

דוח אימוץ אפס אמן



תוכן העניינים

03

מבוא

06

עם מי דיברנו

04

מתודולוגיה

07

תובנות כלליות מהמחקר

05

דברים שכדאי לדעת על
אימוץ אפס אמון

24

מטרות מחקר מפורטות וגיוס
קהל

מבוא

ואסו ג'קאל / סגן נשיא תאגידי, אבטחה, תאימות וזהות

בהתבסס על עקרונות האימות במפורש, שימוש בגישה הפחות מיוחדת והנחת הפרה, ארכיטקטורה מקיפה של אפס אמון יוצרת אמצעי הגנה בתוך ומחוצה לה זהות, נקודות קצה, אפליקציות, תשתיות, רשת ונתונים, בשיתוף פעולה עם הגדלת החשיפה, האוטומציה והתזמור. אנו לא רק ממליצים על גישה זו עם לקוחותינו ושותפינו, אנו מאמצים אותה בגישתנו לאבטחת ופיתוח תוכנה גלובלית כאן ב-Microsoft.

דו"ח זה מאיר את הדרך לאימוץ אפס אמון בשווקים ותעשיות מגוונות. אנו מקווים כי הלמידה שנרכשת על ידי מחקר זה יכולה לסייע בהאצת אימוץ אסטרטגיית אפס האמון שלכם, לשפוך אור על ההתקדמות הקולקטיבית של עמיתכם ולספק תובנות על המצב העתידי של המרחב המתפתח במהירות זו.

השנה האחרונה הייתה יוצאת דופן בהתפתחות אבטחת הסייבר ועלייתה של גישת אפס אמון כאסטרטגיה מנחה לתעשייה ולארגונים שלנו ברחבי העולם.

בתחילת המגיפה, מקום העבודה הפך לריק כמעט לגמרי בין לילה. שינוי זה אילץ ארגונים רבים להסתגל במהירות לתמיכה בעובדים שעושים עבודה בכל דרך שהם יכולים - שימוש במכשירים אישיים, שיתוף פעולה באמצעות שירותי ענן ושיתוף נתונים מחוץ להיקף הרשת הארגונית. כאשר ארגונים הסתגלו לשינוי זה, הם גם התמודדו עם פושעי רשת מתוחכמים יותר ויותר אשר מפתחים ללא הרף את המטרה, הטקטיקה והמשאבים שלהם.

כיום, עבודה היברידית היא המציאות החדשה. על רקע זה, ועל רקע שינויים מהירים, הארגונים שסקרנו אמרו לנו שהם מסתמכים על אפס אמון להגברת זריזות האבטחה והתאימות, מהירות הגילוי והתיקון של האיומים והגברת הפשטות והזמינות של ניתוחי האבטחה.

מתודולוגיה

Microsoft הזמינה את Hypothesis Group, סוכנות תובנות, עיצוב ואסטרטגיה, לביצוע דו"ח ומחקרי אימוץ אמון. המחקר כלל שני שלבים בארה"ב להדגשת מגמות ותנופה באימוץ אפס אמון, כאשר בשלב השני נוספו שווקים נוספים לחשיפת מגמות עולמיות.

מחקר ראשוני התרחש באוגוסט 2020, כאשר נערך בארה"ב סקר מקוון בן 15 דקות עם 300 מקבלי החלטות אבטחה (SDM) המעורבים בהחלטות אסטרטגיות אפס אמון בחברות ארגוניות ממגוון תעשיות. בנוסף לסקר המקוון, חמישה ראיונות עומק נערכו באינטרנט בספטמבר 2020 בקרב SDM מארצות הברית במגוון תעשיות.

באפריל 2021 בוצע מחקר גלובלי בארה"ב, גרמניה, יפן ואוסטרליה/ניו זילנד בקבוצה דומה של מקבלי החלטות ביטחוניות. למעלה מ-900 משתתפים עשו סקר מקוון בן 15 דקות עם שאלות בנוגע לאימוץ אסטרטגיית אפס אמון שלהם, שיטות עבודה מומלצות, הטבות, אתגרים וכיצד הם מתכוונים להשקיע בעתיד.



דברים שכדאי לדעת על אימוץ אפס אמון

01 / ארגונים מוכנים לנצל את האסטרטגיה של אפס אמון, המואצת על ידי המעבר למקום עבודה היברידי ומגיפת הקורונה

מקבלי החלטות אבטחה אומרים שפיתוח אסטרטגיית אפס אמון היא סדר העדיפויות האבטחה מספר 1 שלהם, כאשר 96% מציינים כי היא קריטית להצלחת הארגון שלהם. המניעים העיקריים לאימוץ אסטרטגיית אפס אמון הם שיפור תנוחת האבטחה הכוללת שלהם וחויית משתמש הקצה. המעבר למקום עבודה היברידי, המואץ על ידי COVID-19, מניע גם אימוץ רחב יותר של אסטרטגיית אפס אמון: 81% מהארגונים הארגוניים החלו את המעבר לעבר מקום עבודה היברידי, כאשר 31% מלאים בו. עם זאת, ל-94% יש חששות מהמעבר, בעיקר משימוש לרעה של עובדים, הגדלת עומסי העבודה ב-IT ומתקפות סייבר. בהתחשב בכך, שיקולים מרכזיים לאסטרטגיה כוללים הדרכה מוגברת לעובדים ואימות רב-גורמי (MFA) להבטחת חווית משתמש חלקה ומעבר.

אסטרטגיית 02 / אפס אמון מאפשרת גמישות היכן הארגונים יכולים להתחיל ליישם כך שניתן להתאים את הגישה לצרכיהם

פחות מ-15% מהארגונים החלו ביישום אסטרטגיית אפס אמון באותו אזור סיכון אבטחה. זה במידה רבה מכיוון שהגישה ליישום היא תהליך של קצה לקצה על פני עמודי התווך והיכולות של ארכיטקטורת האבטחה, ולא כסדרה של טכנולוגיות אינדיבידואליות שונות. באופן דומה, הסדר שבו מיושמים רכיבים בודדים של אפס אמון בתחום סיכון אבטחה משתנה מאוד, כאשר אנשי מקצוע בתחום האבטחה שונים באופן מהותי באילו רכיבים הם מתחילים ליישם תחילה.

03 / למרות שאסטרטגיית אפס אמון מאומצת באופן נרחב ומשפרת את האפשרות של ארגונים לנהל איומים, עדיין יש עוד עבודה

76% מהארגונים החלו לפחות ליישם אסטרטגיית אפס אמון, כאשר 35% טוענים שהם מיושמים במלואם. עם זאת, הטוענים כי הם מיושמים במלואם מודים כי לא סיימו ליישם אסטרטגיית אפס אמון בכל תחומי הסיכון והאבטחה. אסטרטגיית אפס אמון משכנעת מכיוון שהיא מספקת זריזות מוגברת, מהירות זיהוי איומים ושיפור היכולת לנהל את Internet of Things (IoT) וטכנולוגיה תפעולית (OT). האימוץ גדל בארה"ב (70% באוגוסט 2020 ל-79% באפריל 2021); ארה"ב גם מתקדמת יותר ביישום אפס אמון ביחס למדינות אחרות שהחלו לאמץ מאוחר יותר, וארגונים בארה"ב טוענים שהם פחות מוגבלים בתקציבים. עם זאת, בעוד ש-57% מהארגונים טוענים שהם מקדימים אחרים בכל הנוגע לאימוץ, כמחצית עדיין יש להם עוד עבודה כיוון שהם לא יישמו במלואם אפס אמון בכל תחומי הסיכון והאבטחה.

