FileWall™ by odix

FileWall™

for Microsoft 365 Exchange Online

מדריך למשתמש

odix | AZTEK MANAGE THE CLOUD

odix ltd © February 2021

תוכן עניינים

1 הקדמה 3
2 פתרון הFileWall של odix 4
2.1 סקירה כללית 4
2.2 סוגי הקבצים הנתמכים 4
2.3 חווית משתמש 4
3 הפעלת שירות FileWall 6
4 הפעלת משתמשים ראשונית 8
5 ממשק ניהול – סקירה 10
6 ממשק הניהול- Dashboard 11
6.1 חלונית סקירה כללית 11
6.2 סטטיסטיקה 13
6.3 הודעות מערכת 15
7 הגדרות ניהול 16
7.1 ניהול משתמשים- User Management 16
7.2 ניהול מדיניות- Policy Management 17
7.2.1 צפייה/ עריכת הגדרות מדיניות 18
7.2.2 הוספת מדיניות 23
7.2.3 מחיקת מדיניות 24
7.3 הגדרות כלליות- Settings 24
7.3.1 הרשאת כניסה להודעות דוא"ל מקוריות 24
8 הודעות דוא"ל- Email Messages 25
8.1 צפייה בפרטי צרופה 27
8.2 שחזור קבצים מקוריים 27
8.3 הסרת קובץ מ- Quarantine 28

odix ltd © February 2021

1 הקדמה

FileWall הינו תוסף הגנה לתיבות הדואר של מיקרוסופט 365. FileWall מונע חדירת נוזקות לארגון על ידי נטרול הקוד זדוני המסתתר בקבצי צרופות בהודעות הדואר האלקטרוני הנסרקות על ידי השירות.

FileWall מבוסס על טכנולוגיית הלבנת קבצים מבית חברת אודיקס הנקראת ™TrueCDR (Content Disarm and Reconstruction). הטכנולוגיה של odix מוטמעת בארגונים רבים והוכחה כיעילה במניעת מתקפות המועברות באמצעות קבצים זדוניים. טכנולוגיית פטנט זו סורקת, מפרקת ובונה מחדש קבצים הנמצאים בשימוש יומיומי לקבצים בטוחים לשימוש הנקיים מנוזקות.

חברת אזטק בשיתוף עם אודיקס מספקת ללקוחותיה רשיונות OEM הניתנים ללא עלות לשנת 2021.

מדריך משתמש זה מיועד ללקוחות אזטק וכולל הסבר על הפעלת השירות ותפעולו השוטף.

פניות בנושא תמיכה במוצר ניתן להפנות ל: support@aztek.co.il

מסמך זה מנוסח בלשון זכר אך פונה לכלל המינים.

2 פתרון הFILEWALL של ODIX

2.1 סקירה כללית

תהליך סריקת הקבצים של odix מסיר ומנטרל את כל הנוזקות, ידועות ובלתי ידועות, המוסתרות בקבצים. תהליך הסריקה מטפל בסוגים שונים של קבצים ומשתמש באלגוריתם מתמטי ייחודי המותאם לכל סוג קובץ. התהליך מתבצע ברקע ללא הפרעה לשימוש השוטף בדואר האלקטרוני.

הקבצים המולבנים שעברו את תהליך הסריקה אינם עוברים המרת פורמטים אלא נשארים זהים לפורמט המקורי (לדוגמא: קובץ אקסל ישאר זהה בפורמט ולא יעבור המרה ל-csv).

תהליך ההלבנה מבצע ניטרול של קודים וכך מבטא את התכונה החזקה ביותר של פתרון ה- odix הוא יכולתו להתמודד עם איומים לא ידועים או איומים עתידיים שבהן פתרונות מדור הקודם נופלים.

לאחר שזוהתה צרופה לדוא"ל, תהליך החיטוי כולל את השלבים הבאים:

- אכיפת מדיניות – על כל משתמש חלה מדיניות הקובעת את סוגי הקבצים רשאים/לא רשאים להיכנס לתיבת הדואר שלהם. ארגון יכול להחיל מספר מדינויות המגדירות "רשימות שחורות" ו"רשימות לבנות " של סוגי קבצים ואת הפעולות הננקטות על צרופות.
- הלבנה – שלב החלת אלגוריתם ההלבנה (TrueCDR). FileWall מנטרל את הקוד הזדוני ומספק עותק מולבן לשימוש בטוח.

הערה: אם FileWall מזהה קובץ פגום, המערכת חוסמת אותו.

2.2 סוגי הקבצים הנתמכים

FileWall תומך בחיטוי של כל סוגי הקבצים הנפוצים ביותר הכוללים קבצי PDF, קבצי Office, תמונות וארכיב.

הערה: בתרחיש בו הודעת דוא"ל מכילה צרופה מסוג קובץ שאינו נתמך, שירות FileWall לא יבצע הלבנה לקובץ ויציג הודעה בגוף ההודעה המציינת כי הקובץ לא עבר הלבנה ויש לפתוח את הקובץ בזהירות.

2.3 חווית משתמש

לאחר הפעלת השירות, כל הצרופות המגיעות לתיבות הדואר של מייקרוסופט 365 בארגונך יעובדו ע"י אודיקס, אין זה משנה אם השימוש בתיבת הדוא"ל של אופיס הוא בדפדפן, בשולחן העבודה או בסמארטפון. הזמן הנדרש לעיבוד תלוי במספר הצרופות וגודלן, עם זאת בדרך כלל העיבוד נמשך שניות ספרות פחות מדקה.

לאחר סיום העיבוד, התוצאות יוצגו בבאנר בצבע בהתאם לסטטוס: ירוק (הצלחה), כתום (לא חוטא), אדום (חסום), צהוב (כשל בשירות), אפור (הודעה מקורית שוחררה/ שוחזרה).

קישור **More info** נמצא בקצה הימני של הבאנר בכדי להציג מידע נוסף.

odix ltd © February 2021

צרופות מולבנות

לאחר חיטוי **מוצלח** של צרופות, מוצג באנר ירוק בראש גוף ההודעה:

תהליך נטרול הצרופות הושלם בהצלחה.

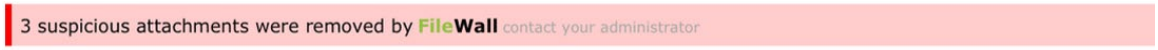
צרופות לא מחוטאות

במקרה שלא ניתן היה לבצע חיטוי של הצרופות, מוצג באנר כתום בראש גוף ההודעה:

תרחיש זה יכול לקרות אם סוג הקובץ אינו נתמך או אם הוגדרה מדיניות לעקוף נטרול סוג קובץ הזה.

צרופות חסומות

במידה וצרופה נחסמת, בראש גוף ההודעה יופיע באנר אדום עם פרטים לסיבת החסימה.
לדוגמא, אם הFileWall קבע שהצרופה חשודה, לא מהסוג המורשה לפי המדיניות, או אם מבנה הקובץ אינו תואם את סוג סיומת הקובץ.



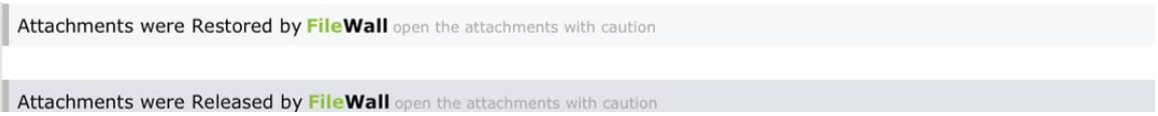
כשל בשירות

במידה והתרחש כשל בשירות, באנר צהוב יוצג בראש גוף ההודעה:

לחץ על הקישור ל**More info** בקצה הימני של הבאנר כדי להציג מידע נוסף. הצרופות לא חוטאו במקרה זה.

