Secure Access Service Edge- SASE שירותי

המהפכה שבדרך

תקציר מנהלים

כחלק מתפיסת ה- Zero Trust שירותי ה- Secure Access Service Edge- SASE הנם שירותים עננים חדשניים שישנו חלקים מרכזיים בתפיסת אבטחת המידע של ארגונים קטנים כגדולים בעיקר באופן החיבור של התקני קצה (מחשבים וטלפונים) למשאבי הארגון – מה שהיה נקרא פעם – "חיבור לרשת הארגונית".

על פי תפיסה זו במקום לרכוש 20-35 מוצרי אבטחת מידע שונים שמותקנים ומתוחזקים על ידי הארגון בנפרד, הארגון ירכוש שירות מספק אחד אשר יספק לו את הפונקציונליות של רובם המכריע של המוצרים הנוכחיים כאשר מלאכת התחזוקה וחיבור המוצרים השונים – מתבצעת על ידי ספק ה- SASE.

בסופו של דבר ה- SASE ישמש לחיבור של המשתמשים למשאבי הארגון באופן אחיד הן בתוך הארגון (סניפים ומטה) והן מחוץ לארגון (מהבית) ובעתיד ניתן יהיה להשתמש באותו העקרון לתקשורת בין משאבי הארגון השונים (east west communication).

מדובר בשינוי מהותי בתפיסת הגנת הסייבר בארגונים. עבודה זהה בין המשרד לבית מבחינת אבטחת המידע. הגנה יותר טובה על הארגון. פחות מוצרים לרכוש (לכן יהיו פחות חברות סייבר), פחות מוצרים לקנפג\לתחזק ולחבר.

רקע: מה הביא להיווצרותם של שירותי ה- SASE

ישנן שלוש תופעות אשר מסבירות את היווצרותם של שירותי ה- SASE.

תופעה ראשונה היא הענן. השימוש במשאבים טכנולוגיות שאינם נמצאים בבעלות ובאתר החברה הופך להיות נפוץ יותר ויותר וישנן הרבה חברות בעיקר הצעירות ושגדלות הכי מהר שלא מחזיקות Data Center (DC) מרכזי כלל כלומר כל משאבי הארגון הטכנולוגיים נמצאים בענן. תופעה זו מקילה עלינו להשתמש בפתרונות ענן גם למוצרי אבטחת מידע. וגם מתחברת לתופעה השנייה והיא העבודה מהבית. בגלל הקורונה יותר ויותר ארגונים מאפשרים לעובדים לעבוד מהבית חלק כזה או אחר משבוע העבודה. ישנן מספר דרכים לבצע עבודה מאובטחת מהבית כאשר דרך נפוצה היא שימוש במחשב מנוהל (מחשב חברה מפוקח) שמתחבר לארגון דרך טכנולוגיית VPN. לעיתים לתוך הארגון עצמו ולעיתים דרך טכנולוגיית SBC- server based computing כמו VDI או Terminal Server (שמראה למשתמש את תמונת המסך). אולם בתצורה זו כאשר המשתמש רוצה לעבוד מול משאבי הארגון שנמצאים בענן הציבורי החוויה שמתקבלת אינה טובה כי התקשורת עוברת ממחשב העובד שנמצא בבית, ל-DC ורק אז יוצאת החוצה לענן. ככל שארגונים מאפשרים יותר עבודה מהבית ובמקביל משתמשים באפליקציות עננית כך האתגר גדול יותר. לעיתים ארגונים מאפשרים עבודה מול אפליקציות ענן ארגוניות ישירות ממחשב העובד בבית (ללא מעבר התקשורת ל-DC בחברה) אולם הדבר מסוכן ומתקשר לתופעה השלישית שמהווה רקע ל-SASE והיא העלייה בהתקפות הכופרה. ארגונים מבינים שעליהם לספק מעטפת הגנה רחבה וחזקה. ולכן חיבור מחשבים לרשת האינטרנט ללא הגנה מלאה היא פעולה מסוכנת במיוחד כעת.

