



DANET

COMMUNICATIONS



Driving your business evolution

דאנת תקשורת הוקמה בשנת 2008, ומספקת שירותי ערך מוסף בתחום תשתיות אבטחת המידע בעולמות הענן והדטה סנטר.

דאנת תקשורת מעניקה מענה הוליסטי לצרכי אבטחת המידע, הסייבר והתשתיות של ארגוני enterprise מכל המגזרים, לחברה כ-400 לקוחות פעילים.

החברה דוגלת במתן ערך מוסף בהיבטי אינטגרציה ואוטומציה של תהליכים בתוך חוות השרתים ובענן.

ערכי ההגנות והאמינות מלווים את החברה במשך שנים רבות, ובשל כך מרבית לקוחות החברה הם לקוחות חוזרים שנמצאים אתנו שנים רבות עם מגוון רחב של פתרונות.

סוד ההצלחה שלנו מתאפיין בשילוב פתרונות של יצרנים מובילים בתחום, כאשר הייחודיות שלנו מתאפיינת ביכולת לחבר את הפתרונות, כדי לספק פתרון הוליסטי מקיף.



CYBER CLOUD NETWORKS - החברה מספקת לדאנת תקשורת את פלטפורמת שירותי האבטחה בענן שלה, ומתמקדת בעיקר בארגוני SMB\SME מ-10 עד 1,000 משתמשים.

PALO ALTO NETWORKS - אנו מתמחים בהטמעה של פתרונות פאלו אלטו בחוות שרתים ובתשתיות ענן של הארגון, ומממשים פתרונות מתקדמים כגון REDLOCK, TRAPS.

ARISTA NETWORKS - דאנת תקשורת היא אחד מספקי ה-TIER1 של אריסתא בישראל, ומתמחה בפתרונות ה-DC, ה-CAMPUS וה-WIRELESS SECURITY.

NETSKOPE - החברה המובילה בעולם בתחום ה-CASB, ומספקת פתרון ייחודי ל-SHADOW IT וכן VISIBILITY בעולמות ה-SAAS וה-IAAS.

F5 NETWORKS - החברה מתמחה בהטמעת פתרונות AWAFF, APM, SILVERLINE וכן LTM - עבור הטמעה ב-PERIMETER וכן ב-DATACENTER של הארגון.

TREND MICRO - אנו מתמחים באספקת פתרון בחוות השרתים ובענן וכן בהטמעת פתרונות Forensic ברמת הרשת.

GIGAMON - אנו מתמחים בהטמעת פתרונות NETWORK VISIBILITY ומתממשים לסביבה הפיסית, הוירטואלית והענן של הארגון ומאפשרים חיבור כלי אבטחה וניטור מתקדמים אל מול תעבורת הרשת.



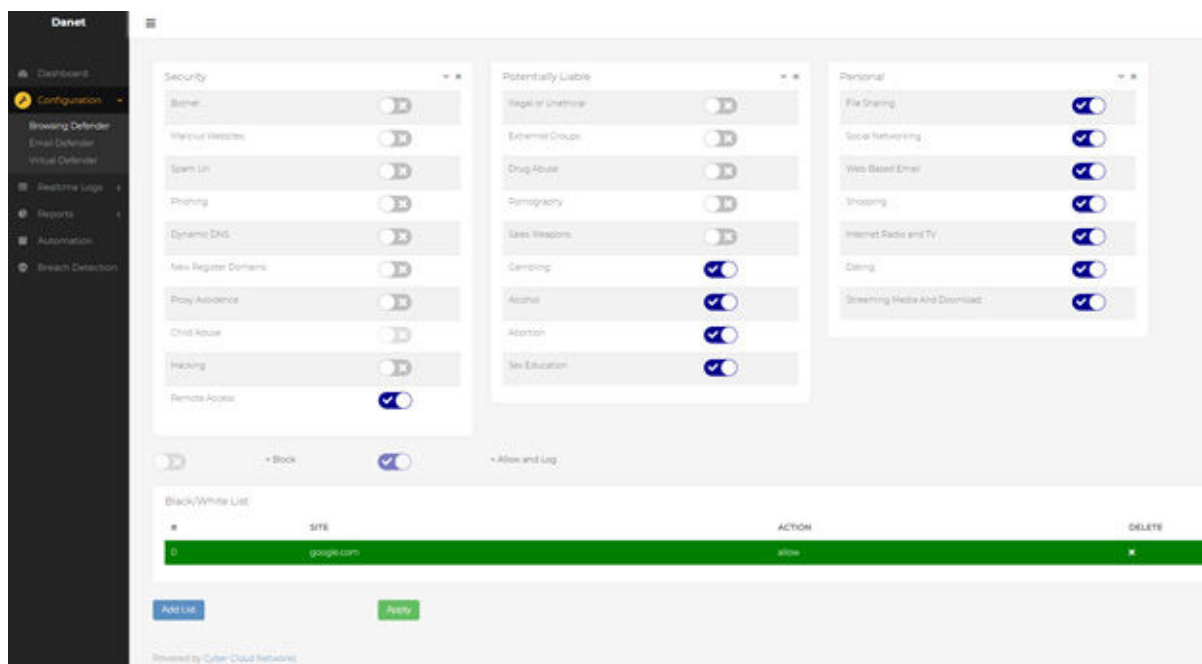
דאנת תקשורת, מספקת שירות אבטחה בענן ללקוחות המדיום שלה.

השירות מבוסס על פלטפורמה של חברת Cyber Cloud Networks. השירות כולל מספר מודולים שפועלים יחדיו תחת ממשק ניהול אחד.

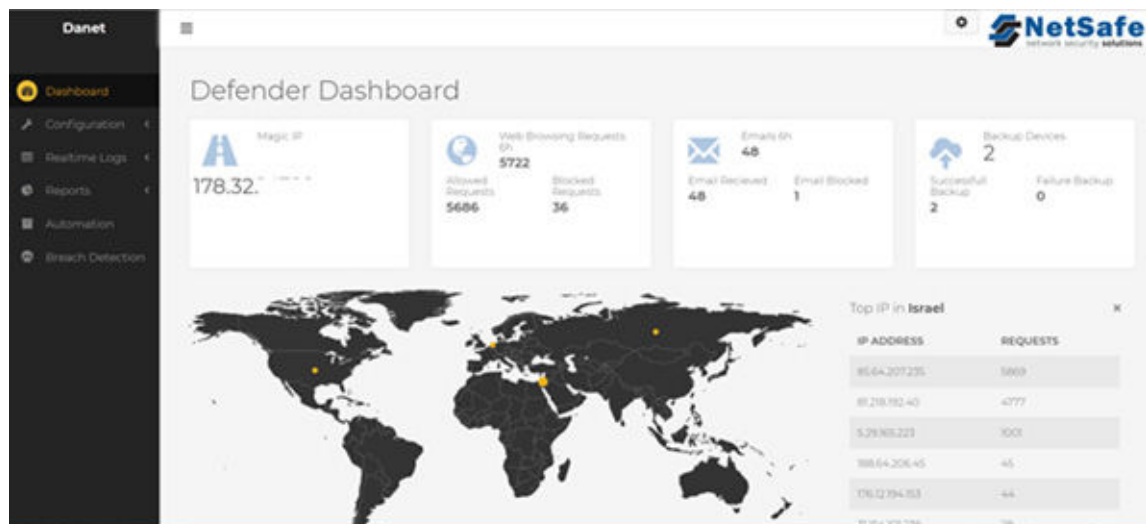
שירות הגנה על הארגון באמצעות סינון פרוטוקול DNS, ומאפשרת לכל ארגון לנהל את הרשאות הגישה לאינטרנט, על בסיס חבילות: Malicious sites protection, SPAM URL, Phishing, Botnet וכמובן קטגוריות נוספות כגון Gambling, Social וכו'.

Browsing Defender

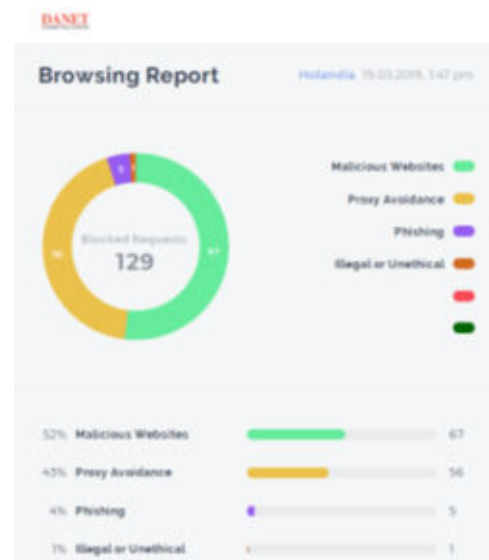
שירות הגנה על הארגון באמצעות סינון פרוטוקול DNS, ומאפשרת לכל ארגון לנהל את הרשאות הגישה לאינטרנט, על בסיס חבילות: Malicious sites protection, SPAM URL, Phishing, Botnet וכמובן קטגוריות נוספות כגון: Gambling, Social וכו'.



