



תרגום נוחות - נוסח הדיווח המחייב הוא נוסח הדיווח באנגלית

סייפ-טי משיקה את פתרון ה-SDP הראשון מסוגו לשיפור האבטחה בשוק המסורתי הענק של ה-VPN

הפתרון מפשט את המעבר של ארגונים מ-VPN מסורתי לטכנולוגיית ה-SDP החדשנית, בטוחה ומשופרת

הרצליה, 1 באוגוסט, 2019 – סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET), ספקית מובילה של פתרונות software-defined access לסביבות ענן היברידי ולסביבות מקומיות, מודיעה היום על השקת ZoneZero, פתרון Software Defined Perimeter (SDP) המוכר גם בשם Zero Trust Network Access (Zero Trust Network Access) מקומי ראשון מסוגו לשיפור האבטחה של רשתות וירטואליות מקומיות (VPN) קיימות בארגונים באמצעות שילוב יכולות Zero Trust ותוך שינוי תשתיות מינימליים.

טכנולוגיות VPN היוו את אבן הפינה של אבטחת רשתות ב-20 השנים האחרונות ויותר, והן מאפשרות למשתמשים להתחבר באופן מאובטח לרשתות ולשירותים. לפי Global Market Insight, ההכנסות בשוק ה-VPN צפויות לעלות מ-17 מיליארד דולר ב-2018 אל יותר מ-54 מיליארד דולר ב-2024.

בעוד שטכנולוגיות VPN עמדו במבחן הזמן, למיטב ידיעתנו, בתעשיית אבטחת המידע מבינים כי ארכיטקטורת אבטחה אמיתית תלויה בעקרונות של Zero Trust Network Access, לפיהם אף גורם או אדם אינו זוכה לאמון באופן אוטומטי, במיוחד אם מדובר בישויות חיצוניות שמקורן בתוך היקף הרשת.

"זהו אירוע מרגש עבורנו בסייפ-טי גרופ. בשנה וחצי האחרונות, עבדנו קשה יחד עם מומחי האבטחה, הוועדה המייעצת והשותפים העסקיים שלנו ברחבי העולם להבאת הבשורה המרגשת", אמר איתן ברמלר, מייסד משותף וסמנכ"ל טכנולוגיות בסייפ-טי גרופ. "ZoneZero פותח בפני סייפ-טי קשת רחבה של הזדמנויות עסקיות וחדשנות בשוק ה-SDP. למיטב ידיעתנו, עבור לקוחותינו, פתרונות VPN הם משאב מצוין, ומתוך ההבנה שיש להגדיר מחדש את היקף האבטחה של הארגון, הם תרים אחר אמצעי בטיחות נוספים למניעת גישה בלתי מורשה למשאבי החברה. עבור השותפים והמשווקים שלנו, פתרונות VPN בפני עצמם הם רק התחנה האחרונה בשרשרת האבטחה, והוספת יכולות SDP ל-VPN יוצרת את פתרון העתיד."

הסטנדרט בשוק ה-SDP הוא לעודד לקוחות להחליף את הגנות ה-VPN שלהם כדי להטמיע את פתרון ה-SDP. למיטב ידיעת החברה, לקוחותינו השקיעו בפתרון VPN מקיף, והם לא ימהרו להחליף אותו. עדות לכך נמצאת בסקר שנערך לאחרונה על-ידי Cloud Security Alliance, ובו ציינו 58% מהמשיבים כי טכנולוגיות VPN קיימות מהוות מחסום לאימוץ SDP, כך שברור כי בעולם ה-SDP נדרשת דרך חשיבה חדשה.

מתוך הזיהוי כי ארגונים אינם מחליפים בקלות את פתרונות ה-VPN שלהם, שחררה סייפ-טי גרסה חדשה של פתרון ה-SDP שלה. הגרסה נקראת ZoneZero והיא מיועדת לעבוד יחד עם תשתית ה-VPN הקיימת של הארגון, ולשפר את האבטחה בעזרת הוספת יכולות SDP, כך שנוצרת תשתית SDP ו-VPN משולבת וחזקה יותר. הטמעת ZoneZero של סייפ-טי מאפשרת לארגונים להתחיל בקלות במסע להחלפת VPN ב-SDP.

ZoneZero של סייפ-טי מהווה כעת את פתרון ה-SDP היחיד בשוק אשר מיועד לשיפור ביצועי האבטחה של פתרונות VPN קיימים, באמצעות הוספת יכולות Zero Trust במקום להחליף אותם.

"כדי להשתמש באופן אפקטיבי בעקרונות Zero Trust, ארגונים פונים לפתרונות SDP, שנועדו לספק בדיוק את החסר בפתרונות VPN – הפרדה פיזית של שכבת הגישה משכבת ההזדהות על בסיס פרטני, מבזר ולפי צורך בלבד", אמר אמיר מיזער, מייסד וסמנכ"ל ארכיטקטורה בסייפ-טי גרופ. "הטמעה של פתרון ZoneZero על גבי תשתית ה-VPN הקיימת יוצרת פתרון Zero Trust ניתן להתאמה, שמעניק ללקוחות ולשותפים שלנו את כל היתרונות של SDP תוך חיסכון בזמן ובמשאבים, תוך כדי שימור של הסגמנטציה המסורתית של הרשת, חומת האש, כללי ה-VPN וקווי המדיניות, הניתוב וחווית המשתמש הפשוטה והשקופה לגישה מרחוק ללא שינוי. אנו מאמינים כי בעתיד, כל תשתיות ה-VPN יכללו יכולות SDP."

