הנגיש באמצעות
המרכז להנגשת מידע של
עמותת נגישות ישראל (ע"ר)

kaspersky BRING ON THE FUTURE

Kaspersky Security for Microsoft Exchange Servers

הגנה מקיפה מפני וקטור ההתקפה מס' 1 בפלטפורמת הדוא"ל המובילה

Kaspersky Security for Microsoft Exchange Server מגן על רשתות IT ארגוניות מאמצעי ההתקפה השכיחים ביותר – העשויים גם לשמש בקמפיינים מזיקים של שיווק, הפצה המונית של תוכנות זדוניות, phishing והתקפות ממוקדות מורכבות במיוחד. Kaspersky Security for Microsoft Exchange Server, שנהנה מאינטגרציית API עם פלטפורמת הדוא"ל הכי פופולרית, מכסה את הטווח הכי רחב של תרחישים שבהם יש חשיבות חיונית להגנה אמינה.

הדגשים

- הגנה רב-שכבתית מפני תוכנות זדוניות ודיוג
- הגנה מאיומים בשעת אפס
- הגנה חכמה בעזרת הענן מפני דואר זבל
- סינון תוכן מתקדם
- חסימת תוכנות כופר
- הגנת BEC ייעודית
- עם תמיכה מבינת האיומים הגלובלית של Kaspersky Security Network
- גישה מבוססת תפקידים לניהול מערכת ולשימוש באינטרנט
- תמיכה ב-Microsoft Active Directory וב-Database Access Group (DAG)
- אפשרות לרישוי במינוי חודשי

מנטרל טווח נרחב של איומים באמצעות סטאק טכנולוגי עם אינטגרציית API

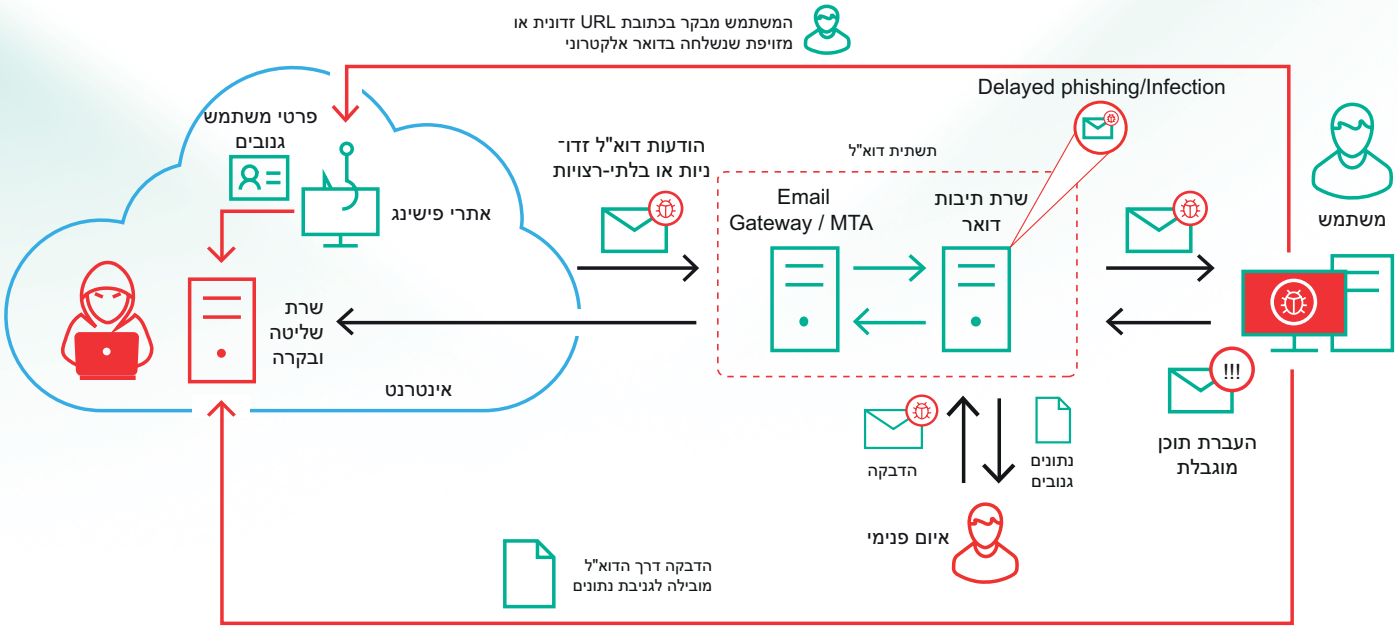
Kaspersky Security for Microsoft Exchange Server נותן הגנה מפני איומים המגיעים דרך הדואר האלקטרוני, הן ברמת השער והן ברמת תיבת הדואר, ובכך מצמצם סיכונים מהתקפות הבנויות על הנדסה חברתית ומניצול לרעה של פגיעויות בנקודות קצה. הוא מאפשר לך לשלוט בהעברות נתונים הכרוכות בסיכון, כדי לצמצם תקריות של שגיאת משתמש, בכלל זה הדבקות, הונאות ודליפת נתונים.