ההודעה המקורית שוחררה/שוחזרה

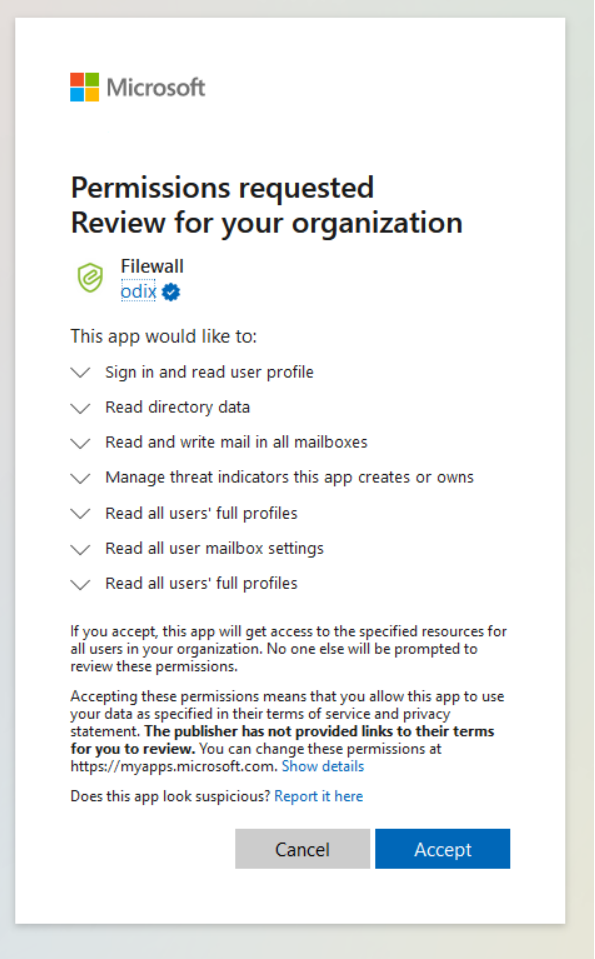
אם הודעה מקורית (כולל קבצים מצורפים שלה) שוחררה/ שוחזרה, מוצג באנר אפור בראש גוף ההודעה:



odix ltd © February 2021

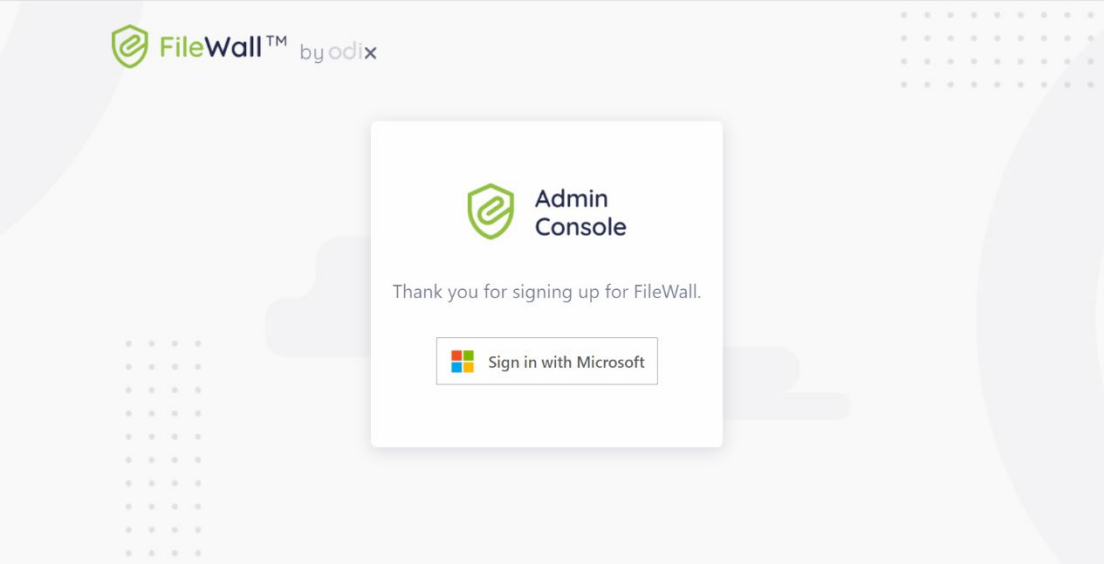
3 הפעלת שירות FILEWALL

1. לחץ על לינק אתחול ה-FileWall שנשלח אליך במייל ע"י אזטק.
2. דף אישור הרשאות הבא יוצג לפניך, לחץ על "Accept".

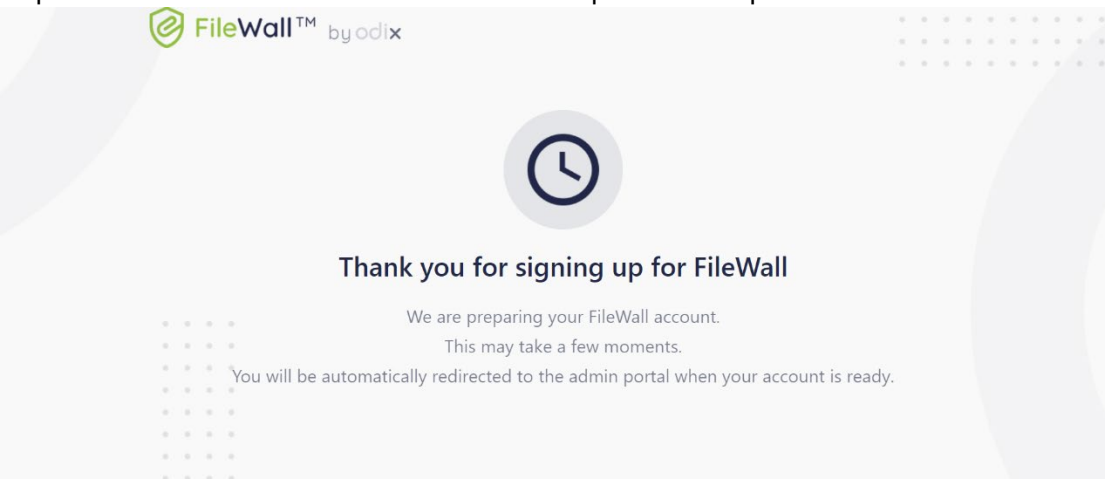


odix ltd © February 2021

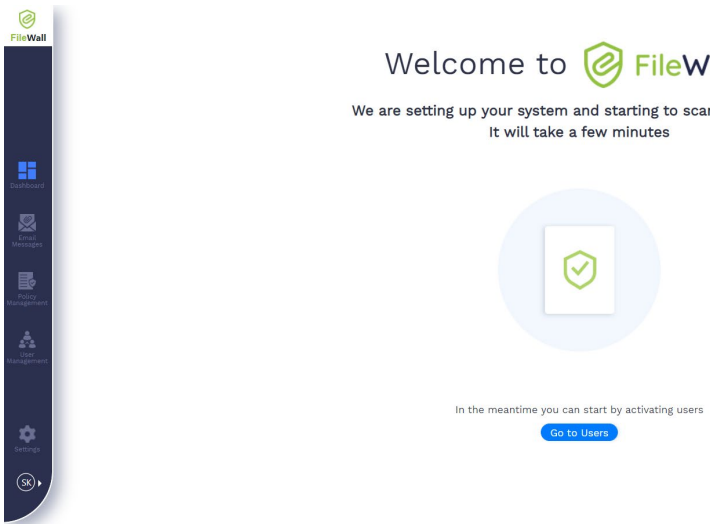
3. מסך הכניסה למערכת ניהול FileWall יופיע, התחבר באמצעות משתמש המייקרוסופט שלך.



4. לאחר ההתחברות תועבר לדף טעינה בזמן שהמערכת מכינה את מערכת הFileWall שלך:



5. המתן מספר שניות, והמסך הבא יפתח אוטומטית.

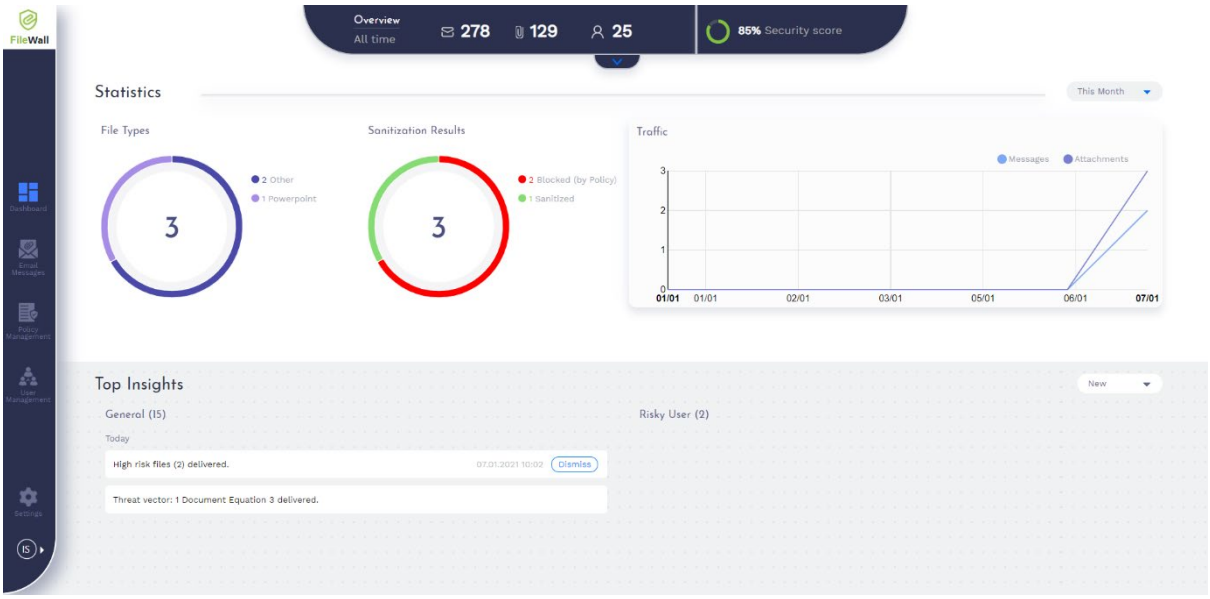


במידה והמסך לא מתקבל תוך מספר דקות, אנא נסו שוב לאחר שעתיים.

