<u>תרגום נוחות - נוסח הדיווח המחייב הוא נוסח הדיווח באנגלית</u>

סייפ-טי משיקה יכולות לניתוח התנהגויות של משתמשים וארגונים לעולם ה-Software Defined Perimeter

טכנולוגיה לאיתור אנומליות המהווה חיזוק משמעותי לפתרון Software Defined Perimeter

הרצליה, 15 אפריל, 2019 – סייפ-טי גרופ בע"מ ("סייפ-טי" - Nasdaq, TASE: SFET) ספקית של פתרונות Software-defined Access לסביבות ענן היברידי, מודיעה היום על השקת מוצר מבוסס משתמש ואינטרנט לאיתור אנומליות, Safe-T Telepath. סייפ-טי סיימה לאחרונה את האינטגרציה של Safe-T Telepath כחלק מפתרון ה-SDP (Software Defined Perimeter) של סייפ-טי. הטכנולוגיה שבבסיס ה-Telepath, אשר נרכשה על ידי סייפ-טי דטה מ-Cykick Labs Ltd. ביולי 2018, היא טכנולוגיה קניינית שמטרתה לזהות מתקפות עוינות על שירותים מבוססי אינטרנט באמצעות זיהוי התנהגויות אנומליות של משתמשים.

מטרתם של פתרונות ה-SDP של סייפ-טי וארכיטקטורות "Zero Trust" הינה למנוע גישה של משתמשים זדוניים ובלתי מורשים לשירותים הפנימיים של הארגונים. עם זאת, בדוח של International Data Corporation's (IDC)[1] נמצא כי מקורן של 40% ממתקפות הסייבר הוא למעשה במשתמשים מורשים שניגשים למערכות אליהן הם אינם מורשים לגשת.

לכן נוצר צורך בפיתוח זן חדש של פתרון SDP, שלא רק ימנע ממשתמשים בלתי מורשים לגשת למידע ולשירותים של הארגונים, אלא גם – ולא פחות חשוב – ינטר את ההתנהגות של משתמשים מורשים ויתריע על שימוש לרעה והתנהגות אנומלית של משתמשים אלו אשר ניגשים למערכות להן הם אינם מורשים לגשת.

מוצר ה-Safe-T Telepath פותח כדי לתת מענה לצורך בבקרה על גישה של משתמשים מורשים למערכות בלתי מורשות. זוהי הטכנולוגיה הראשונה מסוגה לאיתור אנומליות ברמת המשתמש והאינטרנט, המיועדת לפתרונות SDP ולארכיטקטורות "Zero Trust". Safe-T Telepath עושה שימוש בגישה היברידית המבוססת על למידת מכונה ונהלים לזיהוי התנהגויות חשודות.

Safe-T Telepath מעניק לצוותי אבטחת סייבר גישה מוקדמת למידע, שניתן לפעול לפיו, אודות התהוותם של איומים, וכן יכולות פורנזיות מתקדמות ותובנות על מתקפות מחוכמות. הוא מזהה אנומליות ומאפשר לעצור פעילויות הונאה באמצעות הבנה של ההתנהגות הנורמלית של משתמשי היישומים ובחינה של הטרנסאקציות ביישומי הרשת של הארגון ללא הפרעה.

"פתרונות Software Defined Perimeters וארכיטקטורות Zero Trust נועדו ליצור חור שחור סביב השירותים של הארגון, ולמנוע ממשתמשים בלתי מורשים לגשת אליהם. לאור ההיקף הרחב של משתמשים מורשים המבצעים פעולות בלתי מורשות, יש צורך גובר בסוג חדש של פתרון," אמר איתן ברמלר, סמנכ"ל טכנולוגיה בסייפ-טי. "זיהינו את הצורך הזה, עבדנו על פיתוח מענה וכעת אנחנו משיקים את Safe-T Telepath כחלק מפתרון ה-SDP שלנו. המוצר החדש מאפשר לנו להעניק ללקוחותינו הגנה מחוזקת מפני מתקפות סייבר, ובכלל זה איומים פנימיים וחיצוניים."

---

[1] על פי אתר האינטרנט של החברה, IDC הינה ספקית מובילה בעולם של מודיעין שוק, שירותי ייעוץ, ואירועים עבור טכנולוגיות המידע, התקשורת, הטכנולוגיה הצרכן. ניתן לעיין בדוח בקישור הבא:
https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

אודות סייפ-טי גרופ בע"מ

סייפ-טי גרופ בע"מ (סימול Nasdaq, TASE: SFET) היא ספקית של פתרונות Software Defined Access אשר נועדו לצמצם התקפות סייבר על שירותים עסקיים קריטיים ונתונים רגישים של ארגונים. סייפ-טי פותרת את סוגיית הגישה לנתונים על ידי הסתרת הנתונים בסביבת הארגון והגבלת הגישה לגורמים מורשים ורצויים בלבד בסביבות ענן היברידיות. הטכנולוגיה של סייפ-טי מגנה על ארגונים מפני אובדן וזליגת נתונים, דליפות, תוכנות זדוניות, תוכנות כופר והונאות ועל ידי כך מגבירה את היעילות התפעולית, האבטחה והציות לרגולציה של ארגונים אלה. חברות ממגזרי השירותים הפיננסיים, הבריאות והתשתיות, כמו גם ממשלות המשתמשות בפתרונות ה- Software Defined Access הרב-שכבתיים והמוגנים בפטנטים של סייפ-טי יכולות לאבטח את הנתונים, השירותים והרשתות שלהן מפני איומי סייבר פנימיים וחיצוניים.

