



תרגום נוחות - נוסח הדיווח המחייב הוא נוסח הדיווח באנגלית

פתרון SmarTransfer® של סייפ-טי עולה לאוויר לראשונה בחברה ביטחונית ממשלתית

פתרון SmarTransfer® של החברה עבר בהצלחה בדיקות קפדניות של חברה המספקת שירותים ביטחוניים וצבאיים לגופים ממשלתיים

הרצליה, 10 אפריל, 2019 – סייפ-טי, ספקית מובילה של פתרונות software-defined access לסביבות ענן היברידיות, מודיעה היום כי בהמשך להשקת פתרון SmarTransfer® של החברה ולקבלת הזמנה מלקוח בשוק הצבאי, סיימה החברה בהצלחה את הטמעת המוצר בבית הלקוח.

SmarTransfer® הוא חלק מפתרון Software Defined Access (SDA) של סייפ-טי, המיועד לספק למשתמשים פנימיים גישה שקופה לאחסון מאובטח מעבר לפרוטוקול HTTP/S הסטנדרטי. מה שנראה כספריית רשת במבנה סטנדרטי הוא למעשה ערוץ מאובטח ומוצפן בעל בקרת גישה, החושף את הקבצים הרגישים של הארגון למשתמשים בעלי הרשאות הגישה המתאימות בלבד. המשתמשים הניגשים לקבצים באמצעות SmarTransfer מקבלים הרשאות בהתאם לתפקידיהם – העלאה, הורדה, פתיחה, מחיקה, צפייה וכד', והכול על בסיס "need to know".

פתרון SmarTransfer של סייפ-טי מאפשר ללקוחות להחזיר לארגון את השליטה על המידע, ובנוסף מעניק להם את היתרונות הבאים:

- שימוש בגישה למידע רגיש על בסיס "need to know" ללא צורך בהתקנה בצד המשתמש
- ביטול הצורך במיגרציה של נתונים ממקומות אחסון קיימים
- הצפנת קבצים תוך כדי עבודה
- בקרת גישה מלאה
- הפרדה של תכנים בהתאם לתפקידי עובדים שונים

שחר דניאל, מנכ"ל סייפ-טי, ציין: "אנחנו ממשיכים לפעול להשקת פתרונות חדשים בשוק, שיעזרו לארגונים לנטר את הגישה למשאבים רגישים ולמנוע הן איומים חיצוניים והן שימוש לרעה והונאות מבית. אנו גאים על הבעת האמון של הקבלן בשוק הצבאי בפתרון ה-SmarTransfer שלנו."

SmarTransfer מבית סייפ-טי משפר את האבטחה בארגון באמצעות ביטול הצורך להשתמש בפרוטוקול SMB (Server Message Block) הפגיע. כל תהליכי גישה המידע למנוע ההצפנה, לתהליך העבודה ולמדיניות ה-SecureStream של סייפ-טי, מבטיחים גישה מבוקרת ומאובטחת לתכנים ולקבצים מכל סוג, בהתאם לדרישות ממשלתיות, דרישות ביקורת והגדרות של הפרדת תכנים.

ל-SmarTransfer אינטגרציה לפתרון האימות הקיים בארגון (לדוגמה, Active Directory), והוא מבצע אימות של המשתמשים באופן שקוף בעת שהם פותחים את הספריות המשותפות. הרשימה של התיקיות (המקומות הבטוחים) המוצגת למשתמש תלויה בהרשאות ובקבוצה של המשתמש.

אודות סייפ-טי גרופ בע"מ

סייפ-טי גרופ בע"מ (סימול NASDAQ, ת"א: 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's SmarTransfer® Solution Goes Live for the First Time with Leading Government Security Company

Safe-T's SmarTransfer® has successfully passed rigorous testing by a provider of government security and military services

HERZLIYA, Israel, April 9, 2019 — Safe-T Group Ltd. (NASDAQ, TASE: SFET), a provider of software-defined access solutions for the hybrid cloud, today announced that following the launch of Safe-T's SmarTransfer™ solution and the receipt of an order from a military-grade customer, Safe-T has successfully completed the product's implementation at the customer's premises.

Safe-T® SmarTransfer, which is part of Safe-T's Software Defined Access solution, is designed to allow internal users transparent access to secure storages over the standard HTTP/S protocol. What appears as a standard mapped network drive is actually a secure, encrypted and access-controlled channel exposing the organization's sensitive files with the right authorization rights to users. Accessing files via SmarTransfer, users are granted permissions based on their roles - upload, download, open, delete, view, etc., all according to "need to know basis".

In addition to allowing customers the ability to reclaim control over their data, Safe-T's SmarTransfer solution provides the following benefits:

- Employee client-less "need to know access" to sensitive information
- Removing the need to migrate data out of existing storages
- On-the-fly file encryption
- Full access control
- Segregation of duties between various employee roles.

Shachar Daniel, CEO, stated: "We continually strive to launch new solutions to the market which help organizations control access to sensitive resources and prevent not only external threats, but also internal misuse and fraudulent activities. We are proud to receive the vote of confidence from the military contractor to our SmarTransfer solution."

Safe-T's SmarTransfer further improves the security of the organization, by removing the need to use the vulnerable Server Message Block (SMB) protocol. All transactions are subject to Safe-T's SecureStream policy, workflow, and encryption engine, thereby ensuring secure and controlled access to any file type and file content, meeting governance, segregation of duties, and audit requirements.

SmarTransfer integrates with the organization's authentication solution (e.g. Active Directory), transparently authenticating the users when they open their mapped drive. The list of presented Safe Spaces (folders) displayed to the user, depends on the user's group and permissions.

About Safe-T Group Ltd.

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 by masking data at the perimeter, keeping information assets safe and limiting access only to authorized and intended entities in hybrid cloud environments. Safe-T enhances operational productivity, efficiency, security, and compliance by protecting organizations from data exfiltration, leakage, malware, ransomware, and fraud. With Safe-T's patented, multi-layer software-

defined access, financial services, healthcare, utility companies and governments can secure their data, services, and networks from internal and external data threats

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 benefits of its SmarTransfer solution. 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.

INVESTOR RELATIONS:

Michal Efraty +972-(0)52-3044404

michal@efraty.com