odix ltd © February 2021

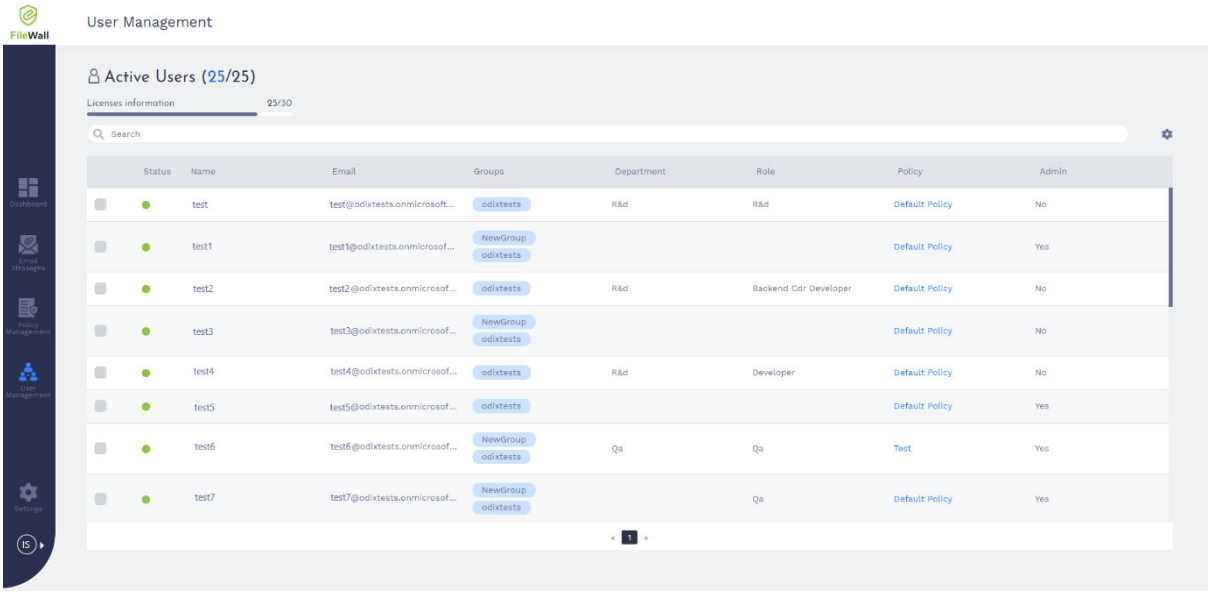
4 הפעלת משתמשים ראשונית

1. הפעלת משתמשים ראשונית מתבצעת דרך ממשק הניהול בפורטל https://app.filewall.com
2. הכניסה לממשק הניהול מתבצעת עם שם המשתמש והסמא של Microsoft.
3. המסך הראשי של ממשק הניהול המוצג לאדמניסטרטור הינו המסך הבא.



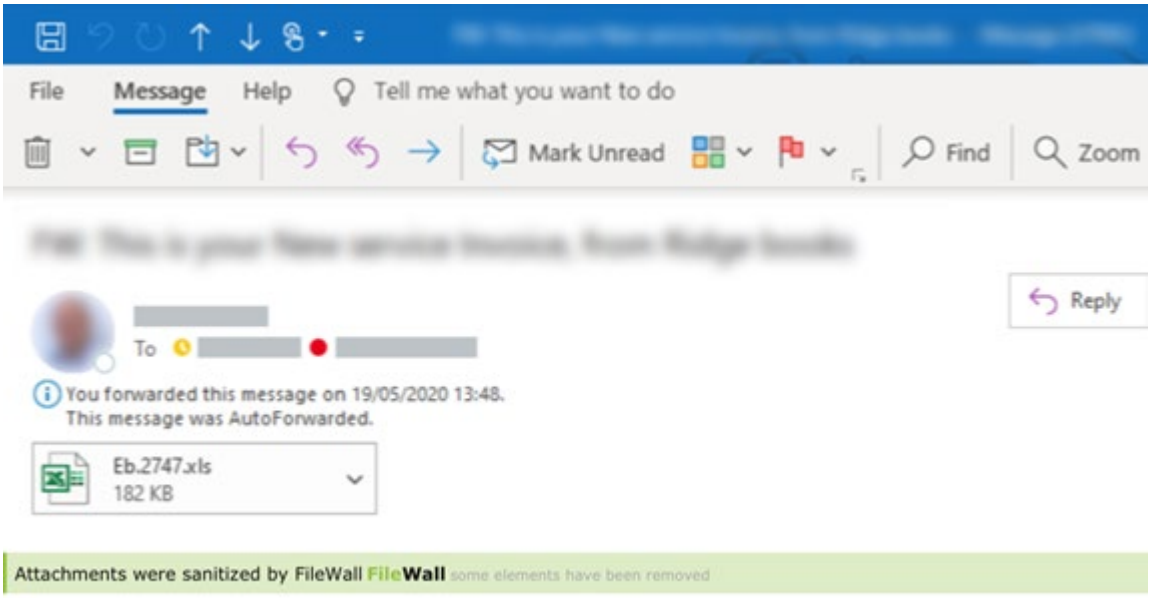
4. להפעלת משתמשים, בחר "User Management" בתפריט הראשי (המופיע באייקון)

5. הפעל את חשבונות המשתמשים עבורם תרצה להפעיל את שירות ה-FileWall.



odix ltd © February 2021

6. על מנת שתוכל לאמת שהשירות אכן פועל, שלח דוא"ל עם קובץ צרופה לבחירתך אל משתמש שהפעלת בשלב הקודם. כאשר הודעת הדוא"ל מגיעה לתיבת הדואר הנכנס, יוצג באנר של FileWall בחלק העליון של גוף ההודעה (טקסט וצבע הבאנר עשויים להשתנות בהתאם לקובץ המצורף שנשלח). עיבוד ההודעות עשוי להימשך מספר שניות, אם אינך רואה את הבאנר בהודעה לאחר דקה אנא פנה לתמיכה: support@aztek.co.il



5 ממשק ניהול - סקירה

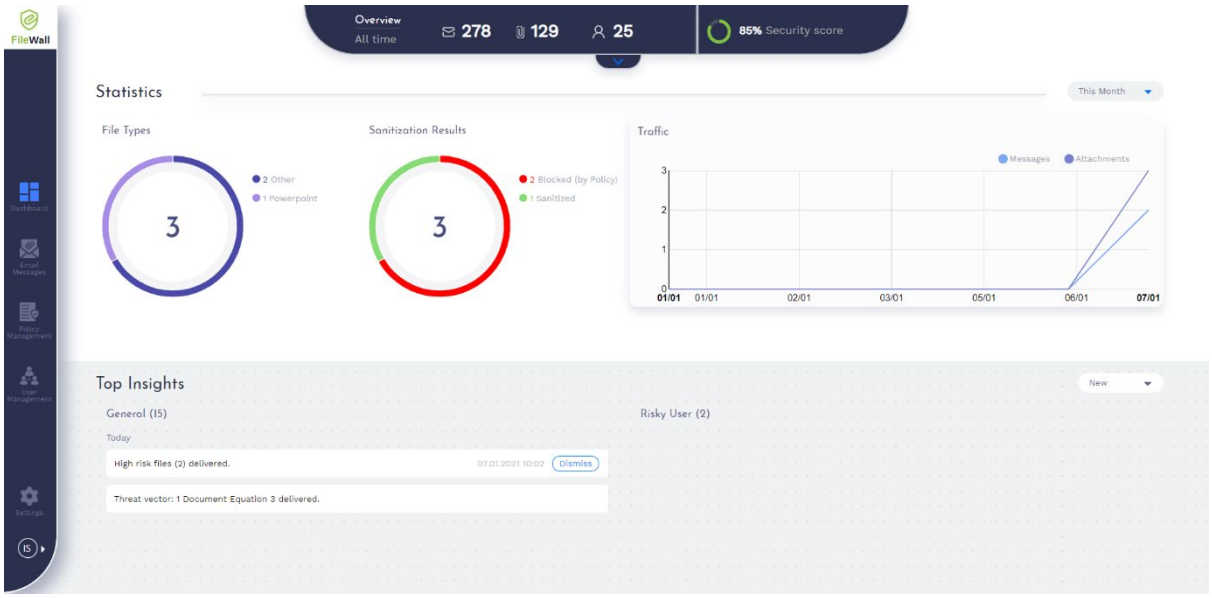
פונקציות הניהול של FileWall מאורגנות בתוך הדפים הראשיים:

- לוח בקרה- מספק ייצוג של פעילות המערכת, הכולל בתוכו נתונים סטטיסטיים על הודעות סרוקות וקבצי הצרופה בהם, הודעות מערכת וציון אבטחה.
- הודעות דוא"ל- מציג רשומות של ההודעות שעובדו ו/ או הועברו לQuarantine ע"י ה-FileWall, ומאפשר שיחזור הודעות מקוריות ושחרור קבצים מה- Quarantine לפי הצורך.
- ניהול מדיניות- מאפשר הגדרת כל המאפיינים הנחוצים של המדיניות הקשורים לביצוע תהליך הסריקה והחיטוי, כולל קביעת אילו סוגי קבצים מותרים או חסומים, ואילו פעולות נטרול מוחלות. באפשרותך לצפות במאפייני מדיניות ברירת המחדל וליצור מדיניות חדשה בהתאם לצרכי הארגנך.
- ניהול משתמשים- מאפשר ניהול מימוש ה-FileWall למשתמשים בארגונך. כברירת מחדל, כלל משתמשי מייקרוסופט 365 בארגונך מופיעים בדף המשתמשים. עליך להפעיל משתמשים על מנת שה-FileWall יוכל לעבד את קבצי הצרופה לדוא"ל שלהם.
- הגדרות- מאפשר קביעת הגדרות מערכת הקשורות לגישת המשתמשים להודעות דוא"ל מקוריות ולקבצי הצרופות בהם. הגדרות נוספות יתווספו בגרסה עתידית.