מהי טכנולוגיית ה-SASE

הבסיס של טכנולוגיית ה- SASE היא שירות ענן ל- VPN כלומר חיבור מרחוק של משתמשים. במקום לרכוש מוצר VPN ולהתקנו בארגון (בדרך כלל ב- DMZ) המשתמש מתקין AGENT על המחשב שמנתב את התקשורת לשירות ה- VPN העננית[1]. בזמן החיבור הראשוני ה- VPN מזהה את המשתמש (באמצעים שלו או דרך שימוש בשירותי הזדהות חיצוניים כגון OKTA, AzureID , OneLogin וכד'), לאחר מכן מתבצעת בדיקה של ההתקן שרוצה להתחבר לרשת ה- VPN לפי מדיניות שהחברה קובעת – האם מערכת ההפעלה עדכנית, האם מותקן EPP\EDR, האם התוכנות שמותקנות בהתקן הנן לגיטימיות וכד'.

לאחר החיבור לשירות ה- SASE (כלומר יש אישור להתחבר) המשתמש יכול להשתמש במשאבים הארגוניים שמותרים לו.

---

[1] ישנם שם יישומים לשימוש ב- SASE ללא התקנת AGENT בעיקר לגורמים חיצוניים שלא מאפשרים התקנה ותחזוקה של AGENT

מאפיין של שירות ה- SASE הוא שכל תעבורת המשתמש מנותבת דרך שירות ה- VPN (SASE) כולל התעבורה שאינה קשורה לעבודה (כמו גלישה ל- YNET).

שירות ה- SASE הנו מבוזר ואמור להיות קרוב למשתמש הסופי (POP[2] קרוב ללקוח) כך שהתעבורה עוברת במהירות וללא עיקוב מהמשתמש ל- POP המקומי ומשם ליעד. הניתוב ל-POP מתבצע באופן אוטומטי – כאשר משתמש עובד מישראל הוא יקבל שירות מה- POP המקומי בישראל אך כאשר נוסע לחו"ל יקבל שירות מה- POP במיקום הגיאוגרפי הקרוב ביותר.

כבכול VPN לאחר החיבור הראשוני מתבצעות שתי משימות עיקריות – חיבור למשאבים הארגוניים הן אם ב-DC (לדוגמה חיבור ל- ERP הארגוני שמותקן ב- DC) והן בענן (לדוגמה חיבור ל-CRM עננ) ללא צורך בהזנת סיסמא נוספת – מה שנקרא Single Sign On – SSO והמשימה השנייה היא הצפנת התקשורת מהמשאב הארגוני למחשב המשתמש. התקשורת מוצפנת על ידי ה- VPN ביציאה מהמשאב ונפתחת כאשר מגיעה למחשב[3].

עד כאן אין ממש מהפכה מבחינת הארגון כי בסך הכל מדובר על שימוש בשירות של VPN במקום רכישה התקנה ותפעול של מוצר VPN מסורתי.

ואולם עכשיו הפואנטה. מכיוון שכל התעבורה של המשתמש עוברת דרך שירות ה- VPN ניתן לבצע על הנתונים שעוברים משימות אבטחה שונות שאינן קשורות למשימה הבסיסית – חיבור המשתמש למשאבים המרוחקים. איזה משימות אבטחה? בעקרון כולן!!

הערה– לאחרונה התחילו גרטנר להסתכל על שוק מצומצם יותר מ- SASE מכיל רק את רכיבי האבטחה, ללא רכיבי התקשורת ואף ללא רכיבי החיבוריות. התחום (המתפתח) נקרא Security Service Edge (SSE).

