

## **סייפ-טי מוכרת ע"י Gartner כספקית נבחרת לפתרונות Zero Trust Network Access במסגרת דו"ח מחקר לחודש יוני 2020**

הרצליה, 22 ביוני, 2020 – סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET), ספקית מובילה של פתרונות software-defined access לסביבות ענן היברידי ולסביבות מקומיות, מודיעה היום על הכרה כספקית נבחרת במסגרת דו"ח מחקר בתחום Zero Trust Network Access<sup>1</sup> של פירמת האנליסטים Gartner. בדו"ח אוזכרה סייפ-טי כספקית נבחרת של פתרון ZTNA עצמאי.

לפי הדו"ח של Gartner, "מודל האבטחה הישן, הגורס כי גורמי פנים הם בטוחים וגורמי חוץ אינם בטוחים, התנפץ. מרגע שהמשתמשים הפכו לניידים ומרגע שנדרשת גישה לשותפים עסקיים "מבחוץ", רשתות VPN ואזורים מפורזים (DMZ) הפכו לנחלת הכלל. כמו כן, הם סיפקו יותר אומון במשתמשים, שתוקפים יכולים לנצל. במציאות של עולם העסקים הדיגיטלי, נדרשת גישה בכל רגע ומכל מקום לכל היישומים, ללא תלות במיקום של המשתמשים ושל המכשירים שלהם."

בנוסף, מצוין בדו"ח כי "גישת Zero Trust מאפשרת גישה מבוקרת-זהות ומודעת תוכן למשאבים, ומפחיתה את שטח הפנים למתקפה. הבידוד שמציעים פתרונות ZTNA משפר את הקישוריות ומבטל את הצורך לחשוף את היישומים ישירות לאינטרנט. האינטרנט עדיין מהווה אמצעי בלתי מאובטח לתנועה; גורם ביניים מאפשר את הקשר בין יישומים ומשתמשים. גורם ביניים כזה עשוי להיות בדמות שירותי ענן של צד שלישי או שירות באחסון אישי (בצורת אמצעי פיזי במרכז הנתונים של הלקוח או אמצעי וירטואלי בענן IaaS ציבורי)."

לפי הדו"ח, "למרות שהחלפת רשתות VPN היא גורם נפוץ לאימוץ פתרונות ZTNA, רק לעיתים נדירות הם מחליפים לחלוטין את רשתות ה-VPN."

פתרונות ה-ZTNA של סייפ-טי מעניקים גישה ליישומים על בסיס need-to-know, תוך מתן גישה מהירה וחלקה למשתמשים למשאבים הדרושים להם. הפתרונות פועלים בגישת "אימות לפני גישה" על פני כל היישומים של הארגון, ומאפשרים לו ליהנות מאבטחה משופרת, משקיפות כוללת ומחוייבת משתמש טובה יותר. כמו כן, הם מאפשרים בקרה על הגישה לשירותים פנימיים ומבצעים אימות זהות לכל משתמש בעזרת ספקי זהות חיצוניים.

הפיתוח החדש של סייפ-טי, ZoneZero, מאפשר לארגון לאמץ ארכיטקטורת ZTNA מבלי לוותר על רשת ה-VPN הקיימת. ZoneZero משפר את רמת האבטחה של רשת ה-VPN באמצעות הוספת יכולות ZTNA ומתן גישה ליישומים ולשירותים רק לאחר שבוצע אימות. הוספת ZoneZero מבית סייפ-טי לרשתות VPN קיימות מאפשרת ליצור פתרון Zero Trust מותאם אישית וניתן להרחבה וליהנות מכל היתרונות של ZTNA תוך מזעור הסיכונים הכרוכים באימוץ טכנולוגיה חדשה.

"אנחנו גאים על ההכרה שקיבלנו בדו"ח של גרטנר זו השנה השנייה ברציפות. אנחנו מאמינים שהכרה זו משקפת את המאמצים המתמשכים שלנו להביא לשוק את פתרון ה-ZTNA הטוב ביותר", אמר שחר דניאל, מנכ"ל סייפ-טי. "אנחנו שמחים כי הפתרונות החדשניים שלנו זכו שוב להכרה המגיעה להם, שתאפשר לנו להמשיך ולהוביל בתחום ה-Zero Trust Network Access. רשתות ה-VPN מתאימות פחות ופחות לשימוש, ואנחנו מרוצים מהיכולת שלנו להציג פתרונות שמסייעים לארגונים לבסס אסטרטגיית Zero Trust על פני כלל הרשתות שלהם."