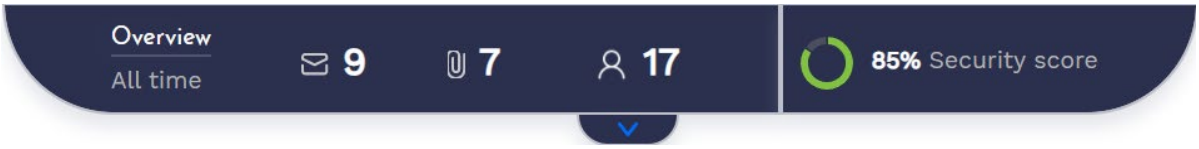
odix ltd © February 2021

6 ממשק הניהול- DASHBOARD

לוח הבקרה מוצג בכל פעם שאתה מתחבר לFileWall.



6.1 חלונית סקירה כללית



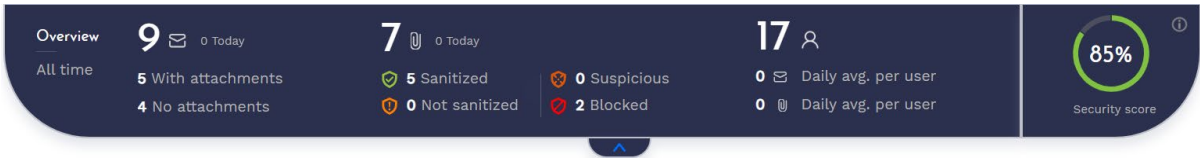
חלונית הסקירה כללית יציג את הפרטים הבאים:

- מספר הודעות הדוא"ל אשר נסרקו
- מספר צרופות דוא"ל אשר נסרקו
- מספר משתמשי תיבות הדואר של מייקרוסופט 365
- 85% ציון האבטחה המצטבר

באפשרותך להרחיב את החלונית באמצעות לחיצה על .

odix | AZTEK MANAGE THE CLOUD

odix ltd © February 2021



החלונית תציג כעת את הפרטים הבאים:

- מספר הודעות הדוא"ל אשר נסרקו:
  - עם צרופות
  - ללא צרופות

- מספר צרופות דוא"ל אשר נסרקו ותוצאות הסריקה:
  - מחוטא (נפתר)
  - לא מחוטא (סוג הקובץ אינו נתמך או שלא נוטרל ע"י המדיניות)
  - חשוד (הקובץ צרופה זוהה כחשוד ועל כן נחסם ע"י השירות)
  - נחסם (הקובץ צרופה נחסם ע"י מדיניות אדמין)

- סה"כ משתמשי תיבות הדואר של מייקרוסופט 365 אשר האימיילים שלהם נסרקו:
  - ממוצע מספר הודעות דוא"ל למשתמש
  - ממוצע מספר קבצי צרופה סרוקים למשתמש

הערה: הממוצע נקבע ע"י מספר משתמשי תיבות הדואר Active Exchange online מורשים.

- 

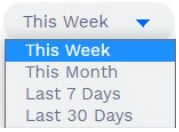
ציון האבטחה המצטבר נקבע על סמך הלוגיקה והחישובים של FileWall.
חישוב ציון האבטחה תלוי במדיניות שנקבעה לארגונך.

odix | AZTEK MANAGE THE CLOUD

odix ltd © February 2021

6.2 סטטיסטיקה

כברירת מחדל, הנתונים בחלק של הסטטיסטיקה בלוח הבקרה מציגים את הפעילות בשבוע האחרון.



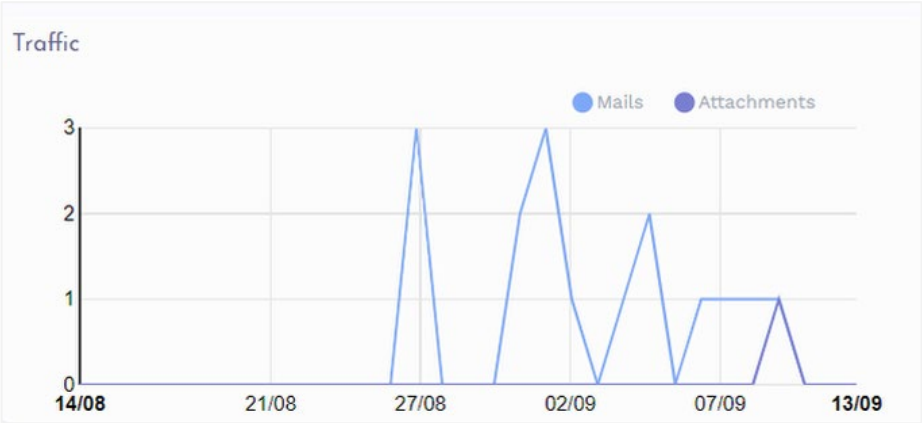
בתפריט נפתח מצד ימין למעלה ניתן לשנות את תקופת הזמן עליו תרצו לראות את הסטטיסטיקה (השבוע הנוכחי, החודש הנוכחי, 30 הימים האחרונים, 7 הימים האחרונים).

החלק הסטטיסטי כולל את רכיבי הנתונים הגרפיים הבאים:

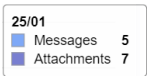
- **סוג קובץ:** מציין את התפלגות הקבצים, לפי סוג, שנסרקו.

- **תוצאות ההלבנה:** מציין את מספר הקבצים שהולבנו לפי תוצאות הסריקה.

- **תעבורה:** מציין את רמת התעבורה של הודעות דוא"ל ושל קבצי צרופה.



באפשרותך להציג את הנתונים של הודעות דואר ו/ או קבצי צרופה יחד או בבידוד על ידי בחירה או ניקוי האפשרויות מיד מעל לתרשים. העבר את העכבר מעל נקודה בגרף



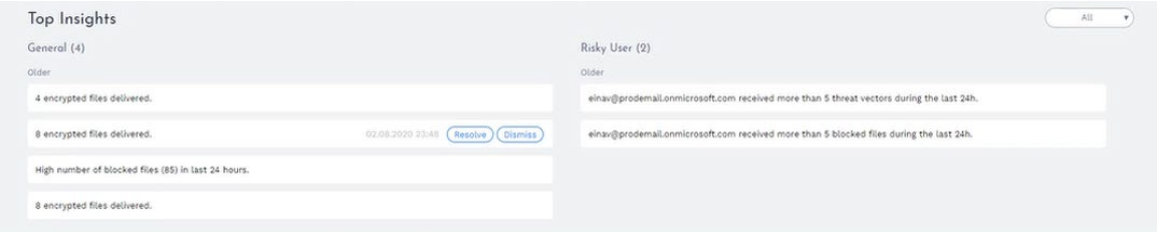
והערכים המדויקים יוצגו בחלונית:

odix ltd © February 2021

6.3 הודעות מערכת

אזור ה- Top Insights מכיל הודעות מערכת אודות פעילות בדבר קבצים חשודים, וקטורי תקיפה שזוהו וכל תרחיש שזוהה כחריג ומצריך אזהרה מטעם המערכת.

כברירת מחדל, הרשימות כוללות את כלל ההודעות. באפשרותך לסנן את הרשימות ע"י בחירה; חדש (**New**) או נפתר (**Resolved**), בתפריט נפתח הנמצא למעלה מימין בחלק זה. ניתן גם לפסול או לפתור הודעות ע"י העברת העכבר על התובנה ובחירה באפשרות הרצויה. לאחר שההודעה נפתרה, יופיע סימן .



החלק של התובנות העליונות מחולק ל2 רשימות:

- כללי: הערכים ברשימת ההודעות הכלליות מספקים תובנות ופרטים חשובים לגבי הודעות הדוא"ל וקבצי הצרופה בארגונך. לדוגמא: מספר הקבצים שנחסמו, מספר הקבצים המוצפנים אשר נשלחו, או התראות בנוגע מספר רב של קבצים שנחסמו בפרק זמן נתון.
- מסוכן: הערכים ברשימת המשתמשים המסוכנים ממקדים את תשומת ליבך למשתמשים המקבלים מספר יוצא דופן של קבצי צרופה חשודים או לא תקינים בדוא"ל. באמצעות מידע זה תוכל לבצע מעקב עם המשתמש בכדי לקבוע את הבעיה ולטפל בה.

