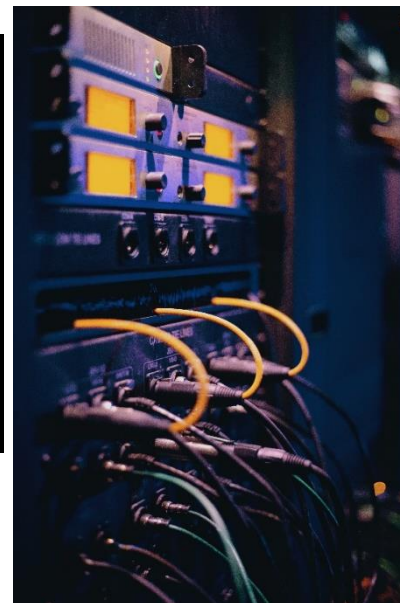


# מושגי ייסוד בהגנת סייבר – חלק ב



Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

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

# נושאי הלימוד



התקפות ZERO DAY ודרכי התגוננות

התקפת DOS , DDOS

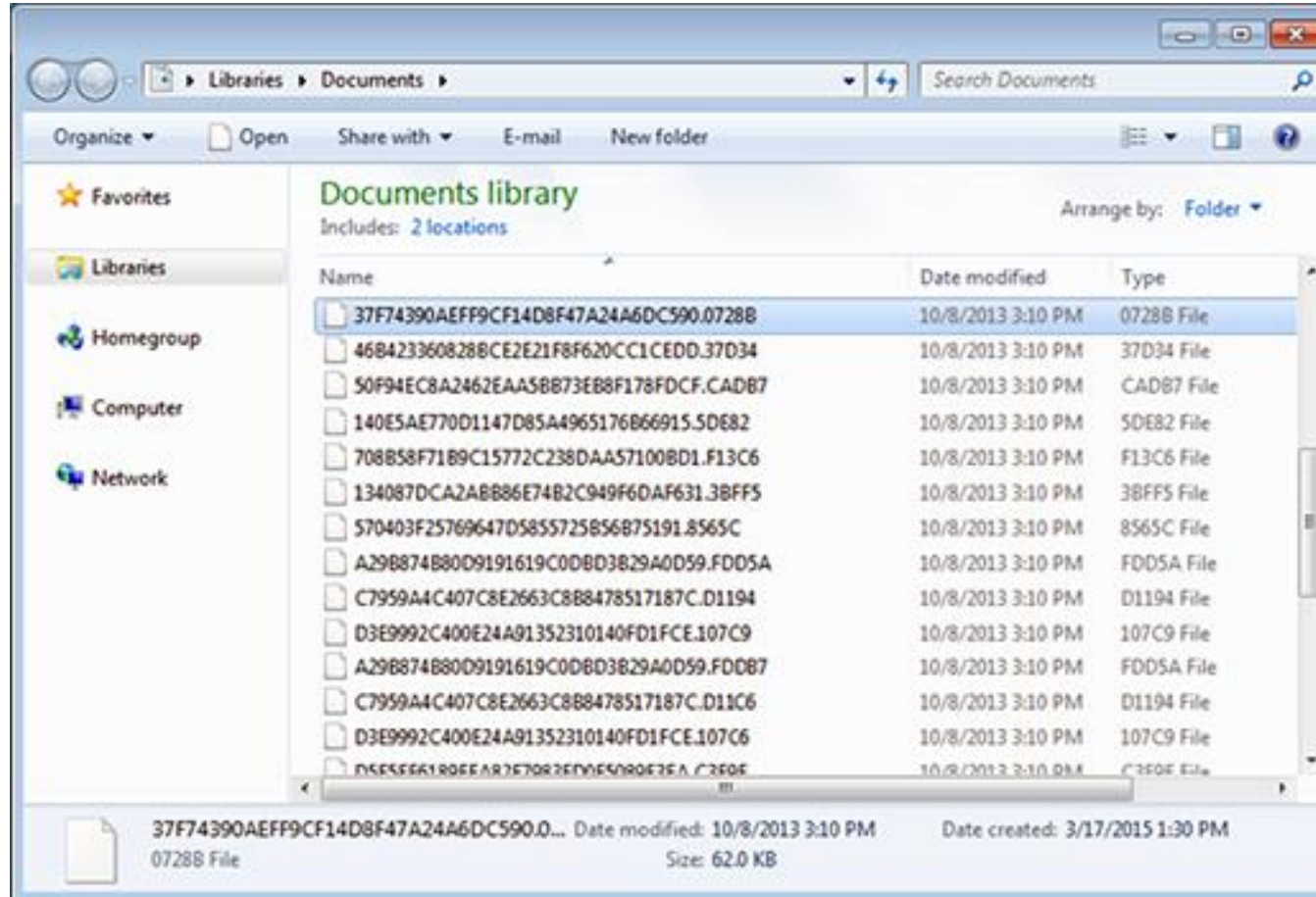
הגנה על האפליקציה – WAF

הגמה על בסיס הנתונים – DAF

הגנה על הכנסת רכיבים זרים לרשת – NAC

הגנה על זליגת מידע – DLP

לאחר הצפנת הקבצים ע"י וירוס כופרה הם נראים כך:



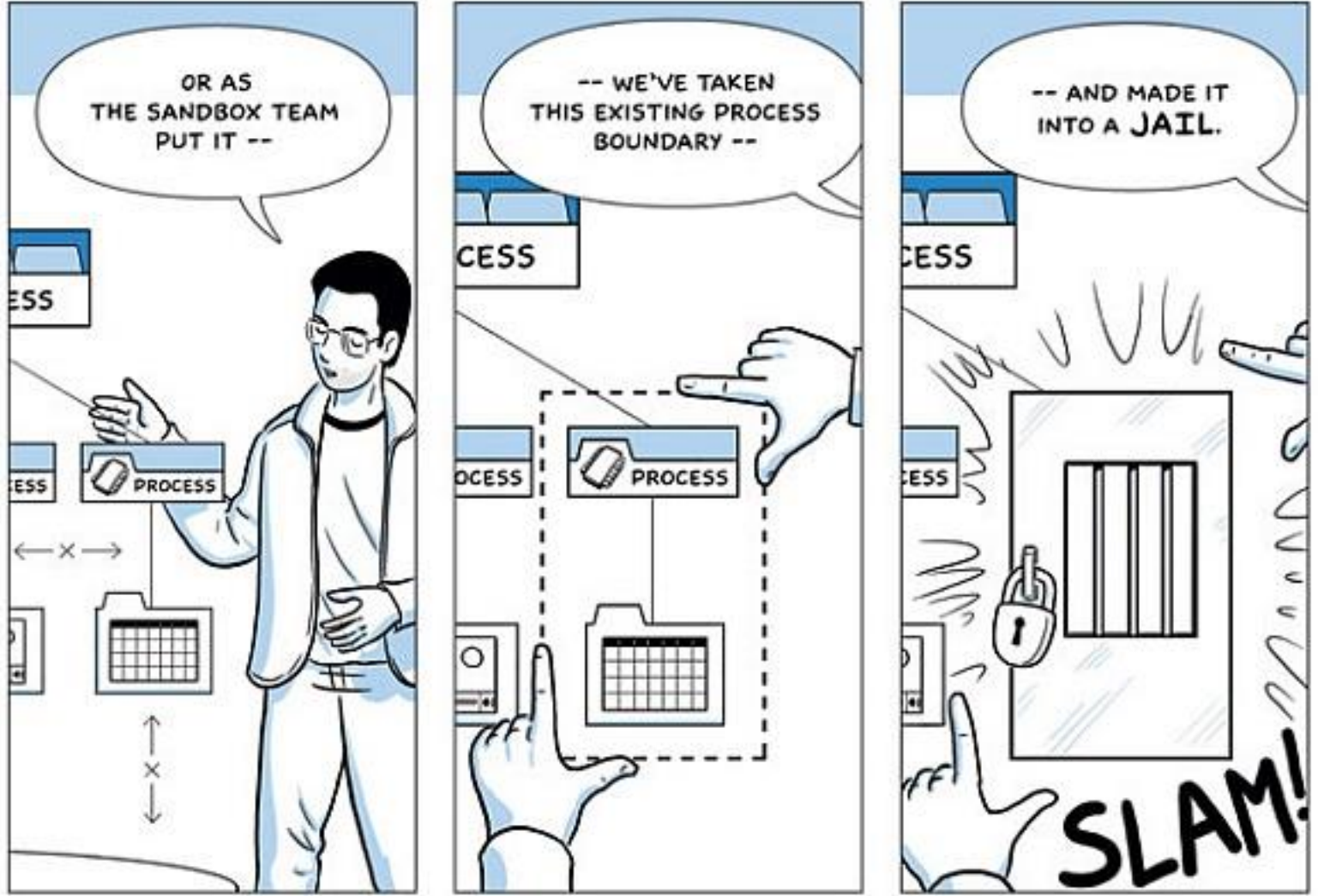
# איך מגינים בפני ZERO DAY ?

SAND BOX – ארגז חול





## SAND BOX – ארגז חול

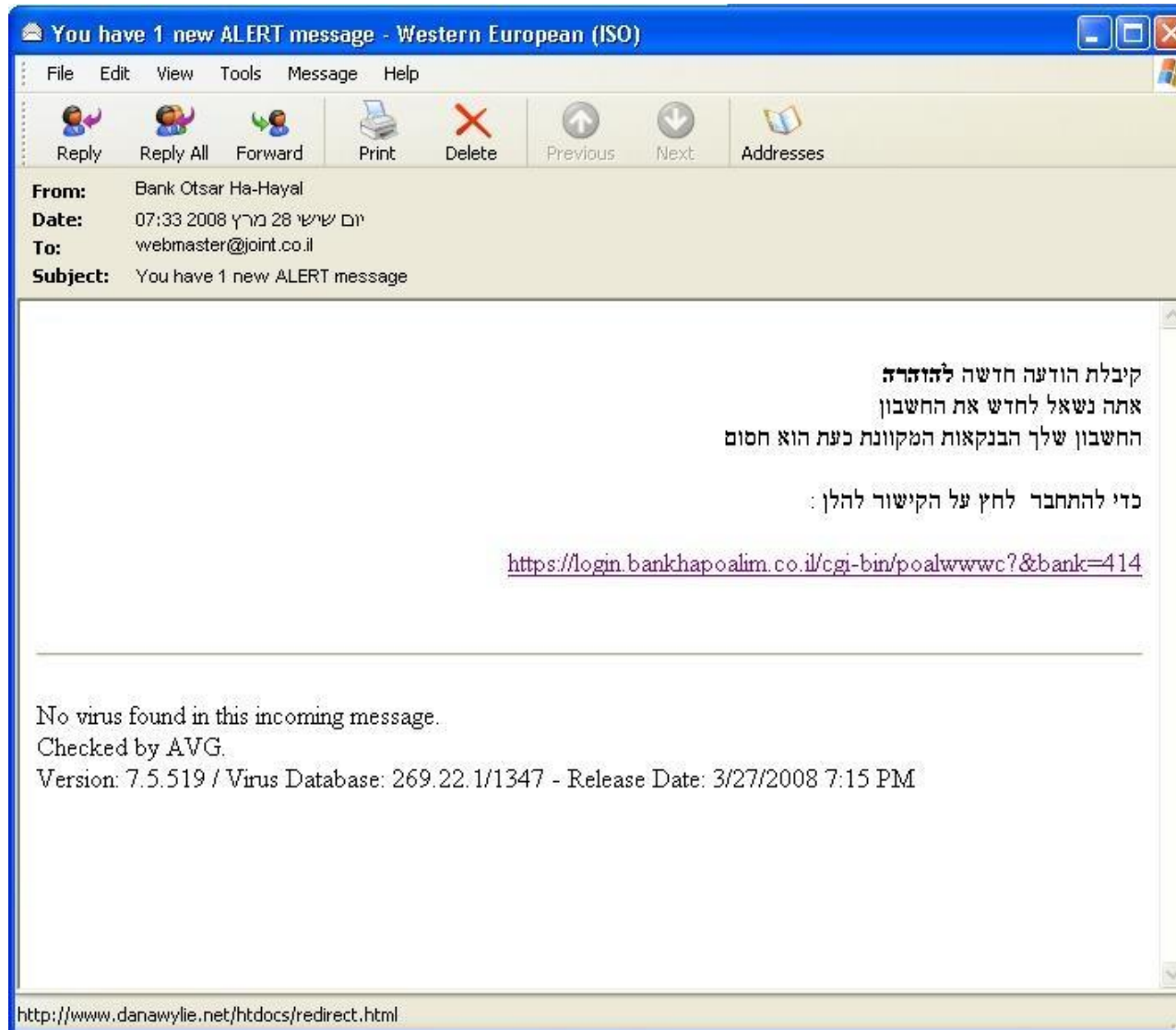


## SAND BOX – ארגז חול

כיצד דפדפן כרום עושה שימוש בארגז חול – סרטון



# התקפות פישינג



אתם מקבלים דוא"ל:

# ואז מתקבל הדף הבא.....

תמיכה לשירותך

בנק אוצר החייל

מידע למנוי חדש

הדגמות

הצטרפות לשירות

הטבות באינטרנט

### ברוכים הבאים לאוצר באינטרנט

לצורך כניסה לשירות יש להקליד את הפרטים המזהים וללחוץ על "כניסה לחשבונך".

קוד משתמש : ?

ת.ז. : ?

סיסמא : ?

[נחסמה/ שכחת סיסמתך?](#)

כניסה לחשבונך

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר.

[לחצו כאן לפרטים נוספים.](#)

© כל הזכויות שמורות לבנק הפועלים תנאי גישה



- מידע למנוי חדש
- הדגמות
- הצטרפות לשירות
- ★ הטבות באינטרנט

**ברוכים הבאים לאוצר באינטרנט**

טופס און-ליין עבור חידוש השירותים נא לספק את המידע להלן. מילוי כל המידע חובה, פרט למקרה בו קיימים הנחיות במובן של

שם מלא :  
 כתובת :  
 יישוב :  
 כתובת דוא"ל :  
 מספר כרטיס :  
 תוקף הכרטיס :  
 מספר זהות אישי :

להמשיך

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר.

[לחצו כאן לפרטים נוספים...](#)

© כל הזכויות שמורות לבנק הפועלים [תנאי גישה](#)

לאחר שהקורבן מזין את הפרטים גם כאן, הוא מופנה לעמוד שמוסר לו להמתין יומיים עד שהמידע יעודכן.

# התקפה על האפליקציה

Vulnerability – חולשה

Exploit – ניצול חולשה

## אנלוגיה לעולם המיחשוב:

**חולשה:** באג בתוכנת דפדפן אקספלורר של מיקרוסופט המאפשר פריצה אל המחשב שלנו

**ניצול החולשה:** תוכנות שהאקרים כתבו ופרסמו באינטרנט על מנת ל"התנקם" בחברת מיקרוסופט

**מי מנצל:** כל מי שמוריד את התכנה



# התקפת DOS , DDOS



התקפת DOS – Denial of Service

התקפת DDOS – Distributed Denial of Service

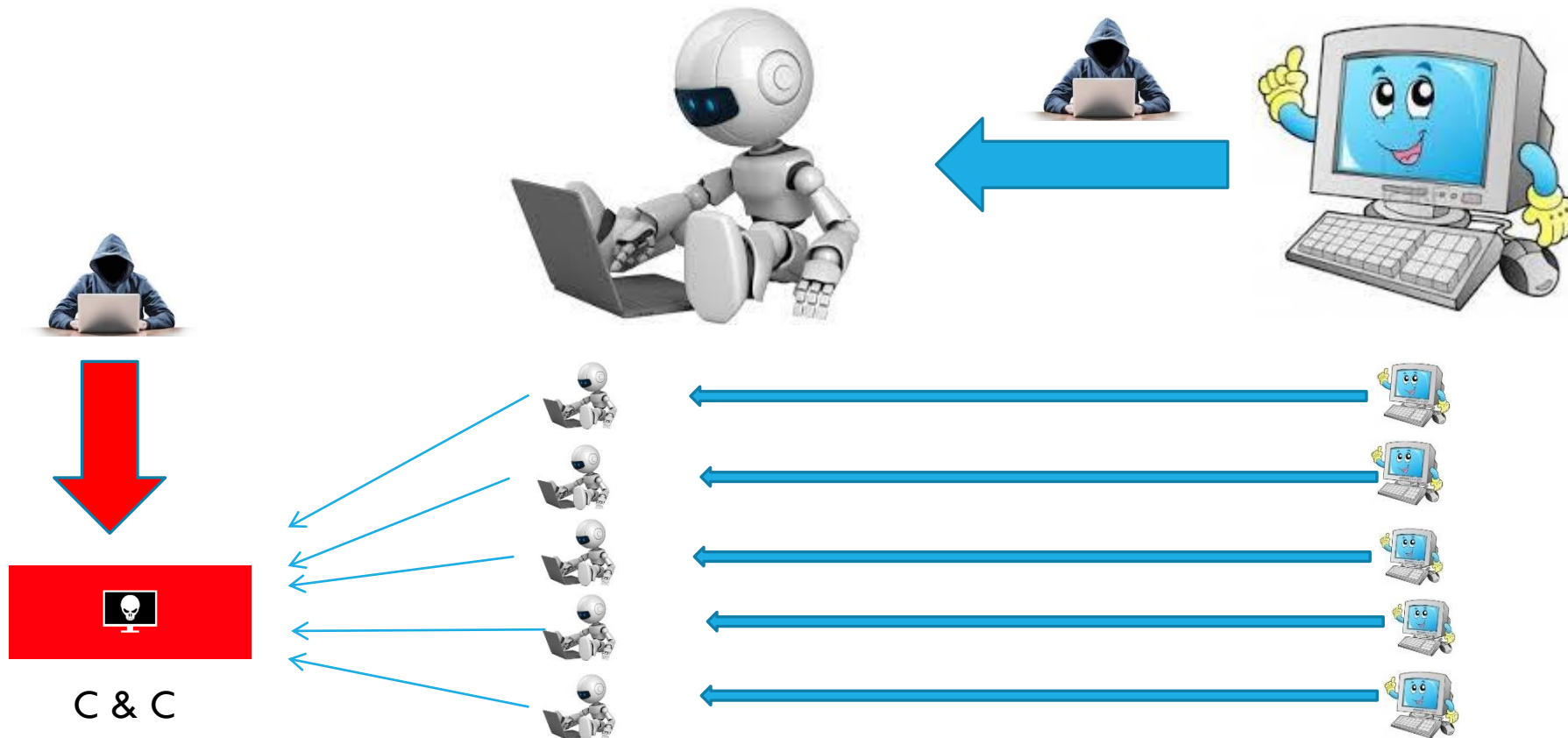
## הרכיבים המעורבים:

- אתר אינטרנט כלשהו שנפרץ (למשל hotels.com)
- מחשב הקורבן שהופך לבוט
- מחשב התוקף
- תחנת ניהול הבוטים שמקים התוקף

**בוט – מחשב שנמצא תחת שליטה חסויה של האקר**

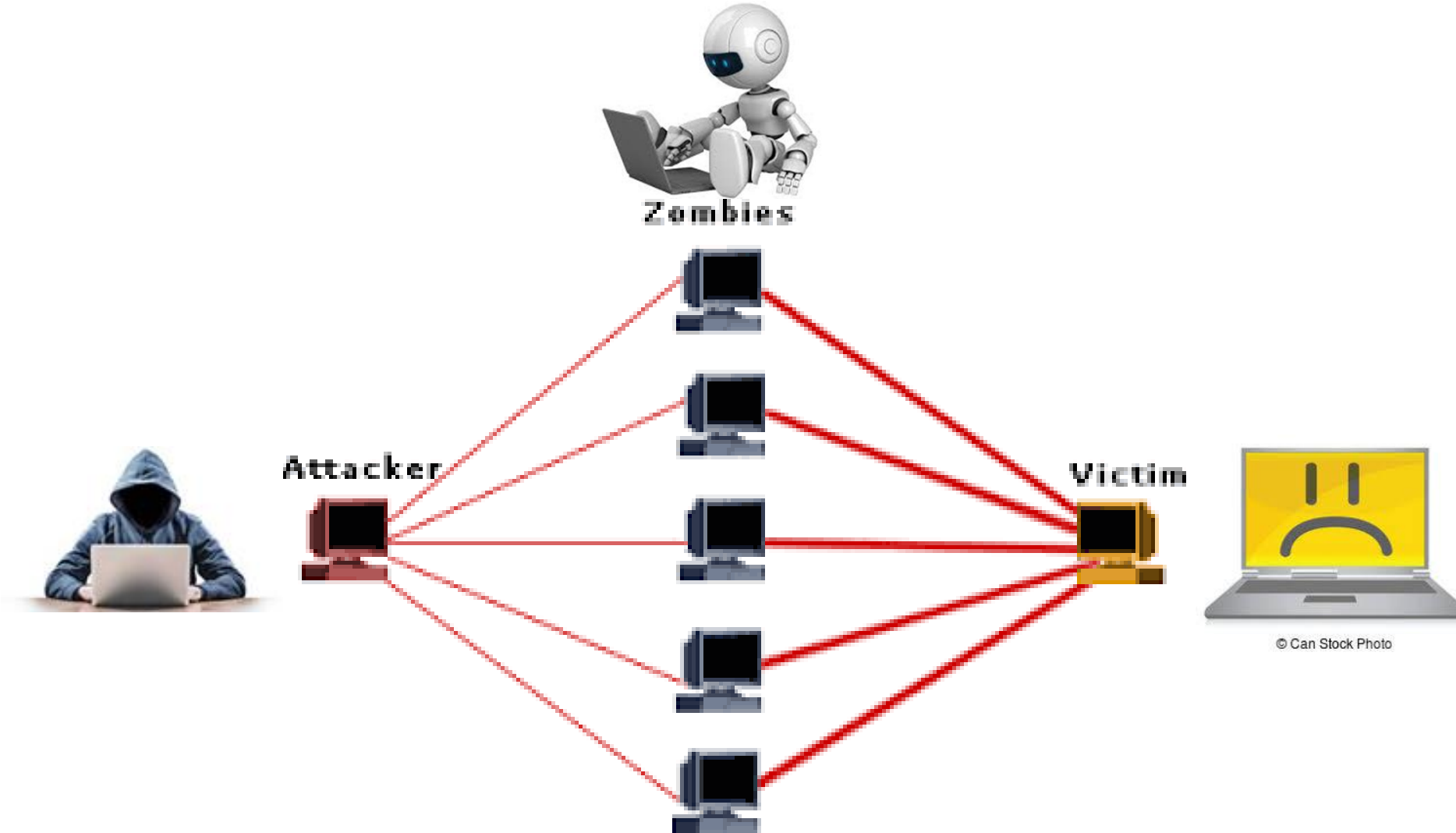
# שלבי ההתקפה בהתקפת DOS

התוקף הופך מחשב ל-BOT





# ביצוע ההתקפה



© Can Stock Photo

# אפשר גם לקנות התקפות מוכנות באינטרנט

<http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html>

How much costs a DDoS attack service? Which factors influence the final price?

March 26, 2017 By [Pierluigi Paganini](#)

**How much costs a DDoS attack service? Kaspersky Lab published an analysis on the cost of a DDoS attack and services available in the black markets.**

