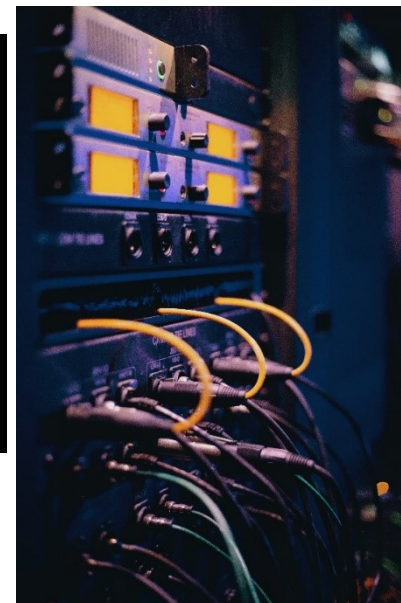


# מושגי ייסוד בסייבר – חלק ד



Yosi Shavit MBA, CISO, CISM, CDPSE - Information Security & Cyber Expert

Cellular: 058-6662242

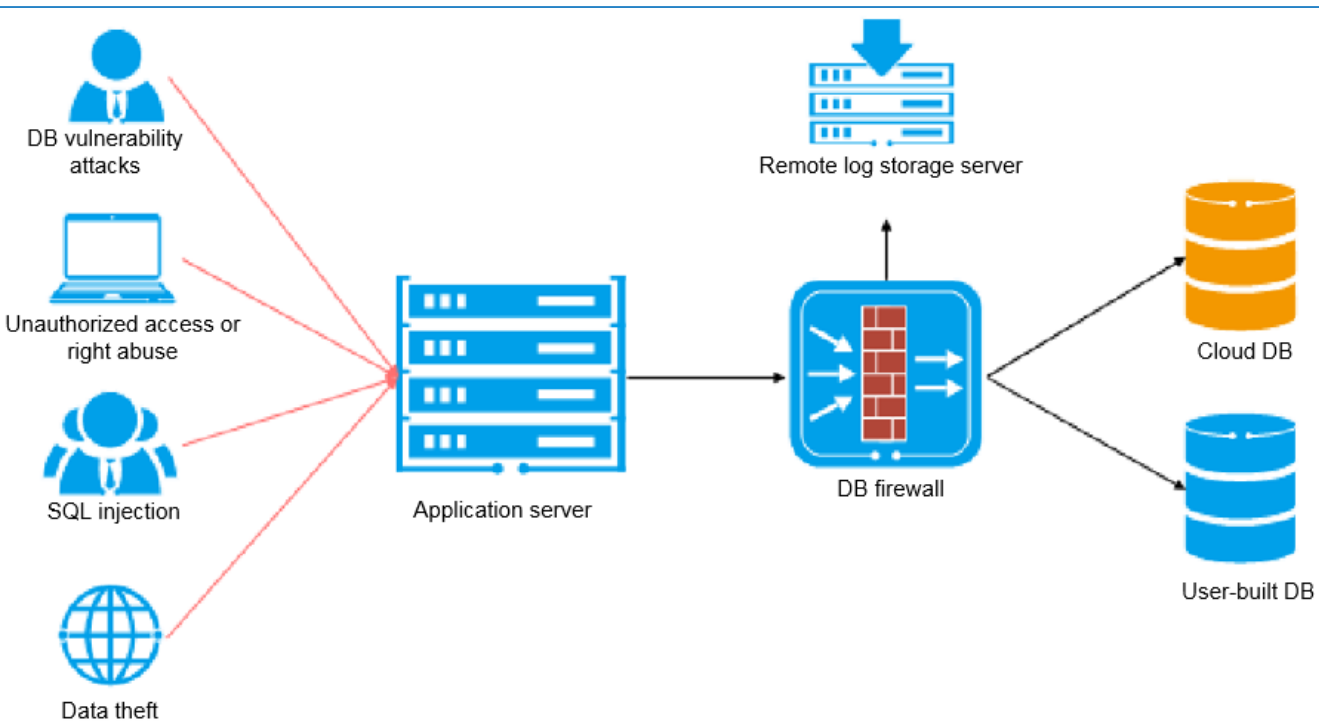
Mail: [yosish@gmail.com](mailto:yosish@gmail.com) , [yosish@sviva.gov.il](mailto:yosish@sviva.gov.il)