השירות מאפשר הגנה על נתבים, רכיבי IoT, רשתות אלחוט ציבוריות, מערכות אבטחה, טלפונים סלולריים ומחשבים ניידים. המערכת מאפשרת צפייה בזמן אמת בכל תעבורת הגלישה מהארגון ומחוצה לו, הן באמצעות מפה, לוגים ודוחות בזמן אמת מתוך הפורטל הייעודי של כל לקוח.



המערכת מאפשרת קבלת דוחות יומיים ושבועיים במייל, מותאמים אישית ללקוח.



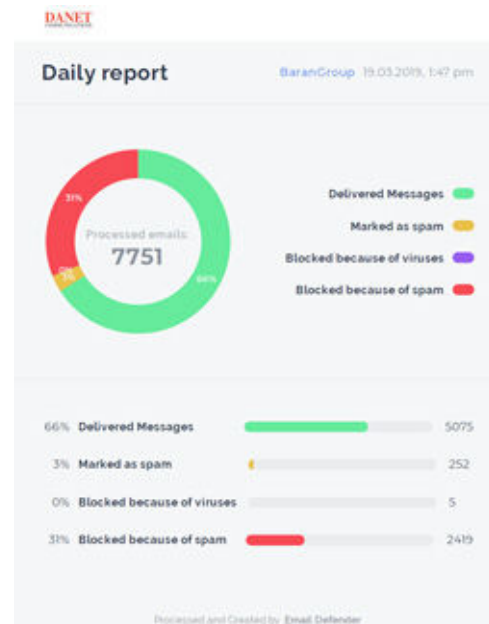
EMAIL DEFENDER

מודול ה-EMAIL DEFENDER כשירות ענן, מאפשר חיבור למערכות 365, EXCHANGE וכן GSUITE, בין אם באופן ישיר או באמצעות התממשקות ל-MAIL RELAY קיים בארגון.

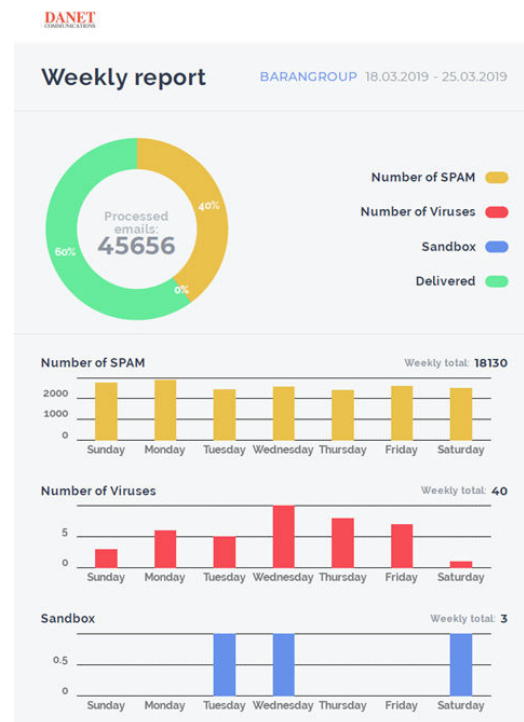
מערכת סינון דואר מתקדמת זו, מאפשרת חיבור במקביל ל-12 מנועי אנטייוירוס, מנועי SANDBOX מתקדמים וכן מנוע הלבנה מקיף, אשר סורק את גוף המייל ותוכנו וכן מנוע ANTISPAM.



המערכת מספקת לכל לקוח ממשק נוח ופשוט לצורך צפייה בלוגים ודוחות יומיים ושבועיים:



וכן דו"ח שבועי:



מודול ה- Automation - Network Snapshot

מאפשר ללקוח לבצע גיבוי ושחזור של כלל רכיבי התקשורת ואבטחת המידע ברשת, לרבות סניפים ואתרים מרוחקים.

המערכת תומכת בלמעלה מ- 200 יצרנים שונים.

המערכת מבצעת גם ניטור ביצועים של ממשקים, מעבד וזכרון המערכות המגובות.

המערכת כוללת מידע מקיף על כל רכיב מגובה, לרבות מספר סידורי, גירסה, טבלאת ניתוב, מידע על ממשקים.

המערכת מאפשרת ביצוע תהליכי אוטומציה מלאים מול המערכות.

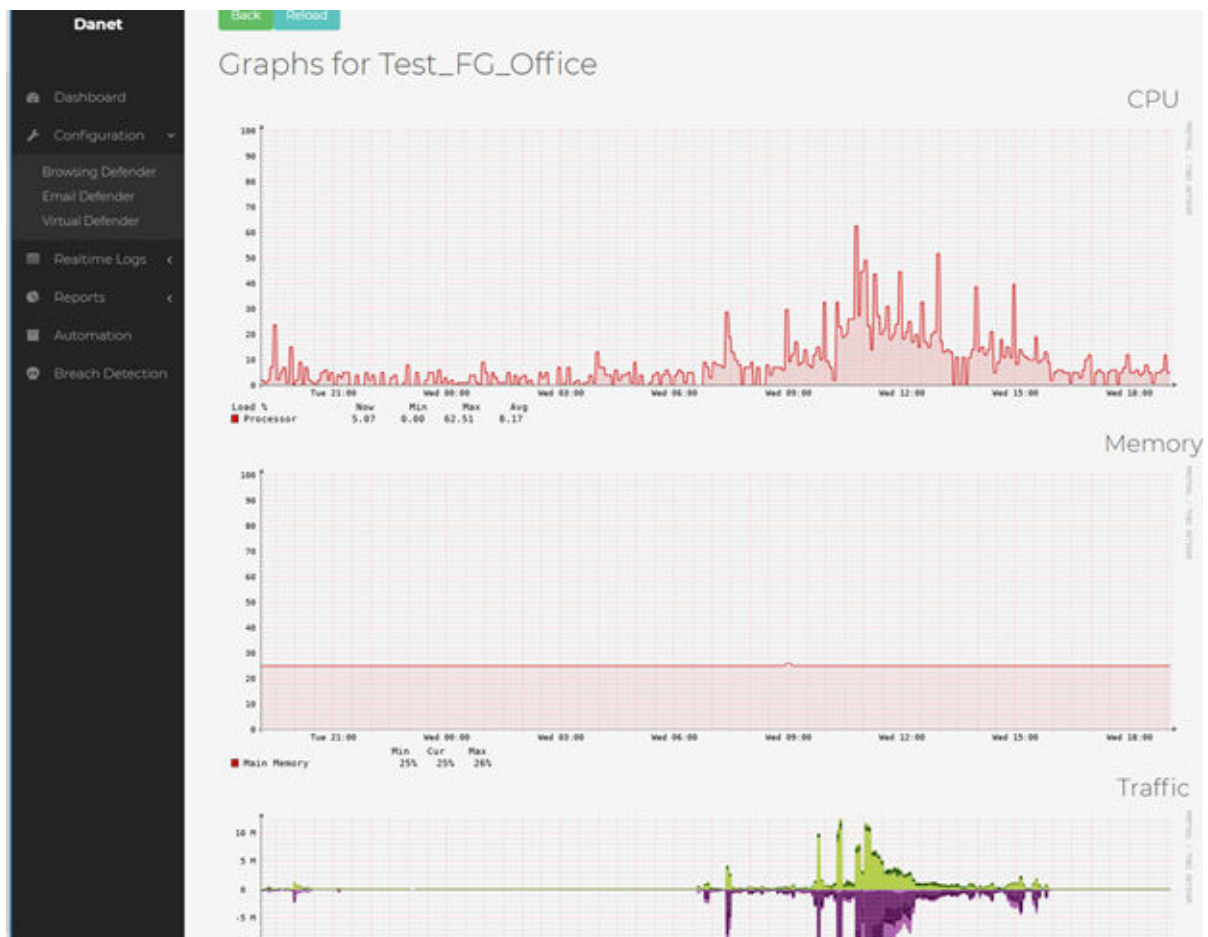
המערכת שומרת 10 גרסאות אחורה (בהם היה שינוי בלבד).

המערכת מאפשרת גיבוי בענן, גיבוי מקומי באתר, וכן פתרון משולב.