איזה משימות אבטחה יכולים שירותי ה-**SASE** לכלול

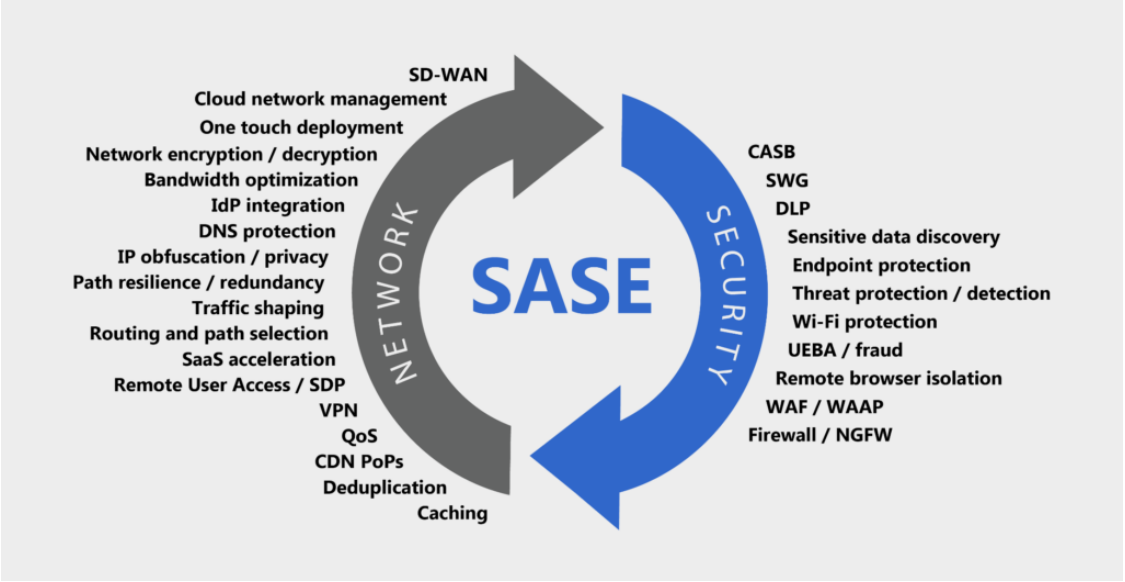
מכיוון שכל התעבורה היוצאת והנכנסת מנותבת דרך ספק השירות ניתן לכלול תחת שירות ה- SASE את כל משימות אבטחת המידע שקשורות לתעבורה של המשתמש למשאבי הארגון (north south).

להלן דיאגרמה שמציינת יכולות פוטנציאליות של שירותי SASE – חלקן אגב קשור לתקשורת ולא לאבטחת מידע:

---

[2] POP – Point of Presence

[3] זאת כאשר אין מכניזם אחר לביצוע ההצפנה- כי בדרך כלל אפליקציות WEB מכילות הצפנה מובנת של התקשורת על ידי HTTPS אולם לא כל האפליקציות בשימוש בארגון הן אפליקציות WEB.



1. FW ו- WAF עד לרמת DPI כך שבמקום שפיקוח על התקשורת ברמת ה- IP , ברמת ה- WEB וברמת האפליקציה הפיקוח\אישור\חסימה יתבצע בתחנת הקצה או בכניסה לארגון הדבר מתבצע כאשר התעבורה מגיעה כולה לשירות ה- SASE.
2. גלישה מאובטחת RBI remote browser isolation– כאשר ישנה תעבורה מאתרים שאינם מוכרים (אבל עדיין רוצים לאפשר את הגישה אליהם) מומלץ לבצע את הגלישה בפועל במקום שאינו חשוף (לא במחשב המשתמש עצמו) ורק להעביר את תמונת המסך. במקום שתשתית ה- RBI תתבצע ב-DC הארגוני שירותי SASE מציעים לבצע משימה זו קרוב למשתמש ב- POP המקומי ובכך לשפר את חויית הגלישה.
3. UBA - user behavior analytics – שמחפשת תבניות להתנהגות שלילית של משתמשים (לדוגמה זיהוי BOTS שמשדרים מתוך המחשב) – במקום להשתמש ב- AGNET ייעודי שמותקן על המחשב ומבצע את הניתוח בעצמו או במרכז – מדובר על שירות מרכזי ורב כוח (כי רואה התנהגות של משתמשים רבים)
4. WIFI PROTECTION – כחלק מהחיבור הראשוני לשירות ה- SASE – בדיקה האם סביבת ה- WIFI לגיטימית
5. יכולות Advanced Threat Protection (ATP) לזיהוי מתקפות מתקדמות באמצעות יכולות AI ML – גם כאן כי מנצלים שכל התעבורה עוברת דרך ה- POP המקומי וניתן לבצע את האנליזה שם.
6. Endpoint protection מסורתית – בדיקה שהתקני ה- EPP עובדים כשורה – לפי המדיניות שקבע הארגון (כל ארגון יכול לקבוע מדיניות אחרת שנחשבת "מאושרת" עד כדי החלטה שרק מחשב בו הדיסק מוצפן נחשב כ"מאושר").

