

## אבטחת מידע:

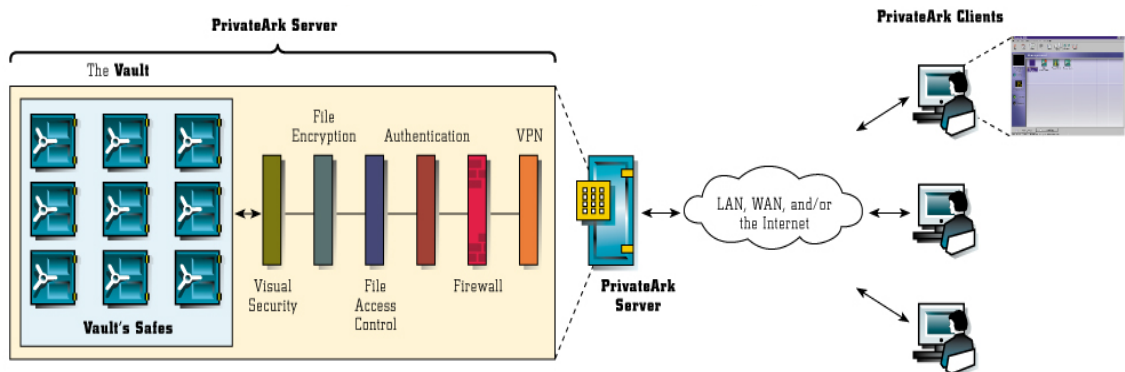
### העיקרון המהפכני בבסיסו של Cyber-Ark® Vault

העיקרון המהפכני העומד בבסיס המוצר הינו בידוד המידע הרגיש. עקרון זה הינו מהפכני בעולם המידע הווירטואלי אך מוכר ומיושם בעולם הפיסי. בעולם האמיתי בונים מקלטים ולא מנסים להגן על כל הבניין, בעולם האמיתי מאחסנים דברי ערך בכספות, ולא מנסים להפוך את הבית למבצר.

חברת Cyber-Ark אימצה את רעיון הבידוד מהעולם הפיסי, ויישמה אותו בעולם הווירטואלי. יישום רעיון הבידוד בשילוב עם טכנולוגיה ייחודיות מתקדמת, עליה רשמה החברה פטנט בינלאומי, מאפשר ל-Cyber-Ark לספק את ההגנה הגבוהה ביותר הקיימת למידע ולאפשר שיתוף מידע באופן הבטוח ביותר.

### שכבות האבטחה של חדר הכספות של Cyber-Ark®

לאחר התקנת חדר הכספות, השרת מצויד בשכבות האבטחה הבאות:



**VPN** – כלל התקשורות בין השרת של Cyber-Ark לבין ה-Client מוגנות בעזרת VPN

(בידוד רשתי וירטואלי) ללא כל קשר למיקום של ה-Client.

**Firewall** – על חדר הכספות של Cyber-Ark מותקן Firewall ייעודי, שתפקידו לחסום כל נסיון

תקשורת שאינו מתבצע באמצעות הפרוטוקול של Cyber-Ark. השילוב בין מחשב ייעודי עליו מותקנת אך ורק תוכנת חדר הכספות, ו-Firewall החוסם כל גישה בלתי מורשית למחשב, יוצר סביבה סטרילית לחלוטין שבה לשרת Cyber-Ark יש שליטה מלאה על המידע. גם רכיבי מערכת ההפעלה אינם נגישים מאחורי ה-Firewall.

**הזדהות** – חובה להזדהות לחדר הכספות על מנת לעבוד עימו.

- **אמצעי הזדהות :** לחדר הכספות ניתן להזדהות במגוון רחב של אמצעי הזדהות. כברירת מחדל, ההזדהות למערכת מבוססת על סימא .
- **פרוטוקול –** פרוטוקול ההזדהות של Cyber-Ark הוא מהחזקים כיום. בשיטה ההזדהות הסוד המשותף (הסימא) לא עובר ברשת, אפילו לא באופן מוצפן.
- **הרשאות גישה למידע –** יחידות המידע הבסיסיות של חדר הכספות הן הכספות. כל כספת נגישה אך ורק לקבוצה מוגדרת של משתמשים השותפים בכספת. משתמש שאין לו הרשאת גישה לכספת, כלל לא ידע על קיומה. עבור כל שותף בכספת, ניתן להגדיר אילו פעולות מותרות לביצוע (קריאה, עדכון, מחיקה וכו'). בכל שלב, ניתן לראות מי ביצע פעולות עם המידע הכספת.
- **הצפנות –** כל המידע השמור בחדר הכספות מוצפן. לכן, גם מי שיגיש פיזית לשרת לא יוכל לקרוא את המידע הטמון בכספות. חשוב לציין שכל הגיבויים שנעשים לשרת מוצפנים.