# DAF - הגנה על בסיס הנתונים

DAF = DATABASE FIREWALL

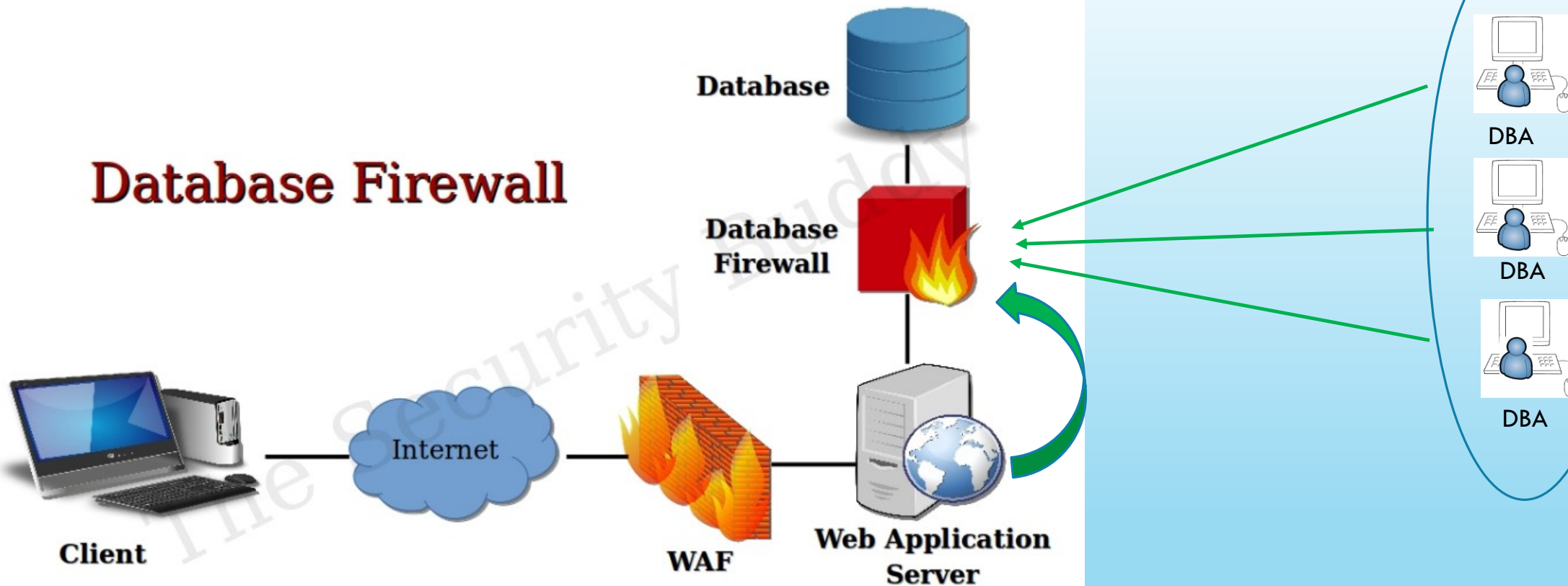
## האתגרים:

- ✓ מניעת חיבור ישיר של משתמשים לגיטימיים בארגון אל בסיס הנתונים (למשל ה-DBA)
- ✓ שימוש נרחב של אנשי הארגון ב-TOAD (לניהול בסיסי נתונים של SQL ו-ORACLE) מתחנות עבודה מקומיות
- ✓ ניהול מרכזי ומאובטח
- ✓ מניעת התקפות על בסיס הנתונים: גניבת מידע, שינוי מידע