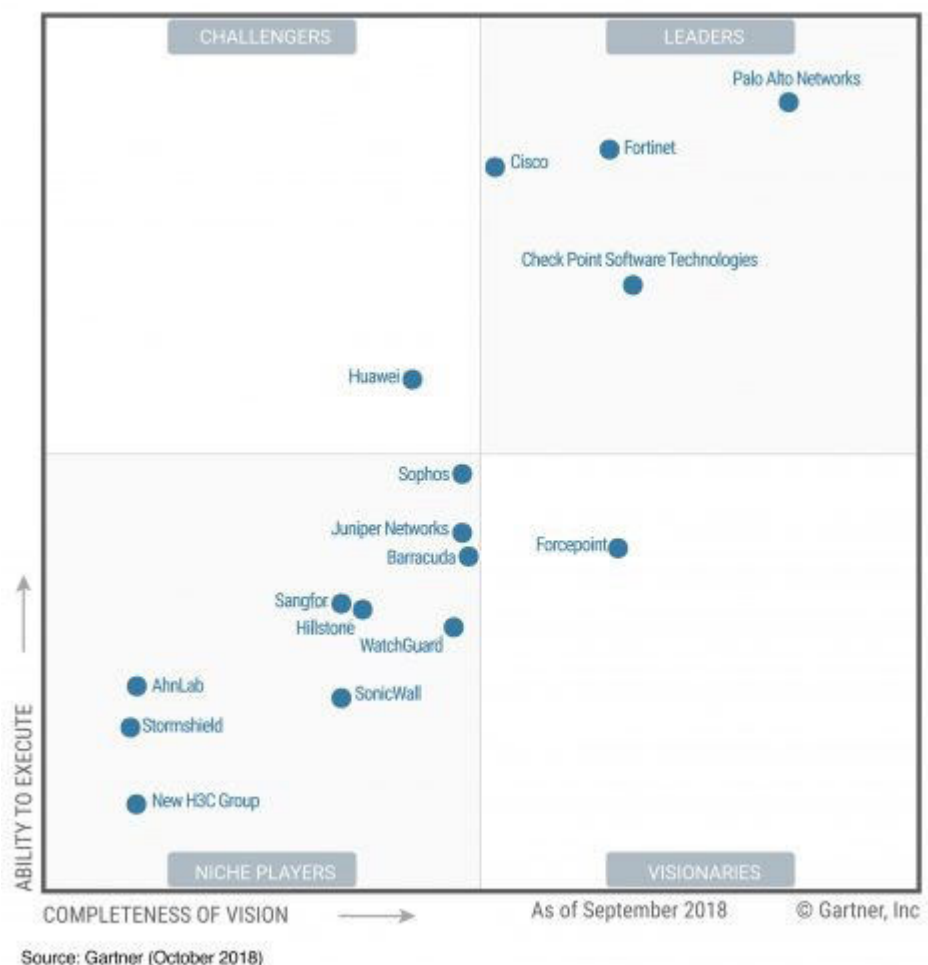
המערכת כוללת מידע מקיף על כל רכיבי התקשורת והאבטחה בארגון:

Snapshot Device List										
#	NAME	IP ADDRESS	MODEL	FIRMWARE	SERIAL	BACKUP STATUS	UPTIME	LOGS	RESTORE	MONITOR
1	Test_FG_Office		FortiGate-90D	v6.0.3.build0200.181009	FG190D3Z16014263	🟢	100%	🔍	👤	Monitoring
2	fortigate_dns		FortiGate-VM64	v5.6.6.build1630.180913	FGVM2V0000176524	🟢	100%	🔍	👤	Monitoring



חברת Palo Alto Networks הוקמה ב- 2005 ע"י ניר צוק והמוצרים הראשונים שיצאו היו סידרת ה- 4000 וה- PA-500 שיצאו לשוק לאחר כשנתיים. מאז ובתוך כ- 10 שנים הפכה פאלו אלטו להיות מובילה עולמית בתחומי הגנת הסייבר. נכון להיום פאלו אלטו מוכרת בלמעלה מ- \$2.5B הרבה מעל מתחרותיה ומקבלת הכרה ברורה מאנליסטים כמו גרטנר לגבי המובילות הברורה של החברה. לפאלו אלטו מרכז פיתוח גדול בת-א היחיד מחוץ לארה"ב הכולל כ-1,000 עובדים. המרכז מתבסס על הרכישות של חברות ישראליות שפאלו אלטו ביצעה בישראל ובהם: Cyvera, LightCyber ו-SecDO.

Figure 1. Magic Quadrant for Enterprise Network Firewalls



פאלו אלטו מיום היווסדה ע"י ניר צוק הציגה חדשנות. זה התחיל ב-FW שעד אז סין תעבורה ברמת פורטים והחידוש של פאלו אלטו היה

זיהוי ובקרת אפליקציות ובנוסף זיהוי משתמשים בשמם ולא בכתובות IP והיכולת לבנות חוקים מבוססי קבוצות או שמות. מאז פאלו אלטו לא נחה על זירי הדפנה והמשיכה בתנופת פיתוח מוצרים.

תפקיד ה- FIREWALL

ה- FIREWALL שניר צוק פיתח התבסס על זיהוי אפליקציות ובניית חתימות ייחודיות לאלפי אפליקציות. כאשר המידע עובר דרך ה- FIREWALL של Palo Alto Networks. לפי החתימות אנו מזהים את האפליקציות.

ה- FIREWALL מתממשק ל- Active Directory הארגוני וכך מזהים את האנשים שמפעילים את האפליקציות.

עם היכולת הזו Palo Alto Networks מאפשרת לבנות חוקים לפי אנשים, קבוצות ב AD ואלו שהוגדרה. נקודה נוספת למחשבה היא, מה תפקיד ה- FIREWALL בעידן ה- Cyber?

ובכן, דיי ברור ומוסכם שהתפקיד המרכזי היום הוא להגן על הארגון ולמנוע מהתקפות סייבר להצלחת. ואכן, Palo Alto Networks מצליחה מאוד בתחום זה ואנליסטים כמו גרטנר ו- Forester מאשרים זאת.

Next Generation Firewall

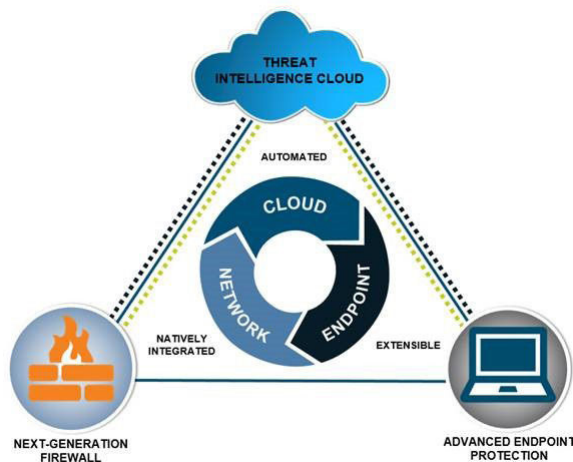
1. APP-ID - טכנולוגיה ייחודית המאפשרת זיהוי וניהול אפליקציות ללא קשר לפורטים (אפליקציות רבות יודעות "לדלג" לפורטים שונים מה שמקשה מאוד לנהל ולחסום).

2. Safely Enabling Applications - לאפשר בצורה בטוחה את האפליקציות הרצויות בארגון והיתר פשוט ייחסמו בהתאמה לארגון ולמשתמש.

3. Palo Alto Networks - Positive Security Control - היחידה שמאפשרת חוקת האבטחה מבוססת "Positive Security Whitelist", מגדירים אילו אפליקציות רוצים לאפשר וכל יתר האפליקציות נחסמות.

4. הגנה מפני איומים בלתי ידועים - מכיוון שפעולת ה- FIREWALL מבוססת Positive Security, הרי שאנו מאפשרים אך ורק תעבורה (אפליקציות) שאנו מזהים ומכירים באופן ספציפי (ניתן לחתום תעבורה לא מוכרת ולהפוך אותה לאפליקציה מוכרת). ולכן תעבורה שאינה מוכרת Unknown אינה עוברת. זוהי הדרך היחידה לאפשר עבודה עם אפליקציות באופן בטוח - Safely Enabling Applications.

5. Single-Pass Architecture - ארכיטקטורה ייחודית המאפשרת להשיג אבט"ח מרבית בצורה יעילה ובמינימום פגיעה בביצועים. כלל המנועים פועלים יחד בטכנולוגית Single Pass תחת חוקה אחת ולוג אחד.



Palo Alto End Point Security - Traps

- 1. Exploit prevention -** מניעת הרצת קוד זדוני ע"י ניצול חולשות אבטחה בתוכנות לגיטימיות זאת ע"י מיקוד בטכניקות הניצול.
- 2. Malware prevention -** מניעת הרצת קוד זדוני בעזרת ניצול המשתמש ע"י שימוש בטכנולוגיית ה sandbox בשילוב עם אנליזה מקומית על תחנת הקצה.
- 3. הקשחת תחנות הקצה -** ע"י שימוש בחוקה אשר מונעת פעולות לא לגיטימיות.
- 4. צריכת משאבים מועטה -** לא סורק ולא מנטר.
- 5. הגנה על מערכות הפעלה ישנות -** XP, Win Server 2003.

Wild Fire Cloud:

1. שליחת קבצים באופן אוטומטי לענן המדמה סביבת Windows חיה עם יציאה לאינטרנט.
2. זיהוי קובץ נגוע מייצר חתימות באופן אוטומטי למנועים השונים (כלל המנועים בבעלות PALO ALTO).
3. בכל 5 דקות ה- NGFWALL מתעדכן למול הענן לקבלת חתימות.
4. הקבצים נבדקים בסביבות של Static Analysis, Dynamic Analysis, Heuristic Engine, Bare Metal Analysis.