<sup>1</sup> Gartner, "Market Guide for Zero Trust Network Access," Steve Riley, et al, 8 June 2020

הפתרון של סייפ-טי מאפשר התקנה בקלות במכשירים מנוהלים ולא מנוהלים. בנוסף, הפתרון כולל כלי לניתוח התנהגות משתמשים, אשר מעניק תובנות חסרות תקדים אודות תנועת המשתמשים ומאפשר לאתר בוטים ופעולות זדוניות מתוך הארגון לפני שיצליחו לגרום נזק.

### **הצהרת Gartner**

Gartner אינה מקדמת אף ספק, מוצר או שירות המתוארים בפרסומיה המחקריים, ואינה ממליצה למשתמשים בטכנולוגיה לבחור רק בספקים שזכו בציונים הגבוהים ביותר או בתארים אחרים. הפרסומים המחקריים של Gartner מורכבים מדעותיהם של גורמים בארגון המחקר של Gartner, ואין לראות בהם אמירות עובדתיות. Gartner לא תישא באחריות, מפורשת או משתמעת, בנוגע למחקר זה, ובכלל זה לסחירות או תאימות למטרה מסוימת.

### **אודות סייפ-טי גרופ בע"מ**

סייפ-טי גרופ בע"מ (סימול Nasdaq, TASE: SFET) היא ספקית של פתרונות Zero Trust Access אשר נועדו לצמצם התקפות סייבר על שירותים עסקיים קריטיים ונתונים רגישים של ארגונים. הפתרונות של סייפ-טי לענן ולשרתים מקומיים מבטיחים שכל תרחיש הגישה של הארגון, לתוך הארגון ומחוץ לו מאובטחים ע"פ פילוסופיית ה"אשר קודם, תן גישה אח"כ" של Zero Trust. גישה זאת מניחה שאין אדם מאושר מראש, ללא תלות במיקומו הפיסי ושיוכו הארגוני, וכל משתמש אשר מנסה לגשת לשירות ארגוני בין אם הוא בענן או בתוך הארגון, חייב לקבל אישור גישה כשלב ראשון.

המגוון הרחב של פתרונות גישה מאובטחת של סייפ-טי מצמצמים את מרחב התקיפה הארגוני ומשפרים את סיכויי הארגון להגן על עצמו בפני מתקפות.

שכבת הגנה נוספת הינה שירות הפרוקסי הארגוני של סייפ-טי שמאפשר גלישה קלה, חסכונית, מאובטחת, וללא ניתוקים לאתרי WEB ברחבי העולם. השירות מאפשר חיבור אין סופי של משתמשים, ע"י התרחבות דינאמית כתלות במספר המשתמשים המחוברים.

בעזרת שימוש בטכנולוגיית ה-reverse-access מוגנת הפטנט של סייפ-טי וטכנולוגיית ניתוב הרשתות הייחודית של החברה, ארגונים מסוגים שונים וגדלים שונים, יכולים לאבטח את המידע והרשתות שלהם כנגד מתקפות חיצוניות ופנימיות.

### **מידע צופה פני עתיד**

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

### **פרטי קשר**

עדי ומיכל קשרי משקיעים - מיכל אפרתי: 0523044404 [michal@efraty.com](mailto:michal@efraty.com)

---

UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
Washington, D.C. 20549

Form 6-K

Report of Foreign Private Issuer  
Pursuant to Rule 13a-16 or 15d-16  
under the Securities Exchange Act of 1934

For the month of: June 2020 (Report No. 2)

Commission file number: 001-38610

SAFE-T GROUP LTD.  
(Translation of registrant's name into English)

8 Abba Eban Ave.  
Herzliya, 4672526 Israel  
(Address of principal executive offices)

Indicate by check mark whether the registrant files or will file annual reports under cover of Form 20-F or Form 40-F.

Form 20-F ☒ Form 40-F ☐

Indicate by check mark if the registrant is submitting the Form 6-K in paper as permitted by Regulations S-T Rule 101(b)(1): \_\_\_\_\_

Indicate by check mark if the registrant is submitting the Form 6-K in paper as permitted by Regulations S-T Rule 101(b)(7): \_\_\_\_\_

---

---

## **CONTENTS**

Attached hereto and incorporated by reference herein is the Registrant's press releases issued on June 22, 2020, titled: "Safe-T named as a Representative Vendor in Gartner's June 2020 Market Guide for Zero-Trust Network Access".

The first through sixth paragraphs, the eighth paragraph, the section titled "Gartner Disclaimer" and the section titled "Forward-Looking Statements" are incorporated by reference into the registration statements Form S-8 (File Nos. 333-233510 and 333-239249) and Form F-3 (File Nos. 333-233724, 333-235367, 333-235368 and 333-236030) of the Company, filed with the Securities and Exchange Commission, to be a part thereof from the date on which this report is submitted, to the extent not superseded by documents or reports subsequently filed or furnished.