פתירת או פסילת הודעות:

- פתירת הודעות: מקל על מיקוד תשומת הלב על הבעיות הפתוחות שנותרו. פתרון הודעה אינו מסיר אותה מן הרשימה. (ניתן לבחור צפיה בהודעות הפתורות לפי הסינון שנבחר).
- פסילת הודעות: כאשר אתה פוסל הודעה, היא מוסרת מן הרשימה.

odix ltd © February 2021

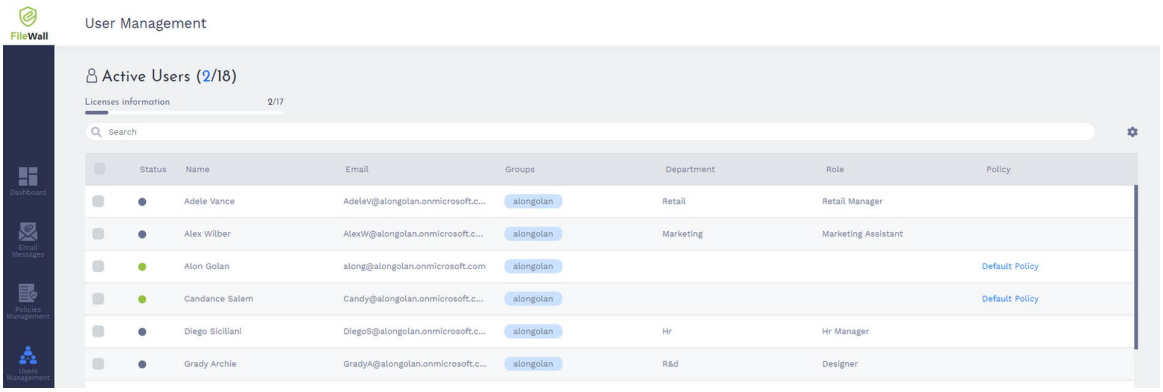
7 הגדרות ניהול

כאדמיניסטרטור המערכת הינך מורשה לנהל הגדרות מדיניות הFileWall , הפעלת/ ניתוק משתמשים ועוד.

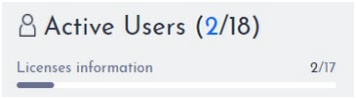
7.1 ניהול משתמשים- User Management

הFileWall שולף את נתוני משתמשי המייקרוסופט 365 בארגונך מן הAzure Active Directory ומציג אותם ברשימה בדף משתמשים. כברירת מחדל, חלה על כלל המשתמשים מדיניות ברירת מחדל עם סטטוס לא פעיל. עליך להפעיל את חשבונות המשתמשים על מנת שהFileWall יוכל לעבד את קבצי הצרופה להודעות הדוא"ל.
הערה: אין באפשרותך ליצור משתמש או לערוך פרטי משתמש.

ניהול משתמשי FileWall מתבצע בחלון User Management, למעבר אליו לחץ על  בתפריט הראשי.



מעל לרשימת הפעלת משתמשים, נמצא מונה המציין את מספר המשתמשים **המופעלים** ומספר סך כל תיבות הדואר בארגונך. בנוסף, מצוין מספר הרישיונות בשימוש.



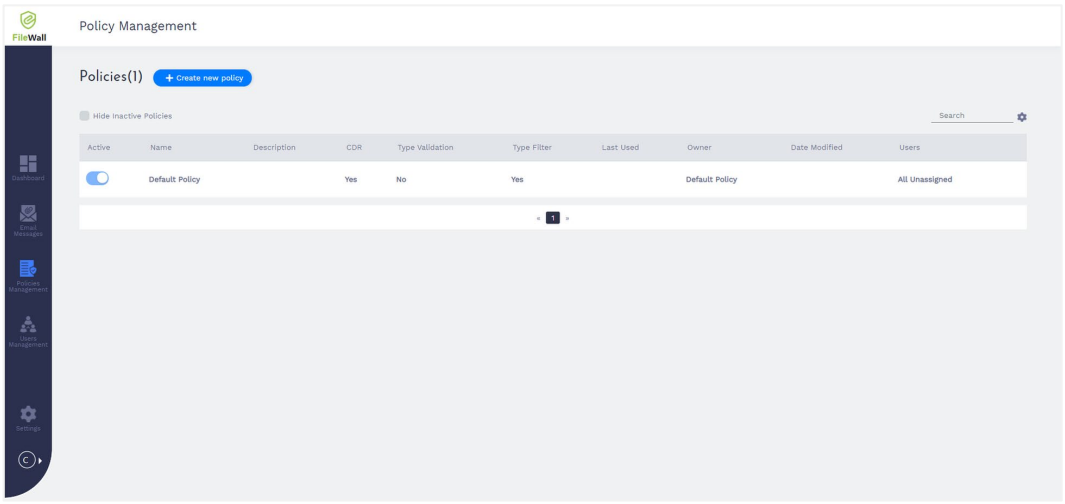
רשימת המשתמשים הפעילים כוללת את פרטי המשתמש המיובאים מ- Azure Active Directory. המדיניות שהוגדרה לכל משתמש מופיעה בעמודת המדיניות. (משתמשים שלא הופעלו לא חלה עליהם מדיניות)

odix ltd © February 2021

7.2 ניהול מדיניות- Policy Management

FileWall מגיע עם מדיניות ברירת מחדל המוגדרת במערכת. באפשרותך להחיל מדיניות זו עבור כל המשתמשים הפעילים, או להגדיר מדיניות ספציפית בהתאם לצרכי ארגונך. הגדרת מדיניות קשיחה המצמצמת אפשרויות קבלת קבצים בעלי סיכון משפיעה על קביעת ציון האבטחה של ארגונך במערכת.

הגדרה והקצאת מדיניות מתבצעת בחלון Policy Management, למעבר אליו לחץ על בתפריט הראשי.



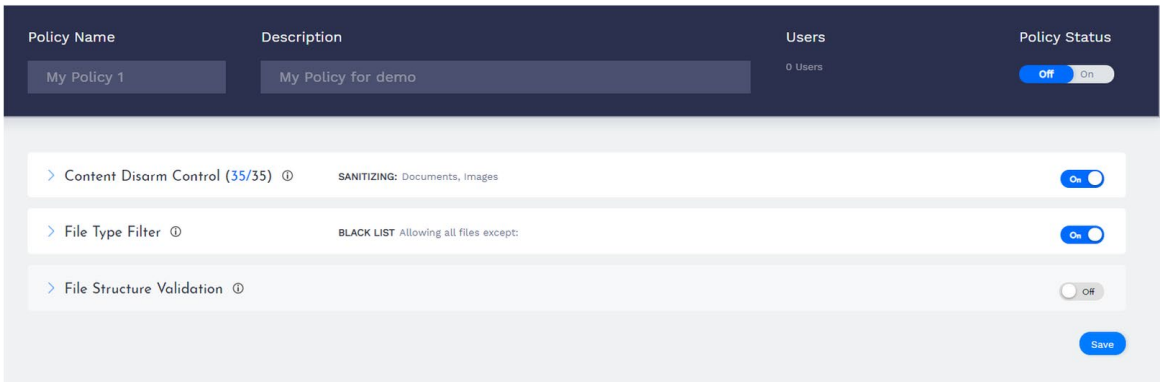
בכל מדיניות מפורט המידע הבא:

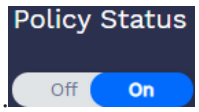
פרמטר	הסבר
Active	מציין את סטטוס המדיניות (מופעל). סטטוס מדיניות ברירת המחדל הוא פעיל ולא ניתן לשינוי. ניתן לשנות סטטוס מדיניות ספציפית ע"י לחיצה על המתג (= לא פעיל, = פעיל)
Name	שם המדיניות.
Description	הסבר קצר על המדיניות.
CDR	מציין האם ההלבנה מוחלת כחלק מהמדיניות(כן/ לא).
Type Validation	מציין האם אימות סוג הקובץ מוחל כחלק מהמדיניות (כן/ לא).
Type Filter	מציין האם סינון סוגי קובץ מוחל כחלק מהמדיניות(כן/ לא).
Last Used	התאריך בו המדיניות הוחלה לאחרונה.
Owner	שם משתמש האדמין אשר יצר את המדיניות.
Date Modified	התאריך בו המדיניות נערכה לאחרונה.
Users	מספר המשתמשים עליהם המדיניות מוחלת.

7.2.1 צפייה/ עריכת הגדרות מדיניות

לצפייה בהגדרת המדיניות:

בדף המדינויות, בתפריט אפשרויות נוספות (⋮) הנמצא בשורה של המדיניות, בחר ב**Edit** או לחץ קליק כפול על שורת המדיניות.