7. DLP – data leak prevention שמוודאים שמידע רגיש אינו עוזב את הארגון – בין אם בכוונה ובין אם בגלל טעות אנוש. גם אם מדובר על מקורות מידע\קבצים שידועים בתור כאלה שמכילים מידע רגיש וגם גילוי בזמן השימוש על מקורות מידע חדשים שמכילים מידע רגיש (sensitive data discovery).
8. Web Gateway protection – לוודא שלא ניגשים לאתרים אסורים לפי מדיניות החברה (הימורים, שיתופי קבצים וכד') URL Filtering.
9. CASB cloud access security broker – לוודא שאין חדירה או פגיעה דרך שירותי הענן שנמצאים בשימוש בארגון (כי הרי לא ניתן להתקין מוצרי אבטחה ארגוניים בסביבת SaaS או PaaS).
10. DNS protection – לוודא שגולשים לאתרים שה- DNS שלהם מוכר ובטוח.
11. שירותי הלבנת תכנים ומסמכים CDR Content Disarm and Reconstruction והשחרה של מידע. גם כאן מנצלים את העובדה שכל התקשורת נכנסת דרך ה-POP הקרוב ניתן לבצע את ההלבנה או השחרה ב-POP ולא בתחנת הקצה (AGENT כבד בדרך כלל) או ב- DC.
12. יכולות Sandboxing – ביצוע פעולות בסביבה מוגנת

עד כאן הזכרנו תכונות אבטחה שניתן לצפות משירותי SASE.
ישנן גם תכונות רבות בהקשרי תקשורת ביניהן – QOS , Caching (ביצוע תיעדוף לתעבורה), Deduplication (לזהות מידע זהה ולהשתמש בו ללא שליחה מיותרת), ניתוב לפי זמינות רגעית של קווי תקשורת (SDWAN), קינפוג מהיר של נתבים (no touch provisioning), ניתוב תקשורת מחודש כשיש תקלה ועוד ועוד.

ספקי **SASE** שפעילים בישראל

להלן מידע של ספקי SASE שפעילים בישראל מסודרים לפי א-ב על פי המידע שנמצא ברשותי. אעדכן רשימה זו ככל שאאתר מידע נוסף.

1. Broadcom\Symantec עם הפתרון שרכשו בישראל Luminate שהיה אחד הפתרונות הראשונים בתחום. כעת משלבת Broadcom את Luminate עם הפתרונות הרבים שקיימים ברשותה בתחום (EPP Bluecoat DLP ועוד).
2. Checkpoint עם Harmony connect הנו שירות חדש יחסית ומבטיח של החברה הישראלית המובילה.

