סייפ-טי מציעה לארגונים בחינה ללא עלות של הרשתות ומרחבי התקיפה בעקבות מתקפות שרשרת האספקה האחרונות דרך SolarWinds

"מתקפות רחבות היקף שנחשפו לאחרונה מעניקות משנה תוקף לאסטרטגיה העסקית ולאסטרטגיית המוצר של סייפ-טי בשנה החולפת, של יישום גישה פרואקטיבית לזיהוי איומים פוטנציאליים ופיתוח מוצרים מתקדמים למניעת ובלימת מתקפות"

הרצליה, 28 בדצמבר, 2020 - סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET), ספקית של פתרונות Secure Access לסביבות ענן היברידי ולסביבות מקומיות, מודיעה היום כי לאור המתקפות האחרונות על שרשראות אספקה, כגון מתקפת Sunburst (או Solarigate), תציע החברה לארגונים בחינה ללא עלות של הרשתות הארגוניות ומרחבי התקיפה שלהן. פתרון הזיהוי הרב-שלבי מבית סייפ-טי, ZoneZero™ Multi-Factor Authentication (MFA), מיועד להוסיף רכיב מרכזי חזק של אימות ומדיניות ניהול הגישה לכל משאבי הארגון ולהגן על ארגונים מפני מתקפות על שרשרת האספקה, כולל מהסוג שנחשף לא מכבר.

לאחרונה, דווח כי גורם עוין הצליח להסתנן למערכות מידע של ארגונים רבים, ובכלל זה מספר סוכנויות ממשלה אמריקניות. הוא עשה זאת באמצעות הפצת תוכנת דלת אחורית (backdoor) בשם SunBurst, בדרך של ניצול חוליה חלשה במערכת העדכונים של תוכנת הניטור והניהול Orion IT מבית SolarWinds והחדרה של קוד זדוני לתוך עדכוני תוכנה אותנטיים ולגיטימיים. לאחר שהושגה הגישה באמצעות הדלת האחורית, פעלו התוקפים להרחיב את ההרשאות שהושגו, לגנוב פרטי הזדהות ולשוטט ברחבי הרשת הפנימית בחיפוש אחר נתונים ספציפיים.

על-פי נתוני SolarWinds, 33,000 ארגונים משתמשים בתוכנות Orion, ו-18,000 נפגעו באופן ישיר מהעדכון הזדוני. עם חשיפתם של פרטים נוספים התברר כי מדובר באחת ממתקפות הסייבר הפולשניות והמשמעותיות ביותר עד היום.

פתרון ZoneZero™ MFA מבית סייפ-טי הוא פתרון ה-ZTNA (Zero Trust Network Access) הראשון מסוגו שנועד להוסיף זיהוי רב-שלבי מרכזי לכל משאבי הארגון, כולל מערכות, שרתים, נתונים, יישומים ועוד. אצל לקוחות המשתמשים בפתרון, כאשר מתבצע ניסיון לגשת לשרת ממערכת שנפגעה, נוצרת בקשה לזיהוי רב-שלבי, אשר עד אישורה נמנעת כניסת המקור הבלתי מורשה לרשת.

"מתקפות רחבות היקף שנחשפו לאחרונה מעניקות משנה תוקף לאסטרטגיה העסקית ולאסטרטגיית המוצר של סייפ-טי בשנה החולפת. אנחנו מיישמים גישה פרואקטיבית לזיהוי איומים פוטנציאליים ופיתוח מוצרים מתקדמים המיועדים למנוע מתקפות מסוג זה ולהכיל את השפעותיהן. פתרון ZoneZero™ MFA שהשקנו מוקדם יותר השנה הוא דוגמה מעולה להתאמות שאנו מבצעים אל מול סוגים חדשים של איומי סייבר," אמר שחר דניאל, מנכ"ל סייפ-טי.