04 / במבט קדימה, אסטרטגיית אפס אמון תישאר בעדיפות עליונה ותדרוש קבלת החלטות קפדנית בכל הנוגע לעובדים ולספקים.

אסטרטגיית אפס אמון צפויה להישאר בעדיפות האבטחה מספר 1 בעוד שנתיים מהיום וארגונים צופים להגדיל את השקעתם. ההתמודדות עם האתגרים עם עובדיהם (כולל צוותי אבטחת צוות וקניית מנהיגות) תהיה המפתח להכפלת ההשקעה של אפס אמון. בכל הנוגע לאסטרטגיית ספקים, למקבלי החלטות אבטחה יש העדפה קלה לעבודה עם ספקים הוליסטיים או מאוחדים בהתחשב בכך שבחירת ספקים תלויה לעתים קרובות בזמינות של מומחיות פנימית. היתרונות של הגישה הטובה ביותר בחבילה כוללים מומחיות מוגברת, משאבים ופשטות, אם כי ייקח יותר זמן ליישם, יהיה קשה יותר להשתלב בארכיטקטורת האבטחה הקיימת והגברת הפגיעות האפשרית.

עם מי דיברנו

גלובלי



מקבלי החלטות בטיחות שעובדים בחברות בגודל ארגוני*



נמצאים בשלב
תכנון/שקילת
הטמעת אפס
אמון

24%

תובנות כלליות מהמחקר

ארגונים מוכנים לנצל את האסטרטגיה אפס אמון

כפי שמקבל החלטות אבטחה אמריקאיות בנושא אירוח, "המטרה היא לשפר את תנוחת האבטחה שלנו באופן כללי, אבל הכל על הפחתת חיכוך בחוויית משתמש הקצה והקלה עליהם."

יתר על כן, 31% מאנשי האבטחה רואים באסטרטגיה של אפס אמון כלי חשוב במעבר הקרוב למקום עבודה היברידי לאחר המגיפה; נהג זה בולט במיוחד באוסטרליה/ניו זילנד (44%).

אסטרטגיית אפס אמון הינה עדיפות אבטחה מספר 1 כיום בשווקים ובתעשיות, כאשר מספר ארגונים מאמצים אסטרטגיית אפס אמון בשנים האחרונות. למרות שאפס האמון הוא ראש המחשבה לכולם, (53%) הוא נמצא בעדיפות גבוהה במיוחד עבור ארגונים בארצות הברית (56%) וגרמניה (53%).

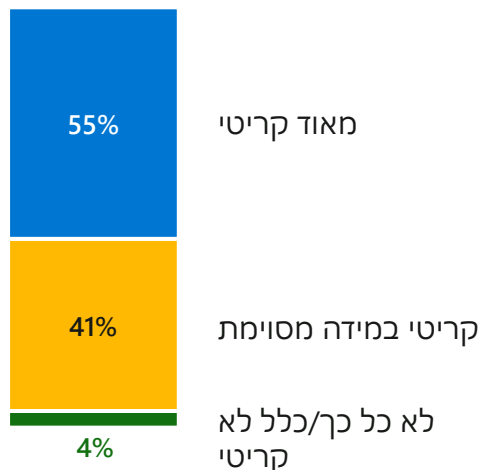
כמעט כל אנשי המקצוע בתחום האבטחה (96%) סבורים כי אסטרטגיית אפס אמון היא קריטית להצלחת הארגון שלהם. (ראה מוצג 1) בנוסף לחיזוק תנוחת האבטחה הכוללת שלהם ושיפור חוויית משתמש הקצה, אנשי מקצוע בתחום האבטחה מחפשים אסטרטגיית אפס אמון כדי לפשט את הליכי האבטחה לעובדים. (ראה מוצג 2)

מוצג 2. מניעים של אפס אמון

מניעים מובילים	
47%	שיפור מערך האבטחה הכולל
44%	שפר את משתמש הקצה ניסיון ופרודוקטיביות
38%	לשנות את האבטחה צוותים עובדים יחד
35%	פישוט מערך האבטחה
35%	צמצום סיכוני האבטחה

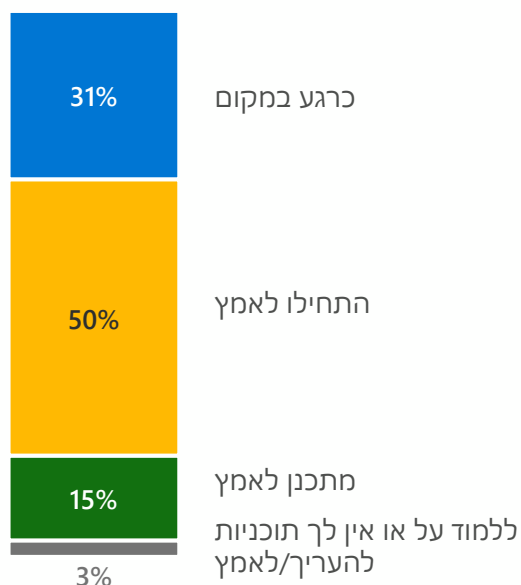
מוצג 1. אפס אמון הוא קריטי

מאוד + במידה מסוימת 96%



המעבר למקום עבודה היברידי מניע אימוץ רחב יותר של אסטרטגיית אפס אמון

מוצג 3. כוונת מקום עבודה היברידי



81% מהארגונים הארגוניים החלו במעבר לעבר מקום עבודה היברידי, כאשר 31% כבר אומצו במלואו. עם זאת, שיעורי האימוץ המלא אינם עקביים בשווקים: בעוד שאוסטרליה וניו זילנד מובילות את החבילה ב-37%, גרמניה נמצאת הרחק מאחור, ורק 20% מהארגונים כבר עברו למודל היברידי. (ראה מוצג 3)

אפילו כשהשווקים הגלובליים מתקדמים לעבר מקום עבודה היברידי בשיעורים שונים, הרוב המכריע (91%) של ארגונים שלא השלימו את המעבר צופים לעשות זאת בחמש השנים הקרובות. באופן מכריע, 94% חוששים מהמעבר, עם שימוש לרעה בעובדים, עלייה בעומסי עבודה ב-IT והגברת הסיכון להתקפות סייבר בראש רשימת החששות. (ראה מוצג 4)

