kaspersky BRING ON THE FUTURE

אבטחה מיטבית עם Kaspersky

להשיג רמה מיטבית של אבטחת סייבר עם הגנה מנוהלת
ויכולות התומכות בענן לזיהוי ולתגובה בנקודות הקצה

האתגר

על העסק שלך צריך להגן ביעילות מפני איומים חדשים, בלתי-ידועים וחמקמקים, מבלי להכביד על הזמן והמשאבים המוגבלים שלך.

ב-30% מהתקפות הסייבר שמצליחות מעורבים כלים לגיטימיים של המערכת[1]

גם ככה אין מספיק משאבים לכסות הכול

כדי לספק את היתרון הנוסף הנחוץ כיום לאבטחה בנקודות קצה, צריך לפתח, בתוך הארגון, יכולות מתאימות של תגובה לתקריות.

אבל העלויות הכרוכות בפרויקט כזה יכולות לצאת משליטה במהירות:

- עלויות התוכנה והחומרה יכולות להצטבר
- כלים ותהליכים של אבטחה, המפורדים ומפוזרים במבני סילו, שוחקים את יעילות האבטחה
- משימות שגרתיות עלולות לבזבז המון זמן.

צריך לחזק את ההגנה בנקודת הקצה

ההתקפות החמקמקות כיום נעשות יעילות יותר ויותר, משום שהפושעים משתמשים בכלי מערכת לגיטימיים ובשיטות ובטכנולוגיות מוכנות אחרות, מה שמאפשר להם לקבל גישה, לשרוד ולבצע פעולות זדוניות בתוך התשתית שלך, מהר יותר ומבלי להתגלות.

המצב בעייתי עוד יותר לאור התפוררות ההגנה ההיקפית והעלייה בעבודה מרחוק, ולכן נקודות הקצה – שהן בדרך כלל נקודת הכניסה הכי אטרקטיבית אל התשתית שלך – זוכות לעוד יותר התייחסות.

ההתקפות המתקדמות במגמת עלייה

האיומים החמקמקים הקיימים היום – שנועדו לעקוף ביעילות הגנות רגילות בנקודות הקצה – טומנים בחובם סיכונים הרבה יותר משמעותיים לעסקים מכפי שהיה עד כה, משום שקשה יותר ויותר לזהות התקפות, לנתח אותן ולהגיב להן. אם איום שלא זוהה יצליח להתבסס בתשתית שלך, הדבר עלול להוביל להפסדים משמעותיים, שישפיעו על השורה התחתונה של העסק:

- שיבוש של תהליכים קריטיים לעסק
- פגיעה משמעותית במוניטין ואובדן לקוחות
- קנסות, עונשים והפסד רווחים.

הפתרון

Kaspersky Optimum Security מספק פתרון אפקטיבי לזיהוי איומים ולתגובה להם, עם ניטור אבטחה כגיבוי מסביב לשעון, תגובות אוטומטיות לאיומים וציד איומים אוטומטי, בנוסף לתמיכה ולהכוונה מהמומחים של Kaspersky.

45% מההתקפות התגלו עקב קבצים חשודים או פעילות חשודה בנקודות קצה[1]

רמות השקעה מיטביות

אין צורך בגיוס אנשים נוספים, בהדרכה חוזרת של עובדים או בהסתבכות בפריסה מורכבת – Kaspersky Optimum Security מפשט תהליכים אוטומטיים וחיוניים של תגובה לתקריות, ומסייע בהם – בדיוק לפי הדרישות שלך.

הוא מותאם לצרכים שלך, עם אפשרויות ליישומים מקומיים ובענן ועם ערכה מוכנה של כלי אבטחה, שעוזרת לך להגביל מורכבות של מערכות IT, להגביר פרודוקטיביות של משתמשים ולשמור על עלויות הטמעה שקופות.

פתרון מוכן מהיר ומדרגי (סקלבילי)

שיטות מניעה אוטומטיות הן הבסיס לכל הגנה על נקודות קצה, אך יש לצרף להן כלים מתקדמים כדי להתמודד עם האיומים החמקמקים והמסוכנים יותר.

Kaspersky Optimum Security נותן יכולות של זיהוי מתקדם ותגובה מהירה – והכול מסופק יחד מהענן. כעת, מהנדסי אבטחת הסייבר שלך יוכלו להתמודד במהירות ובדיוק גם עם איומים שפעם גרמו להם לאבד שלווה.

הגנה מתקדמת מפני איומים

להשיג איזון מיטבי בין פשטות לאפקטיביות, תבונה אנושית ואוטומציה, יעילות ופוקנציונליות – בלי להמר על ההגנה שלך!