Palo Alto Networks - פתרונות לכל שכבות הארגון:

- FIREWALL ל- Gateway - שער הארגון.
 - הגנה בתוך הרשת ועל חוות השרתים.
 - הכל ניזון ממערכת ה- WildFire - Sandbox לקבלת חתימות ועדכונים לגבי התקפות חדשות ווירוסים חדשים.
- Palo Alto Networks מופיעה ראשונה בקבוצת ה- Leaders של גרטנר מזה מספר שנים. החברה גדלה בלמעלה מ- 50% בשנה (השוק גדל בכ- 10% לשנה) לחברה למעלה מ- 30,000 לקוחות. בארץ יש ל- Palo Alto Networks למעלה מ- 400 לקוחות שמפעילים Palo Alto Networks ברשת שלהם.
- רובם החליפו את ה- FIREWALL המרכזי שלהם ובהם: NICE, SAP, Apple, Ceva, ClickSoftware, Clarizen, ביטוח איילון, מדנס, מסלקה פנסיונית, רוח"מ, קק"ל ועוד הרבה אחרים.



חברת אריסתא נטוורקס, הינה חברה המתמחה בפתרונות מתקדמים לסביבת הדטה סנטר והקמפוס. החברה בעלת נתח שוק עולמי של 16%, ומקימה כיום את ספקי השירות, חברות הענן והדטה סנטרים הגדולים בעולם במגוון רחב של לקוחות ממגזרים שונים.

בישראל, החברה פעילה בספקי שירות, גופים פיננסים, הייטק ותעשייה ומספקת פתרונות מתקדמים לסביבת ה- DATACENTERS של הארגונים.

החברה מספקת פתרונות מיתוג יחודיים בעלי יכולות DEEP BUFFER, וזאת לצורך התמודדות עם MICRO BURSTS, ורוחבי פס גבוהים.

בשל היותה של חברת ARISTA, חברה הדוגלת ב-OPEN STANDARDS, החברה משתפת פעולה עם יצרנים נוספים, כגון PALO ALTO.

About Arista Networks

ARISTA



- **Cloud Networking** – Laser Focus
- **15M+** ports shipped
- **\$~2B** Annual Revenue, increase of 45.8% YoY
- **16%** Market Share, 34% 100G (High Speed DC Switching)
- **5000+** customers
- **1** Operating Systems
- **Leader by Analysts**- Forester 2018 leader, Gartner 2015-2018 leader quadrant
- **Fastest** growing tech company, \$20B market cap

לחברת אריסתא נטוורקס היצע רחב של פתרונות, בין אם מדובר במתגים המיועדים לתפקד כ- SPINE או כאלו המתפקדים כ- LEAF בפתרון. הייחודיות בפתרון, שמדובר במערכת הפעלה EOS אחת, לכלל המתגים, כאשר היכולות המרכזיות הינן זהות עבור כל סוגי המתגים.

Arista Product Overview – 2018

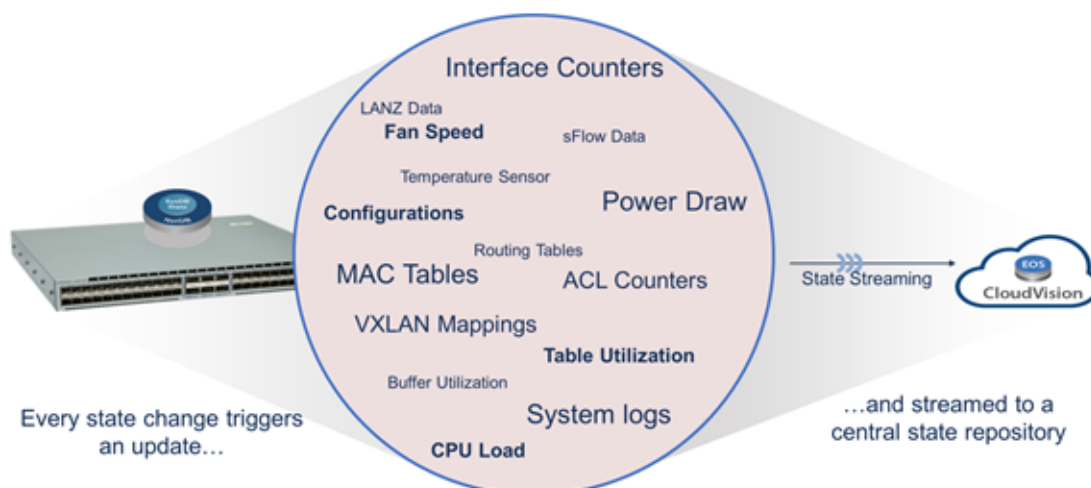


הפתרון של אריסתא מנוהל באמצעות מערכת ניהול מרכזית בשם CLOUD VISION, אשר תומכת במספר יכולות מתקדמות:

- DISCOVERY של כל מתגי הרשת, שרתים, התקנים.
- CHANGE CONTROLS - היכולות לבצע NETWORK SNAPSOTS, לחזור אחורה בזמן, לבצע בחינת COMPLIANCE וכו'.
- יכולות TELEMTRY בזמן אמת.
- יכולות SERVICE INSERTION, של פתרונות אבטחת מידע.
- יכולת TAPPING של מידע (בדומה ל-PACKET BROKER עם TAP).

יכולת ה-STATE STREAMING של מתני אריסתא, הינם כוללים מידע בזמן אמת על כל ה-COUNTERS השונים במערכת, בין אם מדובר בעומסים, ביצועי מעבד, לוגים, קונפיגורציות, וכו'.

What is State Streaming?



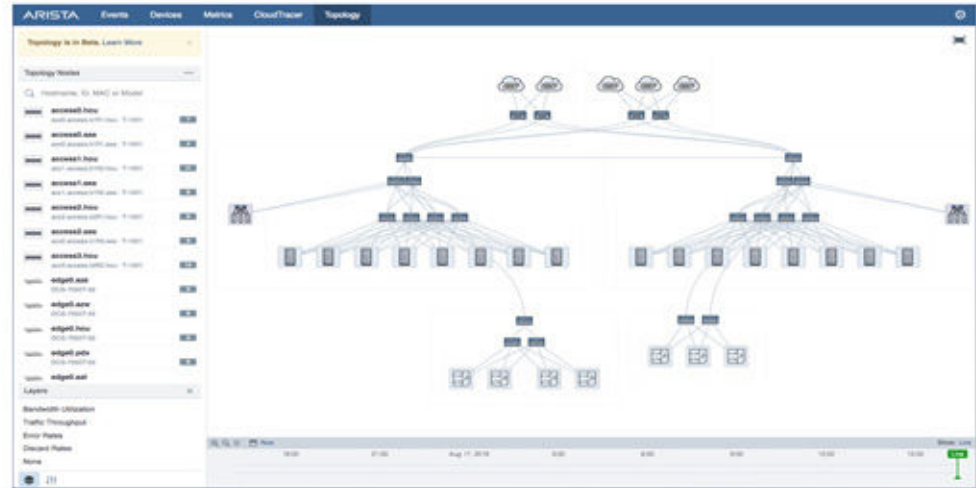
Every SysDB state change. From every device. Instantaneously.

דוגמא ליכולות ה-TELEMETRY של מערכת ה-CLOUD VISION:

CloudVision Telemetry Apps – Granular and Complete



Network-wide Perspective with CloudVision Telemetry



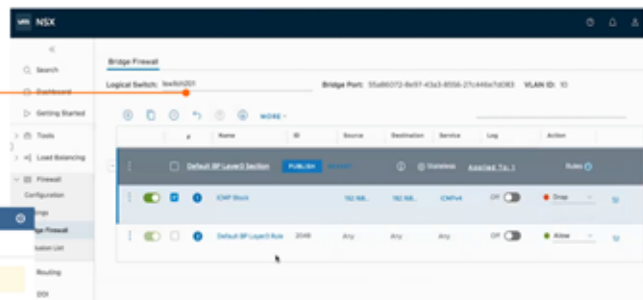
Simpler Visualizations to Parse the Telemetry Noise

חברת אריסטא, מתחברת עם VMWARE בכל הקשור לפתרון משולב בסביבת NSX ב-DATACENTER.

Arista + VMWare NSX

Extending Micro Segmentation for Bare Metal Workloads

NSX Admin implements policies for Virtual-2-Virtual & Physical-2-Virtual workflows



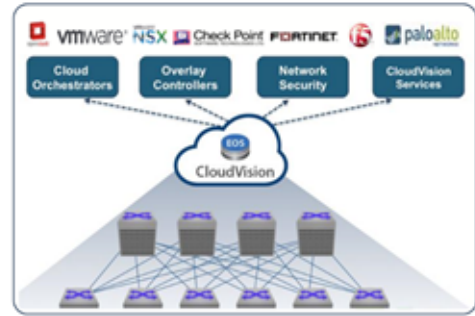
CloudVision with NSX API integration:

- Learns security policies
- Instantiates them on the network ports for Bare Metal workloads

פתרון ה-Macro Segmentation של חברת אריסטא, הינו ייחודי, ומאפשר הפעלת יכולות Firewall בין שרתים שיושבים באותו הסגמנט וזאת בזכות האינטגרציה בין המתגים של אריסטא לבין פתרונות הפיירוול של פאלו אלטו כיום ובעתיד צ'קפוינט ופורטינט.