משפר פרודוקטיביות ומצמצם סיכונים, עם הגנה חכמה בעזרת הענן מפני דואר זבל

היכולות של Kaspersky למניעת דואר זבל, הבנויות על machine learning, יכולות לזהות גם דואר זבל מתוחכם ביותר שאינו ידוע, עם אובדן קטן ככל האפשר של תקשורת חשובה עקב תוצאות חיוביות מוטעות. הגנה חכמה בעזרת הענן מפני דואר זבל מצמצמת את הסיכונים הכרוכים בדואר זבל, על-ידי בלימה שלו, כדי לחסוך משאבי מערכת ואנוש.

השלמה למערך ההגנות הכללי של התשתיות

עם סטאק טכנולוגיות הגנה מהחזקים ביותר בתעשייה, שיעורי זיהוי טובים יותר וכמעט אפס תוצאות אמת מוטעות, Kaspersky Security for Microsoft Exchange Server מאפשר אינטגרציה חלקה עם פתרונות אחרים של Kaspersky, ולחלופין, אפשר להשתמש בו בתור רכיב עוצמתי במערך ההגנות הקיים שלך, המורכב מספקים שונים.



מודל האיומים מבוססי הדוא"ל

תכונות

הגנה ובקרה רב-שכבתיות נגד איומים, הבנויות על מדע נתונים

ההגנה והבקרה מהדור הבא של Kaspersky נגד תוכנות זדוניות כוללות כמה שכבות אבטחה פרואקטיביות, הכוללות:

- **הגנה מתוכנות זדוניות:** טכנולוגיות פרואקטיביות לזיהוי, לניתוח ולסינון, הבנויות על machine learning, מזהות וחוסמות איומים של תוכנה זדונית, בכלל זה רוגלות, סוסים טרויאנים פיננסיים, תוכנות כופר, כורי נתונים ומוחקי נתונים.
- **זיהוי איומים חדשים בזמן אמת:** Kaspersky Security Network, הבנויה על מודיעין בעדכון שוטף מעשרות מיליוני משתמשים ועל המחקר שלנו, המוביל בעולם, תומכת בזיהוי בזמן אמת של איומים אפשריים, גם אם הם חדשים לחלוטין, עם כמה שפחות תוצאות אמת מוטעות.
- **Emulative sandboxing:** הקבצים המצורפים מופעלים ומנותחים בסביבת אמולציה בטוחה, כדי להגן גם מפני התוכנות הזדוניות הכי מתוחכמות ומוסווות.
- **זיהוי Script:** מזהה קובצי Script, שמשלבים תוכנה זדונית בקבצים תמימים למראה, המגיעים לנקודות הקצה שלך, וכאלה המשמשים להתקפות Drive-by באינטרנט.
- **סינון לפי מוניטין:** אפשר להיעזר בדירוגי מוניטין של קבצים וכתובות, המגיעים ממסדי הנתונים בענן של Kaspersky Security Network, כדי לבלום קבצים ומשאבי אינטרנט חשודים או בלתי-רצויים, ללא צורך בניתוח מעמיק יותר.
- **הגנה מתקדמת נגד דיוג(phishing):** ניתוח הבנוי על רשת עצבית, עם תמיכה מבדיקה מבוססת-ענן בזמן אמת של כתובת ה-URL והדומיין של השולח, נותן הגנה גם מפני התקפות הדיוג הכי משכנעות בדוא"ל. בכלל זה פגיעה בדוא"ל עסקי, שבה יש ניצול לרעה של האמון של עמיתים עסקיים וחברות, כדי לשוות עוד יותר אמינות לדיוג הממוקד.
- **זיהוי של התחזות מקורות:** תוקפי הסייבר משתמשים במגוון שיטות להתחזות או להסוואה של פרטי מקור הדואר האלקטרוני, כדי לגרום למקבל ההודעה להאמין שהיא מגיעה משולח מהימן. המומחיות של Kaspersky בתחום האיומים מסוגלת להבחין בכל השיטות האלה, בלי להשאיר שום מקום לטעות אנוש.
- **זיהוי של ניצול נקודות תורפה בדואר:** כמה יישומים של לקוחות דואר אלקטרוני (בייחוד אלה שלא זכו לעדכון) עשויים להכיל פגיעויות שמאפשרות לתוקפים להשפיע על אופן ההצגה של פרטי השולח, וכך למעשה להתחזות למקור אחר של דואר אלקטרוני. המנוע למניעת דיוג של Kaspersky מזהה ניסיונות אלה, ומשתמש בהם נגד התוקף, כדי לחסום את הודעות הדיוג שלו בדוא"ל.
- **הגנה מפני פגיעה בדוא"ל עסקי (BEC):** דיוג BEC כולל ניצול לרעה של האמון בין עובד לעמיתים בעבודה (בדרך כלל בדרג גבוה יותר) או של עמית עסקי (ספק, שותף עסקי וכדומה), על-ידי תוקפי סייבר שמתחזים לשולח מהימן, ומבקשים משהו מהנמען. Kaspersky Security for Microsoft Exchange Server מרכז כמה מחוונים שונים, למשל נתוני השולח, דירוגי מוניטין של כתובות URL, ניתוח לשוני של טקסט בדוא"ל ועוד, כדי לזהות ניסיונות מעין אלה.

הגנה חכמה מדואר זבל

כמויות עצומות של הודעות דוא"ל לא-רצויות צורכות משאבים ואת תשומת לבם של העובדים – ועשויות אף להכיל דבר מה מזיק, ולא רק מציק. Kaspersky Security for Microsoft Exchange Server חוקר את כל היבטי התקשורת, לרבות נתוני השירות שלה, פרטי השולח, גודל, קבצים מצורפים, כתובות URL כלולות ועוד. בהתאם לפריט עצמו, ייעשה שימוש במערך של טכנולוגיות חכמות, כדי לזהות גם דואר זבל פולימורפי או בתמונות.

- **אינטגרציה של KSN:** הפתרון יכול לבצע בדיקות מול מסד הנתונים בענן של Kaspersky, כדי לקבל מידע בזמן אמת על סוגי דואר הזבל החדשים ביותר.
- **סינון לפי מוניטין:** למנהל המערכת יש האפשרות להשתמש בסינון לפי מוניטין, שהוא שירות נוסף לסריקה נגד דואר זבל, המגביר את הדיוק של גילוי דואר זבל, ומקטין את הסבירות לתוצאות אמת מוטעות.
- **אינטגרציה של רשימת חסימות:** להגנה נוספת מפני דואר זבל, ההודעות נסרקות באמצעות רשימות DNSBL של כתובות ספאמרים וטכנולוגיית SURBL לזיהוי כתובות URL של ספאמרים בהודעה.
- **תמיכה בריבוי שפות:** היישום מבצע סריקות נגד דואר זבל של הודעות הכתובות בשפות שונות, כולל שפות אסייתיות.

הידעת?

...תרחישים מסוימים של התקפות מבוססות דוא"ל כוללים תקשורת פנים-ארגונית, השתלה של גורמים רדומים, דיוג מושהה ושיטות אחרות שעשויות לעקוף בדיקות חד-פעמיות על-ידי שער דוא"ל מאובטח. פתרון ברמת תיבת הדואר הוא אפשרות נוחה ואפקטיבית למניעה של כל סוגי התרחישים הללו.