### **שכבות אבטחת מידע חדשניות, ייחודיות למוצר :**

- **Visual Security – Cyber-Ark Vault** מאפשר לכל משתמש לראות את הפעילות שבוצעה על המידע שלו. כל גישה, שינוי או הוספה של קובץ חדש מוצגת מיד למשתמש. המשתמש יכול בכל שלב לראות מי ניגש לכספות ולקבצים שלו, מתי ואיזו פעולות ביצע.
- **Manual Security** - ניתן להגביר את רמת האבטחה על כספות רגישות במיוחד ע"י הוספת הצורך באישור "ידני" של שותפים נוספים, על מנת לאחזר מידע מתוך הכספת.
- **Versioning** – כל עדכון של קובץ, גורם להיווצרות גרסה חדשה שלו. באופן זה, לא ניתן לבצע מניפולציות על המידע, ללא השארת עקבות.
- **Geographical Security – Cyber-Ark Vault** מכיר את אזורי הרשת השונים של הארגון מהם מתאפשרת גישה לחדר הכספות, ויכול להגביל את הגישה של משתמשים לכספות מאזורי רשת ספציפיים.
- **Code Isolation – Cyber-Ark Vault** הוא הקוד היחיד שרץ על שרת חדר הכספות, ועל כן יש לו שליטה מוחלטת על המידע השמור בחדר הכספות. בשום מקרה Cyber-Ark Vault לא יפעיל קוד השמור בתוכו או יפעיל אפליקציה כלשהי. באופן זה, מידע השמור בחדר הכספות מוגן לחלוטין בפני פגיעת וירוסים.
- **Virus Free Safe –** באם אופציה זו מופעלת, Cyber-Ark Vault לא יאפשר שמירת קוד כלשהו - שעשוי להיות וירוס או סוס טרויאני - בכספת מסוג זה.

### מנגנון הזדהות:

במעמד ההצטרפות לערוץ תד"מ הונפקה לכם סיסמת אינטרנט. הקשת מספר ת"ז וסיסמה בעת הכניסה למערכת הם אמצעי הזיהוי המבחינים ביניכם לבין לקוחות אחרים. הסיסמה שאותה קבלתם בסניף במעמד ההצטרפות הינה זמנית וכבר בכניסה הראשונה תדרשו להחליפה. במידה שלא בוצע שימוש בסיסמה שקיבלתם בסניף במשך 30 יום, מיום ההצטרפות לשירות, הסיסמה תבוטל אוטומטית. כמו כן, סיסמה שלא בוצע בה שימוש בחלוף חצי שנה מיום החלפתה, תבוטל.

חשוב לציין כי סיסמתכם היא אישית ואינה ניתנת להעברה. יש להימנע מכתובת הסיסמה ושמירתה במקום החשוף לגורמים זרים, אין למסור את הסיסמה לאיש גם אם הוא מזדהה כעובד בנק דיסקונט. במקרה של חשד או במידה שתתבקשו למסור את סיסמתכם בטלפון ע"י אדם המציג עצמו כנציג הבנק, סרבו ודווחו על כך מיידית לסניפכם או ל"תמיכת יחידת תל"מ" בטלפון מספר: 03-5153145.

### הנחיות להחלפת סיסמא:

את הסיסמה תוכלו להחליף בכל עת. אנא הקפידו, כי אורך הסיסמה יהיה 8 תווים לפחות. הסיסמה תהיה מורכבת מספרות ומאותיות. הסיסמה לא תכיל תווים חוזרים או עוקבים, הימנעו מסיסמאות קלות לניחוש. המערכת תדרוש מכם להחליף את סיסמתכם לפחות כל 180 יום. עם זאת, מומלץ שתחליפו את הסיסמה ביוזמתכם לפחות כל 60 יום, וכמובן מיד כאשר מתעורר בכם חשד שנחשפה.

### מנגנון בקרת גישה:

בכדי להגן על חשבונכם מפני כניסה בלתי מורשית, מערכת "תד"מ" תחסום את החשבון לאחר מספר ניסיונות כניסה כושלים. במידה שחשבונכם נחסם, פנו ל"תמיכת יחידת תל"מ" בטלפון מספר: 03-5153145.

מנגנון אבטחה נוסף, מנתק את השירות לאחר מספר דקות של חוסר פעילות במערכת. אמצעי זה נועד למנוע שימוש בלתי מורשה בחשבון במידה שעזבתם את המחשב מבלי לצאת מהמערכת או במידה שיצאתם מהמערכת באופן בלתי מסודר. מומלץ להקפיד לצאת מהמערכת באופן מסודר ע"י יציאה מהיישום.

### הצפנה ואישור:

לשם הגנה על הנתונים העוברים בתקשורת, כל תעבורת הערוץ מוצפנת בהצפנת RSA של 1024 ביט.

**אבטחת השרתים:**

כל השרתים, מסדי הנתונים ורכיבי התקשורת במערכת "תד"מ" מאובטחים ומוגנים ע"י מערכות אבטחת המידע מהמתקדמות בעולם. השרתים מוגנים על ידי תוכנות Firewall, מערכות הגנה תשתיתיות, אפליקטיביות ופיסיות. כל השרתים מנוטרים באופן רציף לשם איתור ניסיונות חדירה וחסימתם במידת הצורך. רמת האבטחה בשרתים מעודכנת באופן שוטף ונבדקת על ידי מיטב המומחים בארץ בכדי להגן על פרטיותכם באופן הטוב ביותר