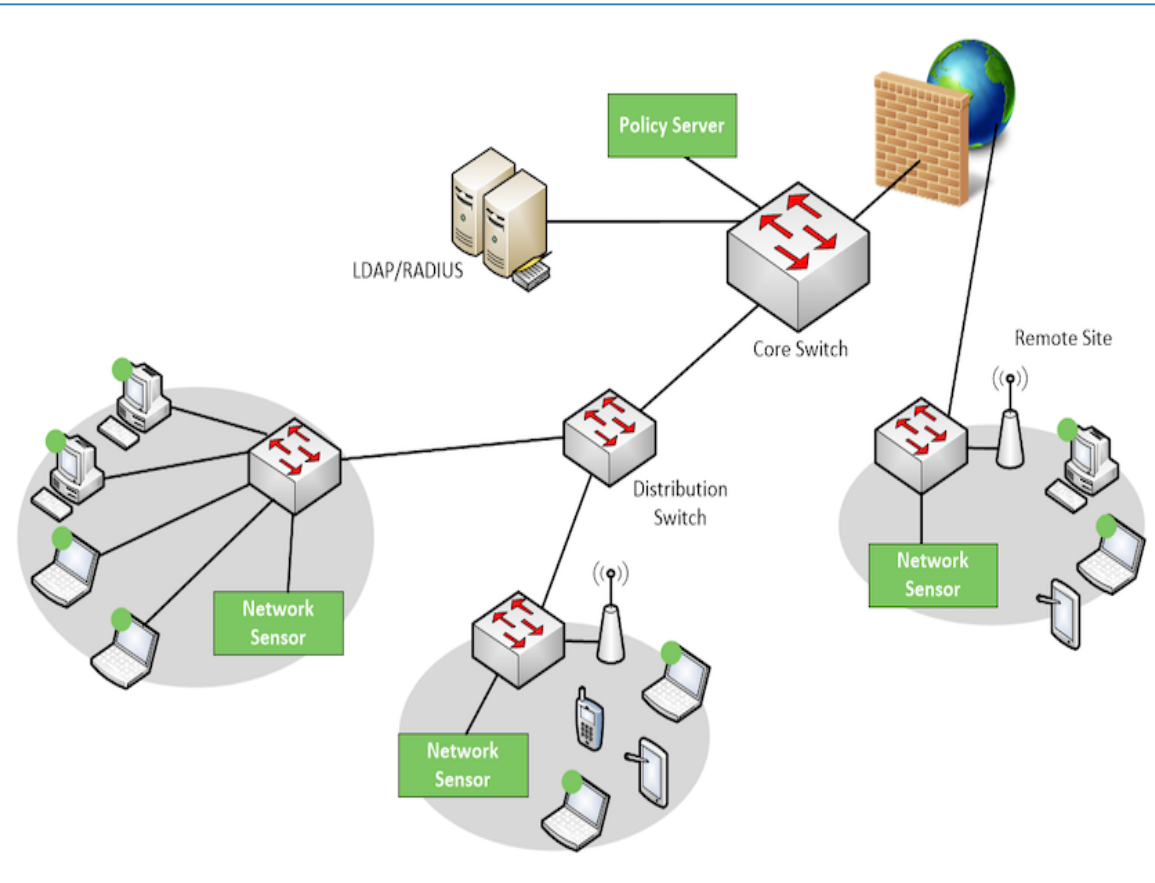
## Database Firewall



source: <https://www.thesecuritybuddy.com/database-security/what-is-database-firewall/>

# NAC - הגנה על הכנסת רכיבים זרים לרשת

**NAC = NETWORK ACCESS CONTROL**



האתגר: מניעת חיבור רכיבים זרים לרשת הארגון

✓ מחשב לא מורשה

מניעת גישה – זיהוי על פי MAC ADDRESS או מזהה חד חד ערכי של הארגון. גם משתמש חוקי של הארגון לא יוכל להכנס.

