

סייפ-טי משיקה את פתרון Zero-Trust Secure File Access – קיבלה הזמנה ראשונה מארגון ביון מוביל

זהו פתרון ה-Proxy הראשון לשיתוף קבצים ב-Windows בפרוטוקול SMB

הרצליה, ישראל, 29 ביוני 2020 – סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET) ספקית של פתרונות Secure Application Access לסביבות ענן היברידי ולסביבות מקומיות, מודיעה היום על השקת אפשרות ייחודית בפתרון Zero-Trust Secure File Access (SFA): Proxy לשיתוף קבצים ב-Windows בפרוטוקול SMB. הפתרון הייחודי נבחר לשימוש על-ידי יחידת ביון מובילה לאחר שהחברה זכתה במכרז. ההזמנה היא לרישיון קבוע, הכולל תחזוקה לשנה, בסכום של כ- 225,000 דולר.

שחר דניאל, מנכ"ל סייפ-טי, ציין: "אנחנו גאים להיות החברה הראשונה שמציגה פתרון Zero-Trust לגישה מאובטחת לקבצים לפרוטוקול SMB, ועל הבחירה בפתרון שלנו על פני ספקים אחרים על-ידי יחידת הביון המתמחה הן באבטחה והן בסייבר. הישגים אלו הם אבני דרך חשובות עבורנו, כיוון שהם מדגישים את מטרת העל שלנו לספק מוצרי אבטחת סייבר חדשניים מהשורה הראשונה, שמעבר להתאמתם לדרישות עסקיות ומסחריות, נותנים מענה מושלם גם לצרכים ממשלתיים וצבאיים. פתרון Zero-Trust SFA הוא פתרון ייחודי וקל לשימוש, ואנו מאמינים שהוא מביא עימו בשורה אמיתית לשוק."

הכלי Zero-Trust Secure File Access הוא חלק ממשפחת מוצרי Zero+ של סייפ-טי. האפשרות החדשה מהווה דרך פשוטה וחכמה עבור לקוחות ועובדים לגישה מאובטחת למערכת שיתוף הקבצים המבוזרת הארגונית באמצעות מערכות הפעלה בפרוטוקול SMB, מבלי לחשוף את התקשורת בפרוטוקול למכשירי הקצה.

לפתרון ה-SFA של סייפ-טי מגוון יתרונות טכניים ותפעוליים, כגון:

- Proxy למערכות שיתוף קבצים מבוזרות בשרתי SMB של Microsoft Windows
- תהליך התקנה, הטמעה ויישום פשוט
- מניעה של גישה או שימוש בלתי מורשים (שינוי סוג הקובץ המקורי, הצפנת קבצים, מתקפות כופר ועוד)

פתרון ה-SFA נשען על התשתית הקיימת בארגון ומעניק להתקנים של משתמשי הקצה תקשורת מאובטחת מבוססת HTTP/S בלבד לרשתות הארגוניות. בעזרת פתרון ה-SFA, יכולים ארגונים להפוך כל שרת SMB מבוזר לשירות ניהול קבצים מאובטח ומבוקר בגישת Trust-Zero, ובכך להגביל את החשיפה למידע רגיש על בסיס need to know, תוך מניעה של גישה ישירה לרשתות ולשרתי ה-SMB המבוזרים של הארגון.

כדי להקנות גישה מאובטחת לאחסון שבשרתי SMB מבוזרים באמצעות פרוטוקול HTTP/S בלבד, פתרון ה-SFA משמש כ-Proxy למערכת שיתוף הקבצים המבוזרת בשרתי ה-SMB של Microsoft Windows. עובדים ולקוחות יכולים להגדיר בעצמם את תצורת כונני הרשת באמצעות דפדפנים מובנים של מערכות ההפעלה (Windows, Mac) וכד'.

פתרון ה-SFA מסתגל ולומד את ההשתייכות לקבוצות ואת ההרשאות המתאימות, כך שהוא מבצע אכיפה של מערכות קבצים בטכנולוגיות חדשות (NTFS) ורשימות בקרת גישה (ACL) ומשקף אותן לתחנות הקצה.