Arista Macro-Segmentation

- Enabled by Arista CloudVision
 - Has knowledge of where every device is within the network (*physical topology*)
 - Visibility into new devices being added / moved / removed from the network – in real time
 - Two-way communication with overlay controllers
- Provides Network Service and Integration with Security Platforms
 - Service devices can be anywhere in the network
 - Devices to which security policies are attached can be anywhere
 - Non-proprietary/standards-based/no new frame format



לחברת ARISTA ישנו פתרון אלחוט ייחודי המתמקד ביכולת ייחודית של WIPS

אריסתא היא המובילה העולמית לפתרון WIPS מוכח לארגונים פיננסים, בטחוניים וכאלו שאינם רוצים ב- ROUGE ACCESS POINTS אצלם בארגון.

הפתרון של ARISTA מבוסס על פתרון של חברת AIRTIGHT, אותה רכשה אריסתא בשנה האחרונה.

הייחודיות בפתרון של ARISTA, הינה ביכולת הסריקה המהירה והממוקדת של כלל תדרי ה- 2.4/5Ghz של האלחוט בטווח של 5 שניות. בכך מתאפשרת מניעה של התחברות של רכיבים, והתקנים אלחוטיים לא מורשים למרחב הארגוני.

Renowned Best WiFi Security for 10+ Years

#1 Gartner
Marketscope for Wireless LAN
Intrusion Prevention Systems

32+
Patents

1000+ WIPS
Customers

IDC
Marketscape



Confidential. Copyright © Arista 2018. All rights reserved.

ARISTA

פתרון ה-WIPS של ARISTA בא להתמודד עם מספר מצבים שונים של חדירה למרחב האלחוט הארגוני, בין אם מדובר בנקודת גישה אישית בטלפון נייד, בין אם מדובר על ניסיון "חטיפה" של SSID, או שימוש ב-EVIL TWIN.

Top Wi-Fi security threats



חברת NETSKOPE הינה החברה המובילה בעולם בכל הקשור ל-Cloud applications visibility and Protection.

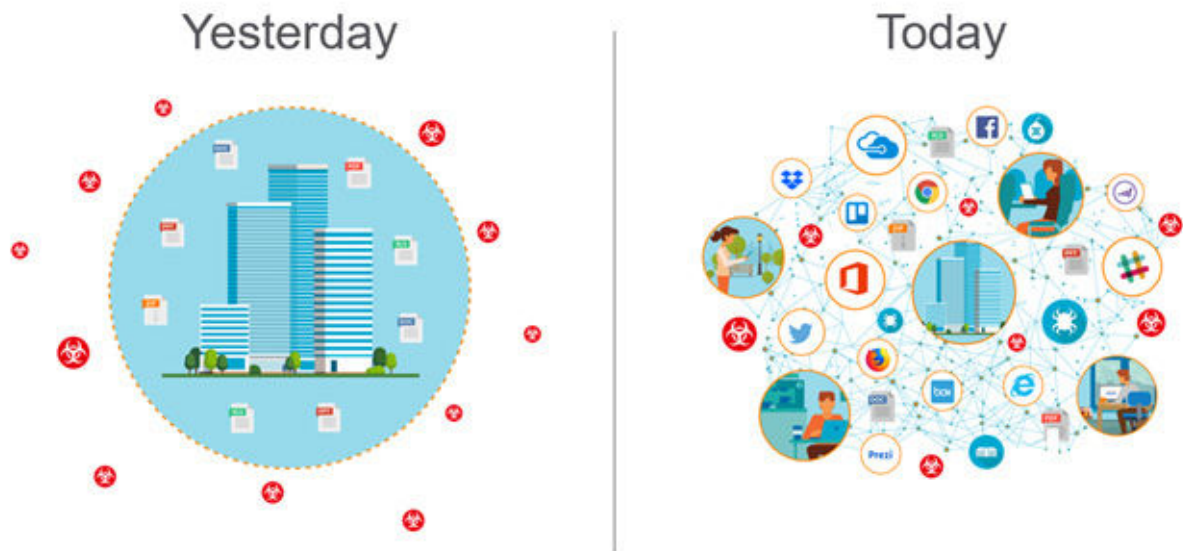
הפתרון של NETSKOPE, מגן כיום על הארגונים הגדולים ביותר בעולם, בכל הקשור לאפליקציות SaaS וה-IaaS.

Figure 1. Magic Quadrant for Cloud Access Security Brokers



הפתרון הייחודי של חברת NETSKOPE, הינו מבוסס על שירות ענן ייחודי, המספק שליטה וניטור של אפליקציות SaaS וכן יודע להתממשק למערכי IaaS של הארגון.

בעבר האפליקציות והמשאבים היו כחלק מהדטה סנטר הארגוני, לרוב בדטה סנטר מרכזי ואתר DR - ואילו כיום, המצב שונה לחלוטין, ולמעשה אנחנו נמצאים בתצורה מבוזרת והיברדית, הן בדטה סנטר בארגון והן שימוש ביישומים רבים בעננים הציבוריים, בין עם מדובר ביישומי Storage, CRM, VOIP, Collaboration וכו'.

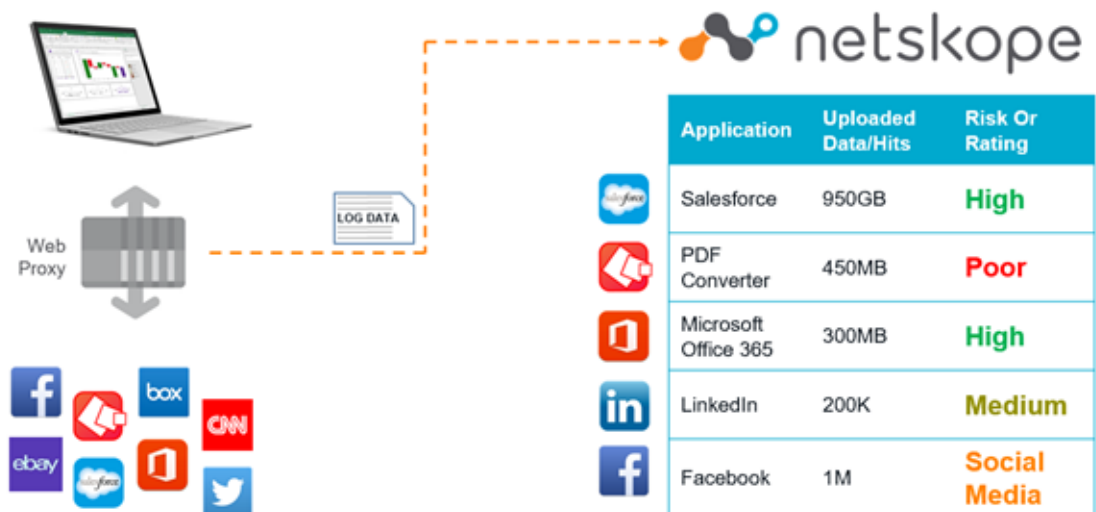


הפתרון של NETSKOPE, כולל יכולות Shadow IT מלאות ומאפשר דגימה של הרשת הקיימת באמצעות לקיחת לוגים ממערך האבטחה הקיים, או לחלופין מתממשק באמצעות: FORWARD PROXY, REVERSE PROXY, API או DNS אל מערך התשתיות בארגון.



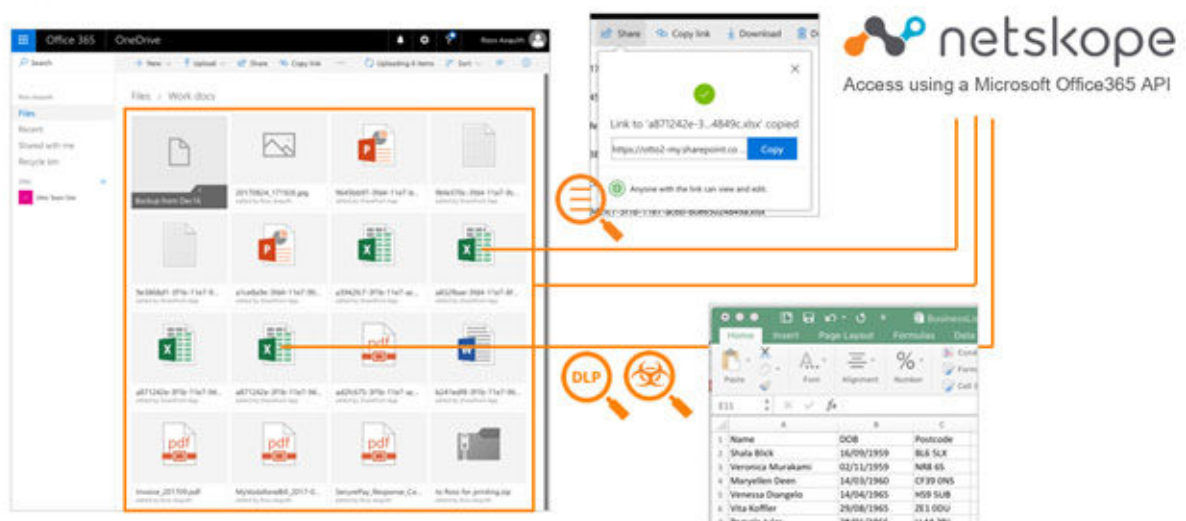
בתחילה מבצעים סקירה של המצב הקיים, ובוחנים אילו אפליקציות ענן בשימוש בארגון, וכן מה ה-RISK שלהם.