מודיעין איומים ללא מתחרים

עם איסוף ועדכון שוטף של נתונים גלובליים על איומים, מחקר מתמיד על-ידי מומחי האבטחה הטובים בעולם ומדעני נתונים ידועים, שפועלים כדי להפוך נתונים לבינה מעשית, על מנת לנטרל איומים גם בשעת האפס. זה היסוד של Kaspersky Security for Microsoft Exchange Server.

שליטה עוצמתית בתעבורת דוא"ל

מי שלא מתכונן, נכשל. Kaspersky Security for Microsoft Exchange Server מציע דרכים רבות-עוצמה לשליטה בתקשורת הדוא"ל שלך, ובכך לצמצם משמעותית את הסיכונים.

סינון תוכן[עודכן]: אפשר לאסור על העברה של קבצים מסוגים הידועים כסוגים שעשויים להיות בעייתיים או בלתי-רלוונטיים, לפי פרמטרים הכוללים שם, גודל, סוג MIME (וידאו, תמונות וכו'), HASH וסיומת/סוג Format Recognizer) משמש לאיתור קבצים עם סיומות כוזבות). לסינון ולמניעה רגילים יותר של דליפות נתונים אפשריות, אפשר ליישם על התוכן קריטריונים מורכבים לחיפוש טקסט.

סיווג הודעות: מנהל מערכת יכול להגדיר כללי עיבוד נפרדים לכל קטגוריה של דואר שלא התבקש, כדי למנוע כל אובדן מידע. למשל, אפשר לחסום הודעות הידועות כדואר זבל; אפשר להפנות דואר חשוד ישירות אל תיקיית הדואר הבלתי-רצוי; ואפשר להעביר הודעות רשמיות, כמו אישורים על העברת הודעה וקריאת הודעה, ישירות לתיבת הדואר הנכנס.

רשימות של שולחים מהימנים/לא מהימנים: כל משתמש יכול ליצור לעצמו רשימות של שולחים מהימנים ולא מהימנים, על סמך הודעות הדוא"ל שלהם, שמות הדומיינים או שם SMTP/כתובת IP של השולח. אפשר גם ליצור רשימת שולחים מהימנים באמצעות כתובת ה-SMTP של הנמען. הודעות משולח שכלול ברשימת השולחים המהימנים לא ייסרקו, ויועברו ישירות אל הנמען. אולם אם הכתובת קיימת ברשימת השולחים הלא מהימנים, ההודעה תתויג בכותרת מיוחדת, ותעובד לפי הכללים שקבע מנהל המערכת.

קטגוריות דואר מוגדרות מראש: תיוג הודעות דוא"ל לפי קטגוריות מאפשר מיון נוח יותר של דוא"ל, ועוזר להתמודד עם סיכוני אבטחה מסוימים.

ניהול ארכיטקטורה, פריסות ויישומים

Kaspersky Security for Microsoft Exchange Server מפחית את הלחץ שעמו מתמודדים מנהלי מערכת בתחום האבטחה, בעזרת מערך נרחב של פונקציות שימושיות.