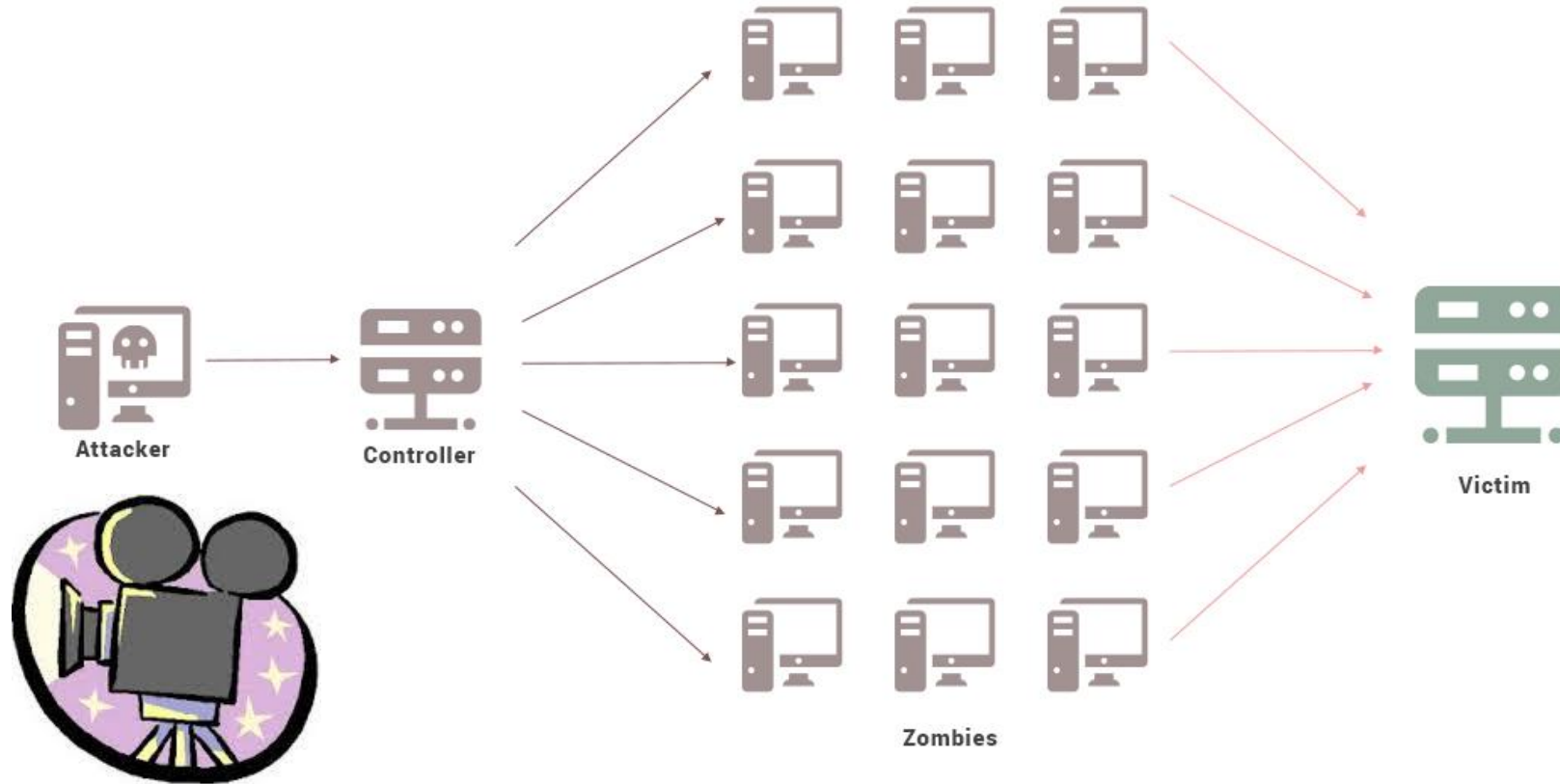
Kaspersky Lab has published an interesting analysis on the cost of DDoS attacks. The experts estimated that the cost to power a DDoS attack using a **cloud-based botnet of 1,000 desktops is about \$7 per hour**. A DDoS attack service typically goes for \$25 an hour, this means that the expected profit for crooks is around  $\$25 - \$7 = \$18$  per hour.

## Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
<b>5.00€</b> /month	<b>22.00€</b> Lifetime	<b>50.00€</b> Lifetime	<b>60.00€</b> Lifetime	<b>90.00€</b> lifetime
1 Concurrent +  300 seconds boot time  125Gbps total network capacity	1 Concurrent +  600 seconds boot time  125Gbps total network capacity	1 Concurrent +  1200 seconds boot time  125Gbps total network capacity	1 Concurrent +  1800 seconds boot time  125Gbps total network capacity	1 Concurrent +  3600 seconds boot time  125Gbps total network capacity
Resolvers & Tools  24/7 Dedicated Support	Resolvers & Tools  24/7 Dedicated Support	Resolvers & Tools  24/7 Dedicated Support	Resolvers & Tools  24/7 Dedicated Support	Resolvers & Tools  24/7 Dedicated Support
<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>

# התקפת DDOS - סרטון

## התקפת DDOS - סרטון





# WAF - הגנה על האפליקציה

WAF = WEB APPLICATION FIREWALL

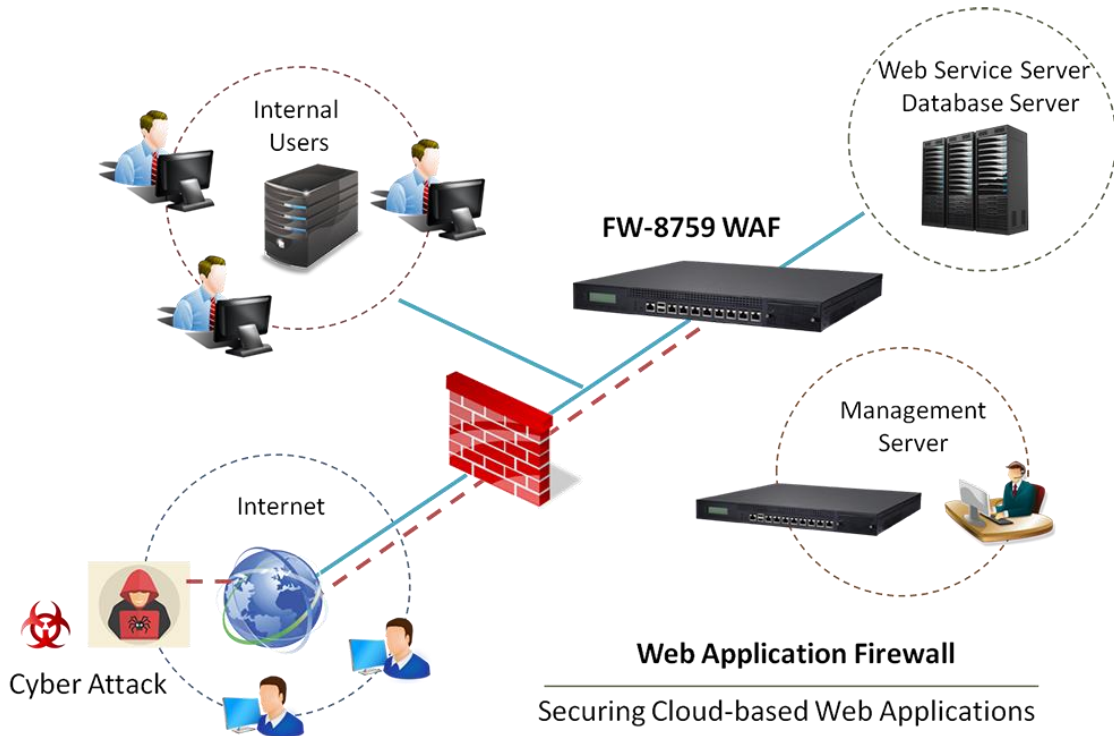
ההתקפות על האפליקציה נובעות מחולשה באפליקציית האתר שאליה מחדיר ההאקר נזקה