1 Understand **which** internet platforms are being used and their **risk**



מבצעים אינטגרציה באמצעות API, לאפליקציות ששומרות מידע רגיש של הארגון, לדוגמא 365, ONE DRIVE וכו'.

2 **Sanctioned or Approved** cloud applications storing or sharing the sensitive data



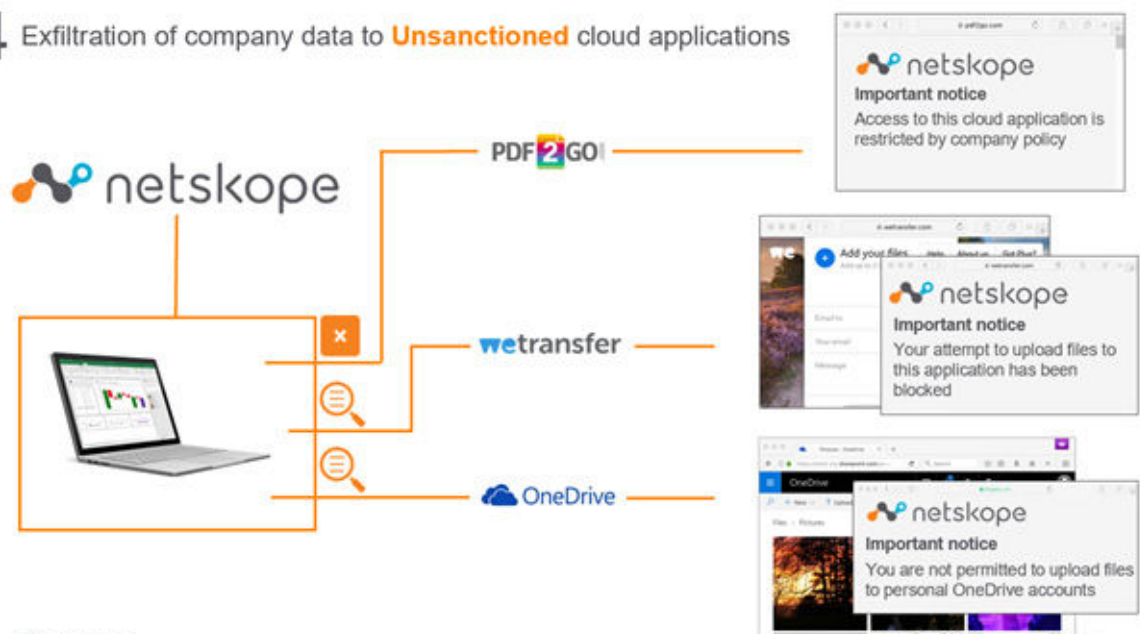
בדיקה של אפליקציות, שאליהן ישנה גישה מהתקנים/מחשבים שאינם מורשים.

3 Sanctioned or Approved cloud applications allowing data to escape to unmanaged devices



ניטור ושליטה על אפליקציות שאינן תואמות את מדיניות האבטחה של הארגון.

4 Exfiltration of company data to Unsanctioned cloud applications



וכמובן שליטה על גישה לאתרים ואפליקציות תוך כדי שימוש במנגנוני סינון מתקדמים, לדוגמא סנדבוקס.

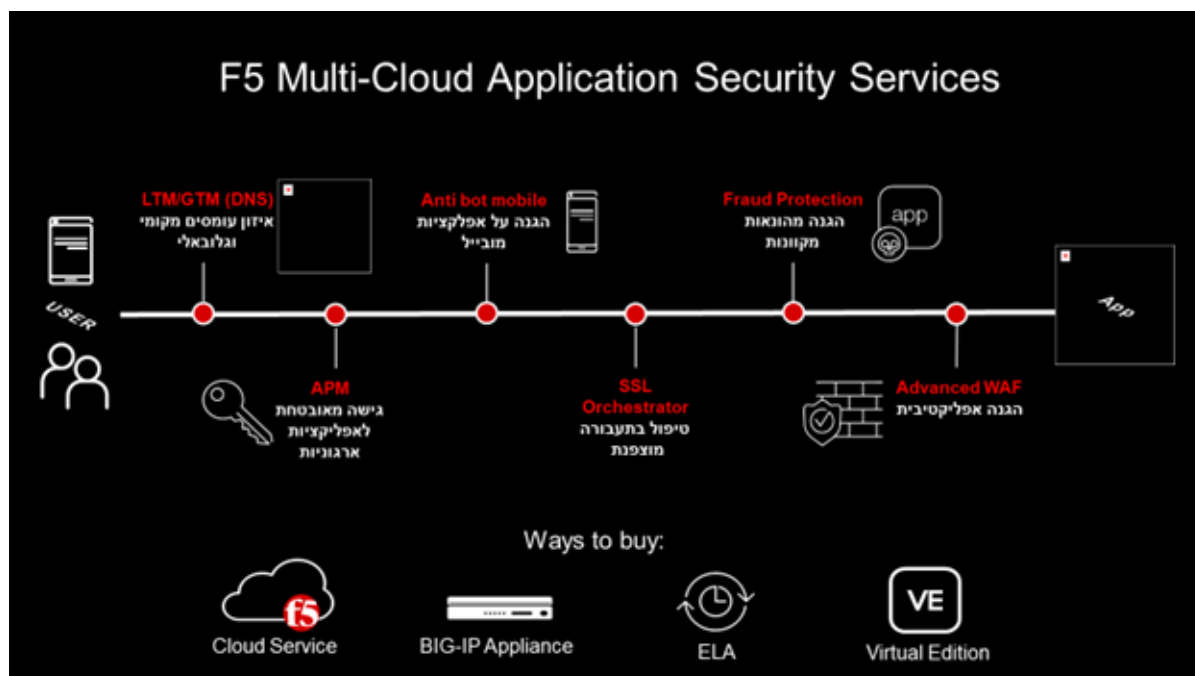
5 Control Access to unwanted **Web** services and **Threats**



חברת F5 הינה המובילה העולמית בכל הקשור להגנה אקטיבית על אפליקציות.

לחברה מספר פתרונות אשר מספקים:

- יכולות של ביזור עומסים אל מול קישורי האינטרנט ואל מול יישומים.
- יכולות של אבטחת גישה לרשת (SSL VPN ו-REVERSE PROXY) באמצעות מודול APM.
- יכולות של הגנה מפני בוטים באמצעות מודול ANTI BOT.
- יכולת מניעת הונאות באמצעות מודול FRAUD DETECTION.
- ניטור ופתיחה של תעבורה מוצפנת באמצעות מודול SSL ORCHESTRATOR.
- וכמובן יכולת הגנה אפליקטיבית על היישומים עצמם באמצעות מודול AWAFF.



המודולים השונים של F5 מוטמעים או כחלק מתשתית ה-IaaS בארגון (AWS, GOOGLE, AZURE) כפלטפורמה וירטואלית VM - או לחלופין על גבי HW APPLIANCE BIG IP - אשר מגיע בגדלים שונים.

Trend Micro היא חברה המובילה בתחום אבטחת IT אשר מפתחת פתרונות אבטחה חדשניים על מנת להפוך את העולם הדיגיטלי לעולם טוב יותר לעסקים. הודות לניסיון וידע נרחב של כמעט 30 שנה.

Trend Micro מוכרת כחברה המובילה באבטחת שרתים, רשתות ושירותי ענן. פתרונות החברה מתאימים לצרכי לקוחות מכל המגזרים מהקטן ועד לארגוני ה-Enterprise.

פתרונות האבטחה של Trend Micro מגובים על ידי Trend Micro™ Smart Protection Network™ global threat intelligence - מאגר מודיעין נרחב ואמין.

למה Trend Micro?

ההסטוריה של Trend Micro מבוססת על חדשנות והשגים טכנולוגיים אשר שינו את מפת עולם אבטחת המידע. משנת 1988 חברת Trend Micro היא חלוצה במספר תחומים - כך למשל TM הייתה ראשונה אשר הרחיבה פתרון להגנת תחנות הקצה לשרתים ומשם - לכניסה לרשת. TM הייתה החברה הראשונה אשר הציעה פתרון אינטגרלי עבור סביבות וירטואליות של VMWare וסביבות ענן של AWS ו-Azure.

בנוסף החברה היתה בין הספקיות הראשונות של פתרונות לזיהוי פרצות רשת (Network Breach Detection). לאחר רכישת פתרון TippingPoint הפכה Trend Micro לחברה מובילה בתחום הגנה רשתית ומוצרי IPS מאפשרים לארגונים לנטר ולחסום התקפות סייבר מתקדמות בזמן אמת.