Kaspersky Optimum Security עוזר לך למזער את הסיכון להפסיד כסף, לקוחות ואת המוניטין שלך, ומתגבר את ההגנות שלך מפני איומים חדשים, לא ידועים וחמקמקים. כך תהיה מוכן להתמודדות עם זירת האיומים העכשווית, המתפתחת במהירות.

יתרונות עיקריים

- להישאר בחזית העדכונים ולהגן על העסק שלך מפני הסיכון הממשי לנזק ולשיבושים עקב הגל האחרון של איומים חמקמקים והרסניים
- לפתח יכולת תגובה לתקריות משלך, עם ערכת כלים פשוטה לזיהוי ולתגובה בנקודות קצה (EDR)
- ירידה משמעותית בסיכוני ההדבקה, הודות להדרכת העובדים ולהגברת המודעות שלהם לאבטחה
- שימור משאבים יקרים על-ידי אוטומציה של פעולות ופונקציונליות מנוהלת
- חיסכון בזמן ובמאמצים, עם פתרון שכל תכונותיו מנוהלות ממסוף יחיד, מקומי או בענן

יכולות עיקריות

55% מההתקפות התגלו רק אחרי כמה שבועות או יותר[1]

Kaspersky Optimum Security מציע מערך פונקציונליות נרחב להגנה מפני איומים חמקמקים, שבמרכזו הזיהוי, הניתוח והתגובה.

תגובה אוטומטית

- יכולת תגובה 'בלחיצה אחת' מאפשרת לך להכיל במהירות תקריות פרטניות
- תגובה מודרכת המבוססת על ניסיון המומחים של Kaspersky מאפשרת לך להתמודד גם עם האיומים הכי מורכבים ומסוכנים
- תגובה אוטומטית בין נקודות קצה שונות עוזרת לך למצוא איומים מנותחים או מיובאים בכל חלקי הרשת ולהגיב להם

חקירה מפושטת

- כל המידע הקשור לתקרית מסוימת נאסף באופן אוטומטי בכרטיס תקרית יחיד
- ייצוג חזותי ותהליך חקירה פשוט מאפשרים לך לנתח במהירות וביעילות את התקרית, בסביבה יחידה, ולהחליט על המשך הפעולה
- במקביל, כל גילוי לפי מחווני ההתקפה זוכה לעדיפות ולחקירה של Kaspersky, כדי לספק לך המלצות המותאמות לך

זיהוי מתקדם

- אלגוריתמים לניתוח התנהגות הבנויים על Machine learning, לחשיפה מהירה ומדויקת של התנהגויות חשודות
- ציד איומים אוטומטי הבנוי על מחווני התקפה קנייניים, לאיתור של איומים מורכבים ומוסתרים, עם תמיכה מהמומחים של Kaspersky
- בקרת חריגות אדפטיבית, לכוונון אוטומטי של תצורת הכלים המשמשים לצמצום שטח התקיפה לפי פרופילי משתמשים

איך ליישם

Kaspersky Optimum Security כולל כמה כלים ויכולות עיקריות, שבהם אפשר לעשות שימוש אפקטיבי כדי למנוע איומים, לזהות אותם ולהגיב להם, בשלבים שונים בהתקפה:

Rooting
שימוש במערך שלם של כלים – כלים לגיטימיים וכלים מקוריים של המערכת – כדי להשיג התמדה ולהתחיל בתנועה אופקית, במידת הצורך

התקנה
ההדבקה הראשונית פורסת את הרכיבים הנחוצים, מתקשרת עם שרת שליטה ובקרה[1], וחוקרת את סביבתה

חדירה
המשתמש מקבל הודעת פישינג בדוא"ל, או ניגש אל משאב אינטרנט זדוני, ומדביק את המחשב המארח

מנגנוני זיהוי מתקדמים, לרבות ניתוח התנהגות הבנוי על למידת מכונה וארגז חול (Sandbox)

מודעות לאבטחה אצל עובדים

Root cause analysis and IoC[3] scanning

Automated threat hunting with IoAs[2]

צמצום שטח התקיפה

תרחישי תגובה אוטומטיים, מונחים ומרוחקים

מניעת איומים אוטומטית

[1] שליטה ובקרה
[2] אינדיקטורים של התקפה
[3] אינדיקטורים שלפגיעה

מהתקפות הסייבר שמצליחות 31% כוללות הודעות זדוניות בדוא"ל, כלומר, העובדים עצמם יכלו למנוע הרבה מהן[1]

הגנה מתוגברת

באפשרותך להוסיף ולחזק את ההגנות שלך עם מגוון כלים המיועדים להיבטים השונים באבטחה שלך – זיהוי, חקירה ומודעות.