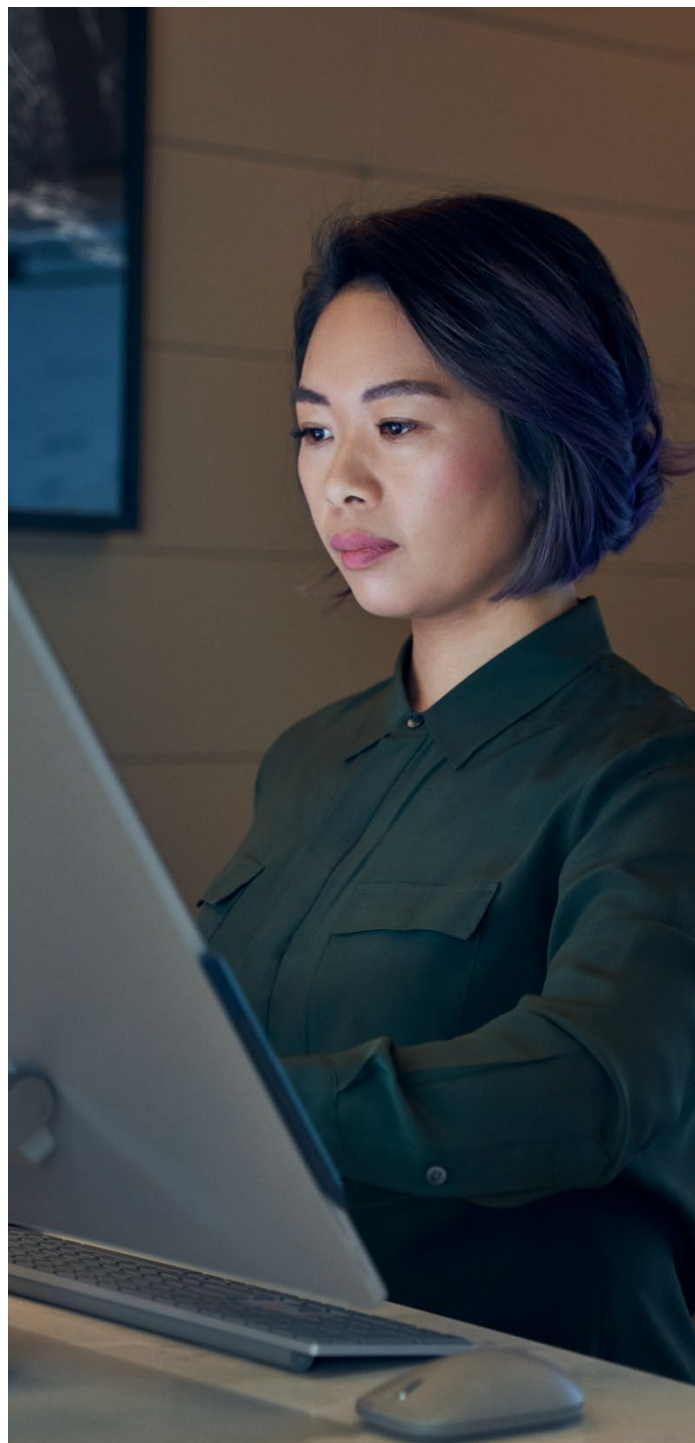
מוצג 4. חששות מקום עבודה היברידי

37%	עובדים מורידים אפליקציות לא בטוחות
37%	עלייה בעומס ה-IT
36%	התקפות תוכנת כופר
35%	התקפות דיוג
34%	שימוש לא נכון במכשירים אישיים
31%	גישה לא מורשית לנתונים
30%	חוסר יכולת לנהל את כל המכשירים
30%	שימוש בחשבונות דוא"ל אישיים
24%	אי ציות לתקנות הנתונים

קוביד-19 העלה שיקולים חדשים המאיצים את המעבר לאסטרטגיית אפס אמון

במטרה לצמצם סוגיות פוטנציאליות, בעלי העניין מדגישים את החשיבות של הכשרה מוגברת לעובדים (54%) (במיוחד ביפן (61%) וגרמניה (58%)) ואימות רב-גורמי (AFM) (50%) (במיוחד בארצות הברית (52%) ובגרמניה (56%)) כדי להבטיח חוויית משתמש חלקה ומעבר.

מכיוון שניתן לסייע בעבודה מאובטחת מרחוק והיברידית על ידי אסטרטגיית אפס אמון, COVID-19 האצה את אימוץ אסטרטגיית אפס אמון עבור 72% מהארגונים, אם כי מתעוררות א-סימטריות בין השווקים. בעוד שהמגיפה זרזה את האימוץ של כשבעה מכל עשרה ארגונים בארה"ב (76%), יפן (71%) ואוסטרליה/ניו זילנד (69%), שיעורי היישום היו נמוכים במיוחד בגרמניה (62%), אולי בשל למעבר איטי יותר למקום עבודה היברידי.



אפס אמון מיושמת באופן נרחב ברחבי העולם וצומחת בארה"ב

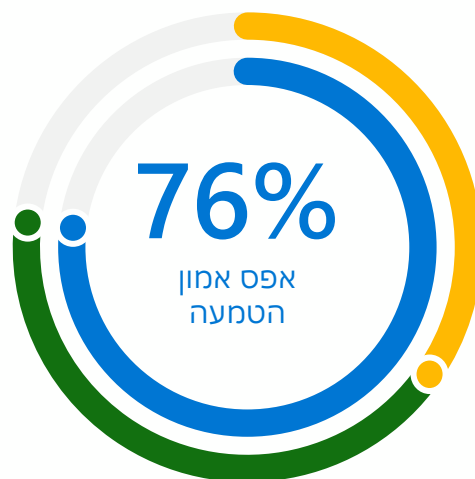
למרות שאסטרטגיית אפס האמון שולטת כיום במרחב האבטחה, הימצאותה בכל מקום היא חדשה יחסית. 82% מהחברות יישמו אסטרטגיות אפס אמון בשלוש השנים האחרונות, כאשר 21% עשו זאת ב-12 החודשים האחרונים. עם זאת, 26% מהארגונים האמריקאים החלו ביישום לפני 3 שנים, לעומת 19% מהארגונים היפנים, 6% מהארגונים באוסטרליה/ניו זילנד ו-3% מהארגונים בגרמניה. יישום מוקדם יותר זה בארה"ב - יחד עם פחות מגבלות תקציב - עשוי לסייע להסביר מדוע ארגונים בארה"ב מקדימים באימוץ אפס אמון לעומת ארגונים בשווקים אחרים. באופן דומה, העוצמה היחסית של אפס אמון בגרמניה מסייעת להקשר את שיעורי האימוץ הנמוכים שלה: 97% מהארגונים הגרמנים החלו ביישום רק בשלוש השנים האחרונות.

