תרגום נוחות - נוסח הפרסום המחייב הוא נוסח הפרסום באנגלית

סייפ-טי נכללה בדוח Tech Tide™: Zero Trust Threat Prevention של פירמת מחקר מובילה לרבעון השלישי של שנת 2020

הרצליה, ישראל, 7 באוקטובר 2020 – סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET) ספקית של פתרונות Secure Access לסביבות ענן היברידי ולסביבות מקומיות, מודיעה היום כי היא נכללה בדוח Tech Tide™ "Zero Trust Threat Prevention"[1] של פורסטר לרבעון השלישי של שנת 2020.

פורסטר היא אחת מפירמות המחקר המובילות בשוק. כבר מעל 35 שנים שהמחקרים של פורסטר מעניקים לגופים מובילים בענפי הצרכנות והטכנולוגיה בעולם תובנות ברורות אודות המתרחש בשטח והמגמות העתידיות.

ZoneZero™ של סייפ-טי הוא פתרון Zero Trust Network Access (ZTNA) שמאפשר פריסה שקופה ופשוטה ומעניק פתרון חדשני וייחודי, ממוקד-רשת, להטמעת מיקרו-פילוח ו-ZTNA לרוחב רשתות VPN, חומות-אש ושירותי יישומים בארגונים.

ZoneZero מאפשר אינטגרציה חלקה על פני כל התשתיות ושירותי ההזדהות המסורתיים הקיימים. מתוך הבנת הצורך בפתרונות ZTNA שיוכלו לתת מענה יעיל ושלם לכל הדרישות והתרחישים הפרטניים של גישה מרחוק, יצרה סייפ-טי את פלטפורמת Perimeter Access Orchestration Platform הראשונה מסוגה, אשר כוללת את הכלים הבאים:

- מיקרו-פילוח לוגי המבוסס על פטנט Reverse Access של החברה
- הטמעת פתרון ה-SDP הקלאסי של סייפ-טי – מודול ZTNA שאינו תלוי בתחנת קצה (clientless)
- אינטגרציה עם רשתות VPN מובילות – הוספת יכולות ZTNA למוצרי VPN קיימים
- תמיכה באימות זהות רציף ושדרוג הזדהות דו-שלבית (2FA) להזדהות רב-שלבית (MFA) אמיתית
- בקרת גישה ליישומים עבור משתמשים פנימיים וחיצוניים
- ניטור ואכיפה רציפים של פעולותיהם של משתמשים ויישומים והפקת דיווחים

"אנחנו גאים על ציון החברה בדוח Tech Tide של פורסטר. האזכור מעניק משנה תוקף לסיבה לכך שארגונים מובילים מכל הסקטורים (ממשלה, צבא, פיננסים, בריאות ועוד) נשענים על פתרון ה-ZTNA של סייפ-טי לפילוח חכם של הרשתות ולבקרה על הגישה למשאביהם," אמר מנכ"ל סייפ-טי, שחר דניאל.

פתרון ZoneZero מבית סייפ-טי מספק הגנת Zero Trust לשירותים מקומיים ולשירותים מבוססי-ענן, ותומך בפרוטוקולים כגון HTTP/S, RDH5, RDP, SSH, יישומים מסורתיים, WebDAV ועוד. באמצעות פתרון ה-ZTNA של סייפ-טי יכולים ארגונים להעניק לכל העובדים, השותפים, היישומים, מכשירי ה-IoT ועוד, גישת Zero Trust מלאה מרחוק, ללא תלות במיקומם, למשאבי החברה.

הפתרון של סייפ-טי מאפשר פריסה פשוטה על מכשירים מנוהלים ולא מנוהלים כאחד. כמו כן, הכלי כולל מודול לניתוח התנהגות המשתמש, שמעניק תובנות ראשונות מסוגן אודות תנועת המשתמשים ומאפשר לאתר בוטים וגורמים זדוניים פנימיים לפני שמתאפשר להם לגרום נזק.

---

[1] The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2020 by David Holmes, Sandy Carielli, Andras Cser, Chase Cunningham, Chris Sherman, Brian Kime, and Claire O'Malley, September 18, 2020.

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 ומחוצה 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 הפיזי ושיוכו הארגוני, וכל משתמש אשר מנסה לגשת לשרות 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 שרות 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 בדין האמריקאי. לפרטים נוספים, ראה נוסח הדיווח המחייב באנגלית להלן.

פרטי קשר

מיה מאירי: +972-9-8666110 Maya.Meiri@safe-t.com

Safe-T Listed in Leading Analyst Firm's Q3 2020 Tech Tide™: Zero Trust Threat Prevention Report

HERZLIYA, Israel, October 7, 2020 - Safe-T® Group Ltd. (NASDAQ, TASE: SFET), a provider of secure access solutions for on-premise and hybrid cloud environments, announced today that it was listed in Forrester's Q3 2020 Tech Tide™: Zero Trust Threat Prevention Report [1].

Forrester is one of the leading analyst firms in the market. For more than 35 years, Forrester's research has given global consumer business and technology leaders a clear vision to see what is now and what is next.

Safe-T's ZoneZero™ is a Zero Trust Network Access (ZTNA) solution which offers a transparent and simple deployment, providing an innovative and unique network-centric solution to implement micro-segmentation and ZTNA within corporate network VPNs, firewalls, and application services.

ZoneZero™ provides seamless integration across all legacy infrastructure and authentication services.

Understanding the need for ZTNA solutions that efficiently and completely address all remote access and micro-segmentation scenarios and requirements, Safe-T has created the first ever Perimeter Access Orchestration Platform, incorporating the following modules:

- Logical micro-segmentation utilizing Safe-T's reverse-access patent
- The Safe-T Classic SDP implementation - a clientless ZTNA module
- Integration with leading VPNs - adding ZTNA capabilities to existing VPNs
- Support continuous authentication and upgrading 2FA to true MFA
- Application access control for internal and external users
- Continuous monitoring, enforcement, and reporting on user/application activities

"We are honored to be listed in the Forrester Tech Tide report. The listing validates the reason why leading organizations of all verticals (government, military, financial, healthcare, etc.) rely on Safe-T's ZTNA solution to logically segment their networks and control access to their resources," said Safe-T's CEO, Shachar Daniel.

Safe-T's ZoneZero™ solution provides Zero Trust protection for on-premises and cloud published services, supporting services such as HTTP/S, RDH5, RDP, SSH, legacy applications, WebDAV, etc. Using Safe-T's ZoneZero™ solution, organizations can now provide complete zero trust access for remote employees, partners, applications, IOT devices and more, to company resources regardless of their location.

[1] The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2020 by David Holmes, Sandy Carielli, Andras Cser, Chase Cunningham, Chris Sherman, Brian Kime, and Claire O'Malley, September 18, 2020.

Safe-T's solution provides 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.

About Safe-T

Safe-T Group Ltd. (Nasdaq, TASE: SFET) is a provider of 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.

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 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 31, 2020, 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
Maya Meiri
Maya.Meiri@safe-t.com
+972-9-8666110