האנשים הם המפתח לאבטחה

המפתח לצמצום שטח התקיפה שלך ומספר התקריות הוא להדריך את העובדים כך שתהיה להם מודעות לאיומי הסייבר שאליהם הם עלולים לחשוף את התשתית שלך, עקב רשלנות או חוסר ידע. **Kaspersky Security Awareness** בונה את הידע והמיומנויות שכל העובדים צריכים להגנה על התשתית שלך, כדי שיפעלו יחד אתך לשמירה על סביבת סייבר בטוחה.

יתרון נוסף בחקירות

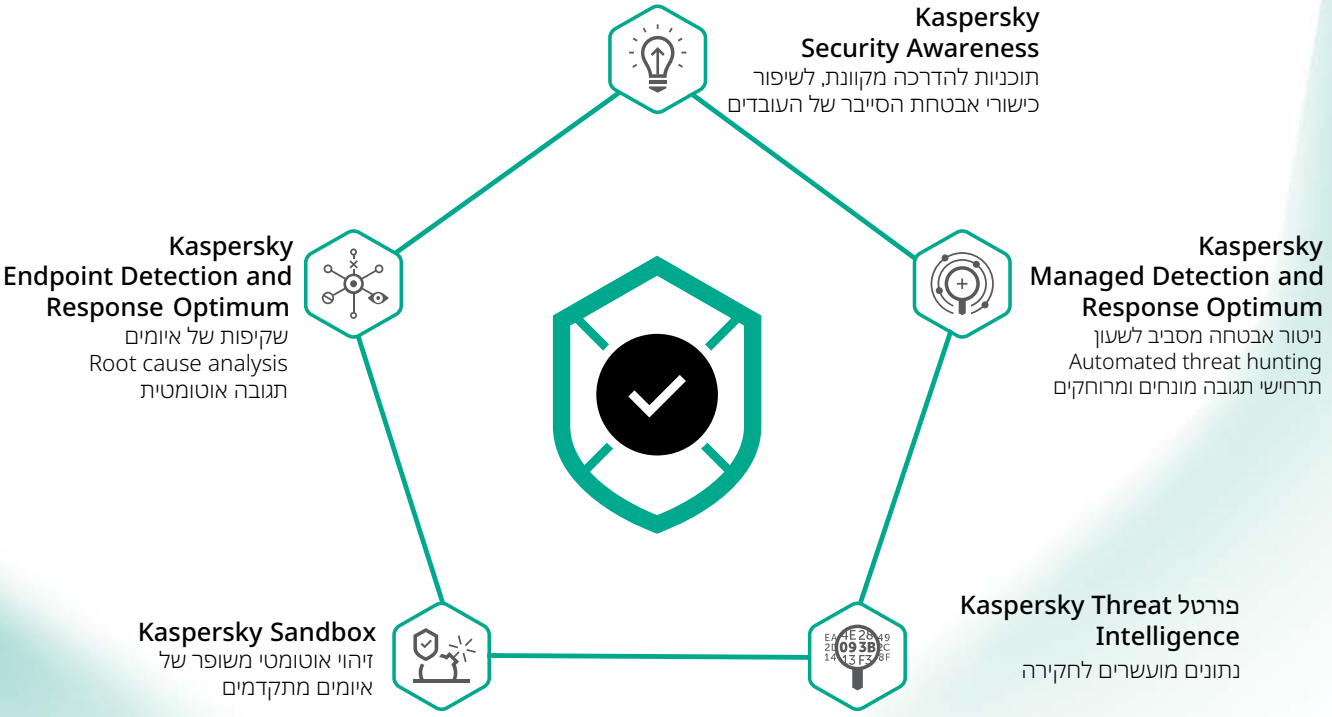
עזור למומחים שלך לאבטחת סייבר לנתח ולהבין איומים באופן יסודי ומהיר יותר, עם המידע העדכני ביותר על קבצים, קודי HASH, כתובות IP וכתובות URL הקשורים לאיומים. את התובנות הנוספות האלה תקבל ללא עלות נוספת מ**פורטל Kaspersky Threat Intelligence** הידידותי למשתמש.

שכבת זיהוי נוספת

לחשוף איומים חדשים ולא ידועים באופן אמין ומהיר יותר עם **Kaspersky Sandbox** – לניתוח אוטומטי של איומים בסביבה מבודדת, באמצעות אלגוריתמים לזיהוי, המוגנים בפטנט, ושיטות למניעת התחמקות. התגובות המוגדרות מיושמות באופן אוטומטי על האיומים שהתגלו, וכך משפרות משמעותית את יכולות הגילוי שלך, ללא צורך בניהול אחרי הפריסה ההתחלתית.