פתרון ZoneZero של סייפ-טי מציע את היתרונות הבאים:

- אין צורך לפרק ולהחליף תשתית VPN טובה קיימת
- חיסכון לצוותי אבטחת המידע בארגון בכאב הראש ובטרחה הכרוכים בהחלפת ארכיטקטורות VPN קיימות
- המשתמשים ממשיכים להשתמש בפתרון הקצה שלהם ללא צורך בשינוי
- אין צורך להסיר או לשנות רכיבי רשת ורכיבי אבטחה קיימים
- אימות זהות המשתמשים לפני מתן גישה, כמעט ללא שינויים ברשת
- גישה דינמית לפי דרישה ליישומים, בהתאם לתפקידי המשתמשים או להרשאותיהם
- הורדת משתמשים מהרשת וסגירת פתחים בחומת האש לאבטחה משופרת

אודות סייפ-טי גרופ בע"מ

סייפ-טי גרופ בע"מ (סימול Nasdaq, TASE: SFET) היא ספקית של פתרונות Zero Trust Access אשר נועדה לצמצם התקפות סייבר על שירותים עסקיים קריטיים ונתונים רגישים של ארגונים. הפתרונות של סייפ-טי לענף ולשירותים 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 the First Ever SDP Solution for Enhancing Security of the Huge Traditional VPN Market

The solution simplifies organization's journey from traditional VPN to innovative and better secured SDP

HERZLIYA, Israel, August 1st, 2019 - Safe-T® Group Ltd. (Nasdaq, TASE: SFET), a provider of Secure Access solutions for on-premises and the hybrid cloud, announced today the launch of ZoneZero, the first ever Software Defined Perimeter (SDP - otherwise known also as Zero Trust Network Access) on-premises solution designed to enhance organizations' existing Virtual Private Network (VPN) security with Zero Trust capabilities and minimum infrastructure changes.

VPN technologies have been a cornerstone of secure networking for the last 20+ years, allowing users to connect securely to internal networks and services. According to Global Market Insight, VPN revenue will exceed \$54 billion by 2024, up from \$17 billion in 2018.

While VPNs have stood the test of time, to the best of our knowledge, the information security industry has become aware that a true security architecture is hinged upon the concept of Zero Trust Network Access. This means that no one and nothing is trusted by default, especially if they are external entities that originate inside the network perimeter.

"This is an exciting event for us at Safe-T Group. We have been working very hard over the past year and a half with our security experts, advisory board, customers and business partners around the globe to bring this exciting news," said Eitan Bremler, Co-Founder and VP technology at Safe-T Group. "ZoneZero creates a junction of business opportunities for Safe-T's SDP market, roadmap and innovation. As far as we know, for our customers, VPNs are a great resource, and while understating that organizations perimeter must be redefined, they are constantly looking to add additional safeguards in place to prevent unrestricted access to company resources. For our partners and resellers, VPN on its own is no more the last stop in the security equation and adding SDP capabilities into the VPN is the solution for the future."

The SDP industry standard is to encourage customers to rip and replace their VPN, in order to deploy their SDP solution. To the best of the Company's knowledge, its customers have invested in a comprehensive VPN and are reluctant to replace it. A testament to this is a recent survey conducted by the Cloud Security Alliance, in which 58% of respondents stated that existing VPN technologies are a barrier to SDP adoption, it is clear a new way of thinking is required in the SDP space.

Recognizing that organizations don't easily replace their existing VPN deployment, Safe-T has released a new version of its SDP solution dubbed ZoneZero which is designed to work together with the organization's existing VPN infrastructure, enhancing VPN security by adding SDP capabilities while yielding a more fortified SDP and VPN infrastructure together. Deploying Safe-T ZoneZero allows organizations to easily start a journey towards VPN replacement with SDP.

Currently, Safe-T's ZoneZero is the only SDP solution in the market targeted at enhancing VPN security by adding Zero Trust capabilities, rather than replacing it.

"To effectively enact Zero Trust principles, organizations are turning to SDP solutions which are designed to provide exactly what VPN solutions are missing – individual, granular and need-to-know basis only, while physically separating the access layer from the authentication layer," said Amir Mizhar, Founder and Chief Software Architect at Safe-T Group. "Implementing our ZoneZero solution on top of existing VPN deployment creates a customized and scalable Zero Trust solution that gives our customers and partners all the benefits of SDP, while saving time and resources, keeping traditional network segmentation, firewall, VPNs policies and rules, routing and same old simple and transparent user remote access experience - untouched. We believe that in the future, all VPN infrastructure deployments will include SDP capabilities."

Safe-T's ZoneZero solution offers the following benefits:

- Forget about ripping and replacing a perfectly capable VPN.
- Save IT teams the headache and hassle that come along with changing existing VPN architectures.
- No behavior changes to the users – continue using their VPN client
- No need to remove/change existing network and security components
- Authenticate users before granting access, with almost zero network change
- Dynamic, on-demand application access according to user role/permission
- Takes users off the network and closes firewall ports for enhanced security

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

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

+972-9-8666110