בפתרון SFA של סייפ-טי, המשתמשים יכולים לקבל גישה רק לקבצים אשר תואמים את ההרשאות והגדרות השיוך שלהם בהתאם לגישת Zero-Trust Network Access. הפתרון מאפשר גישה מאובטחת לקבצים בפרוטוקול HTTP/S למשתמשים פנימיים וחיצוניים, עם ובלי צורך בחיבור VPN. כמו כן, מאפשר הפתרון לארגונים לשתף מיפוי כונני רשת מאובטח בכל מקום בעולם, ללא צורך באינטגרציה של צדדים שלישיים או בשימוש בפרוטוקול SMB. בנוסף, ארגונים יכולים לבטל את השימוש בפרוטוקול SMB בין התקני קצה ואחסוני קבצים, ולהפחית משמעותית את הסיכון של מתקפות כופר על שרתי אחסון מרכזיים.

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 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 בדין האמריקאי. לפרטים נוספים, ראה נוסח הדיווח המחייב באנגלית להלן.

פרטי קשר

עדי ומיכל קשרי משקיעים - מיכל אפרתי: 0523044404 michal@efraty.com

Safe-T® Launches its Zero-Trust Secure File Access Solution Received First Order from a Leading Intelligence Unit

The Solution is the First-to-Market SMB Proxy for Windows File Sharing

HERZLIYA, Israel, June 29, 2020 - Safe-T® Group Ltd. (NASDAQ, TASE: SFET), a provider of secure access solutions for on-premise and hybrid cloud environments, today announced that it has launched a unique implementation of its Zero-Trust Secure File Access (SFA) Solution as Server Message Block (SMB) Proxy for Windows File Sharing. The unique solution was selected by a leading intelligence unit, after successfully winning a tender process. The purchase order, in a gross amount of approximately US\$225,000, is for a perpetual license, with a one-year maintenance period.

Shachar Daniel, Safe-T Group's CEO, commented: "We are proud to be the first to introduce our Zero-Trust SFA solution as SMB proxy and to have been selected over other file access vendors to provide our solution to a leading intelligence unit specializing both in cyber and security. These achievements are important milestones for us as they reiterate our mission to provide world class, innovative cyber security products which not only fit business and commercial needs but which we believe are also perfectly suited to government and defense requirements. Our Zero-Trust SFA solution is unique and easy to deploy, and we believe it entails great potential in the market."

The Safe-T Zero-Trust Secure File Access solution is part of Safe-T's Zero+ family of products. This new implementation offers a simple and a smart means to provide employees and customers with secure access to corporate distributed file sharing over SMB operating systems, without exposing the direct SMB communication protocol to endpoint devices.

Safe-T's SFA solution offers the following technical and operational benefits:

- A Distributed File System Proxy for Microsoft Windows SMB servers;
- Simplified installation, integration, and rollout process; and
- Prevention of any unauthorized access or usage (changing original file format, encrypting files, ransomware attacks, etc.).

The SFA solution leverages the organization's existing infrastructure and provides end-users' devices with secure HTTP/S-based communication only, to corporate networks. With the SFA solution, organizations can transform any distributed SMB Server into a Zero-Trust, access-controlled secure file access service, thus limiting exposure of sensitive information on a "need to know basis" only, while eliminating direct access to corporate distributed SMB servers and networks.

To provide secure access to distributed SMB servers' storage, using HTTP/S protocol only, the SFA solution acts as a Distributed File System Proxy for Microsoft Windows SMB servers. Using any Web Client Desktop typically built-in under all Operating Systems (Windows, Mac, etc.), employees and customers can natively configure Drive Mapping under their Operating Systems.

The SFA solution adaptively learns group memberships and the corresponding permissions, so that New Technology File Systems (NTFS) and Access Control Lists (ACL) are enforced and reflected to endpoint users.

With Safe-T's SFA solution, users are only able to see and access files according to their specific group and permissions and in conjunction with Safe-T's Zero-Trust Network Access solutions. The SFA

solution enables secure access to file sharing over HTTP/S for internal and external users, with or without the need for a VPN connection. The SFA solution allows organizations to share the secure map drive all over the world, without any need for third party integrations, or the use of SMB protocols. In addition, with the SFA solution, organizations can eliminate the use of SMB protocols between endpoint devices and file storages, to significantly reduce the chances of dangerous ransomware infection on centralized storages.

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. Safe-T's SDP solution on AWS Marketplace is available [here](#). 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 customer purchases of its products, the fulfillment of customer's orders, the advantages of its Secure File Access solution, its positioning in the market and its potential to address market needs and/or requirements. 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.

COMPANY CONTACT:

Karin Tamir

Karin.Tamir@safe-t.com

+972-9-8666110