כיצד זה עובד

אפשר לבחור כיצד להשתמש ב-Kaspersky Optimum Security - בתור פתרון מנוהל להגנה מסביב לשעון, בתור ערכת כלי EDR ידידותיים למשתמש או בתור שילוב של השניים, כדי ליהנות מהניסיון ומהידע של המומחים של Kaspersky ובמקביל לפתח את יכולות פנימיות משלך לזיהוי ולתגובה. Kasperky Optimum Security מאחד כמה מוצרים בפתרון אחד:



בפעולה

לדברי 56% מהמשיבים, הארגונים שלהם נמצאים בסיכון עקב מחסור בעובדי אבטחת סייבר[2]

את Kaspersky Optimum Security קל לנהל ממסוף יחיד, כדי שתוכל להפיק כמה שיותר מהזמן ומהמשאבים המוגבלים שלך.

חיסכון בזמן ובמשאבים

- ההגנה המנוהלת עוזרת לארגונים, שאין להם מספיק עובדי IT או מומחיות, לבנות יכולות של זיהוי ותגובה, בלי ההשקעות באבטחה הנלוות לכך
- תהליכים חיוניים של אבטחת סייבר עוברים אוטומציה, כדי להגיב לתקריות מהר יותר ובאופן מדויק ויעיל יותר
- שיפור המודעות של העובדים לאבטחה פירושו חדירה של פחות איומים מבעד לאמצעי ההגנה – ולכן פחות תקריות שצריך לעבד!

ניהול קל

- מסוף הניהול בענן נותן שליטה מהירה ויעילה מכל מקום בעולם
- האפשרויות לפריסה מקומית או בענן נותנות את אותה חוויה של ניהול מערכת
- פריסה מהירה ובלי טרחה, גם אם עוד אין לך פתרונות של Kaspersky
- שליטה קלה ואינטואיטיבית בכל הכלים, בלי צורך בתהליך היכרות ממושך או בהדרכה חוזרת

החבילה המלאה

- חלק מהאקוסיסטם של Kaspersky, שבונה את ההגנות שלך מיסודות האבטחה ועד לתכונות מתקדמות ומיועלות
- את התכונות המגוונות של Kaspersky Optimum Security אפשר לנהל ממסוף ענן יחיד
- פתרון עם כמה שכבות הגנה, לטיפול באיומים רגילים וחמקמקים ובהזדמנויות לטעות אנוש

הגישה המדורגת של Kaspersky

ביחד, נוכל לבנות את ההגנות שלך על תשתית הגנה מהימנה עם Kaspersky Security Foundations, התומך בהתרחבות חלקה כדי לספק מענה חיוני לתקריות עם Kaspersky Optimum Security – ולבסוף צומח ליישום של כלים רבי-עוצמה שנועדו לספק הגנה מפני האיומים המתקדמים ביותר, עם Kaspersky Expert Security.

בחר בשלב שמתאים לך:

Kaspersky Expert System

היערכות להתקפות מורכבות ודמויות ATP, בארגונים שבהם יש:

- סביבות IT מורכבות ומבוזרות
- צוות בוגר לאבטחת IT או מרכז מבוסס לבקרת אבטחה (SOC)
- סלידה מסיכונים עקב העלויות הגבוהות של תקריות אבטחה ופריצות לנתונים
- התחשבות בציות לדרישות תקינה

אבטחה מיטבית עם Kaspersky

בניית הגנות מפני איומים חמקמקים עבור ארגונים עם:

- צוות קטן לאבטחת IT, עם מומחיות בסיסית באבטחת סייבר
- סביבת IT עם עלייה בהיקף ובמורכבות, המגדילה את שטח התקיפה
- מחסור במשאבי אבטחת סייבר – לעומת הצורך בשיפור ההגנה
- חשיבות גוברת לפיתוח של יכולת תגובה לתקריות

Kaspersky Security Foundations

חסימה אוטומטית של רובם הגדול של האיומים

- מניעה אוטומטית רב-וקטורית של תקריות הנגרמות עקב איומים רגילים – הרוב המוחלט של כל התקפות הסייבר.
- שלב היסודות בבנייה של אסטרטגיית הגנה משולבת, לארגונים בכל גודל או מידת מורכבות
- הגנה אמינה על נקודות קצה עבור ארגונים עם צוותי IT קטנים ומומחיות אבטחה הנמצאת בשלב הפיתוח

להסבר נוסף על המענה של Kaspersky Optimum Security לאיומי סייבר, תוך שימוש חסכוני במשאבים ובצוותי אבטחה, נא לבקר בכתובת: http://go.kaspersky.com/optimum.

1 דוח ניתוח תגובה לתקריות של Kaspersky לשנת 2019, Kaspersky, 2020

2 (ISC)2 מחקר על כוח אדם באבטחת סייבר, (ISC)2 2020

חדשות על איומי סייבר: www.securelist.com
חדשות אבטחת IT: business.kaspersky.com

www.kaspersky.com