✓ משתמש לא מורשה

מניעת גישה גם אם המחשב המתחבר מזהה ושייך לארגון

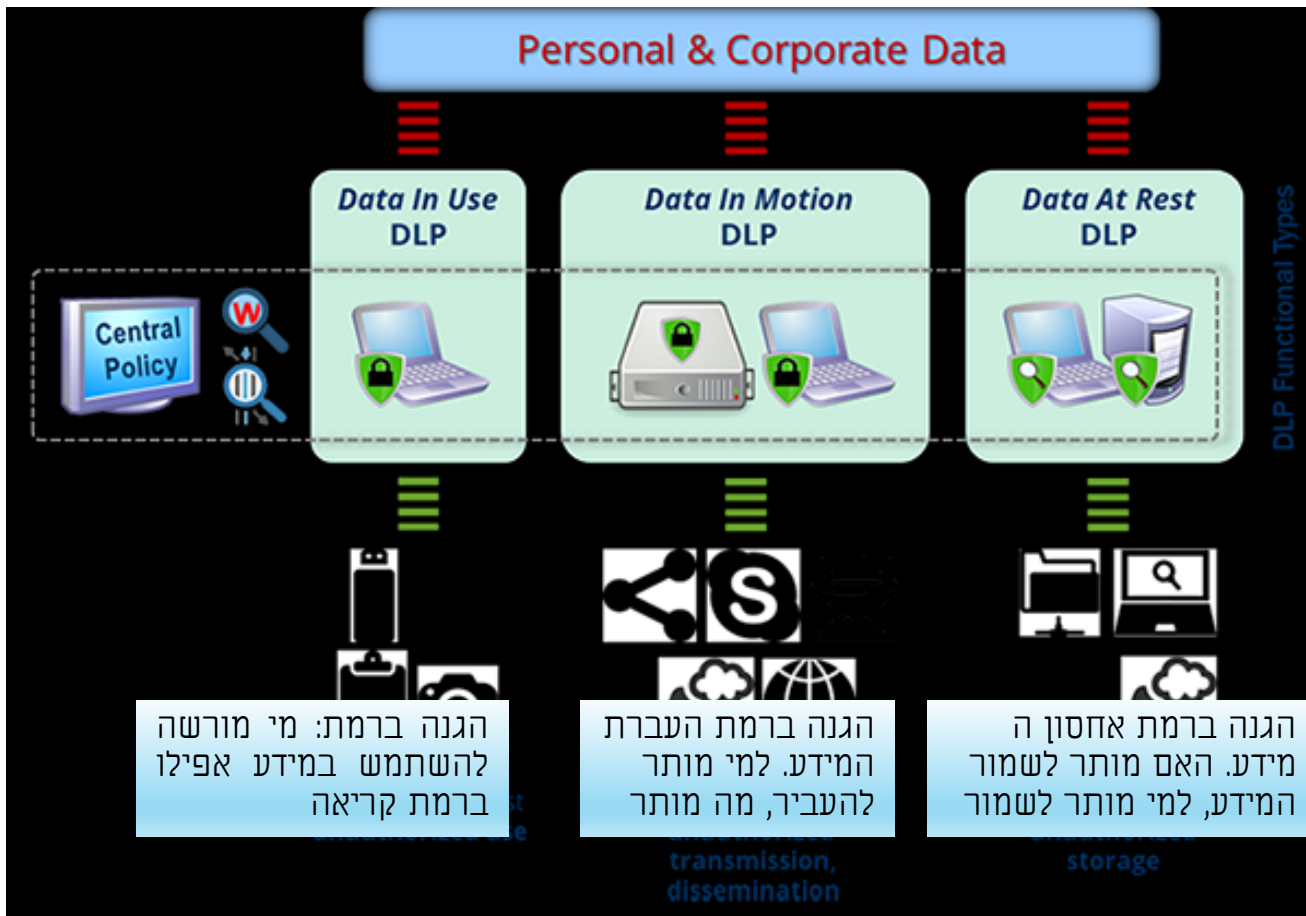
✓ מחשב מורשה ולא מוגן

הכנסה לבידוד, אפשרות ל"טפל" בו וכשהוא נקי לאפשר לו גישה לרשת, אפשר לתת לו עבודה מצומצמת באתר הבידוד

