אבטחה לכל אפליקציית AI בארגון

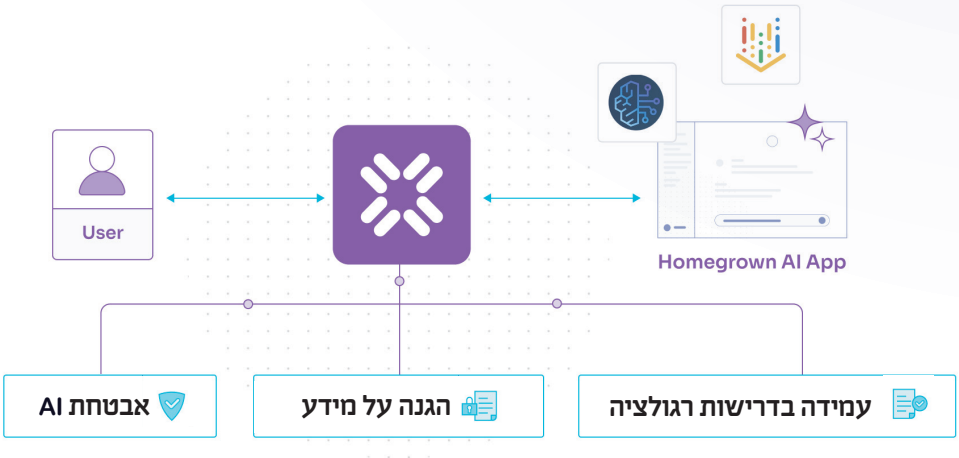
נראות, שליטה והגנה לכל יישום בינה מלאכותית

AI מאיץ צמיחה - אך גם מגביר סיכונים

ארגונים משלבים יותר ויותר יכולות AI במוצרים שלהם ומפתחים אפליקציות AI מותאמות בצורה אישית כדי לשפר תהליכי עבודה פנימיים, תמיכת לקוחות ופונקציות עסקיות קריטיות נוספות. לצד היתרונות העסקיים המשמעותיים, פתרונות אלו גם יוצרים סיכונים חדשים של דליפת מידע, הפרות רגולציה ואיומי סייבר. אבטחת אפליקציות אלו חיונית להגנה על פעילויות קריטיות, שמירה על תאימות רגולטורית והבטחת המשכיות והצלחה עסקית לאורך זמן.

פלטפורמה מאוחדת לאבטחת אפליקציות AI בארגון

Ovalix מאבטחת את אפליקציות וסוכני ה-AI הפנימיים של הארגון באמצעות מתן נראות מלאה, הגנה על מידע, אכיפת מדיניות רגולטורית והתגוננות מפני איומים מתקדמים-במטרה לתמוך ברציפות תפעולית ולהניע חדשנות עסקית. באמצעות הגנה על יישומי AI וסוכנים מותאמים אישית, Ovalix מאפשרת לארגונים לאמץ חדשנות-בביטחון, שליטה ואבטחה מלאה.



יתרונות מרכזיים

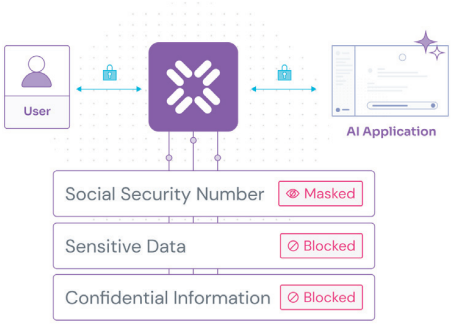
נראות מקיפה
קבלו נראות מלאה על הסכנות בשימושי ה-AI בארגון.

הגנת מידע מתקדמת
אבטחו מידע רגיש ומנעו חשיפה או דליפה של נתונים.

מניעת סיכונים פרואקטיבית
עצרו איומי AI לפני שהם מתפתחים לאירוע אבטחה.

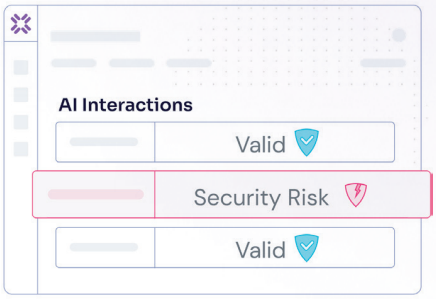
עמידה בדרישות רגולציה
הבטיחו תאימות לתקנים ורגולציות גלובליות.