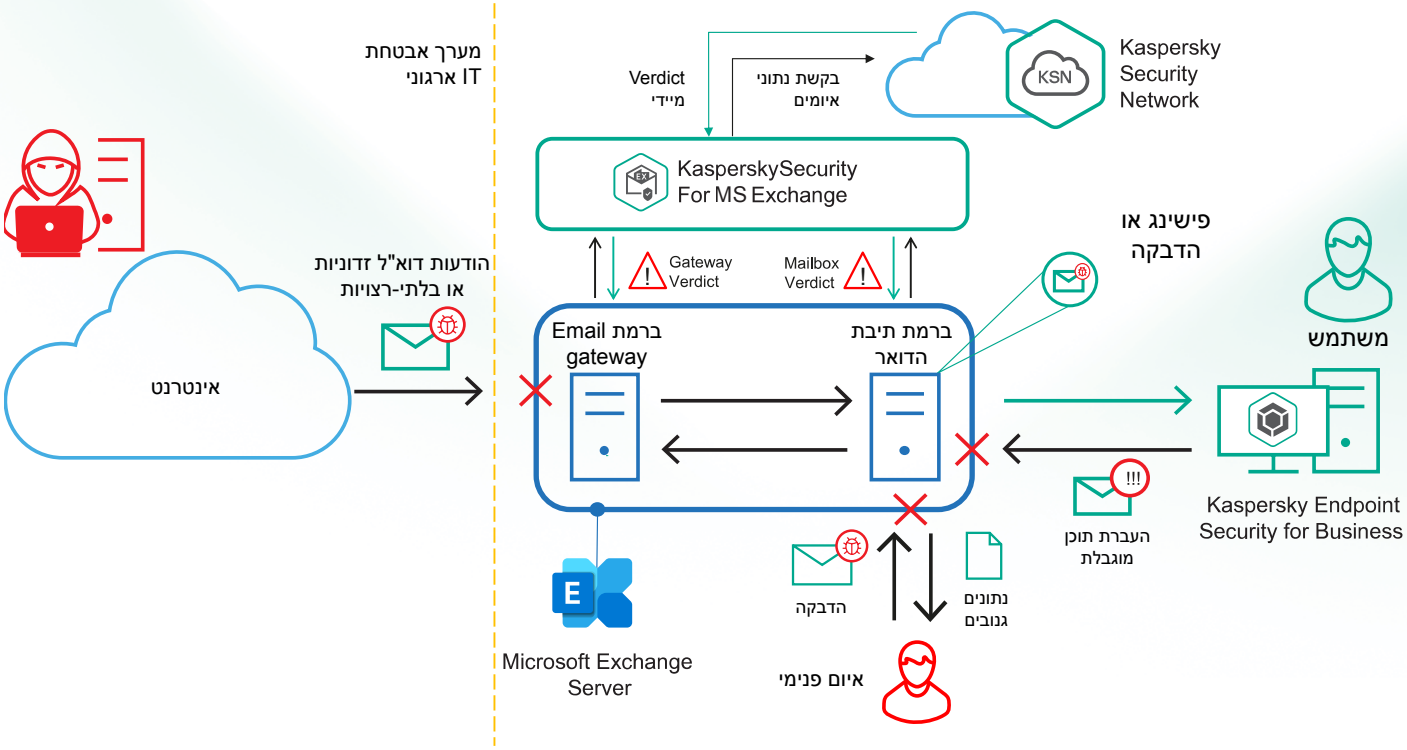
הגנה ברמת השער וברמת תיבת הדואר בפתרון אחד: ל-Kaspersky Security for Microsoft Exchange יש אינטגרציה מלאה ברמת ה-API, כדי לספק הגנת דוא"ל גם ברמת השער וגם ברמת תיבת הדואר. יכולת זו מכסה הרבה יותר תרחישי התקפה בהשוואה לפתרונות שער דוא"ל מאובטח (SEG).

ניהול לפי CLI[חדש]: אפשר להתקין, לעדכן, לשחזר ולהסיר את היישום באמצעות שורת הפקודה, מבלי להשתמש בממשק המשתמש הגרפי.

אינטגרציה עם תשתית הבנויה על פתרונות Microsoft: היישום תומך באינטגרציה עם Microsoft Active Directory, לתהליך נוח יותר של הגדרת התצורה, והוא תואם ל-DAG (קבוצת זמינות של מסד נתונים), עם כל יתרונות העמידות בפני אסונות ש-DAG מספקת.

שליטה מלאה על תקשורת רגישה

למרות מגמת המעבר של תשתיות פרודוקטיביות ארגוניות – בכלל זה דואר אלקטרוני – לעננים ציבוריים, הרבה חברות מעדיפות להשאיר את הנכסים שלהן בסביבה המקומית. בדרך כלל, הסיבה לכך היא החשש מההתמודדות עם נתונים רגישים ועניני ציות. ואם נוסיף את הגבולות המטושטשים של 'האחריות המשותפת' לספק הענן ולדייר, קל להבין למה ההנהלה הבכירה בארגונים נוקטת בגישה זהירה.



כיצד Kaspersky Security for Microsoft Exchange Server מנטרל איומים מבוססי דוא"ל

ניהול אבטחה פשוט יותר

ככל שהכלים שלרשותך נוחים ואפקטיביים יותר, כך מתחזקת האבטחה של החברה שלך. Kaspersky Security for Microsoft Exchange Server מציע יעילות ונוחות, עם שפע של כלים לניהול האבטחה.

