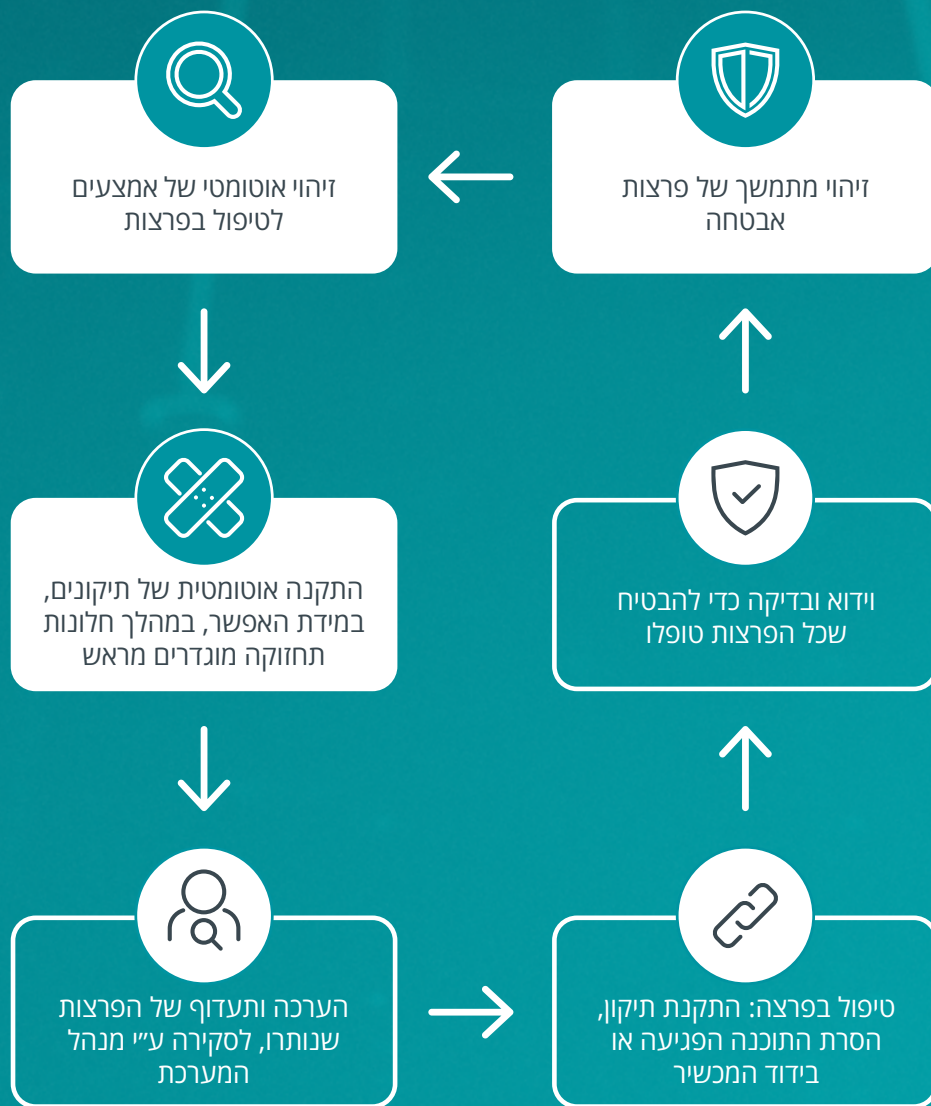
### ניהול התקנת תיקון אבטחה

- הפעלה של עדכונים והתקנה של תיקוני אבטחה באופן מיידי באמצעות אפשרויות הניתנות להתאמה אישית או באופן ידני
- הפיכה של תהליך התקנת תיקון האבטחה לפשוט יותר: הגדירו תעדוף גבוה יותר לנכסים קריטיים והשאירו את עדכון יתר הנכסים לשעות שאינן עמוסות כדי למנוע הפרעה.
- ניהול רישום ומעקב של מקרים ספציפיים של תיקונים שלא הותקנו.
- הפתרון מספק רשימה עדכנית של תיקוני האבטחה הכוללת את שם התיקון, גרסת התוכנה החדשה, CVE, מידת החומרה/חשיבות של התיקון ואפליקציות מושפעות.
- כל התיקונים זמינים מתוך ממשק ESET PROTECT בענן.