היסודות להגנה על פיתוח מקומי של אפליקציות AI



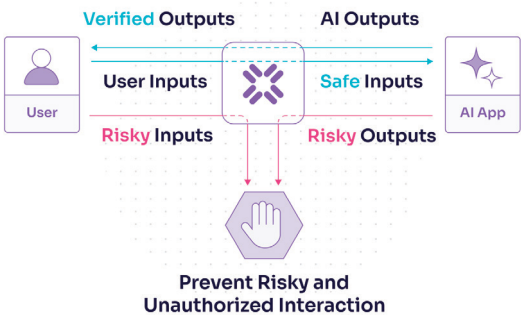
הגנה על מידע רגיש

מנעו חשיפה או דליפה של מידע רגיש באמצעות בקרות אבטחה מתקדמות, טשטוש מידע בעת הצורך ואכיפת מדיניות שמבטיחה שהמידע הקריטי של הארגון יישאר מוגן.



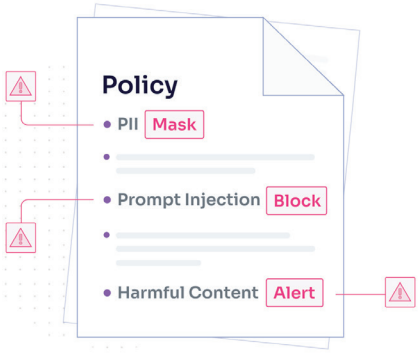
ניטור וניתוח אינטראקציות AI

קבלו שליטה מלאה על פעילות ה-AI בארגון, עם זיהוי חריגות, סיכונים והפרות מדיניות בזמן אמת, גם באפליקציות מאושרות וגם בכלים לא מורשים.



מניעת סיכונים באופן פרואקטיבי

זהו ועצרו איומי AI בזמן אמת, עם זיהוי מתקדם של פעילות חריגה, צמצום סיכונים אוטומטי לעבודה רציפה, מאובטחת וללא הפרעות.



אכיפת מדיניות בזמן אמת

יישמו מדיניות אבטחה ובקרות שימוש על כל יישומי ה-AI בארגון באופן אוטומטי, עם חסימה מיידית של בקשות זדוניות, הגבלת תוצאות לא בטוחות ושמירה על עמידה בדרישות רגולציה.

מאיצים חדשנות עסקית

רציפות תפעולית

אינטגרציה חלקה

אבטחת AI מקיפה

כיצד מגנים על הארגון בעידן ה-AI מבלי להאט את החדשנות?

סיכוני Shadow AI

עובדים משתמשים יותר ויותר בכלי AI שאינם מאושרים ע"י הארגון, רבים מהם מגיעים ממקורות לא מוכרים או בעלי רמת סיכון גבוהה. כלים אלו פועלים לעיתים ללא נראות מצד צוותי ה-IT, ויוצרים חשיפה בלתי מבוקרת למידע ונתונים. בחלק מהמקרים, אותם כלים אף מציינים במפורש כי המידע המוזן אליהם עשוי לשמש לאימון מודלים או להישמר במדינות זרות דבר שמעלה חששות משמעותיים סביב פרטיות מידע, עמידה בדרישות רגולציה וביטחון לאומי.

זיהוי ושליטה ב- Shadow AI

Ovalix מזהה שימוש ב-Shadow AI ברחבי הארגון, כולל כלי GenAI לא מאושרים שאינם נמצאים תחת ניטור. המערכת מנטרת שימושים, מבצעת הערכות סיכון כדי לאתר את היישומים המסוכנים ביותר, ומאפשרת לחסום כלי AI בעלי רמת סיכון גבוהה ישירות מהפלטפורמה. כך הארגון מקבל שליטה מלאה ונראות רחבה לניהול סיכוני Shadow AI בצורה יזומה.

דליפת מידע דרך יישומי AI ציבוריים

כלי AI מתבססים על מידע שמוזן אליהם כחלק מהשימוש השוטף, דבר שעלול לגרום לעובדים לשתף בטעות מידע רגיש עם יישומי AI ציבוריים, שאינם כוללים מנגנוני הגנה ובקרות מידע מספקות. מידע רגיש זה עשוי לכלול נתוני לקוחות, מידע פיננסי, חוזים, קניין רוחני ונתונים עסקיים חסויים נוספים.