3. Cyolo הישראלית עם פתרון ייחודי שמאפשר עבודה במודל SASE גם בתוך הרשת הארגונית כך שה"מוח" שאחראי על פעולות ההתחברות וההגנה משוכפל גם בתוך הארגון ולכן יכול לספק את אותה רמת ההגנה גם ללא אינטרנט.
4. Netscope שמיוצגת על ידי One. המקור של Netscope הוא ב-CASB ולכן ההגנות ברמת הענן הן מהמשופרות כמו גם בשכבת ה- secure web gateway. למוצר POP בישראל. ישנה תמיכה בפרוטוקולים רבים שרלוונטים לארגונים מוסדיים כגון SAP GUI.
5. Palo alto – עם המוצר Prisma SASE. המוצר מתבסס על סט המוצרים הנרחב של פלו אלטו במיוחד בכל מה שקשור לתחומים המסורתיים של החברה- FW WAF וכד' אך כולל גם רכישות של פתרונות חדשים. המוצר מתבסס על GCP ומציע הפרדה מלאה של הארגונים על ידי יצירת tenant נפרד לכל ארגון.
6. Perimeter81 הישראלית עם פתרון מתקדם כאשר לחברה יש בעלות מלאה על החומרה שנמצאת ב- POP והדבר מאפשר לבצע קינפוגים ספציפיים לפי דרישות הלקוח. החברה מיוצגת על ידי יעל תוכנה.
7. Zscaler – עם ייצור דיי ותיק בבינת וכעת גם We-Ankor. הפתרון ותיק בתחום ה-VPN ולכן יכולות חיבור וניתוב מתקדמות.

מה עוצר או מעקב את כניסת **SASE** לארגונים

כאמור ל-SASE הבטחה אדירה לשינוי מהותי באופן התנהלות ארגונים בתחום של הגנת הסייבר. אולם הכניסה של SASE לארגונים אינה חלקה ואינה מהירה. סיבה ראשונה לכך היא שהשירותים עצמם אינם בשלים. המוצרים אינם מספקים את מלא הפונקציונליות שתוארה בפסקה הקודמת וגם אם מכילה את הפונקציונליות לעיתים מדובר על מוצרים שנרכשו או שותפויות שהתבצעו אך בפועל המוצרים עדיין עובדים בנפרד ומנוהלים עם קונסולים נפרדים (ראה פסקה שדנה בהבדלים בין הפתרונות).

אולם הסיבה המהותית יותר היא שה-SASE אמור ויכול להחליף סט גדול של פתרונות שכבר קיימים בארגון, כשכל פתרון נמצא בשלב אחר במחזור החיים שלו. כלומר לארגונים כבר יש פתרון VPN, פתרון DLP פתרון CASB פתרון FW ופתרון WAF וכד'. כשכל פתרון נרכש בשלב אחר ולכן יש הסכם שירות ותחזוקה לאותו פתרון. וכעת כאשר רוצים להיכנס פתרון

SASE שיכול להחליף מספר פתרונות אבטחה נראה שיש בזבוז כי הדבר מייתר פתרונות שכבר נמצאים בארגון[4].

מכשלה מאתגרת נוספת היא שינוי התפיסה של הגורמים הבכירים בארגון שאחראים על נושא ההגנה בתחום הסייבר ה- CISO. באופן מסורתי ישנה הסתכלות על פתרונות ההגנה כ"מעגלים" כך שאם מעגל אחד נכשל אז יש מעגל פנימי יותר, נפרד לגמרי, שיכול לתת הגנה. ולפי ה- SASE המעגלים או הפונקציונליות עדיין קיימת אך מגיעה כולה מאותו בית היוצר- דבר שונה מהפרדיגמה הידועה.

מי "באמת" מספק את הפונקציונליות

יצרן SASE יכול לבחור בין מספר אופציות לאספקת פונקציונליות מסוימת. דרך ראשונה והטבעית ביותר היא אם לספק ה-SASE יש את היכולות הספציפיות על ידי טכנולוגיה שסיפק מראש. לדוגמה Netscope היה יצרן CASB לכן טבעי שיספק את הפונקציונליות בתחום זה על ידי המוצר שלו עצמו. אך אם היצרן לא הגיע מתחום הפונקציונליות הספציפית וגם לא רכש כזו (ואכן אין יצרן בתחום שיש לו את כל היכולות האפשריות) הרי שכאן היצרן יכול להטמיע במהירות יחסית יכולות פונקציונליות שקיימות בקוד הפתוח (כגון DLP קוד פתוח, FW קוד פתוח וכד'). אפשרות אחרת היא לבנות שת"פ עם פתרון צד שלישי שכבר קיים בשוק. דבר זה פותח פתח (לפחות תאורטי) לאופציה של bring your own license. בכל מקרה חשוב לבדוק "מה המקור לפונקציונליות" הספציפית של כל יכולת שמציעים.