באפשרותך להפעיל ולכבות את המדיניות במתג הבא 

.

בכדי להרחיב חלק או תת חלק, לחץ .
בכדי לצמצם את החלק או תת חלק, לחץ .
הערה: בין חלק לתת-חלק מתקיים קשר היררכי. הגדרות המוחלות על חלק מוחלות על תת-חלק שלו. לדוגמא; אם תכבה את File Type Filter ברמה ההיררכית הגבוהה, הסנן יהיה כבוי לכלל סוגי הקבצים.

7.2.1.1 הגדרות הלבנה (Content Disarm Control)

הגדרות ההלבנה קובעות את הפעולות המבוצעות על קבצי הצרופה בדואר הנכנס.
מספר סוגי הקובץ שהוגדרו לסריקה מסומן בסוגרים בכחול, עם מספר המקסימלי של הסוגים הזמינים (בשחור) Content Disarm Control (13/35) . סוגי קבצי הצרופות מחולקים לשני חלקים ראשיים- מסמכים ותמונות.

odix ltd © February 2021

קבוצת המסמכים כוללת בתוכה תתי- חלקים. באפשרותך להציג את סוגי סיומת הקבצים המשויכים לתת- חלק ע"י הרחבת חלק זה. לדוגמא:

קבוצת התמונות לא כוללת בתוכה תתי- חלקים.

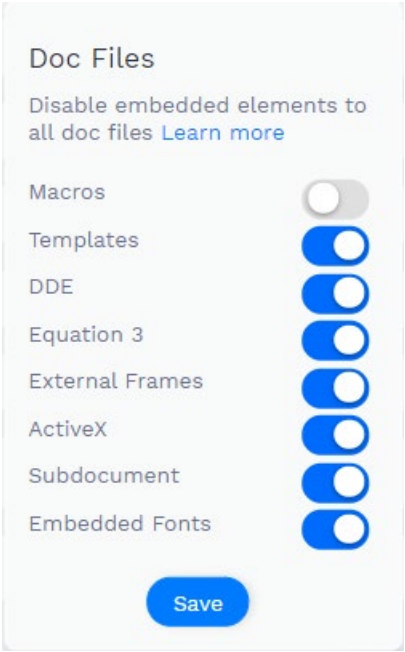
7.2.1.1.1 ביטול הסרת רכיבי קובץ מוטמעים

רמה נוספת של הבחנה הנוגעת בביטול הסרת רכיבי קובץ מוטעמים (אלמנטים שמצורפים) בתוך מסמכים. רכיבים מוטעמים הם אובייקטים, תוכן פעיל ופונקציות היכולים להתקיים במסמך אופיס. יכולת זו לעיתים מנוצלת ע"י תוקפים מפני שבאפשרותם להטמיע קוד זדוני הנראה סטנדרטי. תהליך ההלבנה מאפשר הסרת רכיבים אלו. משמעות ביטול הסרת רכיבי קובץ מוטמעים היא אי הסרה של רכיבי הקובץ במקרה של הימצאותם בסריקה.

בכדי לבטל הסרת רכיבי קובץ מוטמעים לכלל סיומות הקבצים הקשורים לקבוצה (מסמכים או תמונות) לחץ על **Configure** בשורה של הקבוצה. באפשרותך לאפשר או לבטל סוגים ספציפיים של רכיבים.

בכדי לבטל הסרת רכיב קובץ מוטבע עבור סוג סיומת קובץ ספציפי, לחץ על ⚙ בשורה. באפשרותך לאפשר או לבטל סוגי רכיבים ספציפיים ולחץ **Save**.

odix ltd © February 2021

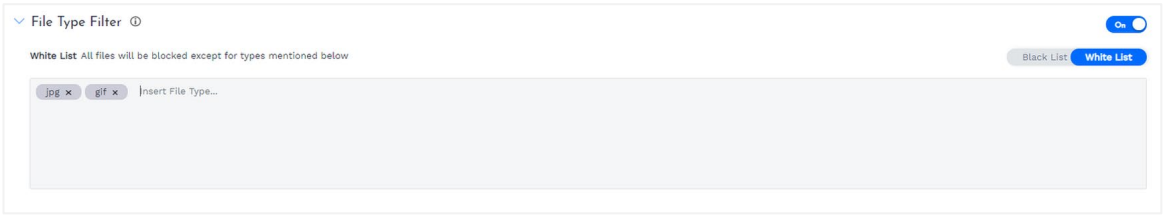


7.2.1.1 הגדרות סינון סוג קובץ (File Type Filters)

בהגדרת File Type Filters באפשרותך לחסום או לאפשר קבלת צרופה בדוא"ל מסוג ספציפי.
הגדרות אלו מוגדרות בשימוש במנגנון **White List** "רשימה לבנה" או **Black List** "רשימה שחורה".

הרשימה השחורה מגדירה את סוגי הקבצים שאין להם הרשאה להתקבל כצרופה בדוא"ל. הגישה לסוגי קבצים שהוגדרו ברשימה השחורה נדחית. (קבצי צרופה מסוגי קבצים שלא מוגדרים תחת הרשימה השחורה יוכלו להתקבל).

הרשימה הלבנה מגדירה את סוגי הקבצים בעלי ההרשאה להתקבל כצרופה להודעת דוא"ל, כלומר, הפרטים ברשימה מורשים ועובר את תהליך החיטוי.



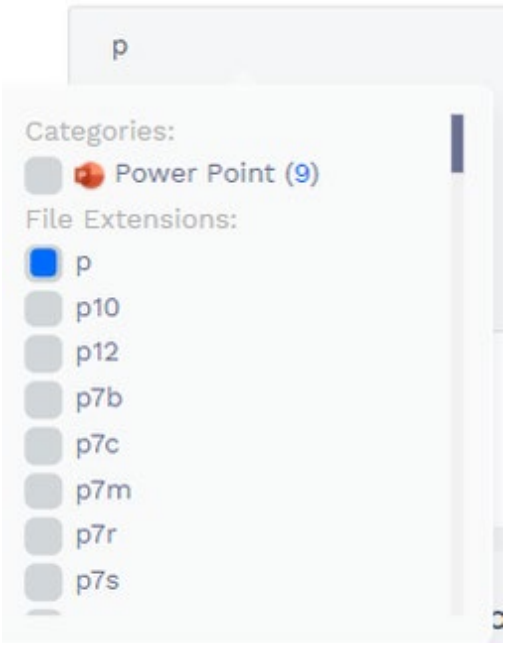
הערה: באפשרותך לבחור להגדיר רשימה שחורה **או** רשימה לבנה- לא את שתיהן.

odix ltd © February 2021

הגדרת מסנן סוג קובץ

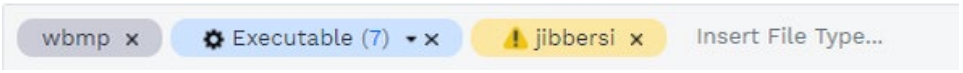
בכדי להוסיף סוג קובץ ספציפי:

1. הזן את סוג סיומת קובץ או חלק ממנו בחלונית **Insert File Type**. השלמה אוטומטית מפרטת את סוגי קבצים/ קטגוריות התואמים להקלדה.



2. בחר את סוג הקובץ או הקטגוריה בכדי להוספה לרשימה.

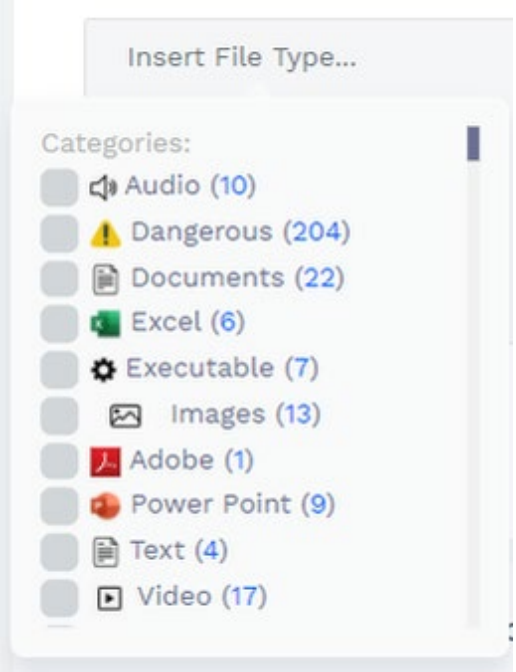
הערה: במידה ותזין מחרוזת שלא מופיעה בתוצאות ההשלמה האוטומטית ותלחץ על Enter, המחרוזת תתווסף לרשימה עם התווית "unknown" והתג עצמו יסומן בצהוב עם סמל זהירות ברשימת סוגי הקבצים.



odix ltd © February 2021

בכדי להוסיף את כל סוגי סיומות קובץ בקטגוריה מסוימת:

1. הזן רווח בשדה **Insert File Type**. סוגי קטגוריות קבצים מופיעים בראש התפריט נפתח. מספר סוגי הקבצים בכל קטגוריה מצוין בסוגריים.