מניעת דליפת נתונים של GenAI

Ovalix עוקב באופן רציף אחר אינטראקציות בין משתמשים לבין יישומי GenAI כדי לזהות התנהגות מסוכנת וחשיפת נתונים פוטנציאלית. זה מסייע בזיהוי דפוסים של שימוש לא בטוח והפרות מדיניות, ומאפשר אכיפה בזמן אמת כדי למנוע דליפת נתונים.

אכיפת מדיניות

למרות שרוב הארגונים מגדירים נהלים ומדיניות לשימוש בכלי AI באופן ידני, אכיפה אפקטיבית בקנה מידה ארגוני אינה אפשרית ללא תהליכים אוטומטיים.

אכיפת מדיניות AI בזמן אמת

Ovalix מאפשרת אכיפת מדיניות בזמן אמת, מצמצמת הפרות ומבטיחה שהעובדים יפעלו בהתאם להנחיות הארגון באופן עקבי - ללא צורך בפיקוח ידני.

חוסר בניהול ובקרה על שימושי AI

ככל שאימוץ כלי AI בארגונים גדל, כך גובר הקושי לקבל נראות מלאה על אופן השימוש בהם, לאן מידע רגיש זורם והאם קיימת בקרה ארגונית מספקת. היעדר פיקוח מרכזי יוצר שטחים מתים, תהליכי עבודה לא אחידים ועלייה ברמת הסיכון הארגוני

ניהול ובקרה מרכזיים על פעילות AI

Ovalix מספקת פיקוח מרכזי על כלל פעילויות ה AI בארגון, ומאפשרת לנטר שימושים, לאכוף מדיניות ולשמור על זרימת מידע אפקטיבית בין מחלקות, עובדים וכלים שונים.

חשיפה לאיומי סייבר המכוונים למערכות AI

מערכות AI עלולות להיות יעד לניסיונות תקיפה שעוקפים הגנות, מטעים את המערכת וגורמים לחשיפה של מידע רגיש. תוקפים יכולים להזין הוראות זדוניות שמנסות לגרום ל-AI להתעלם מהמדיניות שהוגדרה, לחשוף מידע פנימי ולבצע פעולות שלא אושרו. בניגוד למערכות סייבר מסורתיות, איומים אלו מותאמים לעולמות ה-AI ופתרונות אבטחה רגילים לא תמיד יודעים לזהות ולעצור אותם בזמן.

ניהול ובקרה מרכזיים על פעילות AI

Ovalix מנטרת באופן רציף פעילות חריגה במערכות AI, כולל ניסיונות להטעות את המערכת, לעקוף מנגנוני הגנה או לנצל חולשות באמצעות קלט זדוני. המערכת מזהה בזמן אמת ניסיונות שימוש חריגים או מסוכנים שעלולים לחמוק מפתרונות אבטחה מסורתיים, ומסייעת לארגון לעצור איומים לפני שהם הופכים לאירוע אבטחה משמעותי.

הדרכת עובדים לשימוש אחראי ב-AI

גם כאשר קיימים נהלים ובקרות אבטחה, עובדים לא תמיד מודעים לסיכונים שעלולים להיווצר משימוש לא נכון בכלי AI. טעויות אנוש ושימוש לא מבוקר עלולים להוביל לחשיפת מידע רגיש, הפרות מדיניות וסיכוני אבטחה.

התראות Real Time להדרכת עובדים באופן שוטף

Ovalix מסייעת להדריך עובדים בזמן אמת באמצעות התראות, הודעות והכוונה חכמה במהלך השימוש בכלי AI. כאשר מתרחשת פעולה חריגה או הפרת מדיניות, המערכת מספקת הסבר ואינדיקציה מיידית כדי להפוך טעויות להזדמנות ללמידה ושיפור. בנוסף, הפלטפורמה מספקת דשבורדים ותובנות שמאפשרים לזהות את סוגי ההפרות הנפוצים ביותר, יישומים בעלי רמת סיכון גבוהה ומשתמשים עם שימוש חריג - כך שהארגון יכול למקד את ההדרכות והמודעות במקומות שבהם יש להן את ההשפעה הגדולה ביותר.

מי אנחנו

Ovalix שואפת להעצים ארגונים לרתום את מלוא הפוטנציאל של הבינה המלאכותית על ידי מתן פלטפורמת אבטחה חזקה המבטיחה את האבטחה והשלמות של מערכות הבינה המלאכותית. **התחילו את המסע שלכם לאימוץ בטוח של בינה מלאכותית עוד היום !**