"הגישה המרכזית שלנו מתבססת על ההנחה כי התוקף כבר נמצא בתוך הרשת, ומונעת ממנו להתקדם ולשוטט בתוך הרשת. באמצעות הוספת ZoneZero™ MFA לרשת, ניתן כעת להבטיח שכל בקשה מצד משתמש או יישום לגשת ליישום פנימי כלשהו תתניע פעולת זיהוי רב-שלבי, כך שלהאקרים ולתוקפים חיצוניים לא יתאפשר לנוע בתוך הרשת. הפתרון שלנו מאפשר ללקוחות להטמיע בקלות זיהוי רב-שלבי ומודעות להזדהות בכל תרחישי הגישה - משתמשים פנימיים ומשתמשים מרחוק, רשתות VPN, יישומי רשת ויישומים שאינם ברשת.

"אלפי חברות, גופים ממשלתיים וארגונים לא ממשלתיים משתמשים ב-SolarWinds. למרות שלא ניתן לחשוף מי מבין לקוחותינו חוו פריצה, אנו מאמינים כי השימוש בפתרון ZoneZero™ MFA מסוגל למנוע מההאקרים תנועה מפתרון SolarWinds הפגוע למשאבים אחרים ברשת, ובכך למעשה לקטוע את שרשרת התקיפה הראשית. מניעת החדירה של מתקפת הסייבר פנימה מבטיחה כי לקוחותינו מוגנים מפני החלק המסוכן ביותר של המתקפה, והם ערוכים לשרוד מתקפות עתידיות על שרשרת האספקה. אנחנו מעודדים ארגונים אשר נשענים על אמצעי אבטחה מסורתיים לשקול שימוש בפתרון שלנו להגנה על הרשתות שלהם. למרות שמדובר באחת ממתקפות האבטחה הרחבות בהיסטוריה, ברור לנו שהיא לא תהיה האחרונה," סיכם מר דניאל.

למידע נוסף אודות ZoneZero™ MFA והמתקפה על SolarWinds, קראו את הפוסט בבלוג שלנו כאן.

אודות סייפ-טי

סייפ -טי גרופ בע"מ (סימול NASDAQ, TASE: SFET) היא ספקית של פתרונות גישה אשר נועדו לצמצם התקפות סייבר על שירותים עסקיים קריטיים ונתונים רגישים של ארגונים תוך שמירה על המשכיות עסקית רצופה. הפתרונות של סייפ-טי לענן ולשרתים מקומיים מבטיחים שכל תרחישי הגישה של הארגון, לתוך הארגון ומחוצה לו, מאובטחים ע"פ פילוסופיית "אשר קודם, תן גישה אח"כ" של Trust Zero. גישה זאת מניחה שאין אדם מאושר גישה מראש, ללא תלות במיקומו הפיזי ושיוכו הארגוני, וכל משתמש אשר מנסה לגשת לשירות ארגוני, בין אם הוא בענן או בתוך הארגון, חייב, כשלב ראשון, לקבל אישור גישה.

המגוון הרחב של פתרונות הגישה המאובטחת של סייפ-טי מצמצם את מרחב התקיפה הארגוני ומשפר את סיכויי הארגון להגן על עצמו מפני איומי סייבר מודרניים. 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 דינמית, כתלות במספר המשתמשים המחוברים ואינטגרציה פשוטה עם השירותים שלנו. 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. אנו בסייפ-טי מעניקים לארגונים אפשרות לעבור בבטחה לעבודה בענן ומאפשרים טרנספורמציה דיגיטלית.

את פתרון ה-SDP של סייפ-טי ב-AWS Marketplace ניתן למצוא כאן

למידע נוסף אודות סייפ-טי, בקרו באתר www.safe-t.com

מידע צופה פני עתיד

פרסום זה כולל מידע צופה פני עתיד כמשמעותו בדין האמריקאי. לפרטים נוספים, ראו נוסח הדיווח המחייב באנגלית להלן.