אפס אמון אינה רק מילת מפתח; זו מציאות. 76% מהארגונים החלו לפחות ליישם אסטרטגיה זו ו-35% סבורים שהם מיושמים במלואם. עם זאת, נתונים אלה מציינים תמונה אופטימית מדי שכן ארגונים רבים הרואים עצמם מיושמים במלואם, על פי הודאתם, לא סיימו לבצע בכל תחומי הסיכון הביטחוני. כיום, ארה"ב מקדימה את אימוץ האסטרטגיה של אפס אמון ביחס לשווקים אחרים וממשיכה לצמוח במהירות: בהשוואה לאוגוסט 2020, יישום האסטרטגיה של אפס אמון בארה"ב עלה מ-70% ל-79%, זינוק ניכר תוך שמונה חודשים בלבד. (ראה מוצג 5)

מוצג 5. יישום אפס אמון

AUS / NZ	JP	ח	ארה"ב	לנו (2020)	
71%	76%	75%	79%	70%	יישום אפס אמון
28%	32%	19%	44%	27%	• מיושם במלואו
43%	44%	56%	35%	43%	• בתהליך

35% מיושם במלואו ●
42% יישום מתבצע ●

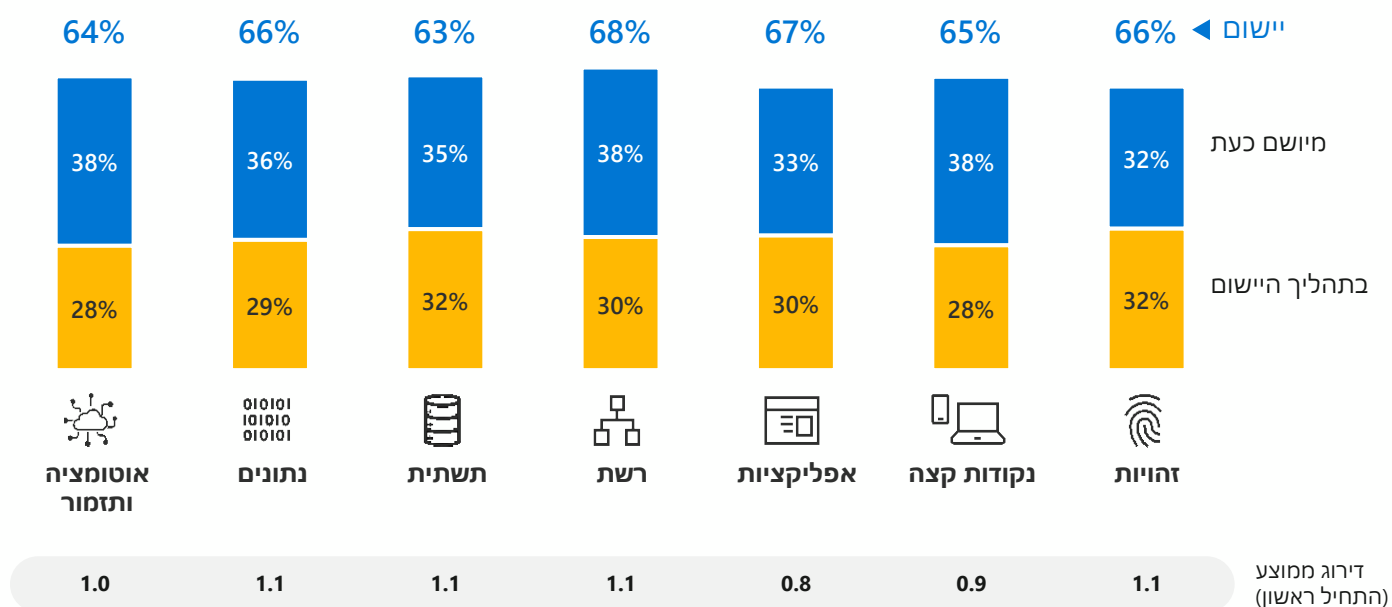


אין גישה חד-פעמית ליישום אפס אמון, המאפשרת הרשאה להתחיל מכל מקום

מעבר לתחומי סיכון האבטחה של אסטרטגיית אפס אמון, על הארגונים לזהות את המרכיבים האישיים של כל אזור סיכון אבטחה כדי לתת עדיפות. לגבי נקודות קצה, אפליקציות, רשת, נתונים ואוטומציה/ תזמור, אין נקודת התחלה ברורה; אנשי מקצוע בתחום האבטחה משתנים במידה ניכרת באילו רכיבים הם מדורגים כעדיפות עליונה. עם זאת, אימות חזק מיושם בדרך כלל תחילה עבור זהויות, וכלים לאיתור איומים הם בראש סדר העדיפויות של התשתיות. (ראה מוצג 7)

אין אזור סיכון אבטחה יחיד (זהויות, נקודות קצה, אפליקציות, רשת, תשתיות, נתונים, אוטומציה ותזמורת) בולט כנקודת מוצא ראשית לאסטרטגיית אפס אמון, שכן פחות מ-15% מתחילים באותו אזור סיכון אבטחה. ארגונים מתחילים במקומות שונים ככל הנראה על בסיס הצרכים שלהם והמשאבים הפנימיים הזמינים. בסופו של דבר, הם מבקשים לאמץ אסטרטגיית אפס אמון בכל תחומי סיכון האבטחה כדי להבטיח הגנה נוספת מפני איומים, כך שאפס האמון נתפס כאסטרטגיה מקצה לקצה שתושלם לאורך זמן. (ראה מוצג 6)

מוצג 6. יישום אפס אמון הנוכחי - אזורי סיכון אבטחה



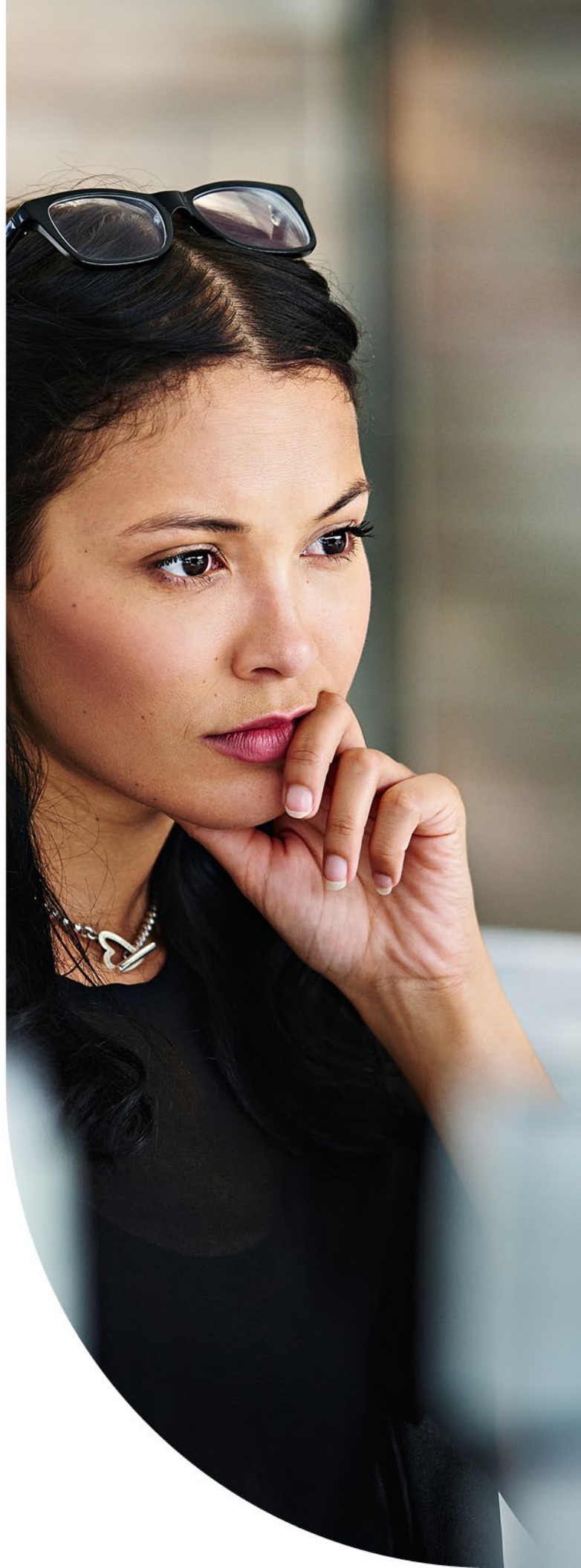
מוצג 7. יישום רכיב אפס אמון (שלושת המובילים) - מדורג במקום הראשון (מיושם ראשון)