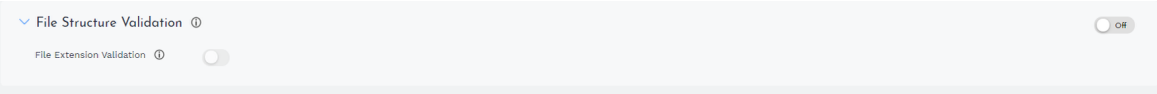
2. בחר קטגוריה בכדי להוסיף אותה לרשימה.
תג הקטגוריה מופיע בכחול וכולל את סמל הקטגוריה.

בכדי להסיר סוג קובץ או קטגוריה:

לחץ על × הנמצא בימין התג של סוג קובץ/ קטגוריה ברשימה.

7.2.1.2 הגדרות אימות מבנה קבצים (File Structure Validation)

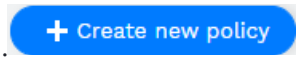
File Structure Validation מאמת שתוכן הקובץ והמבנה תואמים את סיומת הקובץ. דבר זה יכול להועיל בזיהוי/ חסימה של ניסיונות זיוף קבצים (לדוגמא, קובץ הפעלה עם סיומת txt.).

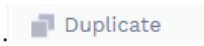


7.2.2 הוספת מדיניות

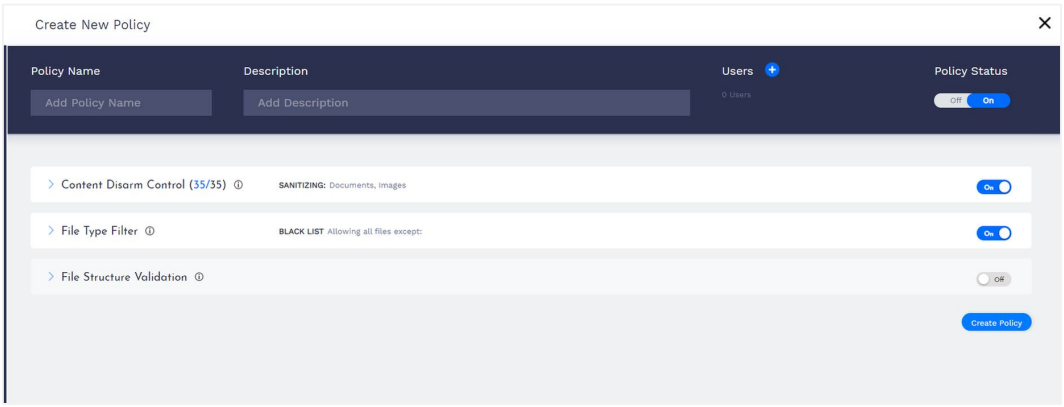
באפשרותך ליצור מדיניות מותאמת אישית על בסיס צרכי ארגונך.
הערה: מדיניות מותאמת אישית מוחלת על משתמשים שהוקצו אליה. שאר המשתמשים יישארו תחת מדיניות ברירת המחדל.

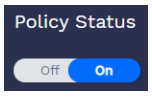
בכדי להוסיף מדיניות:

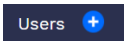
1. בחלון ניהול מדינויות, לחץ על 

. במידה ותרצה ליצור מדיניות חדשה בהתבסס על מדיניות ברירת המחדל, לחץ על תפריט בימין השורה של מדיניות ברירת המחדל (⋮) על 

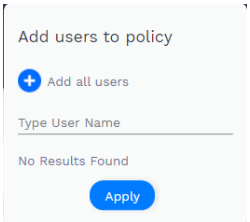
.



2. הזן את שם המדיניות ופירוט קצר על המדיניות בשדות המתאימים.
3. הגדר את הגדרות המדיניות. לפירוט על השדות:
   - הגדרות הלבנה
   - הגדרות סינון סוג קובץ
   - הגדרות אימות מבנה קבצים
4. אם ברצונך ליישם את המדיניות, שנה את סטטוס המדיניות 

.
5. בכדי להקצות משתמשים למדיניות זו:
   - לחץ על 

בקדמת המסך.
   - באפשרותך להוסיף משתמשים ספציפיים או את כלל המשתמשים בתפריט הנפתח הבא:



הערה: ניתן להקצות משתמש למדיניות אחת בלבד בכל זמן. במידה והנך מחיל

odix ltd © February 2021

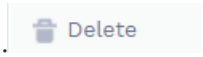
מדיניות חדשה על משתמש, הקצאתו למדיניות הקודמת תוסר. במידה ותסיר משתמש מהמדיניות, המשתמש יוקצה מחדש אוטומטית למדיניות ברירת המחדל.

לחץ על **Save**.

7.2.3 מחיקת מדיניות

באפשרותך למחוק מדיניות מותאמת אישית שאינה רלוונטית יותר עבור ארגונך. במידה ותמחק מדיניות, המשתמשים אשר הוקצו לה יוקצו אוטומטית למדיניות ברירת מחדל.
הערה: אין באפשרותך למחוק את מדיניות ברירת מחדל.

בכדי למחוק מדיניות:

בחלון המדינויות, בתפריט הנפתח (⋮) הנמצא בשורה של המדיניות ולחץ על 

.

7.3 הגדרות כלליות- Settings

ההגדרות הכלליות חלות על כל המשתמשים וכל המדינויות.

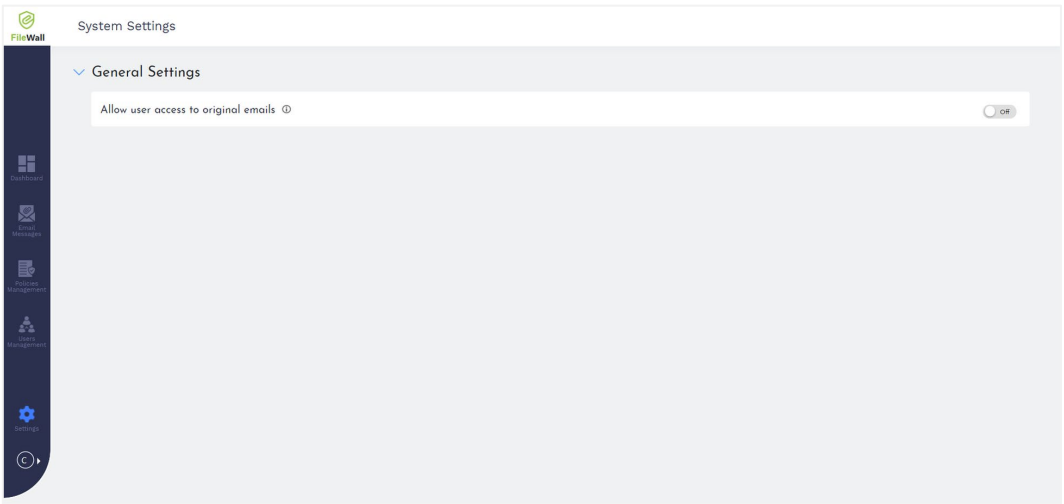
7.3.1 הרשאת כניסה להודעות דוא"ל מקוריות

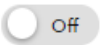
באפשרותך לאפשר לכל המשתמשים, גישה ישירה להודעות הדוא"ל החסומות והמקוריות בתיקיה ייעודית (odix-backup) שתתווסף אוטומטית לתיבת הדוא"ל. תייקת odix-backup מכילה העתק מקורי של כל הודעת דוא"ל נכנסת עם קבצי צרופה המקוריים שלהם (טרום חיטוי).

הערה: במידה והרשאה אינה מופעלת, משתמש חייב לפנות לאדמיניסטרטור במקרה שנדרשת גישה להודעת הדוא"ל המקורי.

בכדי לתת/ לבטל הרשאה להודעות הדוא"ל המקוריות:

1. בתפריט הראשי לחץ על  בכדי להיכנס לחלון הSettings .