### הערכת חולשות ופרצות

- סריקה של אלפי אפליקציות, כמו Adobe Acrobat, Zoom, Mozilla Firefox, יחד עם תמיכה במספר גרסאות Windows (בקרוב תתווסף תמיכה macOS -)
- זיהוי מעל 35,000 חולשות ופגיעויות ידועות (CVEs) – והמספר הולך וגדל
- סריקות אוטומטיות באמצעות הגדרות תזמון הניתנות להתאמה אישית
- תיעדוף וסינון של פרצות לפי ניקוד החשיפה והחומרה של כל אחת מהן
- דו"חות פגיעויות של התוכנות והמכשירים הפגיעים ביותר
- תמיכה בניהול מאוחד, בסביבות רשת מורכבות, אפשרות לצפייה בפרצות בחלקים ספציפיים של הארגון
- בסיס נתונים של פרצות, CVSS 2.0 ו-CVSS 3.1
- סקירה מאוחדת באמצעות ממשק ESET PROTECT בענן, הכולל תמיכה במספר שפות ואינו מקשה על תשתית ה-IT שלכם

# איך זה עובד?



צעדים אוטומטיים

צעדים ידניים

# מקרים לדוגמה

המספר ההולך וגדל של עובדים מרחוק והאימוץ של שירותי ענן אמנם הפכו את מרחב האיומים למגוון יותר כך שכיום הוא לא כולל רק פרצות אבטחה. עם זאת, התקנת תיקוני אבטחה לאפליקציות ולמערכות הפעלה היא עדיין חלק קריטי במניעת תקריות אבטחה.

כפי שכל מנהל רשת יגיד לכם, התקנת תיקונים לפרצות אבטחה היא אחת מהמשימות התובעניות יותר ב-IT. כשהמשאבים הקיימים כבר נמתחו לקצה שלהם, התקנה של תיקוני אבטחה נדחית פעם אחר פעם ופרצות אבטחה יכולות להתפתח כמעט ללא הפרעה. עלייה במורכבות סביבת ה-IT יכולה להוביל גם לירידה בתיאום בין צוותים מרובי-תפקידים, לפערי ציוד ולשקיפות מוגבלת כלפי מרחב האיומים.

## אנחנו לא עומדים בקצב התקנת תיקוני האבטחה

## מחסור במשאבי IT

### הבעיה

אני צריך שהאפליקציות שלנו יהיו מעודכנות, אך אין לי את משאבי ה-IT כדי לבצע זאת

### הפתרון

נצלו את היתרונות של ניהול אוטומטי מלא של הערכת פרצות והתקנת תיקוני אבטחה, ושל התמיכה של ESET:

✓ סריקה אוטומטית של התוכנות והאפליקציות החיצוניות בתחנות הקצה בארגון, הכוללת דיווח מיידי לממשק הניהול ומאפשרת שקיפות מיידית לפרצות אבטחה.

✓ כדי להבטיח הגנה מתמשכת על הארגון, הגדירו התקנה אוטומטית של תיקוני אבטחה באמצעות בחירה באסטרטגיית עדכונים (עדכון כולל, עדכון חלקי, עדכון כולל עם החרגה) והגדרת מועדים ספציפיים בהם העדכון צריך להתרחש.

### הבעיה

צוות ה-IT שלנו עמוס מדי, ולא מצליח לעמוד בקצב התקנת תיקוני האבטחה.