**יש בקרה מפצה?**

# DLP - הגנה על זליגת מידע מהרשת

DLP = DATA LOSS PREVENTION



DLP = DATA LOSS PROTECTION

DLP = DATA LEAK PREVENTION

אתגרי הטמעה - ארגון צריך לדעת לקטלג את המידע

## דוגמאות:

- למי מותר לראות מה?
- איזה מידע אי אפשר לשמור היכן שרוצים ?
- איזה מידע אי אפשר להדפיס?
- איזה מידע לא ניתן לשלוח במייל ?
- לאיזה מידע לא ניתן לבצע COPY ?

איך ניתן לעקוף את ההגנה הזו?

# הלבנת קבצים - CDR

CDR = **C**ontent **D**isarm and **R**econstruction

מערכת הלבנת הקבצים בוחנת את סוגי הקבצים המועברים בעסק מסויים ועוקבת אחריהם:



- קבצים בעל סיומת חשודה
- חסימת קבצים המכילים מרכיבים אסורים כגון: Macro, Virus
- קבצים בעלי מבנה לא נכון לפי סטנדרטים.

דרכים ליישום הלבנת קבצים בארגון

- ✓ הלבנה ברמת קיוסק
- ✓ הלבנה ברמת סוכן
- ✓ ICAP SERVER

Source: <https://odi-x.com/hebrew/>

# הצורך בהלבנה



כדי למנוע הכנסת וירוסים דרך יציאת ה-USB של המחשב ישנן מספר אפשרויות העיקריות שבהן:

אפשרות א' – חסימת יציאות USB ושאר התקנים כך שלא ניתן להכניס כלל קבצים למחשב

אפשרות ב' – שימוש בהתקנים של הארגון שמזוהים ע"י המחשב

אפשרות ג' – לאפשר הכנסת קבצים דרך המדיות השונות אך לבדוק מה מכניסים:  
✓ ברמה גבוהה יותר מאנטי-וירוס

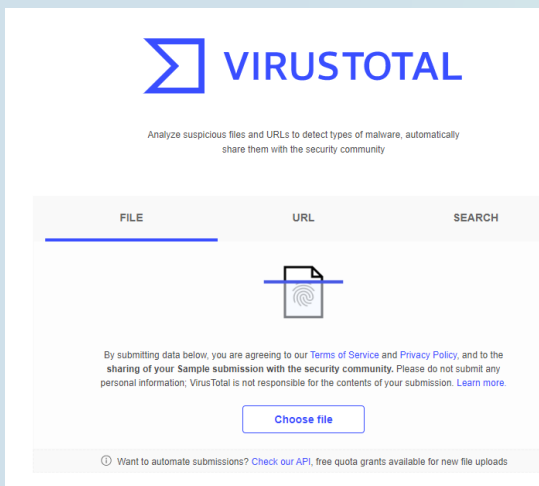
✓ מטפל גם בהתקנים נוספים (CDROM , דיסקטים)

# טכנולוגיית הלבנת קבצים מורכבת משלושה קווי הגנה

**קו הגנה ראשון** - סריקה ראשונית של מספר מנועי אנטי-וירוס\* לחסימת קבצים הנושאים נזקות ידועות

**קו הגנה שני** - אימות בין סוג הקובץ, מבנה הקובץ, הסיומת שלו ופרמטרים נוספים על מנת לוודא כי הקובץ חוקי

**קו הגנה שלישי** - הפעלת אלגוריתם ייחודי לכל סוג קובץ המנטרל נזקות.





# עמדת Kiosk

עמדת הלבנה פיסיית, מוקשחת ומוגנת בפני התקפת סייבר (יכולה לשמש כקו ראשון)