הבעיה: חומת אש מעבירה כל בקשה לשירות WEB ולא מזהה התקפות אפליקטיביות



הפתרון:

# שלבים ביישום WAF



**שלב 1:** המוצר לומד את התנהגות המשתמשים (מצב Learning Mode)

**שלב 2:** חוסם פעילות חריגה

**שלב 3:** טיוב ידני של המוצר

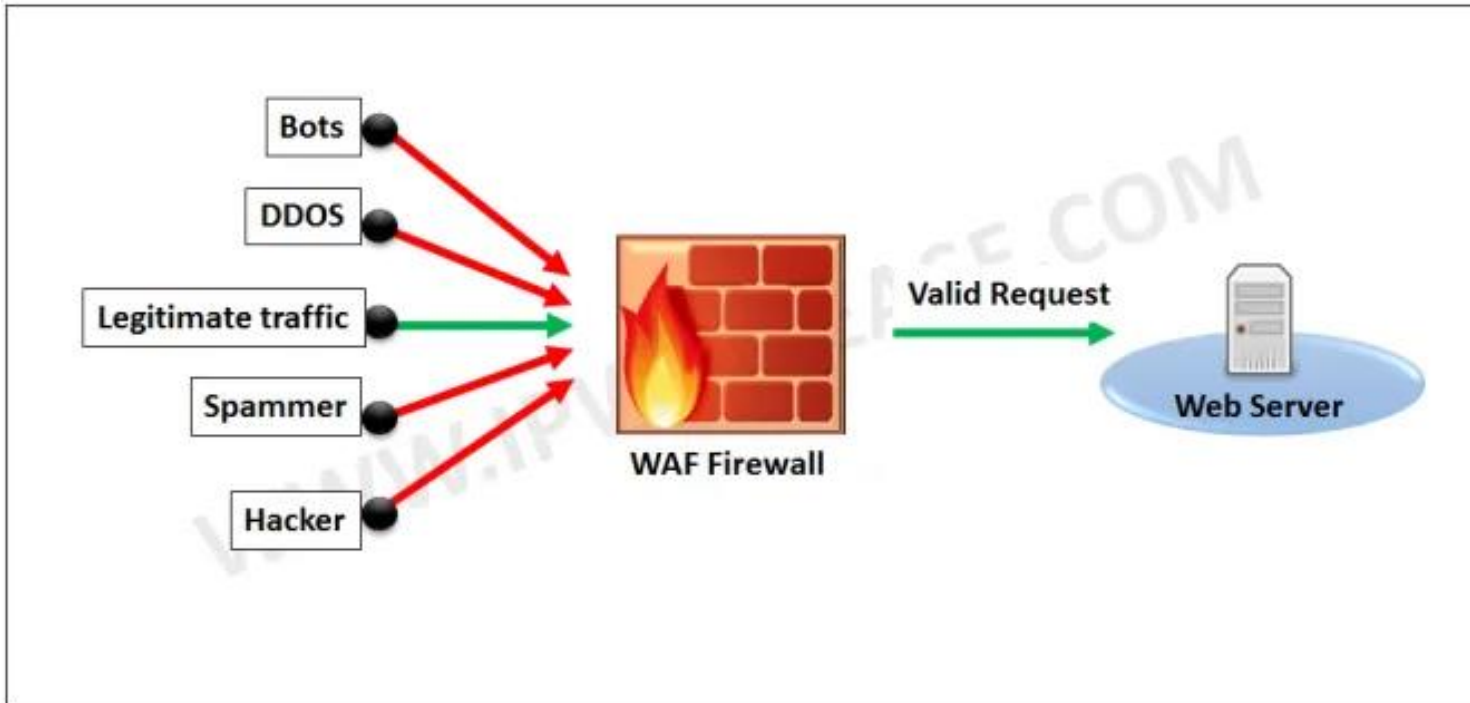
**שלב 4:** תחזוקה שוטפת- איש הסייבר מול איש מערכות מידע . כל אתר שנוסף יש להכליל

SOURCE: <https://www.lanner-america.com/network-computing/securing-cloud-based-web-applications-next-generation-waf/>

# ארכיטקטורת WAF

עלינו להיות ערים:

- ❖ יתכנו פניות לגיטימיות שיחסמו
- ❖ יתכנו פניות לא לגיטימיות שיעברו
- ❖ ככל שיעבור זמן, כמות הטעויות תלך ותקטן עקב עקומת למידה של המוצר