נקודות קצה	זהויות
מדיניות/פקדי מניעת אובדן נתונים עבור כל המכשירים הלא מנוהלים ומנוהלים 27%	אימות חזק (כלומר אימות רב-גורמי, אימות ללא סיסמה) 32%
הערכת סיכון מכשירים בזמן אמת / זיהוי איום נקודת קצה 26%	זיהוי ותיקון סיכונים אוטומטיים 27%
התקנים רשומים עם ספק זהות 24%	מדיניות גישה מותאמת לשער גישה למשאבים 22%
רשת	אפליקציות
בקורות גישה מאובטחות להגן על רשתות 25%	צל מתמשך גילוי IT והערכת סיכונים 23%
הגנה וסינון איומים עם אותות מבוססי הקשר 24%	בקרת גישה מדויקת לאפליקציות שלך (כגון חשיפה מוגבלת או קריאה בלבד) 22%
כל התעבורה מוצפנת 20%	בקרת גישה מבוססת מדיניות לאפליקציות 20%
נתונים	תשתית
החלטות הגישה נשלטות באמצעות מנוע מדיניות האבטחה 21%	גישה לצוות פעולות האבטחה לכלים לאיתור איומים 25%
הנתונים מסווגים ומתויגים 21%	הגנה על עומס עבודה בענן על פני היברידי ורב ענן 19%
הקבצים הרגישים ביותר מוגנים בהתמדה באמצעות הצפנה 20%	נראות מדויקת ובקרת גישה בכל עומסי העבודה (מכונות וירטואליות, שרתים וכו') 17%
	אוטומציה ותזמור
	נראות מקצה לקצה עם פלטפורמה מרכזית לחקירה ותגובה 29%
	נתוני איומים נאספים ומנותחים על פני תחומים (זהויות, נקודות קצה, אפליקציות, רשת, תשתיות) 28%
	חקירה אוטומטית והתגובה מופעלת 22%



לא התייחסנו לזה כאל
סדרה של טכנולוגיות,
אלא כאסטרטגיה וגישה
להתייחס לכל משאב
משתמש, בין אם בתוך
הרשת שלנו או מחוץ
לרשת שלנו, כבלתי
מהימן עד שניתן יהיה
לאמת אותם."

מקבל החלטות אבטחה בארה"ב
אירוח



ברגע שהארגונים מתחילים ליישם אסטרטגיית אפס אמון, היתרונות המרכזיים כוללים זריזות, מהירות והגנה מוגברת; יתרונות המשאבים פחות נפוצים

לאחר יישום אסטרטגיית אפס אמון, ארגונים נהנים מהגברת זריזות (37%), מהירות (35%) והגנה על נתוני לקוחות (35%). (ראה מוצג 8) עם זאת, הטבות ישירות לעובדים כולל צוות אבטחה משוחרר (27%) וצורך בפחות משאבים לניהול התשתית (22%) מתמשות פחות.

חשוב לציין, ארגונים מאמינים שאסטרטגיית האמון שלהם אפס תעזור להם לנהל את רוב האיומים והשינויים בסביבה, במיוחד ביחס לאבטחת IoT - OT (47%).

מוצג 8. הטבות אפס אמון





ארגונים מרגישים בטוחים להפיק את המרב מאסטרטגיית האמון שלם

79% מרגישים בטוחים ביכולתם להתמודד עם איומי אבטחה בכללותם, אם כי ביטחון זה הולך ופוחת כאשר האיום כרוך בבדה של אמת: אנשי SDM מרגישים פחות בטוחים בהתמודדות עם איומים הכרוכים בזהויות סינתטיות (20%) וזיופים עמוקים (10%).

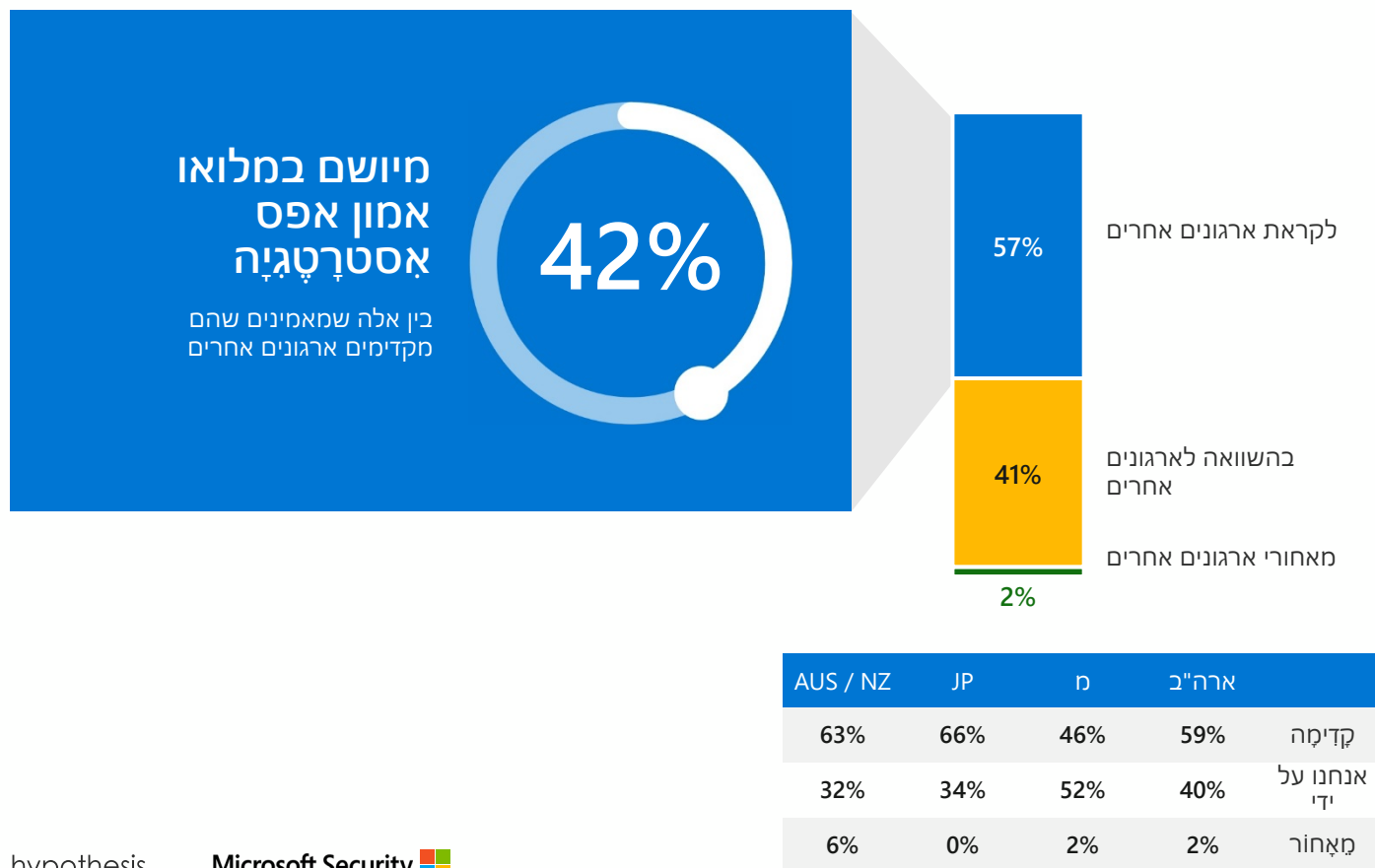
לאור היתרונות שהושגו, אפס אמון בדרך כלל צוברת אסוציאציות חיוביות. בכל ארבעת השווקים, SDM רואים בגישה של הארגונים שלהם פרקטית ושאיפה בעת ובעונה אחת, ומתארים אותה כבטוחה (37%) ויעילה (31%) כמו גם מניע (25%), מעוררת השראה (25%) ומרגשת (25%). ביפן ספציפית, אנשי אבטחה מתארים את אפס האמון כתובעניים (27%) וגם טרנספורמטיביים (25%), מה שמרמז כי יתרונותיה אמנם לא פשוטים ליישום, אך לאחר אימוץ.