מה מבדיל בין השירותים השונים

מעבר לנקודה הבסיסית והיא "איזה פונקציונליות קיימת בשירות והאם הפונקציונליות הקיימת מתאימה לי[5]", מה אופן התמחור וכד', להלן מספר נקודות למחשבה\בדיקה:

1. האם יש POP בישראל? עד כמה ה- POP הוא redundant.
2. עד כמה "מוברג" ה-AGENT לתוך מערכת הפעלה של ההתקן ומחייב שכל התקשורת תעבור דרכו?
3. התחייבות הספק לנפח תעבורה ול-latency ל-POP הקרוב (שלא יהיה מצב שבו יצרן חתם הסכמים עם הרבה ארגונים וכעת ה-POP עמוס ויש עיכובים במתן השירות)
4. כיצד מונעים מצב שבו אחד הלקוחות שמקבל מעמד של spammer לא פוגע מלקוחות אחרים שמקבלים שירות מאותו POP ?

---

[4] גם אם בוחרים להחליף מספר פתרונות בשירות ה- SASE אבל להישאר עם חלק מהפתרונות הקיימים – צריך להתמודד עם משימת חיבור המוצרים דבר שמוסיף על המאמץ הראשוני

[5] אין ברשותי מידע על פתרון שמספק כעת את מלא הפונקציונליות שהוגדרה

5. האם קינפוג כל הפונקציונליות מתבצע מתוך מסך אחד או בפועל מדובר על מסכים שונים (מספר מוצרים שנרכשו\שיתפו פעולה אך עדיין פועלים באופן עצמאי)?
6. איזה פרוטוקולים של אפליקציות ארגוניות השירות יודע להחצין והאם יש פתרון למצב שבו אין פתרון לפרוטוקול של אפליקצית Legacy. רק הפתרונות ידעו להצפין (ולפתוח) אפליקציות שמשתמשות ב- HTTP ולחילופין לאפשר השתלטות על מסך מרוחק (RDP, TELNET). רובם ידעו גם להעביר פרוטוקולים של SBC (כגון ICA). ואולם לגבי אפליקציות לגסי שמותקנות היום במחשבי העובדים – כגון SAP GUI אין וודאות שהדבר אפשרי. כאשר פתרון שלפעמים היצרנים מציעים הוא אפשור אפליקציית LEGACY על ידי בניית סביבת VDI והחצנת תמונת המסך למשתמש.
7. האם ניתן להגדיר מדיניות שמשתנה באופן דינאמי (משתנה בין יום ללילה, משתנה כאשר יש אירוע מסוים וכד').
8. ידע וניסיון לחיבור שירות ה- SASE למערכת ה-SIEM הארגונית
9. באופן כללי יכולת אינטגרציה של שירות ה- SASE לפתרונות שכבר קיימים בארגון

המלצה

אנו ממליצים לארגון ללמוד את התחום ולעקוב אחריו מקרוב.

בפרט אם יש פונקציונליות שכיום לא קיימת או אתגרים בפתרון ה- VPN הנוכחי – רצוי לבדוק התאמה לפתרון SASE.

ארגונים צריכים להיות עם ידע ב-SASE לפני שמבצעים תהליך של חידוש התחזוקה של פתרון ה- VPN שקיים ברשותם. בכדי לשפר את רמת האבטחה בארגון ולהקל על ניהול מוצרי אבטחת המידע ארגונים צריכים להסתכל על SASE כפתרון לא רק לחיבור מהבית אלא גם ממקום העבודה. כלומר גם העבודה השוטפת מהמשרדים בסניפים השונים ובמטה תתבצע באמצעות SASE.

בברכה

פיני כהן