בקרת גישה מבוססת תפקידיםעודכן**:** אוסף חדש של תפקידים מאפשר לך לנהל בנפרד גישת משתמשים עבור פרופילים שונים של יישומים. כך מנהל המערכת יכול להגביל מנהלי מערכות במחלקות אחרות כך שיוכלו לגשת רק אל שרתי אבטחה מסוימים, במידת הצורך.

דוחות מפורטים: אפשר לנטר את הפעילות של היישום ואת סטטוס ההגנה באמצעות דוחות ה-HTML המפורטים, או על-ידי צפייה ביומן האירועים של Windows. יש לך שליטה מלאה בתדירות יצירת הדוחות ובמידע שייכלל בהם. את כל הדוחות אפשר לשמור בכונן הקשיח או לשלוח בדוא"ל.

ניהול וניטור מרכזיים: מסוף יחיד לניהול המערכת, עם יכולות מרכזיות לדיווח ולגיבוי, עוזר לשלוט בכל שרתי Exchange שלך. ל-Kaspersky Security for Microsoft Exchange יש אינטגרציה עם Kaspersky Security Center, ולכן באפשרותך לנטר את סטטוס ההגנה, אירועים חשובים וסטטיסטיקה מאוחדת של הארגון כולו, ממסוף יחיד.

סריקה ברקע לפי דרישה ולפי לוח זמנים: כל התיקיות וההודעות השמורות בשרת נסרקות ברקע, כדי להבטיח עיבוד של כל האובייקטים באמצעות הנתונים העדכניים ביותר של מודיעין איומים. אפשר להגדיר לוח זמנים גמיש לפעולה ברקע או לבצע סריקה לפי דרישה, לכל תיבת דואר ספציפית, בכל עת. והכול עם כמה שפחות השפעה על העומס בשרתים ועל הפרודוקטיביות העסקית.

תצורה בהתאמה אישית: אפשר לקבוע את תצורת היישום לפי מדיניות אבטחת ה-IT ויכולות החומרה של החברה. למשל, אפשר להחריג מהסריקה קבצים מסוגים מסוימים ולהגדיר את עוצמת הסינון של דואר זבל. אפשר גם להגדיר תרחישי עיבוד נגד וירוסים ונגד דואר זבל, עבור קטגוריות שונות של הודעות, וליצור רשימות של שולחים מהימנים ובלתי-מהימנים, לפי הכתובות של השולחים או המקבלים.

גמישות בעדכוני האבטחה: עדכונים למסדי הנתונים ולמודלים של למידת מכונה זמינים לפי דרישה, ואפשר גם להשלים אותם באופן אוטומטי לפי לוח זמנים. אפשר להוריד עדכונים ישירות מאתר האינטרנט של Kaspersky או משרת מקומי.

ניהול נוח: ממשק ניהול המערכת מבוסס על מסוף הניהול הפופולרי של Microsoft, ואפשר לנהל את המערכת מרחוק.

מערכת רישום והתראות: האירועים שקשורים לפעילות היישום מתועדים ביומן האירועים של Windows, מטעם המקור של KSE. האירועים מופיעים ביומני היישום וביומני השירות, במקטע Kaspersky Security for Exchange Servers. מנהל המערכת יכול גם להירשם לקבלת התראות בדוא"ל על כל אירוע קריטי בפעילות היישום.

רישוי גמיש: אפשר לבחור מרישוי חודשי גמיש, עם אפשרויות מדרגיות לתשלום לפי שימוש או רישוי שנתי קבוע. עבור ספקי שירותים מנוהלים, קל לנהל מרחוק את האבטחה של כמה לקוחות, באמצעות המסוף התומך בריבוי דיירים.