רבים מאמינים שהם מקדימים עם יישום אפס אמון, אך עדיין יש להם עוד מה לעשות

למרות שארגונים רבים בטוחים באסטרטגיית ה- אפס אמון שלהם והם מרגישים שהם מוכנים להתמודד עם איומי אבטחה עתידיים, יש עדיין הרבה עבודה לביצוע ליישום מלא בכל תחומי הסיכון. בקרב ארגונים הרואים באסטרטגיית אפס האמון שלהם מיושמת במלואה, למשל, כמעט מחצית לא יושמו כיום בתחומי סיכון אבטחה, כאשר התשתיות והזהויות הן הפחות ישימו.

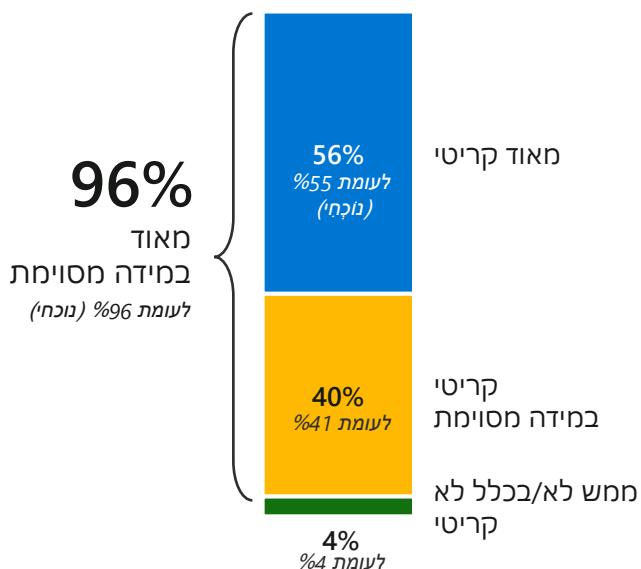
בעוד שרק 35% מהארגונים יישמו במלואם את אסטרטגיית ה- אפס אמון שלהם, 52% אומרים שהם מקדימים את המקום בו הם תכננו להיות ו- 57% מאמינים שהם מקדימים את הארגונים האחרים. הארגונים רואים עצמם מקדימים במיוחד אחרים ביפן (66%) ואוסטרליה/ניו זילנד (63%). בעוד שהאמון שופע בשווקים, נראה שיש פער בין תפיסה למציאות: בקרב אלה שמרגישים שהם מקדימים את הארגונים האחרים, רק 42% טוענים כי יישמו באופן מלא אסטרטגיית אפס אמון. (ראה מוצג 9)

מוצג 9. השוואת יישום אפס אמון



במבט קדימה לשנתיים הקרובות, אסטרטגיית אפס אמון תישאר בעדיפות אבטחה עליונה

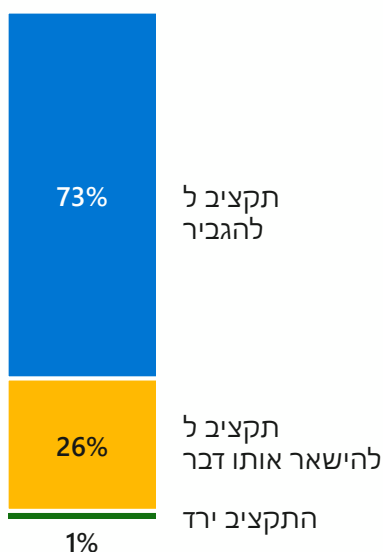
מוצג 10. הביקורת הצפויה של אפס אמון בשנתיים הקרובות



לארגונים יש אסטרטגיה של אפס אמון, ומקבלי ההחלטות אומרים כי היא תמשיך להיות בראש סדר העדיפויות הביטחוני במהלך השנתיים הקרובות. החשיבות היחסית של אסטרטגיית אפס אמון כיוזמת אבטחה צפויה לעלות (53% עד 58%) עד שנת 2023, שכן SDM צופים כי האסטרטגיה תישאר קריטית להצלחה הכוללת (96%). (ראה מוצג 10)