בנוסף Trend Micro מציעה ללקוחות את הפתרון ההוליסטי המשלב בתוכו את כל רכיבי ההגנה כולל אמצעים לזיהוי התקפות ממוקדות

(APT) כאשר כל המוצרים מנוהלים בצורה מרוכזת והיתרון העיקרי הוא שיתוף הממצאים בין מוצרי Trend Micro המוטמעים בארגון.

לפי דוח של מכון IDC יותר מ- 34% מהשרתים בעולם מוגנים על ידי מערכות ההגנה של Trend Micro. זה הופך את TM לחברה מובילה בעולם בהגנת שרתים לאורך 7 השנים האחרונות.

גם בתחומים אחרים זכתה חברת Trend Micro לציונים גבוהים. למשל, מכון Gartner ממקם אותה כחברה מובילה בתחום של הגנה על תחנות הקצה במשך מספר שנים.



עליונות טכנולוגית של Trend Micro

מערך מודיעין גלובלי החזק בעולם.

רשת (SPN) Smart Protection Network מכילה מידע עדכני על דירוגי אמינות של כל האובייקטים מהם מורכבת רשת האינטרנט העולמית - כתובות IP, שמות דומיין, קישורי URL וקבצים. מאפשר לצמצם מגבלות אשר נוצרו על ידי צורך בשימוש קבצי חתימה ולעצור את תהליך גדילתם. שימוש ב-SPN מאפשר לשפר יכולת זיהוי של אנטייורוס תוך שמירה על ביצועים גבוהים.



רשת SPN מחזיקה מיליארדים של כתובות IP וידע רב על מערך התקפות מתקדמות (APT) אשר קיימות היום. זה מאפשר לבצע קורלציה בין נתוני תעבורת הלקוח ולזהות או לחסום ניסיונות התקפה.

קבוצת Zero Day Initiative (ZDI) היא חלק חשוב ממערך SPN. הודות ל-ZDI מדי שנה נחשפות פגיעויות רבות במערכות ההפעלה ויישומים רבים. זיהוי מוקדם של חולשות מאפשר למנוע התקפות רבות עוד הרבה לפני שיצרני מערכות ההפעלה ויישומים מספקים טלאי לסגירה של פגיעויות האלה.

רשת SPN מחזיקה מידע על מאות אלפי יישומים בעולם כגון: דירוג מוניטין, מעורבות בהפצת איומים, "גיל" ותפוצתם לפי אזורים שונים בעולם. יכולת זאת מאפשרת לנהל בצורה אוטומטית רשימות שחורות של יישומים ומניעת התפרצויות וירוסים, גניבת תוכן וכו'.

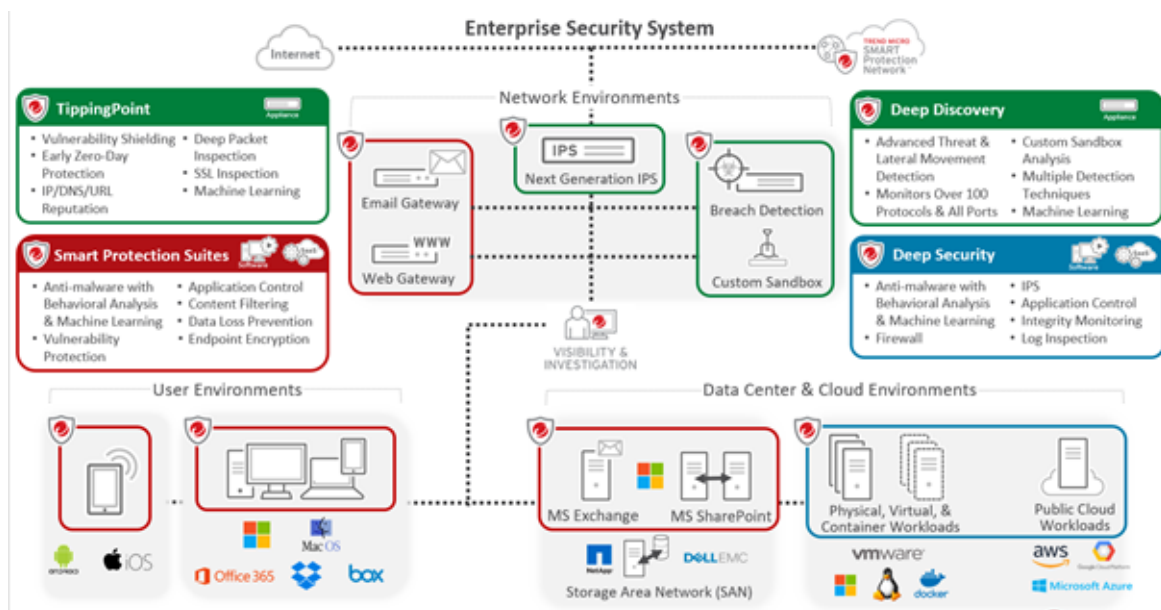


טכנולוגיית XGen

הצורך להתמודד עם איומי Zero Day מעודד את יצרני פתרונות אבטחת המידע לפתח שיטות זיהוי מתקדמות אשר אינן תלויות בקבצי החתימה. שיטות אלו מבוססות על אלגוריתמים מתמטיים ולימוד מכונה - Machine Learning.

טכנולוגיית Xgen של חברת Trend Micro משלבת שיטות המבוססות על קבצי חתימה, דירוגי אמינות, ניטור התנהגותי ולימוד מכונה. שילוב זה מאפשר לצמצם ניצול משאבים גבוה וטעויות זיהוי אשר נגרמים ע"י תהליכי לימוד מכונה. הודות לשימוש בטכניקה נכונה חל שיפור משמעותי בהגנה מפני איומי Zero Day בצורה היעילה ביותר תוך שמירה על ביצועים גבוהים של פתרון.

סל פתרונות של Trend Micro



ניתן לחלק את כל הפתרונות של Trend Micro לשלוש קבוצות מוצרים:

- הגנת משתמש קצה:** לקבוצה זו רכיבי הגנה רבים, הגנה על תחנות הקצה בפני איומים, ניטור התנהגותי ולימוד מכונה, בקרת יישומים, פתרונות למניעת זליגת מידע, ניהול התקנים נתיקים, פיירוול ומערכת להפעלת טלאיים וירטואלים, הצפנת דיסקים, תיקיות וקבצים, כמו כן

גם פתרונות להגנת שרתי MS Exchange ו-SharePoint, מוצרי Gateway (הגנה על תעבורת דואר וגלישה) ומוצר להגנת שרתי אחסון.

2. הגנה על סביבת Data Center היברידי (פיזי, וירטואלי

ומבוססי ענן): מוצר Deep Security משלב טכניקות רבות להגנה על סביבת שרתים, עמידה לדרישות רגולציה וצמצום עלויות ניהול ותחזוקה.

3. הגנה על תעבורת רשת ומניעת התקפות מתקדמות:

קבוצה זו מכילה מוצרים לניטור מתקדם של הרשת הארגונית (סניפר), פלטפורמה להרצת sandbox ומוצרי IPS להגנה רשתית.

כלל המוצרים מתעדכנים על ידי SPN - SMART PROTECTION NETWORK. מערך מודיעין גלובלי של חברת TrendMicro. כל מוצר אשר מכיל יכולת אנטייורוס מסוגל לשלוח אובייקטים חשודים ל-Sandbox ולקבל חתימות מקומיות מייד לאחר זיהוי האיום. בנוסף, המערכת לניהול מרכזי מאפשרת ריכוז ארועים והצגתם בהתאם לצורך, ניהול מרכזי של רב הפתרונות ממסך אחד, עדכון מרכזי ועוד.

Deep Security הינה פלטפורמה אוניברסלית להגנה על סביבות שרתים פיזיים, וירטואליים, מבוססי ענן וסביבות משולבות. הפתרון מאפשר שימוש בהתקנת סוכנים או בתצורה ללא סוכן בהתאם לסביבות הוירטואליות בארגון. DS מאפשר אוטומציה של תהליכים ניהוליים ומצמצם הוצאות של ניהול ותחזוקה.

הפתרון נבנה לצורך אינטגרציה עם הפלטפורמות הבאות: Amazon Web Services (AWS) ו-VMware, Microsoft@Azure הפתרון תומך בטכנולוגיות חדשות של עולם השרתים:

VMware NSX ו-VMware Cloud on AWS הפתרון עובד בסביבות, Citrix Xen Server, Microsoft Hyper-V, OpenStack ואחרים.

פתרון תומך במערכות הפעלה רבות כולל Windows ו-Linux.

עיקר רכיבי פתרון Deep Security:

פתרון Deep Security עבור שרתים מכיל מספר רכיבים וניתן ליישמו בצורה מודולרית בהתאם לצרכי הארגון:

• רכיב להגנה רשתית

- רכיב מאפשר ביצוע של Virtual Patching. מזהה חולשות במערכות הפעלה, שירותי WEB, בסיסי נתונים ותוכנות רבות.
- רכיב מבצע הטמעה אוטומטית של חוקי CVE בהתאם לצורך של כל שרת בזמן בנקודת זמן מסוימת.
- רכיב מספק יכולת Firewall מתקדם המאפשר מידור בין סביבות שרתים שונים.

