



סייפ-טי גרופ מוכרת ע"י גרטנר כספקית נבחרת במסגרת דוח "טכנולוגיות מתפתחות: תובנות להרחבת האימוץ בתחום Zero Trust "Network Access"

הרצליה, 6 באפריל, 2021 - סייפ-טי גרופ בע"מ (NASDAQ, TASE: SFET), ספקית של פתרונות גישה מאובטחת ואיסוף נתונים חכם, מודיעה היום כי החברה הבת בבעלות מלאה של החברה, סייפ-טי דטה א.ר. בע"מ, הוכרה כספקית נבחרת במסגרת דוח של גרטנר, אשר פורסם במרץ 2021, בשם "טכנולוגיות מתפתחות: תובנות להרחבת האימוץ בתחום Zero Trust Network Access".¹

הדוח דן בשוק ה-ZTNA הצומח במהירות וכולל סקירה מקדימה של פתרונות ZTNA ותובנות אודות השוק ומגמות הקנייה בו.

לפי גרטנר, "על-מנת למקסם את ההכנסות, על מנהלי מוצרים למקד את מפות הדרכים ואת מאמצי השיווק שלהם בענף הממשלתי, בחברות גדולות ובקניינים בעלי תפקידים טכניים", והם מציינים בממצאיהם העיקריים כי קניינים ממשלתיים וארגונים גדולים מביעים את העניין הרב ביותר בפתרונות ZTNA בהשוואה לביקוש מצומצם מצד ארגונים קטנים יותר.

נוסף על הממצאים העיקריים, דן הדוח בשוק ה-ZTNA כשוק מתפתח, בו ארה"ב וקנדה מביעות את העניין הרב ביותר בהשוואה לטריטוריות אחרות. עם זאת, צמיחת השוק גבוהה בעולם כולו. כמו כן, על אף שההתעניינות גבוהה ביותר בקרב ארגונים גדולים וממשלות, הזדמנויות רבות טמונות בכל הענפים, בפרט בשנת 2020, בה נרשמה עלייה של 230% בהיקף ההתעניינות. ניתן לייחס עלייה זו לשיבושים הגלובליים שנגרמו כתוצאה ממגפת הקורונה.

פתרונות ה-ZTNA של סייפ-טי מאפשרים להעניק גישה ליישומים על בסיס need-to-know, כאשר המשתמשים נהנים מגישה חלקה ומהירה למשאבים הדרושים להם. בגישת Zero Trust מתבצע האימות בשלב הראשון, ורק לאחר מכן ניתנת גישה למשאבי הארגון, והיא מאפשרת אבטחה מוגברת, שקיפות גבוהה יותר וחווית משתמש משופרת. הפתרון שולט על הגישה לשירותים הפנימיים, ונשען על ספקיות זהות חיצונית לאימות הזהות של כל משתמש.

פתרון [ZoneZero](#) מבית סייפ-טי מאחד את כל צורכי הגישה מרחוק בפתרון Zero Trust Network Access יחיד: משתמשים אנושיים (משתמשי VPN, משתמשים ללא VPN ומשתמשים פנימיים), יישומים, ממשקי API ומכשירים מקושרים. הוא מעניק גישה בטוחה לכל משאבי הארגון, ליישומים ולשירותים, כולל יישומים קנייניים, יישומים מבוססי Client, יישומים מבוססי Web ויישומים המבוססים על SSH, RDP, SFTP, SMB, TCP, ממשקי API ועוד. פתרון [ZoneZero](#) מיישם מודלי אבטחה בגישת Zero Trust באמצעות שילוב בין עקרונות "אשר קודם, תן גישה אח"כ", הזדהות חזקה ורציפה והזדהות רב-שלבית לכל המשאבים.

"אנחנו גאים על ההכרה בטכנולוגיית ה-ZTNA שלנו במסגרת הדוח. אנחנו מאמינים שהכרה זו משקפת את מאמצינו המתמשכים להביא לשוק את פתרון ה-Zero Trust הטוב ביותר", אמר שחר דניאל, מנכ"ל סייפ-טי.

¹ Gartner, "Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access," by Analysts Nat Smith, Mark Wah, 22 במרץ, 2021

הפתרון של סייפ-טי מאפשר פריסה פשוטה עבור מכשירים מנוהלים ומכשירים לא מנוהלים. כמו כן, כלי ניתוח התנהגות המשתמשים של הפתרון מעניק תובנות ראשונות מסוגן אודות תנועת המשתמשים, ואלו מאפשרות לזהות בוטים וגורמים זדוניים פנימיים לפני שהם יכולים לגרום לנזק.

Gartner הצהרת

Gartner אינה מקדמת אף ספק, מוצר או שירות המתוארים בפרסומיה המחקריים, ואינה ממליצה למשתמשים בטכנולוגיה לבחור רק בספקים שזכו בציונים הגבוהים ביותר או בתארים אחרים. הפרסומים המחקריים של Gartner מורכבים מדעותיהם של גורמים בארגון המחקר של Gartner, ואין לראות בהם אמירות עובדתיות. Gartner לא תישא באחריות, מפורשת או משתמעת, בנוגע למחקר זה, ובכלל זה לסחירות או תאימות למטרה מסוימת.