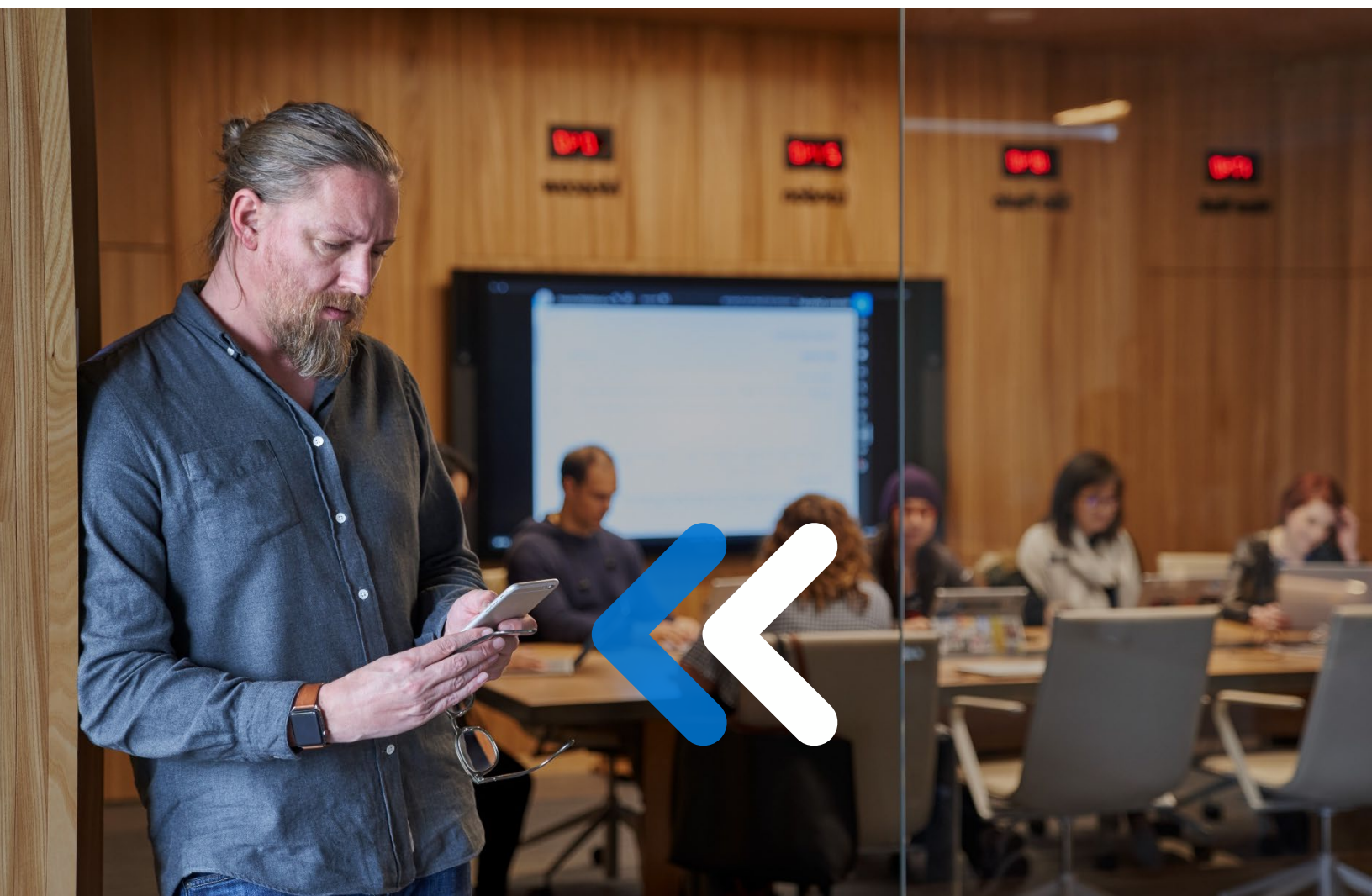
הביקורת הצפויה גבוהה במיוחד בקרב ארגונים יפנים, כאשר 70% אמרו כי אסטרטגיית אפס אמון תהיה קריטית מאוד בשנתיים הקרובות בהשוואה לממוצע הכולל של 56%. תקציבי האסטרטגיה של אפס אמון צפויים גם הם לצמוח כאשר 73% מהארגונים מצפים להגדיל את התקציבים שלהם. למרות שמספר זה מעט נמוך יותר בגרמניה (67%), שם 31% צופים שהתקציבים שלהם יישארו על כנם. (ראה מוצג 11)

לְהַצִּיג 11. תקציב אפס אמון צפוי בשנתיים הקרובות



ארגונים שחיבקו מכל הלב את אפס ארון מצפים להכפיל את השקעתם בשנתיים הקרובות, ואלו שטרם החלו לאמץ סיכונים ירדו מאחור. ארגונים אלה לא רק עוקבים אחר עמיתיהם המיושמים במלואם בכל הנוגע לתעדוף אפס ארון בתוכניות האבטחה שלהם (42% לעומת 66%) וציפייה להגדלת התקציב (66% לעומת 72%), אלא גם מרגישים פחות בטוחים בניהול IoT באופן משמעותי. ואבטחת OT בעתיד (40% לעומת 53%).

הוכחת הצלחות של אסטרטגיית אפס ארון עשויה להניע השקעות נוספות



ההתמודדות עם האתגרים עם העובדים תהיה המפתח להכפלת ההשקעה אפס אמון

לדוגמה, 21% ממערכות ה-SDM מציינות קשיים בהוכחת ההחזר על ההשקעה של השקעה ב- אפס אמון כחסם ליישום, אתגר שעשוי להוביל לחוסר רכישת C-suite. מכיוון שלשווקים שאינם אמריקאים יש סיכוי גבוה יותר לאילוצים תקציביים (60% מהארגונים ביפן; 57% מהארגונים בגרמניה; 57% מהארגונים באוסטרליה/ניו זילנד), ייתכן שיש לזה אפקט אדווה, מה שמוביל ליישום נמוך ואיטי יותר של אסטרטגיות אפס אמון ביפן, גרמניה ואוסטרליה/ניו זילנד בהשוואה לארה"ב.

למרות ההתקדמות המהירה באימוץ האסטרטגיה של אפס אמון, ארגונים חייבים להתגבר על שלל אתגרים אם הם רוצים להתקדם הלאה עם היישום. [\(ראה מוצג 12\)](#) אתגרי משאבים ומנהיגות נפוצים ביותר בקטגוריות אלה. הזמן הדרוש ליישום אסטרטגיות אפס אמון וחוסר תמיכה מצד מנהיגות C-suite עומדות בראש רשימת המחסומים, כשהאחרונים בולטים במיוחד באוסטרליה/ניו זילנד (65%).

יתרה מכך, אילוצי תקציב - ש-45% מהארגונים מזהים אותם כמחסום - ממלאים כנראה גם תפקיד באתגרי משאבים ומנהיגות.

מוצג 12. אפס חסמי אמון

אתגרי משאבים 60%	הנהגה 53%	טכנולוגי 46%	מוכר 46%	מגבלות תקציב 45%
20% לוקח יותר מדי זמן ליישם	20% חוסר תמיכה מצד מנהיגות רחבות יותר C - ב	21% קושי בשילוב פתרונות אבטחה	21% צריך תמיכה ביישום מצד ספקים	21% עלות יישום אסטרטגיית אפס אמון
19% חוסר ניהול פנימי של שינויים	19% חוסר תמיכה מצד בעלי עניין	19% חוסר תאימות עם מערכות מדור קודם	21% קושי לזהות את הספקים הנכונים	21% קושי להוכיח החזר ROI
18% צריך יותר חומרי חינוך	19% צריך עזרה כדי להפוך מקרה עסקי משכנע	19% קושי בקנה מידה בכל הארגון	17% חוסר יכולת למצוא שותפים חדשניים	14% אין לך גדול תקציב מספיק
17% לא נחוץ לארגון בסדר גודל שלנו	18% חוסר רכישה ארגונית			
16% אין לך את הכישור הנכון ליישם כראוי				

“ הרכישה הראשונית הייתה
מאתגרת אבל ברגע
שהסכמנו כבעלי עניין
שאנחנו הולכים להשקיע
בפרויקט הזה, כולם היו על
הסיפון ”.