### **Exhibits**

<b>Exhibit No.</b>	<b>Description</b>
--------------------	--------------------

99.1	<a href="#"><u>Press release issued by Safe-T Group Ltd. on June 22, 2020, titled: "Safe-T named as a Representative Vendor in Gartner's June 2020 Market Guide for Zero-Trust Network Access".</u></a>
------	---

### SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

Safe-T Group Ltd.  
(Registrant)

By /s/ Hagit Gal  
Name: Hagit Gal  
Title: Corporate Legal Counsel

Date: June 22, 2020



**Safe-T named as a Representative Vendor in Gartner's June 2020 Market Guide for Zero Trust Network Access**

**HERZLIYA, Israel, June 22, 2020** - Safe-T Group Ltd. (Nasdaq, TASE:SFET), a leading provider of secure access solutions, today announced that it has been identified as a Representative Vendor in the Gartner Market Guide for Zero Trust Network Access ("ZTNA") report<sup>1</sup>. Safe-T was named a Representative Vendor of Stand-Alone ZTNA.

According to Gartner, "The old security model of "inside means trusted" and "outside means untrusted" is broken. When users became mobile and when business partners on the "outside" required access, virtual private networks (VPNs) and demilitarized zones (DMZs) became common. They also granted excessive implicit trust - trust that attackers abused. The reality of digital business is that it requires anywhere, anytime access to any application, regardless of the locations of the users and their devices."

Further, Gartner stated that, "ZTNA provides controlled identity and context-aware access to resources, reducing the surface area for attack. The isolation afforded by ZTNA improves connectivity, removing the need to directly expose applications to the internet. The internet remains an untrusted transport; a trust broker mediates connections between applications and users. The broker can be a cloud service managed by a third-party provider or a self-hosted service (in the form of a physical appliance in the customer's data center or a virtual appliance in a public infrastructure as a service [IaaS] cloud)."

According to the report, "Although VPN replacement is a common driver for its adoption, ZTNAs rarely replace VPN completely."

Safe-T's ZTNA solutions grant access to applications on a need-to-know basis, while giving users fast and seamless access to the resources they need. This creates a "verify-first, access-second" zero-trust approach across an organization's applications, enabling enhanced security, greater visibility, and a better user experience. It controls the access to internal services and utilizes third-party identity providers to authenticate each user.

Safe-T's newest development, ZoneZero™, enables the organization to adopt a Zero Trust Network Access architecture without getting rid of its VPN. ZoneZero enhances VPN security by adding ZTNA capabilities, allowing access to applications and services only after trust has been verified. Deploying Safe-T's ZoneZero on top of the existing VPN offers a customized and scalable zero trust solution—with all the benefits of ZTNA while lowering the risks involved in adopting the new technology.

"We are honored to be recognized in the report for the second year in a row. We believe that it reflects our continuous efforts to provide the best SDP solution to the market," said Shachar Daniel, CEO of Safe-T. "We are proud that our innovative solutions have again gained what we believe to be well-deserved recognition, allowing us to maintain Safe-T's leadership in Zero Trust Network Access. As VPNs become less and less fit for use, we are pleased to be able to deliver solutions that help organizations establish a Zero Trust strategy across their networks."

---

<sup>1</sup> Gartner, "Market Guide for Zero Trust Network Access," Steve Riley, et al, 8 June 2020.

Safe-T's ZoneZero solution provides a simple deployment for both managed and unmanaged devices. In addition, the solution's user behavior analysis module, provides unparalleled insight into user traffic, which allows it to detect bots and malicious insiders before they have the chance to cause damage.

**Gartner Disclaimer**

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

**About Safe-T®**

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, while ensuring uninterrupted business continuity.

Safe-T's cloud and on-premises solutions ensure that an organization's access use cases, whether into the organization or from the organization out to the internet, are secured according to the "validate first, access later" philosophy of Zero Trust. This means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network or in the cloud.

Safe-T's wide range of access solutions reduce organizations' attack surface and improve their ability to defend against modern cyberthreats. As an additional layer of security, our integrated business-grade global proxy solution cloud service enables smooth and efficient traffic flow, interruption-free service, unlimited concurrent connections, instant scaling and simple integration with our services.

With Safe-T's patented reverse-access technology and proprietary routing technology, organizations of all size and type can secure their data, services and networks against internal and external threats.

At Safe-T, we empower enterprises to safely migrate to the cloud and enable digital transformation.

Safe-T's SDP solution on AWS Marketplace is available [here](#).

For more information about Safe-T, visit [www.safe-t.com](http://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 potential of its products, maintaining leadership in Zero Trust Network Access, and continuing to provide customers with the tools they need to prevent unauthorized users from accessing company resources. 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. Safe-T is not responsible for the contents of third-party websites.

#### **PRESS CONTACT**

Karin Tamir  
[Karin.Tamir@safe-t.com](mailto:Karin.Tamir@safe-t.com)  
+972-9-8666110