אודות סייפ-טי

סייפ-טי גרופ בע"מ (סימול NASDAQ, TASE: SFET) היא ספקית של פתרונות גישה ואיסוף נתונים חכם. הפתרונות שלנו לענן ולסביבות מקומיות מצמצמים התקפות סייבר על שירותים עסקיים קריטיים ונתונים רגישים של ארגונים תוך שמירה על המשכיות עסקית רצופה.

כל 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, אשר נשענים על טכנולוגיית Reverse Access מוגנת הפטנט ועל טכנולוגיית הניתוב הייחודית שלנו, משפר את סיכויי הארגון להגן על עצמו מפני איומי סייבר מודרניים ומאפשר לו לבצע מיגרציה דיגיטלית חלקה למעבר לעבודה בענן.

כמו כן, אנו מציעים שירות איסוף נתונים חכם, מבוסס-ענן, אשר נשען על רשת ה-Business Proxy המהירה, המתקדמת והמאובטחת ביותר בעולם, שמאפשרת ללקוחות לאסוף נתונים מדויקים, שקופים ורגישים ממקורות ציבוריים מקוונים.

את הפתרונות 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 בד"ר האמריקאי. לפרטים נוספים, ראו נוסח הדיווח המחייב באנגלית להלן.

INVESTOR RELATIONS CONTACTS

Chris Tyson
Executive Vice President
MZ Group - MZ North America
949-491-8235
SFET@mzgroup.us
www.mzgroup.us

מיכל אפרתי

052-3044404

michal@efraty.com



Safe-T Recognized by Gartner as a Representative Vendor in "Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access" Report

HERZLIYA, Israel, April 6, 2021 — [Safe-T® Group Ltd.](#) (NASDAQ, TASE: SFET), a provider of secure access solutions and intelligent data collection, today announced that its wholly owned subsidiary, Safe-T Data A.R Ltd., has been recognized as a Representative Vendor in Gartner's March 2021 report titled, "Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access"¹.

The report discusses the fast-growing ZTNA (zero-trust network access) market and includes an introduction to ZTNA and insights into the market and buyer trends.

According to Gartner, "To maximize revenue, product leaders should focus roadmaps and go-to-market efforts on the government industry, larger companies and technical role buyers," stating in its key findings that government buyers and large organizations have the most interest in ZTNA, compared to a diminishing appeal by smaller organizations.

In addition to key findings, the report discusses that ZTNA is an emerging market, with North America shoring the most interest compared to any other geography; however, growth is strong worldwide. Additionally, while government and large organizations are the most interested industries, there is strong opportunity in all industries, particularly in 2020, which showed a 230% growth in interest. This can be attributed to the global disruption caused by the COVID-19 pandemic.

Safe-T's ZTNA solutions grant access to applications on a need-to-know basis, while giving users fast and seamless access to the resources they need. This creates a "verify-first, access-second" zero-trust approach across an organization's applications, enabling enhanced security, greater visibility, and a better user experience. It controls the access to internal services and utilizes third-party identity providers to authenticate each user.

[Safe-T ZoneZero®](#) unifies all remote access needs in one zero-trust network access solution: human users (VPN users, non-VPN users, internal users), applications, APIs, and connected devices. It grants secure access to all corporate resources, applications and services, including Web, SSH, RDP, SFTP, thick applications, proprietary applications, SMB, TCP, APIs, and more. ZoneZero® applies Zero Trust security models by orchestrating authentication first, access later concepts, with strong and continuous authentication, and multifactor authentication to all resources.

"We are honored to be recognized in the report for our ZTNA technology. We believe that it reflects our continuous efforts to provide the best zero-trust solution to the market," said Shachar Daniel, CEO of Safe-T."

¹ Gartner, "Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access," by Analysts Nat Smith, Mark Wah, March 22, 2021

Safe-T's solution provides a simple deployment for both managed and unmanaged devices. In addition, the solution's user behavior analysis module, provides unparalleled insight into user traffic, which allows it to detect bots and malicious insiders before they have the chance to cause damage.

Gartner Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Safe-T®

Safe-T Group Ltd. (Nasdaq, TASE: SFET) is a provider of access solutions and intelligent data collection.

Our cloud and on-premises solutions mitigate attacks on enterprises' business-critical services and sensitive data, while ensuring uninterrupted business continuity. 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 Safe-T's 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.

The wide range of access solutions, empowered by our patented reverse-access technology and proprietary routing technology, reduce organizations' attack surface, improve their ability to defend against modern cyberthreats and enable them smooth digital transformation and to safely migrate to the cloud.

We also offer intelligent data collection cloud service, based on our world's fastest and most advanced & secured business proxy network which enables clients to collect accurate, transparent & sensitive data from public online sources.

Safe-T's solutions on AWS Marketplace are 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 the advantages of its ZoneZero® solution and continuing to provide customers with the tools they need to prevent unauthorized users from accessing company resources. 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

22, 2021, 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 CONTACTS:

Chris Tyson
Executive Vice President
MZ Group – MZ North America
949-491-8235
SFET@mzgroup.us
www.mzgroup.us

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