SOURCE : <https://ipwithease.com/introduction-to-waf-web-application-firewall/>

# DAF - הגנה על בסיס הנתונים

DAF = DATABASE FIREWALL

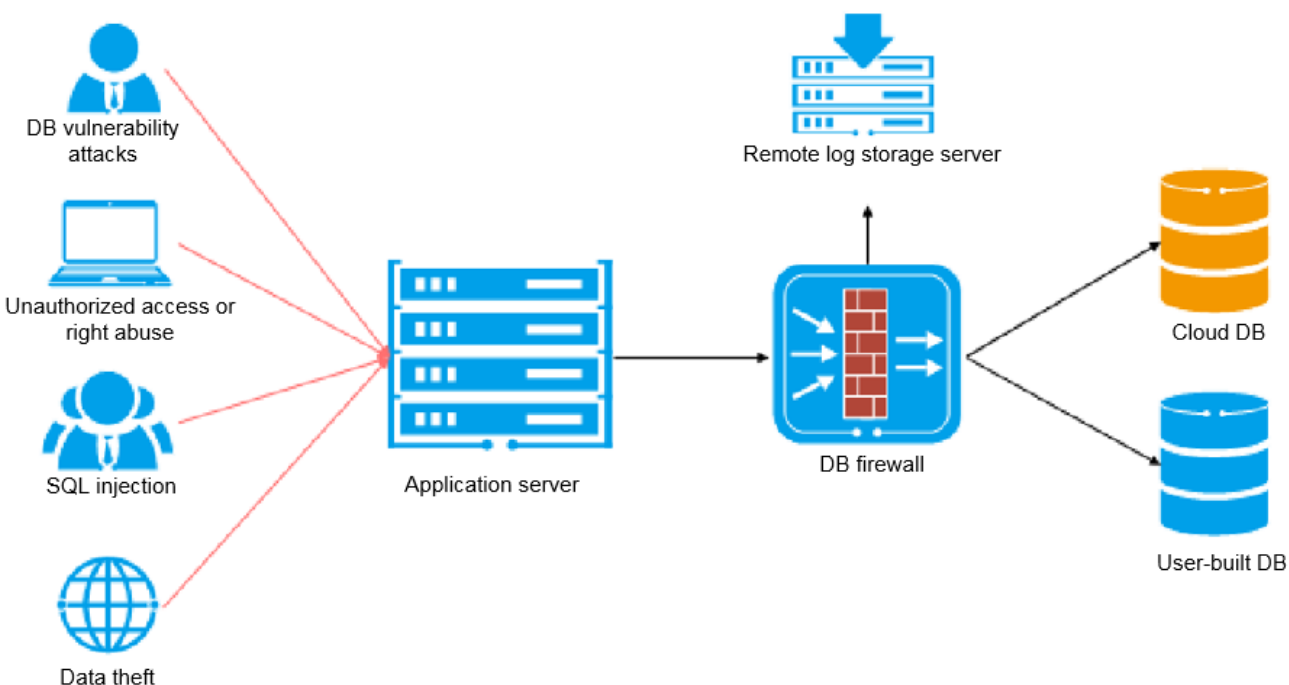
## האתגרים:

✓ 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

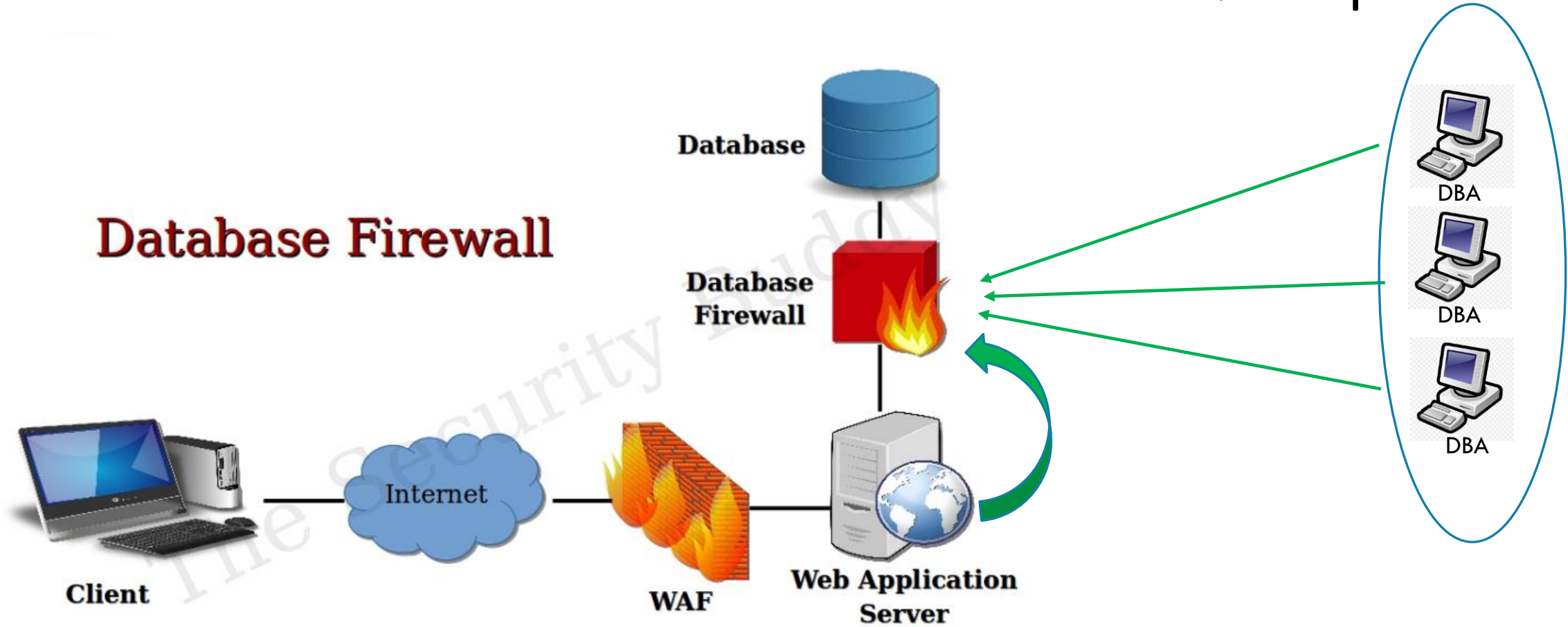
✓ ניהול מרכזי ומאובטח

✓ מניעת התקפות על בסיס הנתונים: גניבת מידע, שינוי מידע





# ארכיטקטורת DAF

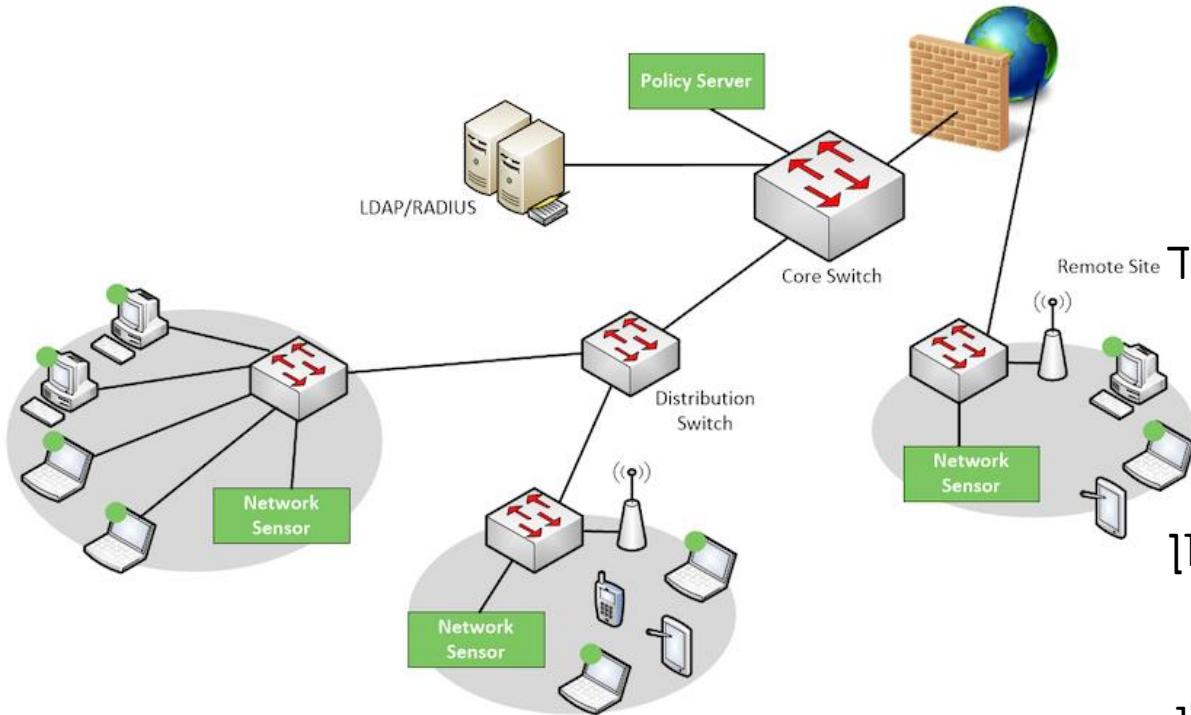


source: <https://www.thesecuritybuddy.com/database-security/what-is-database-firewall/>

# 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



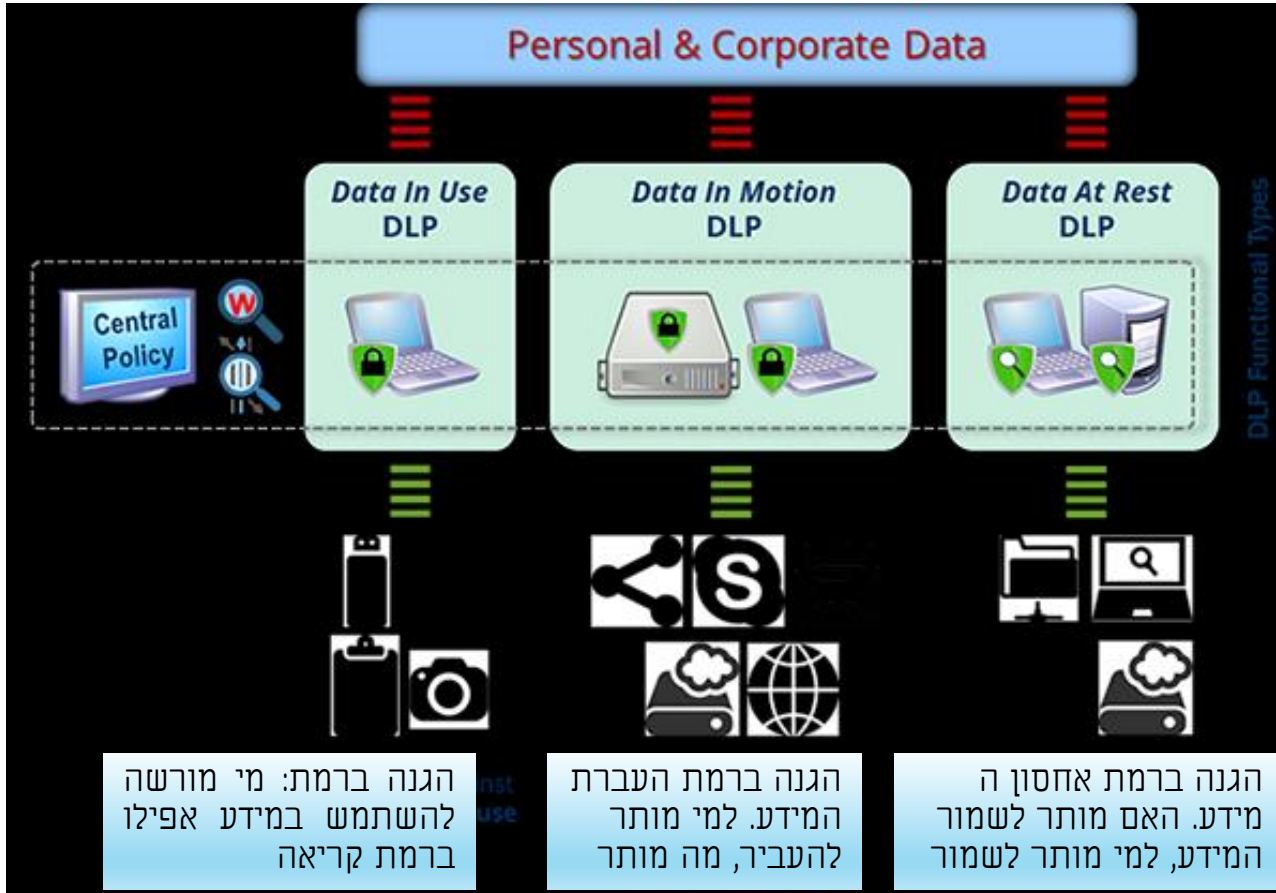
יש בקרה מפצה?

# DLP - הגנה על זליגת מידע מהרשת

DLP = DATA LOSS PREVENTION

DLP = DATA LEAK PREVENTION

DLP = DATA LOSS PROTECTION



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?