כיצד לרכוש:
אפשר להפעיל את Kaspersky Security for Microsoft Eaxchange Server במוצרים ובפתרונות הבאים:

- Kaspersky Security for Mail Server
- Kaspersky Total Security for Business

דרישות חומרה ותוכנה

דרישות מינימום מבחינת חומרה ותוכנה

כדי שהיישום יפעל כראוי, על המחשב לעמוד בדרישות המינימום שלהלן:

1. התקנה של Security Server עם מערך המודולים המלא:

דרישות חומרה:
- מעבד – לפי דרישות החומרה של שרת Microsoft Exchange המותן;
- לפחות 2 GB שטח RAM פנוי;
- 6 GB שטח פנוי בדיסק. ייתכן שיהיה צורך בשטח נוסף בדיסק, בהתאם להגדרות היישום ולמצב ההפעלה.

מערכת הפעלה:
- Microsoft Windows Server 2019 Standard או Datacenter (חוויית שולחן העבודה);
- Microsoft Windows Server 2019 Core;
- Microsoft Windows Server 2016 Standard או Datacenter;
- Microsoft Windows Server 2012 R2 Standard או Datacenter.

שרת דואר:
- פריסה של Microsoft Exchange Server 2019 באחד לפחות מהתפקידים הבאים: Mailbox או Edge Transport;
- פריסה של Microsoft Exchange Server 2016 באחד לפחות מהתפקידים הבאים: Mailbox או Edge Transport;
- פריסה של Microsoft Exchange Server 2013 SP1 בתפקיד אחד לפחות מהבאים: Mailbox, Hub Transport או Client Access Server (CAS).

מערכת לניהול מסד נתונים:
- Microsoft SQL Server 2019 Express, Standard או Enterprise;
- Microsoft SQL Server 2017 Express, Standard או Enterprise;
- Microsoft SQL Server 2016 Express, Standard או Enterprise;
- Microsoft SQL Server 2014 Express, Standard או Enterprise;
- Microsoft SQL Server 2012 Express, Standard או Enterprise.

תוכנה נוספת:
- Microsoft .NET Framework 4.5.

2. התקנה של מסוף הניהול בלבד:

דרישות חומרה:
- מעבד Intel Pentium 400 MHz או מהיר יותר (מומלץ 1000 MHz);
- 256 MB RAM פנוי;
- 500 MB שטח בדיסק עבור קובצי היישום.

מערכת הפעלה:
- Microsoft Windows Server 2019 Standard או Datacenter (חוויית שולחן העבודה);
- Microsoft Windows Server 2019 Core;
- Microsoft Windows Server 2016 Standard או Datacenter;
- Microsoft Windows Server 2012 R2 Standard או Datacenter;
- Microsoft Windows Server 2012 Standard או Datacenter;
- Microsoft Windows 10;
- Microsoft Windows 8.1;
- Microsoft Windows 8;
- Microsoft Windows 7 SP1 Professional, Ultimate או Enterprise.

תוכנה נוספת:
- Microsoft Management Console 3.0;
- Microsoft .NET Framework 4.5.

3. התקנת התוסף לניהול:
- Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1;
- Kaspersky Security Center 10 Service Pack 2 Patch a;
- Kaspersky Security Center 10 Service Pack 3.

4. ניטור הפעילות ביישום באמצעות System Center – Operations Manager:
- System Center 2012 Operations Manager;
- System Center 2012 R2 Operations Manager.
- תוכנה נוספת:
- Windows PowerShell 3.0 ומעלה.

חדשות על איומי סייבר: www.securelist.com
חדשות אבטחת IT: business.kaspersky.com
אבטחת IT למגזר ה-SMB: kaspersky.com/business
אבטחת IT למגזר תאגידי: kaspersky.com/enterprise

www.kaspersky.com

2021 AO Kaspersky Lab
הסימנים המסחריים הרשומים וסימני השירות הם קניינם של בעליהם הרלוונטיים.

יש לנו יכולות מוכחות. אנחנו פועלים בצורה עצמאית. אנחנו פועלים בשקיפות. אנחנו מחויבים לבנייה של עולם בטוח יותר, שבו הטכנולוגיה תורמת לשיפור חיינו. מסיבה זו אנו דואגים לאבטח אותו, כדי שכל אחד, בכל מקום יוכל ליהנות מכל היתרונות שהוא טומן בחובו. אבטחת סייבר המפתח שלכם לעתיד בטוח יותר.

למידע נוסף kaspersky.com/transparency

Proven.
Transparent.
Independent.