פרטי קשר
מיכל אפרתי
עדי ומיכל קשרי משקיעים
0523044404
michal@efraty.com

Investor Relations Contact
Gary Guyton
MZ Group - MZ North America
469-778-7844
SFET@mzgroup.us
www.mzgroup.us

Safe-T Offers Free Review of Organizations' Networks and Attack Footprint in Face of Recent SolarWinds Supply Chain Attacks

"Recent wide-range attacks provide further confirmation of Safe-T's business and product strategy in the past year, of executing a proactive approach to identify potential threats and develop advance products for the prevention and containment of attacks"

HERZLIYA, Israel, December 28, 2020 -- Safe-T® Group Ltd. (NASDAQ, TASE: SFET), a provider of secure access solutions for on-premise and hybrid cloud environments, announced today that in the face of recent supply chain attacks, such as the Sunburst (or Solarigate) attack, it is offering free of charge review of organizations' networks and attack footprint. Safe-T's ZoneZero™ Multi-Factor Authentication (MFA) solution is designed to add the core component of a strong identity and access management policy to any corporate resource and secure organizations against supply chain attacks, including the recent attacks.

Recently, it was reported that a threat-actor managed to infiltrate a large number of organizations, including several U.S. government agencies. It did this by distributing backdoor software, named SunBurst, by utilizing a weak link in SolarWind's Orion IT monitoring and management software update system and then inserted malicious code into otherwise legitimate software updates. Once backdoor access was achieved, attackers worked to gain privilege escalation, steal credentials and then laterally traverse the internal network scanning for targeted data.

Based on SolarWind's data, 33,000 organizations use Orion's software, and 18,000 were directly impacted by this malicious update. As more details have become available, it has become clear that this is one of the most invasive and significant cyberattacks to date.

Safe-T's ZoneZero™ MFA is the first ever Zero Trust Network Access (ZTNA) solution which is designed to add centralized MFA to any corporate resource including system, server, data, application, and more. For clients using the solution, when an attempt to access a server from an infected system occurs, it invokes an MFA request that until approved, prevents the infiltration of the unauthorized source.

"Recent wide-range cyber-attacks affirm Safe-T's business and product strategy in the past year. We are executing a proactive approach to identify potential threats and develop advanced products designed to prevent and contain such attacks. Our ZoneZero™ MFA solution, which was launched earlier this year, is a great example of our alignment against new types of cyber threats," said Shachar Daniel, CEO at Safe-T.

"Our centralized approach assumes the attacker is already in the network and prevents the spread of the attack from moving laterally throughout the network. By deploying ZoneZero™ MFA in the network, it is now possible to ensure that any request from any user or application to any internal application would invoke an MFA action, blocking hackers or third-party attacks from moving around the network. Our solution allows customers to easily integrate MFA and identity awareness into all access scenarios – remote and internal users, VPNs, web, and non-web applications.

“SolarWinds is used by thousands of companies, government agencies and NGOs. Although any breach to our customers' systems remains confidential, we believe that using our ZoneZero™ MFA could successfully prevent the hackers from traversing from the infected SolarWinds solution to other resources in the network, thus cutting the main attack vector. Stopping the infiltration of a cyber-attack ensures that our customers are protected against the most dangerous part of the attack and are well positioned to survive future supply chain incidents. We encourage organizations who rely on traditional security measures to consider our solution to protect their network. Although this has been one of the widest security attacks in history, we know it will not be the last,” concluded Mr. Daniel.

To learn more about ZoneZero™ MFA and the SolarWinds attack, please read our blog post here.

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 types and sizes 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 benefits of its ZoneZero™ MFA solution, such as that it would successfully prevent the hackers from traversing from the infected SolarWinds solution to other resources in the network. 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.

INVESTOR RELATIONS CONTACT

Gary Guyton
MZ Group - MZ North America
469-778-7844
SFET@mzgroup.us
www.mzgroup.us

Michal Efraty
+972-(0)52-3044404
michal@efraty.com

COMPANY CONTACT

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