✓ מומלץ שתהיה ללא דיסק קשיח

✓ מיועדת לסריקת מדיות זיכרון נתיקות כגון:  
Disk on Key (DOK), CD, DVD, Smart Phone, Camera

✓ מערכת ההפעלה (רצוי שתבוסס לינוקס) והתוכנה של העמדה  
עולים מכרטיס מוקשח

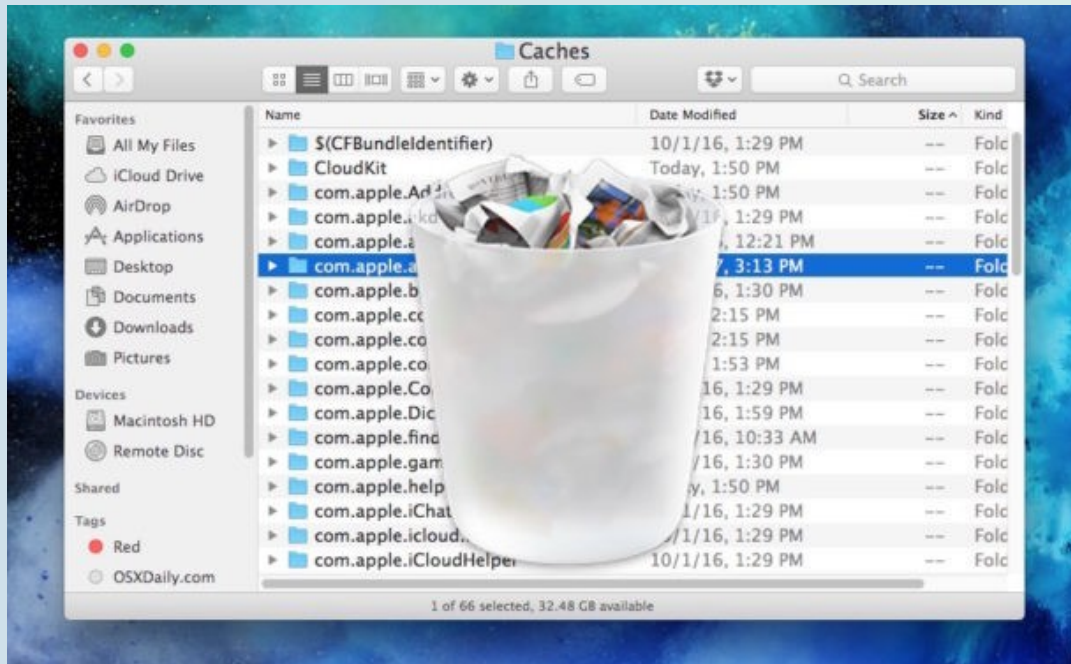
✓ תוכנת ההפעלה מוצפנת



Source [https://www.sasa-software.com/wp-content/uploads/2019/02/GateScanner\\_Kiosk.pdf](https://www.sasa-software.com/wp-content/uploads/2019/02/GateScanner_Kiosk.pdf)

# הלבנה ברמת סוכן

- התקנת סוכן על כל המחשבים בארגון / המחשבים המורשים להכניס DOK
- מאפשר סריקה של תהליכים רצים בכל מחשב ומחשב תוך כדי עבודה רגילה של המחשב
- יכול לבצע סריקה מלאה או במקומות מסויימים שקבענו מראש (תיקיות, קבצים, כונני רשת)
- ניהול הסוכן מעמדת מרכזית או מהענן