### הפתרון

✓ נצלו את היתרונות של טכניקות תעדוף ואוטומציה מתקדמות

✓ הגדירו תדירויות מיטביות לביצוע סריקה וסנכרנו ביניהן ובין מועדי התקנת התיקונים כדי לטפל בפרצות אבטחה רלוונטיות הניתנות לניצול לרעה, מבלי להעמיס על צוותי ה-IT שלכם

✓ בצעו סינון של פרצות האבטחה על פי מידת החומרה שלהן. הגדירו תעדוף של פרצות המהוות סיכון עסקי משמעותי

✓ התאימו אישית את מדיניות התקנת התיקונים. הגדירו תעדוף של נכסים קריטיים באמצעות טיפול ידני בפרצות חמורות, ולאחר מכן הגדירו התקנת תיקונים אוטומטית בנכסים אחרים מחוץ לשעות העומס כדי למנוע הפרעות

✓ נהלו רישום של החרגות בהתקנת תיקונים, הימנעו ממעקב אחר כל תיקון באופן פרטני

# אתגרים בתיאום צוותים מורכבים

## הבעיה

תשתית ה-IT שלנו הופכת למורכבת יותר ויותר, מה שהופך את התיאום בין צוותים מרובי-תפקידים למאתגר יותר

## הפתרון

נצלו את היתרונות של פלטפורמת ESET PROTECT, המאפשרת לכם לנהל את ESET Vulnerability & Patch Management ואת יתר מערך האבטחה המגן על כל הנכסים הדיגיטליים והציוד

✓ הביאו משימות אבטחת וניהול IT שונות לממשק ניהול אחד והפכו אותן לאוטומטיות באמצעות פלטפורמת ESET PROTECT, הכוללת את ESET Vulnerability & Patch Management

✓ נצלו את יתרונות התמיכה של ESET Vulnerability & Patch Management & בניהול מאוחד: קבלו שקיפות מלאה לכל הרשת תוך כדי יכולת להתמקדות באזור הספציפי שלכם

✓ נהלו רשימת מלאי מעודכנת וטפלו בכל השטחים המתים של ניהול התשתית

✓ נצלו את היתרונות של אסטרטגיות המניעה, הזיהוי והתגובה של ESET PROTECT כדי לצמצם את החשיפה שלכם לאיומים שאינם מוגדרים כחולשות שמקורן בתוכנות

✓ פתרון ESET Vulnerability & Patch Management הופך את העמידה שלכם בתקנות רגולציה, כמו GDPR, HIPAA, PCI DSS ואחרים לפשוט יותר

# שקיפות מוגבלת של מערך ה-IT

## הבעיה

אין לי שקיפות מלאה בנוגע לאבטחה של מערך ה-IT

## הפתרון

נצלו את היתרונות של התצוגה המרכזית שאתם מקבלים כחלק מפתרון ESET PROTECT בענן

✓ קבלו שקיפות מלאה לתחנות הקצה, הרישיונות ומצב הפרצות ועדכוני האבטחה של כל הנכסים בארגון. הנתונים מתעדכנים באופן מיידי עם כל שינוי.

✓ צפו בסטטוס אבטחת ה-IT שלכם בזמן אמת דרך הממשק של ESET PROTECT בענן

✓ התחברו בכל זמן, מכל מקום ומכל דפדפן – כך תוכלו להגיב באופן מיידי

✓ צרו דו"חות רלוונטיים שיאפשרו לכם למדוד את האפקטיביות וההתקדמות של מדיניות ניהול הפרצות והתקנת תיקוני האבטחה שלכם.

ניצד לרכוש:

ESET Vulnerability & Patch Management מגיעה רק כחלק מהפתרונות הבאים:

 PROTECT COMPLETE

 PROTECT ELITE

# ESET אודות

כשאלה משולבים עם חקר ומודיעין האינפורמטיבי 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](http://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

מעל 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,  
שנת 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

