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

סייפ-טי מגינה על רשתות IOT תעשייתי באמצעות פתרון Zero Trust

החברה מודיעה על גרסה חדשה שתגן על לקוחות IOT תעשייתי ממכשירי IOT

הרצליה, 28 מרץ, 2019 – סייפ-טי (Nasdaq, TASE:SFET), ספקית מובילה של פתרונות software-defined access לסביבות ענן היברידי, מודיעה היום על שחרור גרסה חדשה לפתרון ה-SDP (Solution Defined Perimeter) של החברה, שנועדה לארגוני IOT (Internet Of Things – "האינטרנט של הדברים") תעשייתי (IIOT). הגרסה החדשה מרחיבה את פתרון ה-SDP ורשת ה-Zero Trust לעולם ה-IOT.

בשנים האחרונות, מכשירי IOT הפכו לרכיב חשוב במגוון תעשיות. מכשירי מדידה מרחוק ותאורה מקושרת, לדוגמה, נפוצים כיום כמעט בכל הארגונים. העלייה בשכיחות מכשירי IOT הובילה להופעתם של ספקי פתרונות אבטחה לתחום ה-IOT. עד כה, ספקים אלו התמקדו בהגנה על המכשיר עצמו מפני האקרים, והשאירו לארגון להגן על המידע שבו בעזרת פתרונות מסורתיים, שאין באפשרותם להתמודד עם הדרישות הייחודיות של IOT.

לסייפ-טי ידע ומומחיות בתכנון רשתות Zero Trust ו-SDP, והיא זיהתה את הצורך ופיתחה את פתרון ה-SDP הראשון מסוגו המעניק הגנה לא רק למכשירי ה-IOT, אלא גם למרכזי הנתונים של חברות IIOT מפני מכשירי IOT חיצוניים.

פתרון ה-Zero Trust של סייפ-טי מבוסס על הפלטפורמה הטכנולוגית מוגנת הפטנט של החברה, Reverse Access Technology, המצמצמת את השטח החשוף להתקפה ברשת ה-IIOT באמצעות בקרה על מכשירי ה-IOT המורשים לגשת למערכת בצד השרת (מערכות ניהול נתונים, פלטפורמות IOT וכד'). כך מתאפשר למכשירי IOT שאושרו להשתתף באסטרטגיית Zero Trust.

הפתרון החדש של סייפ-טי מאפשר זאת באמצעות דרישה ממכשיר ה-IOT להזדהות כבר בשלב הראשון, לפני מתן הרשאת גישה. ההזדהות יכולה להתבצע על-ידי שליחה של פרטי הזדהות או טוקן מוגדרים מראש ממכשיר ה-IOT אל פתרון ה-SDP של סייפ-טי. רק לאחר שפתרון אבטחת הגישה של סייפ-טי מוודא את זהותו של מכשיר ה-IOT יקבל המכשיר גישה לפי דרישה למערכת הספציפית בצד השרת.

התהליך שבמסגרתו הזיהוי מתבצע לפני מתן הגישה מוודא כי מכשירי IOT פרוצים, בלתי מאובטחים או שאין להם את ממשק API של סייפ-טי לעולם לא יקבלו גישה לרשת ה-IIOT.

"כיום, מתמקדים ספקי Zero Trust בעיקר בבני אדם, אך הכמות של היישומים ושל מכשירי IOT המנסים לקבל גישה למערכות בצד שרת גבוהה הרבה יותר, ועד היום לא ראינו ספקי Zero Trust מנסים לתת מענה לבעיה זו," אמר איתן ברמלר, סמנכ"ל טכנולוגיה בסייפ-טי. "זיהינו את הבעיה האפשרית הזו וביצענו התאמות לפתרון ה-SDP שלנו כדי שייתן מענה למקרים של יישום ליישום ו-IOT ליישום."

בנוסף לתמיכה במכשירי IOT, תומך פתרון הגישה המאובטחת של סייפ-טי גם ברכזות IOT שאליהם מתחברים מכשירי IOT. כך מופחתים השינויים הנדרשים במכשיר, ואילו רכזת ה-IOT מבצעת את ההזדהות בשם המכשיר.

אודות סייפ-טי גרופ בע"מ

סייפ-טי גרופ בע"מ (סימול NASDAQ, ת"א:SFET) היא ספקית מובילה 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 Protects Industrial IOT Networks with Zero Trust Solution

Announces new version to protect IIOT customers from IOT devices

HERZLIYA, Israel, March 28, 2019 — Safe-T® (Nasdaq, TASE:SFET), a provider of Software-defined Access (SDA) solutions for the hybrid cloud, today announced the launch of a new version of its Software Defined Perimeter (SDP) solution, designed for Industrial Internet Of Things (or IIOT) organizations. The new version extends the Zero Trust network and SDP solution to the world of IOT.

In recent years, IOT devices have become an important element across a wide range of industries. For instance, devices such as remote meters and connected lighting are now commonplace in any organization. With the increase of IOT devices, there has been a rise in the emergence of IOT security vendors. Until now, these vendors have focused on protecting the device itself from hackers, while leaving the organization to defend their data with legacy solutions that fail to address the unique requirements of IOT.

Safe-T, having the know-how and expertise in Zero Trust network design and SDP, has recognized this need and developed the first-ever SDP solution, protecting not only the IOT devices but also the IIOT organizations' data center from remote IOT devices.

Safe-T's Zero Trust solution is built on the company's patented reverse-access technology platform, which reduces the attack surface of the IIOT network by controlling which IOT device can access the backend systems (meter data management systems, IOT platforms, etc.), enabling "qualified" IOT devices to participate in a Zero Trust strategy.

Safe-T's new solution achieves this by forcing the IOT device to authenticate first before being granted access. Authentication can be done by sending a predefined token or credentials from the IOT devices to Safe-T's SDP solution. Only after Safe-T's secure access solution has authenticated the IOT device, it is granted on-demand access to the specific backend system.

This process of authentication first, access later, ensures that breached/hacked IOT devices or IOT devices which do not have the Safe-T API (Application Programing Interface) will never be granted access to the IIOT network.

"Today, Zero Trust vendors mainly target humans, but they are exceeded by the number of applications and IOT devices trying to access backend systems and we haven't seen Zero Trust vendors trying to tackle this issue," said Eitan Bremler, VP Technology at Safe-T. "Recognizing this potential problem, we adapted our Software Defined Perimeter solution to support application-to-application use cases, as well as IOT-to-application use cases."

In addition to supporting IOT devices, Safe-T's secure access solution also supports IOT bridges to which IOT devices connect. This reduces the changes required on the IOT device, and instead has the IOT bridge perform the authentication on behalf of the device.

About Safe-T

Safe-T® Data A.R Ltd., a wholly-owned subsidiary of Safe-T Group Ltd. (Nasdaq, TASE: SFET), is a provider of 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 SDA 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
Rona Susel
Rona.susel@safe-t.com
+972-9-8666110