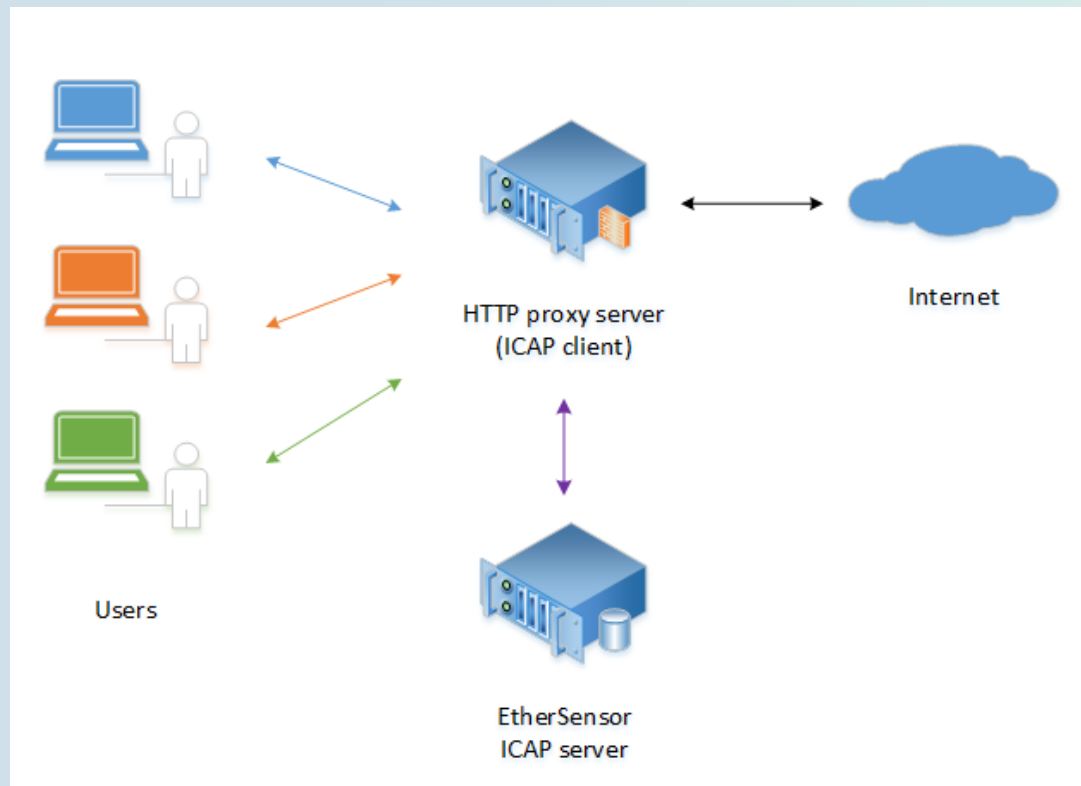


Source: <https://osxdaily.com/2017/04/18/clean-caches-temporary-files-mac/>

# עמדת ICAP SERVER

קבצים המועלים לפורטל החברה ע"י צרכנים, ספקים או כל משתמש אחר

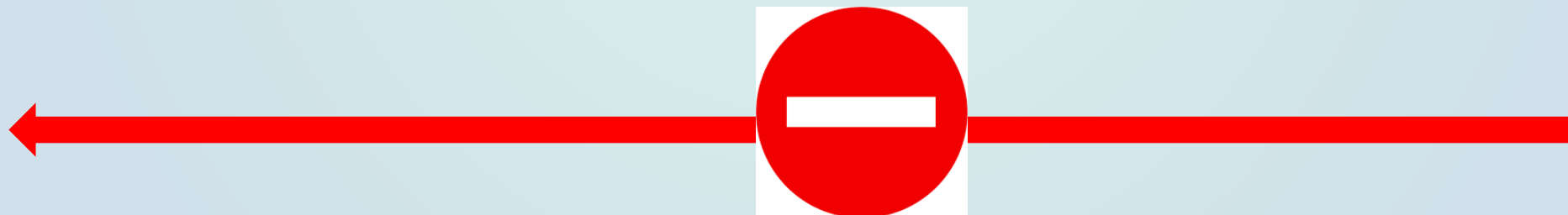
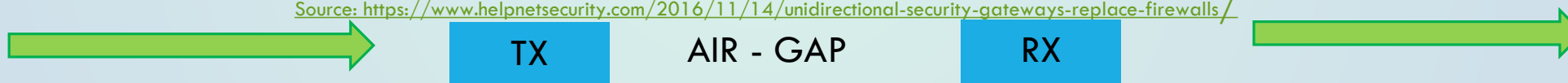
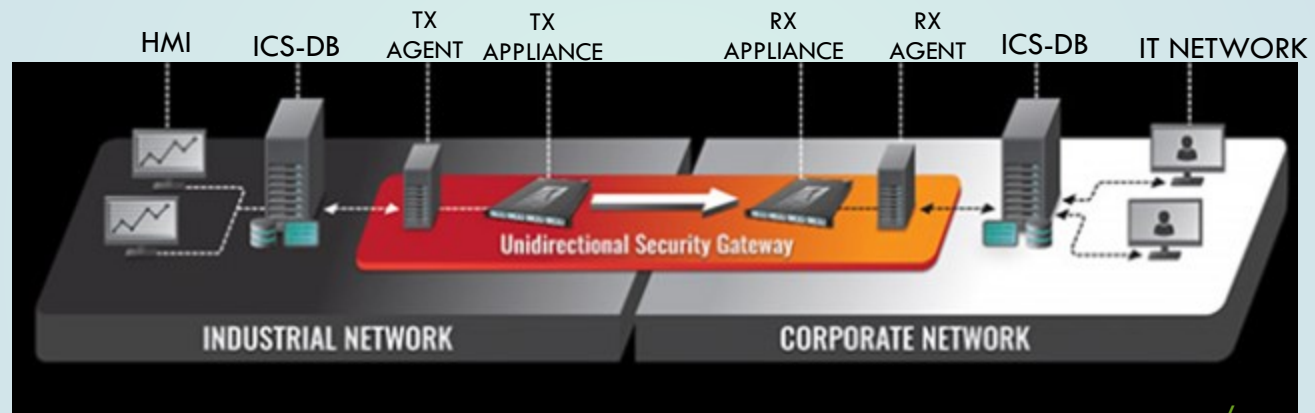
שלבים:



- הלקוח מעלה קובץ אל הפורטל
- הקובץ מועבר דרך ICAP CLIENT אל ICAP SERVER
- הקובץ נבדק ב-ICAP SERVER
- במידה ותקין – הקובץ נטען בהצלחה לשרתי החברה
- במידה ולא תקין – נשלחת הודעה ללקוח כי הקובץ נגוע

# הפרדת רשתות פיסית

## דיודה חד כוונית – UNIDIRECTIONAL SECURITY GATEWAY



# הגנה על הבקר



ערכי סף בקוד הבקר (טמפ, לחץ, רמת PH)

יישום משתמש וסיסמא ייעודיים בבקר

בידוד הבקר מרשת ה-IT

גישה ישירה לבקר עם LAPTOP ייעודי ומוקשח

החלת הגנות מובנות בבקר

[https://download.schneider-electric.com/files?p\\_enDocType=Technical+leaflet&p\\_File\\_Name=STN+-+How+can+I+reduce+vulnerability+to+cyberattacks+v3+Feb2019.pdf&p\\_Doc\\_Ref=STN+v2](https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=STN+-+How+can+I+reduce+vulnerability+to+cyberattacks+v3+Feb2019.pdf&p_Doc_Ref=STN+v2)



מצב הבקר -

○ RUN - מצב ריצה (המצב הרצוי!)

○ Program - מצב תכנות

○ Remote - ניתן מרחוק לשנות את המצב

✓ התקנת עדכוני SOFTWARE

✓ התקנת עדכוני FIRMWARE