מידע צופה פני עתיד

פרסום זה כולל מידע צופה פני עתיד כמשמעותו בדין האמריקאי. לפרטים נוספים, ראה נוסח הדיווח המחייב באנגלית להלן.

פרטי קשר
עדי ומיכל קשרי משקיעים - מיכל אפרתי: 0523044404 michal@efraty.com

Safe-T Introduces User and Entity Behavior Analytics Capabilities to the World of Software-Defined Perimeter

Bolsters Software Defined Perimeter Solution with User and Web-Based Anomaly Detection Technology

HERZLIYA, Israel, April 15, 2019 — Safe-T Group Ltd. (Nasdaq, TASE: SFET), a provider of Software-defined Access (SDA) solutions for the hybrid cloud, today announced the launch of its user and web-based anomaly detection product, named Safe-T Telepath. Safe-T has recently completed integrating the Safe-T Telepath as part of Safe-T's Software Defined Perimeter (SDP) solution. The Telepath technology, acquired by Safe-T Data from Cykick Labs Ltd. in July 2018, is a proprietary technology aimed to recognize hostile attacks on web-based services through the identification of the users' anomalous behavior.

The goal of Safe-T's SDP solutions and "Zero Trust" platform architectures is to prevent access by malicious and unauthorized users to organizations' internal services. However, according to International Data Corporation's (IDC) report[1], 40% of cyber breaches actually originate with authorized users accessing unauthorized systems.

Therefore, a new breed of SDP solution is required, which not only prevents unauthorized users from accessing the organizations' data and services, but of equal importance, tracks the behavior of authorized users and alerts on service misuse and anomalous behavior of authorized users accessing unauthorized systems.

Safe-T Telepath was originated to answer the need to control authorized access to unauthorized resources. It is the first ever user and web-based anomaly detection technology designed for SDP solutions and Zero Trust architectures. Safe-T Telepath employs a hybrid approach based on rules and machine learning to identify suspicious activities.

Safe-T Telepath empowers cyber security teams with early access to actionable intelligence on emerging threats and comprehensive forensics capabilities, as well as insights into sophisticated attacks. It detects anomalies to stop fraudulent activities by understanding the normal behavior of application visitors and non-intrusively inspecting enterprise web application transactions.

"Software Defined Perimeter solutions and Zero Trust architectures are designed to create a black hole around organizations' services, by preventing unauthorized users from ever reaching them. With the percentage of authorized users performing unauthorized actions being so high, there is a growing need for a new type of solution" said Eitan Bremler, VP Technology at Safe-T. "Recognizing this need, we have worked to develop an answer and are now launching Safe-T Telepath as part of our SDP solution. The new product will allow us to provide our customers with robust protection against cyber-attacks, including external and internal threats."

About Safe-T

[1] According to its website, IDC is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. The report can be reviewed in the following link: https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

Safe-T® Data A.R Ltd., a wholly-owned subsidiary of Safe-T Group Ltd. (Nasdaq, TASE: SFET), is a provider of software-defined access and zero trust access solutions which mitigate attacks on enterprises' business-critical services and sensitive data. Safe-T solves the data access challenge. The company's software-defined access (SDA) platform reduces the attack surface, empowering enterprises to safely migrate to the cloud and enable digital transformation. With Safe-T's patented, multi-layer software-defined access, financial services, healthcare, utility companies and governments can secure data, services, and networks from internal and external threats.
For more information about Safe-T, visit www.safe-t.com

Forward-Looking Statements

This press release contains forward-looking statements within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995 and other Federal securities laws. Words such as "expects," "anticipates," "intends," "plans," "believes," "seeks," "estimates" and similar expressions or variations of such words are intended to identify forward-looking statements. For example, Safe-T is using forward-looking statements in this press release when it discusses the advantages of its new SDP solution and its potential to address market need and/or demand. Because such statements deal with future events and are based on Safe-T's current expectations, they are subject to various risks and uncertainties and actual results, performance or achievements of Safe-T could differ materially from those described in or implied by the statements in this press release. The forward-looking statements contained or implied in this press release are subject to other risks and uncertainties, including those discussed under the heading "Risk Factors" in Safe-T's annual report on Form 20-F filed with the Securities and Exchange Commission ("SEC") on March 26, 2019, and in any subsequent filings with the SEC. Except as otherwise required by law, Safe-T undertakes no obligation to publicly release any revisions to these forward-looking statements to reflect events or circumstances after the date hereof or to reflect the occurrence of unanticipated events. References and links to websites have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release.

PRESS CONTACT

Michal Efraty
+972-(0)52-3044404
michal@efraty.com