



## **תרגום נוחות - נוסח הדיווח המחייב הוא נוסח הדיווח באנגלית**

### **סייפ-טי משיקה שירות SDP ייחודי בענן**

#### **השירות הוא פתרון ה-SDP היחיד המאפשר לארגונים לשמור על שליטה**

**הרצליה, 25 ביוני, 2019** – סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET) ספקית של פתרונות Secure Access לסביבות ענן היברידיות, גאה להודיע על השקת שירות ה-SDP (Software Defined Perimeter) – מוכר גם כ-Zero Trust Network Access) הייחודי שלה. השירות מספק גישה הוליסטית לאבטחת רשתות, המשלבת מספר עקרונות וטכנולוגיות.

טכנולוגיות SDP הפכו לסטנדרט החדש עבור גישה מרחוק ליישומים, ומיישמות את התפיסה לפיה סיכונים קיימים הן מתוך הרשת והן מחוצה לה, ולכן אין לאפשר גישה אוטומטית לאף משתמש, מערכת או שירות.

פתרון ה-SDP של סייפ-טי לוקח את השירותים הקיימים צעד אחד קדימה ומנגיש אותם לחברות ולארגונים המחויבים בבקורות. השירות החדש של סייפ-טי נבנה מהיסוד, והוא מיועד לאפשר לארגונים מכל סוג וגודל ליהנות מהחיסכון המשמעותי בעלויות, המאפיין שירותים מבוססי ענן, תוך שמירה על שליטה במידע הרגיש ומבלי שהארגון יאלץ לוותר על השליטה בפרטי ההזדהות, אישורי האבטחה או הרשאות בעלות רגישות.

"בניגוד לגישה המסורתית לאבטחת רשתות מחשוב, אבטחת Zero Trust מניחה כי אף גורם, בתוך הרשת או מחוצה לה, אינו אמין כברירת מחדל, כך שמכל גורם שמנסה לגשת למשאבים ברשת נדרש תהליך אימות, "ציין איתן ברמלר, סמנכ"ל מוצר וטכנולוגיה בסייפ-טי. "הבנה זו מהווה את הבסיס לשירות ה-SDP בענן החדש שהשקנו, המצטרף לפתרונות ה-SDP הקיימים שלנו, המיועדים להתקנה באתר הלקוח. השירות החדש משלב בין טכנולוגיית SDP מוכחת, הגנת זהות, אימות רב-שלבי (2FA) והכלי שלנו לניתוח נתונים, Telepath, ויוצר את שירות ה-SDP האולטימטיבי."

שירות ה-SDP בענן של סייפ-טי מוגדר ומבוקר ישירות על ידי הארגון, כולל בין היתר הרשאות פרוטוקול Secured Sockets layer (SSL), פרטי הזדהות של משתמשים ועוד. השירות תומך בקשת רחבה של יכולות, המיועדות לארגונים אשר מעוניינים להטמיע פתרון SDP מתקדם:

- נוכחות גלובלית בעשרות מקומות בעולם
- חומת האש הארגונית נמצאת במצב קבוע של חסימה, ומאפשרת גישה ברמת יישום בלבד
- כל התנועה אל הארגון וממנו מנוהלת בחיבורים יוצאים
- תמיכה ב-HTTP/S, SMTP, APIs, RDP ו-WebDAV
- אפשרות גישה מבוססת IPSEC או ללא פעולה בתחנת הקצה לנתונים וליישומים
- תמיכה בכל תרחישי הגישה – משתמשים אנושיים, יישומים, IoT
- אפשרויות אימות מגוונות – Token, Microsoft AD, Azure AD, Okta, DUO Security, built-in OTP ועוד
- שילוב כלי לניתוח התנהגות (UBA) המאפשר איתור של התנהגות משתמשים חריגה, ומונע איומים מבית לפני גרימת הנזק
- בקרה, מעקב ודיווח מלאים אחר שינויי קונפיגורציה
- דיווחים מפורטים על ביצועי המערכת ופעילויות המשתמשים

•  
השירות החדש עלה לאוויר ויעמוד לרשות הלקוחות הקיימים והפוטנציאליים של סייפ-טי באמצעות אתר האינטרנט של החברה ב- [www.safe-t.com](http://www.safe-t.com).

### **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 הפיסי 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**

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



## **Safe-T Launches Exclusive SDP Cloud Service**

*The Only SDP Service Allowing Enterprises to Retain Control*

**HERZLIYA, Israel, June 25, 2019** - [Safe-T® Group Ltd.](#) (Nasdaq, TASE: SFET), a provider of Secure Access solutions for the hybrid cloud, is proud to announce the launch of its unique Software Defined Perimeter (SDP - otherwise known also as Zero Trust Network Access) cloud service. The service provides a holistic approach to network security, incorporating several different principles and technologies.

SDP technologies have become the new standards in remote application access, implementing the philosophy that there are risks both from within and outside of the network, so no users, systems or services should be automatically trusted.

Safe-T's SDP cloud service takes the currently available services to the next level by catering it to enterprises and regulated organizations sector. Safe-T's new service has been designed from the ground up to allow organizations of any size and type to benefit from the significant cost reduction associated with cloud-based services, while retaining control of their sensitive data and not being forced to give up control of their sensitive keys, certificates or user credentials.

"Unlike the traditional IT network security approach, Zero-Trust security 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," said Eitan Bremler, VP Products & Technology at Safe-T. "This understanding is the basis of our newly launched SDP cloud service which has joined our existing SDP on-premises solution. Our new service integrates proven SDP technology, with identity protection, Multi Factor Authentication (2FA), and our Telepath user behavior analysis tool, to form the ultimate SDP service."

Safe-T's SDP cloud service is controlled and configured by the organization itself, which includes Secure Sockets Layer (SSL) keys and certificates, user credentials and more.

Safe-T's SDP cloud service supports a wide range of capabilities designed for organizations that wish to utilize an advanced SDP solution:

- Global presence with dozens of locations around the globe
- Enterprise Firewall is constantly in deny-all state, providing only application-level access
- All traffic to and from the enterprise is handled on outbound connections
- Supports native HTTP/S, SMTP, SFTP, APIs, RDP, WebDAV
- Allows IPSEC-based or client-less access to applications and data
- Supports all access scenarios - human users, applications, IOT
- Robust authentication options – Microsoft AD, Azure AD, Okta, DUO Security, built-in OTP, Token and more.

- Integrated User Behavioral Analysis (UBA), enabling detection of anomalous user behavior, preventing insider threats before they do harm
- Full auditing, tracking and reporting of any configuration changes
- Robust reporting on system performance and user activities.

The new service is live and will be available for Safe-T's customers and prospects through our website at [www.safe-t.com](http://www.safe-t.com).

### **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.

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 advantages of its new SDP solution, its positioning in the market 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**

Karin Tamir

[Karin.Tamir@safe-t.com](mailto:Karin.Tamir@safe-t.com)

+972-9-8666110