מקבל החלטות אבטחה בארה"ב
FinTech



האסטרטגיה האחרונה, הטובה ביותר בגזע, כוללת השגת רכיבי טכנולוגיה בודדים של אפס אמון מספקים מיוחדים. בשונה מ- best-in-suite, אסטרטגיה זו מסתמכת על ספקים המתמחים בתחומים שונים ובכך מציעים גמישות רבה יותר ויכולים להתאים יותר לאסטרטגיה של הארגון. עם זאת, אנשי מקצוע בתחום האבטחה רואים במיטב הזנים יקר יותר, דורשים יותר משאבים ומעכבים נראות, חסרונות שמובילים בסופו של דבר לאתגרים של ספקים ותקציביים. (ראה מוצג 14)

בעוד שהארגונים מפוצלים ברובם, רוב קטן של SDM (55%) מעדיפים לעבוד עם ספקי הוליסטיות (הטובות ביותר). (ארגונים באוסטרליה/ניו זילנד, לעומת זאת, נוטים בכיוון ההפוך, כאשר 52% מעדיפים את הטובים ביותר בגזע.)

מוצג 14. היתרונות והמכשולים הטובים ביותר בגזע-מדורגים בדירוג 2 המובילים

+ הטבות הטובות ביותר בגזע	
33%	גמישות להמשיך בפתרונות הטובים ביותר עבור כל מרכיב באסטרטגיית אפס אמון
30%	יכול ליישר יותר את הפתרון עם הארכיטקטורה או האסטרטגיה של הארגון שלי
26%	הגדלת ההזדמנות לחדשנות מול ספקים שונים

- החסרונות הטובים ביותר בגזע	
29%	עלויות מוגברות
26%	חסר יכולת לשתף נתונים על פני פתרונות שונים
26%	כמות פתרונות גבוהה לצוותים פנימיים לאמץ ולנהל

למקבלי ההחלטות הביטחוניות יש נטייה קלה לספקים הוליסטיים או מאוחדים

בכל הנוגע לאסטרטגיית ספק אפס אמון, ארגונים מתמודדים עם גישה הטובה ביותר בחבילה או הטובה ביותר. האסטרטגיה לשעבר כרוכה ברכישת חבילת מוצרים לכל ארכיטקטורת אפס אמון של האדם מספק הוליסטי או מאוחד, פתרון שלדעת SDM מציע מומחיות, משאבים ופשטות יותר עבור מי שעמוסי משאבים פנימיים. עם זאת, החששות מגישה זו כוללים פגיעות מוגברת וחוסר גמישות. (ראה מוצג 13)

מוצג 13. הטבות ומחסומים הטובים ביותר בסוויטה-מדורגים בדירוג 2 המובילים

+ הטבות הטובות ביותר בסוויטה	
24%	לספק יש מומחיות ספציפית לתעשייה על פני פתרונות
23%	עוד משאבים זמינים לסייע בתכנון אסטרטגיית אפס אמון
22%	ערימת אבטחה פשוטה יותר

- החסרונות הטובים ביותר בסוויטה	
34%	הסתמכות על ספק אחד מגביר את הפגיעות
33%	דורש אינטגרציה מורכבת יותר עם ארכיטקטורה מדור קודם
29%	פחות גמישות לתפקוד מיוחד

דברי סיכום

עם זאת, אפילו למתאמי האסטרטגיה המתקדמים ביותר של אפס אמון נותרה עוד עבודה, והתפיסות המוטעות של הארגונים סביב בגרותם של אפס אמון עשויות להשאיר חלק עם פגיעות שהם אפילו לא יודעים שיש להן.

רוב הארגונים בשווקים מאמינים שהקריטיות של אסטרטגיית אפס אמון רק תלך ותגבר עם הזמן והם מצפים שהתקציבים שלהם יגדלו בתורם. שינוי צפוי זה בסדר העדיפויות הוא קריטי במיוחד לשווקים שאינם אמריקאים, כאשר חששות תקציביים הם חסמים בולטים לאימוץ. השאיפה ליישום מלא עשויה להכריע כלכלית ולוגיסטית; ובכל זאת, יתרונותיה של גישת אפס אמון אינם ניתנים להכחשה, ו-Microsoft תהיה שם כדי להדריך ולתמוך בארגונים כשהם יוצאים לגבול המתפתח הזה.

מכיוון שסיכוני האבטחה הופכים לא רק תכופים יותר, אלא גם מזיקים יותר, ארגונים בשווקים ובתעשיות בוחרים באסטרטגיית אפס אמון שמנחה אותנו "לעולם אל תבטח, תמיד תוודא". אסטרטגיית אפס אמון הינה בראש סדר העדיפויות האבטחה של ארגונים השואפים לשפר את תנוחת האבטחה הכוללת שלהם, את חוויית משתמש הקצה ואת התפוקה, לפשט את הליכי האבטחה לעובדים ולהוזיל עלויות. עם זאת, בעוד שהיתרונות של אסטרטגיית אפס אמון מבוססים היטב, משאבים מוגבלים וספקנות בקרב מנהיגות עומדים בדרך ליישום אוניברסלי.

אימוץ אסטרטגיית אפס אמון הואץ בשלוש השנים האחרונות, בין היתר בשל מגיפת הקורונה. באופן משמעותי, המעבר למקומות עבודה מרוחקים והיברידיים מניע אימוץ רחב יותר של גישות אפס אמון, המבטיחות להגן על מערכות ונתונים גם כאשר העובדים ניגשים אליהם מחוץ לאתר, לפעמים במכשירים אישיים. אימוץ מואץ עקב COVID הוא מנבא טוב למוכנות אפס אמון באופן כללי, כאשר ארגונים שאימצו את האסטרטגיה במהלך המגיפה יישמו באזורים רבים יותר של סיכון ביטחוני מאשר עמיתיהם.

למידע נוסף על אפס אמון ולהערכה של בגרות האמון של אפס הארגון שלך, בקר באתר

aka.ms/zerotrust



מטרות מחקר מפורטות וגיוס קהל

מטרות המחקר כללו:

להבין את המצב הנוכחי של גישות אפס אמון
חשף את הלך הרוח, השיטות הטובות ביותר,
היתרונות ואתגרים של אימוץ גישות אפס אמון
חקור את העתיד של גישות אפס אמון
הקשרי הקשר בין חידושים ומגמות בגישות
אפס אמון

כדי לעמוד בקריטריוני המיון, מקבלי ההחלטות
הביטחוניות צריכים להיות:

אחראי על האבטחה בארגון שלהם, כולל אבטחת
סייבר, פעולות אבטחה, הגנת איומים, ניהול
זהויות, ניהול סיכונים, אבטחת יישומים, פלילי
דיגיטלי ותגובה לאירועים.

מועסק במשרה מלאה בחברה ברמה ארגונית
(1000 עובדים בארה"ב, 500 עובדים
ב- DE/JP/AU/NZ)

גילאי 25 - 75

מכיר אפס אמון

מעורב בקבלת החלטות לפיתוח/יישום
אסטרטגיה של אפס אמון

מבין 911 מקבלי ההחלטות הביטחוניות
שהתראיינו לגל המחקר באפריל 2021:

בארה"ב, 477 אנשי SDM התראיינו

בגרמניה התראיינו 201 אנשי SDM

באוסטרליה/ניו זילנד התראיינו 126 אנשי SDM

ביפן התראיינו 107 אנשי SDM

הערה: מחקר נערך במהלך מגפת COVID-19 העולמית,
שהייתה בשלבים שונים של הסלמה/בלימה

© קבוצת השערות 2021. © Microsoft 2021
כל הזכויות שמורות. 07/21