safetica

הגנת AI

הגנה על מידע רגיש לצד שימוש פרודוקטיבי ב-AI

בינה מלאכותית יוצרת (GenAI) משנה את הדרך שבה עובדים עובדים - ובמקביל פותחת נתיבים חדשים ומסוכנים לחשיפת מידע רגיש. ככל שהשימוש בכלי AI מאושרים ובכלי Shadow AI גדל, צוותי האבטחה זקוקים לנראות שחורגת מעצם הידיעה באילו כלים משתמשים: עליהם להבין מי משתמש ב-AI, איזה מידע רגיש משותף והיכן נדרשת הגנה נוספת - מבלי לפגוע ביתרונות הפרודוקטיביות ש-AI מעניק.

שליטה מלאה - בלי לחסום את הגישה לכלי AI

Safetica AI Protection מספקת נראות לפעילות AI ולשיתוף מידע רגיש, עם בקרות גרנולריות שמגנות על המידע ומאפשרות לעובדים להמשיך להשתמש ב-AI באופן פרודוקטיבי.

עם Safetica, צוותי האבטחה יכולים:

לזהות שימוש ב-AI מאושר ובלתי מאושר (Shadow AI)

בכל רחבי הארגון, כדי להבין באילו אפליקציות העובדים משתמשים.

לראות מידע רגיש בהקשר המלא

כולל מי משתף אותו, לאן הוא נשלח וכיצד נעשה בו שימוש.

להגן על המידע לפני שהוא מגיע ל-AI

באמצעות מדיניות DLP השולטת בקבצים רגישים, בתוכן מודבק, בפרומפטים ובפעולות משתמש מסוכנות.

להחיל בקרות גרנולריות

לפי אפליקציית ה-AI, רמת רגישות המידע, העובד, המחלקה והפעולה.

לחקור סיכוני AI עם הקשר רחב יותר

ולקבוע את התגובה המתאימה - במקום לחסום לחלוטין את הגישה ל-AI.

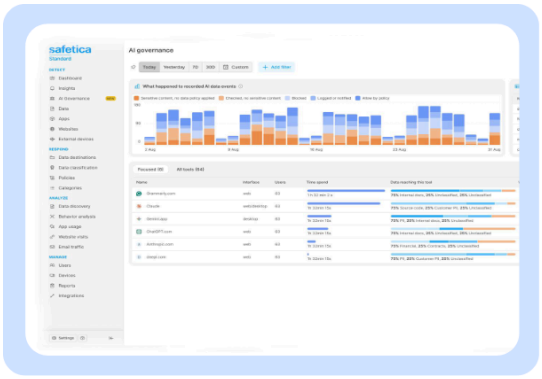
safetica

לנהל את השימוש ב-AI. להגן על מידע רגיש.

Safetica מספקת הגנת AI רב-שכבתית, המשלבת נראות לשימוש הארגוני ב-AI עם הבקרות שצוותי האבטחה צריכים כדי להגן על מידע רגיש מפני חשיפה ולנהל סיכונים - מבלי לפגוע באימוץ פרודוקטיבי של AI.

נראות ושליטה ככל שהעובדים מגבירים את השימוש ב-AI

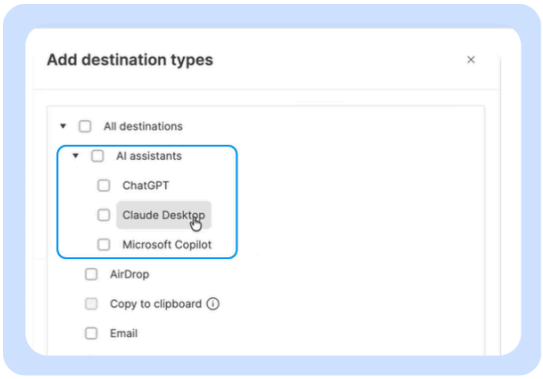
Safetica AI Governance מסייע לצוותי האבטחה להבין ולנהל שימוש ב-AI מאושר ובלתי מאושר (Shadow AI), באמצעות נראות לאפליקציות שבהן העובדים משתמשים, למידע שהם משתפים ולמקומות שבהם יש להחיל בקרות. באפשרותכם:



- **לגלות את סביבת ה-AI שלכם.** לקבל תמונה מרוכזת של אפליקציות AI מאושרות ובלתי מאושרות ברחבי הארגון.
- **להבין את פעילות ה-AI.** לראות מי משתמש ב-AI, באיזו תדירות ניגשים לאפליקציות, אילו נתונים וקבצים משותפים ומהי רמת ההגנה הקיימת.
- **להפוך נראות לשליטה.** לנטר פעילות, להגביל שיתוף מידע רגיש, להגביל גישה למשתמשים או לקבוצות מסוימים, או לחסום לחלוטין כלים מסוכנים.
- **לחקור בהקשר מלא.** להשתמש בפרומפטים מובנים מונחי AI כדי לבחון שימוש וסיכון, לסכם ממצאים ולזהות פעולות שיחזקו את ההגנה.

הגנה על מידע רגיש לפני שהוא מגיע ל-AI

Safetica מרחיבה את הגנת ה-DLP לעוזרי AI נפוצים ומסייעת לצוותי האבטחה לשלוט במידע רגיש המשותף באמצעות קבצים מצורפים, תוכן מועתק ומודבק ופרומפטים - תוך מתן אפשרות לשימוש נאות ב-AI. צוותי האבטחה יכולים:



- **להגן על מידע רגיש לפני שהוא מגיע לכלי AI.** להחיל מדיניות DLP לניטור ולשליטה בקבצים מצורפים רגישים, בטקסט מודבק, בפרומפטים ובמידע אחר המשותף עם ChatGPT, Claude ו-Microsoft Copilot.
- **להחיל בקרות מבוססות הקשר.** להגדיר מדיניות לפי רגישות המידע, כלי ה-AI, העובד, המחלקה ופעולת המשתמש הספציפית - במקום לחסום לחלוטין את הגישה ל-AI.
- **להגן על המידע באפליקציות ובדפדפן.** לשמור על הגנה באפליקציות שולחניות נתמכות ובדפדפנים מבוססי Chromium, במערכות macOS ו-Windows.
- **לאפשר שימוש פרודוקטיבי ב-AI.** להגביל פעולות מסוכנות של שיתוף מידע בלי לחסום שלא לצורך את הגישה הפרודוקטיבית לכלי AI מאושרים.

עם Safetica מקבלים את הנראות הדרושה להבנת השימוש ב-AI, את ההקשר לזיהוי סיכונים אמיתיים ואת השליטה להגנה על מידע רגיש.