2. במתג באפשרותך לבחור 

(=לא לאשר גישה) או 

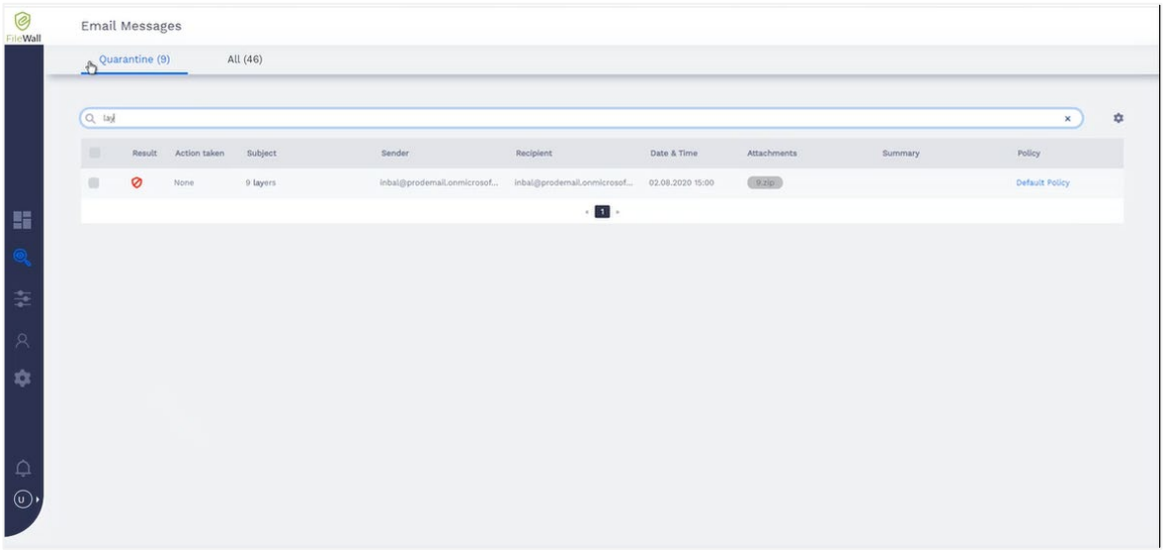
(=לתת הרשאה לגישה).

odix ltd © February 2021

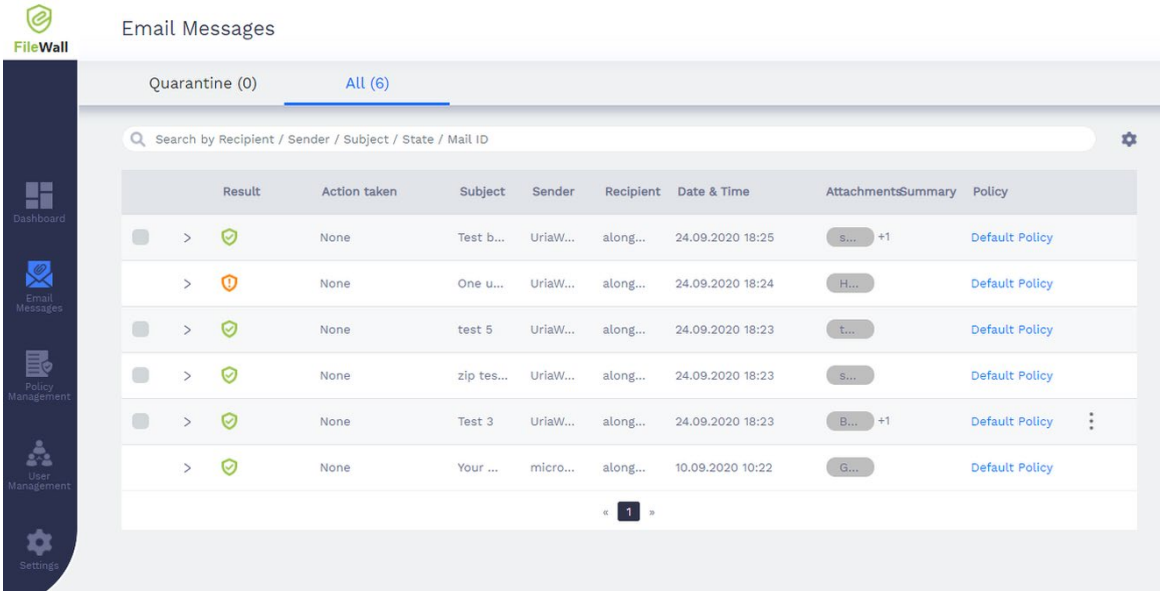
8 הודעות דוא"ל- EMAIL MESSAGES

חלון ה Email Messages מציג פרטים על ההודעות שעברו את התהליך או הוכנסו לQuarantine ע"י FileWall בשבועיים האחרונים.

בתפריט הראשי לחץ על  בכדי להיכנס לחלון הודעות הדוא"ל. חלון הודעות דוא"ל שהוכנסו לQuarantine (הודעות דוא"ל שנחסמו) יופיע כברירת מחדל.



בכדי לצפות בכלל ההודעות, לחץ על חלונית **All** .



odix | AZTEK MANAGE THE CLOUD

odix ltd © February 2021

הפרטים הבאים מוצגים לכל הודעת דוא"ל:

פרמטר	הסבר
Result	מציין את התוצאה של עיבוד קבצי דוא"ל: • אייקון ירוק מציין כי ההודעה חוטאה בהצלחה. • אייקון כתום מציין כי קבצי הצרופה לא עברו חיטוי. • אייקון צהוב מציין על כשל בשירות. • אייקון אדום מציין כי הודעת הדוא"ל נחסמה. • אייקון אפור מציין כי מצרופות מספר צרופות להודעת דוא"ל בעלות תוצאות עיבוד שונות.
Action Taken	הפעולות שננקטו על הודעת הדוא"ל.
Subject	שורת הנושא של הודעת הדוא"ל המקורית.
Sender	שולח ההודעה.
Recipient	רשימת התפוצה.
Date & Time	התאריך והשעה בהם נשלחה הודעת הדוא"ל.
Attachments	קבצי הצרופה להודעת הדוא"ל. אם ההודעה כללה יותר מצרופה אחת, מספר הצרופות מופיע כפלוס ליד שם הקובץ. לחיצה כפולה על השורה עם פרטי ההודעה תפתח מידע נוסף על כל צרופה להודעת הדוא"ל הזו. למידע נוסף- צפייה בפרטי צרופה.
Mail ID	המספר מזהה המלא של הודעת מייקרוסופט. העבר את העכבר מעל שדה הID בכדי להציג את הID בחלונית.
Summary	תקציר, האם קיים.
Policy	המדיניות המוחלת על המשתמש.

הערה- במידה והמוען שולח הודעת דוא"ל עם צרופה למספר נמענים, המערכת מתייחסת אליהם במספר שורות (לכל נמען שורה נפרדת ברשימות הודעות הדוא"ל).

באפשרותך לחפש הודעת דואר אלקטרוני ספציפית על ידי הזנת מחרוזת מלאה או חלקית בשדה החיפוש. הטבלה מסוננת באופן אוטומטי כדי לכלול רק את הערכים המכילים את המחרוזת הספציפית.

odix ltd © February 2021

8.1 צפייה בפרטי צרופה

באפשרותך להציג מידע מפורט על כל אחד מקבצי הצרופה להודעת דוא"ל ע"י לחיצה כפולה על שורת הודעת הדוא"ל זו.

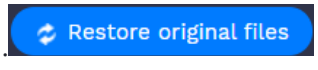
הפרטים הבאים מוצגים לכל צרופה להודעת דוא"ל:

פרמטר	הסבר
Status	מציין את תוצאת תהליך סריקת הקבצים: • אייקון ירוק מציין כי ההודעה עברה את תהליך החיטוי בהצלחה. • אייקון כתום מציין כי קבצי הצרופה לא עברו חיטוי. • אייקון צהוב מציין על כשל בשירות. • אייקון אדום מציין כי הצרופה להודעת הדוא"ל נחסמה.
Name	שם הקובץ.
Type	סוג הקובץ.
Size	גודל הקובץ.
Original Hash	hash המקורי של הצרופה.
New Hash	hash המוקצה לעותק המחוטא של הצרופה. (לא רלוונטי לקבצים חסומים.)
Block Reason	סיבת חסימת הקובץ (לדוגמא; הלבנה או מדיניות).
CDR Summary	הסבר קצר המשקף את ממצאי תהליך ההלבנה (לדוגמא; קובץ לא מאושר ע"י המדיניות, קישורים זוהו בקובץ, אובייקטים פעילים הוסרו, צלח, וכו').

8.2 שחזור קבצים מקוריים

במידה ומשתמש זקוק להודעת דוא"ל טרם ההלבנה והצרופות לה, יש באפשרותך לשחזר את הקבצים המקוריים, ולהפוך אותם לזמינים למשתמש.

בכדי לשחזר קבצים מקוריים:

1. בחלונית **All** בחר בהודעת דוא"ל אחת או יותר ולחץ על 

.
2. כאשר תתבקש לאשר, לחץ 

.

הודעת הדוא"ל המקורית והצרופות המקוריות ישוחררו מהQuarantine וישלחו לתיבת

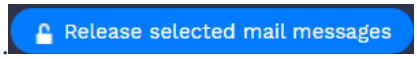
odix ltd © February 2021

הדואר הנכנס של המשתמש (ללא נטרול). באנר אפור יופיע בתחילת ההודעה.

8.3 הסרת קובץ מ- Quarantine

במידה והינך בטוח כי קובץ הצרופה לא מהווה איום לארגונך, באפשרותך לשחרר אותו מQuarantine.

בכדי לשחרר קובץ:

1. בחלונית בהQuarantine בחר הודעת דוא"ל אחת או כמה ולחץ 

.
2. כאשר תתבקש לאשר, לחץ 

.

הודעת הדוא"ל המקורית והצרופות המקוריות ישוחררו מQuarantine וישלחו לתיבת הדואר הנכנס של המשתמש (ללא נטרול). באנר אפור יופיע בתחילת ההודעה.

odix ltd © February 2021