• רכיב Antimalware

- רכיב מבוסס על טכנולוגיית XGen לזיהוי וחסירה של איומים מתקדמים.
- רכיב מאפשר שימוש בטכנולוגיות File/Web Reputation.
- רכיב מאפשר שליחת קבצים חשודים למערכת sandbox.

• רכיב Integrity Monitoring

- רכיב מאפשר ניטור שינויים אשר מתבצעים ברמה של כל רכיב במערכת ההפעלה קובץ, תיקיה, שירות, תהליך, ערך Registry וכו'.

• רכיב Application Control

- מאפשר ניהול רשימות שחורות/לבנות של תוכנות ויישומים.



פתרון DEEP DISCOVERY

Deep Discovery Analyzer

- יכולת איתור וחסימת התקפות מדוייקת וגבוהה (לפי מבדק ICSA 2016 - Detection rates 99.5%).
- איתור ניסיונות התחמקות ומניעתם.
- זמן תגובה מהיר בהרצת קבצים - **2800 קבצים לשעה**.
- קסטומיזציה של המערכת לפי האימג' הארגוני.
- קורלציה מול מאגר נתונים "מודיעין סייבר".
- שיתוף ממצאים עם מערכות צד ג'.
- ממשק API פתוח המאפשר חיבור למערכות חיצוניות.

Deep Discovery Network Inspection

- זיהוי Lateral movement.
- איתור התקפות וניטור ערוץ הגלישה לרשת האינטרנט.
- תמיכה בלמעלה מ- 100 פרוטוקולי תקשורת.
- זיהוי אנומליה ברמת הרשת.
- זיהוי התקפות במערכות Windows, Mac OS X, Android, Linux ובכל מערכת אחרת.
- שיתוף מידע (IOC) עם מערכות צד ג'.



פתרון נראות רשת גיגמון - דגשים עיקריים על אפליקציות.

גיגמון הנה מובילת השוק, עם נתוני מכירות כפולים מהמתחרה הקרוב ביותר שלה, ועם קצב גידול מהיר פי שלושה, וזאת בזכות מיקוד בתחום אחד והצטיינות בו.

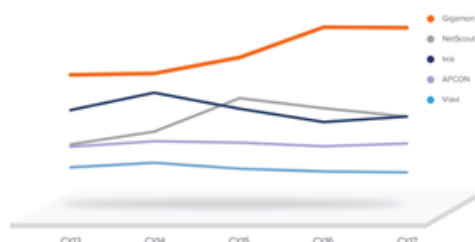
חברת גיגמון מספקת את פתרון נראות הרשת המוכח ביותר, המקיף ביותר, העמוק ביותר והגמיש ביותר שקיים בתחום, תוך דגש על החזר השקעה גבוה והוספת יכולות בלתי פוסקת לשימור המעמד כמובילים טכנולוגיים. בשנתיים האחרונות בלבד הוצגו למעלה מ- 300 תכונות חדשות המוטמעות על ידי לקוחות החברה, לרבות מערכת ניהול מרכזית, יכולת שרשור, זמינות תכונות מתקדמות על cluster מלא, תמיכה במערך הווירטואלי המוסמך ע"י VMware ב- NSX ויכולת פתיחת תעבורה מוצפנת Inline SSL. הדבר מתורגם להצעה בעלת הערך הגבוה ביותר עבור ארגונים ועבור 80% מלקוחות ה- Fortune 100 הנמנים על לקוחות החברה. בישראל הגידול הינו ביחס דומה עם רצף זכיות משמעותיות בכלל המגזרים, לרבות ביטחון וצבא. האמון בחברה מתקבל מהשוק ואת הביטוי לנ"ל ניתן להמחיש בביצועי החברה, יוצאי הדופן בכל קנה מידה, ובמיוחד אל מול התחרות.

#1 Market Leader in Network Visibility for Five Years

IHS Markit: Gigamon is the 2017 Market Share Leader



IHS Markit



“Gigamon is the largest vendor in the space, accounting for 37% of revenue in CY17 and is 21 points ahead of the next closest competitor.”

37% overall market share in 2017

2x our closest competitor

37% enterprise market share in 2017

2.5x our closest competitor

61% government market share

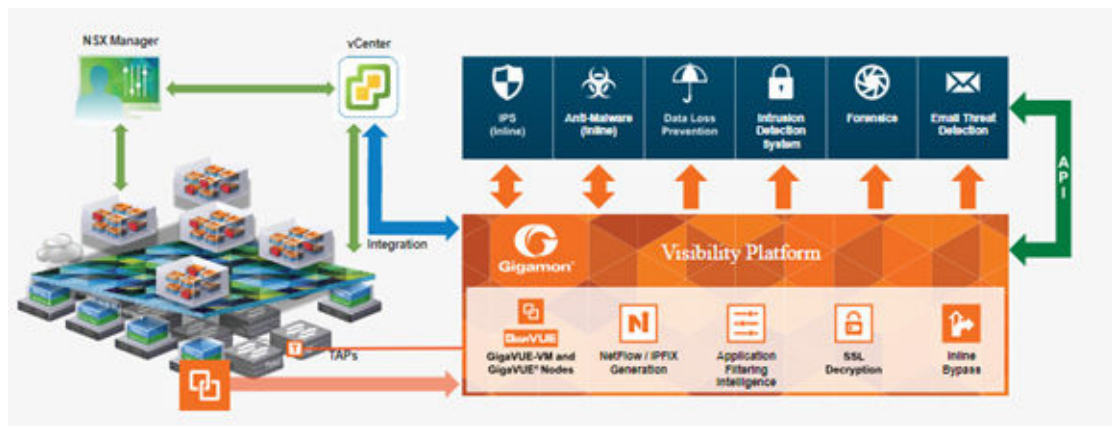
4x our closest competitor

Get a copy of the IHS report [here](#).

Source: IHS Markit: Network Monitoring Equipment Annual Market Report, June 22, 2018 by Matthias Machowinski

להלן מספר יתרונות ייחודיים בפתרון:

1. מערכת ניהול מרכזית לניהול מערך כלי נראות הרשת הן לרכיבים ברשת הפיזית והן לפתרון בסביבות הווירטואליות, למערכת הניהול יכולת לספק את התכונות הבאות הנדרשות בפרויקט:
 - מסך מרכזי להגדרת מערך נראות הרשת על גבי מכונות בודדות ו/או מערך של מכונות המוגדרות בקלאסטר.
 - יכולת מונחת ליצירת קונפיגורציה בעלת תכונות מתקדמות.
 - מערך לוגים והתראות מרכזי על כלל הרכיבים.
 - גיבויים מתוזמנים, המערכת מספקת יכולת גיבוי ושחזור להגדרות מערכת וקונפיגורציה.
 - יכולת עדכוני תוכנה מרכזית ממערכת הניהול על כלל רכיבי הפתרון.
 - יצירת לוג למעקב אחר ביצוע ושינויים פעולות במערכת.
 - מערך ניהול משתמשים וקבוצות לפי הרשאות כולל התחברות לשרתי הזדהות צד שלישי כגון: Radius, Tacacs, AAA & LDAP.
 - יכולת ממשק מול רכיבים צד שלישי ע"י RestAPI מרכזי, שאר היצרנים מאפשרים חיבור מול מכונה בודדת ולא בצורה מרכזית.
 - ניהול רישיונות.
2. תמיכה מלאה להגדרות המערכת ב- CLI וב- GUI.
3. יצירת מערך קלאסטר של כל המכונות כולל מכונת מאסטר ומכונת גיבוי לקלאסטר במידה והראשית נופלת. במערך ניתן לשלב מכונות בסיסיות ומכונות מתקדמות.
4. שימוש במנוע ה- L7 filtering ביותר מפילטר אחד, אף יצרן אינו תומך ביכולת הזאת מלבד גיגמון. התכונה מאפשרת ניצול יעיל יותר של משאבי המכונה וחיסכון בכמות המכונות הנדרשות.
5. תמיכה רשמית בפתרון של VMware ESXi & NSX. גיגמון היחידים שמצוינים באתר של VMware כפתרון נתמך.
6. יכולת יצירת Tunnel בין מכונות, תכונה המאפשרת להעביר תעבורה מאתר אחד לשני עבור תחקור אירועים.



7. שיטת הרישוי בגיגמון מאפשרת למכונות לעבוד גם אם חידוש התחזוקה פג תוקף.
8. מוצרי אגריגציה בעלי פורטים מרובים לרשתות של 10 גיגה, 40 גיגה ו- 100 גיגה. גמישות המאפשרת גידול עתידי וחיבורם למערך נראות הרשת.
9. שימוש ביכולות המתקדמות על גבי כל המכונות בקלאסטר ולא רק במכונה הראשית. בגיגמון ניתן להשתמש במשאב ה- GigaSMART על גבי כל המכונות השותפות במערך קלאסטר.
10. יכולת פתיחת תעבורה מוצפנת ב- Out of Band וגם ב- MiTM Inline. הנושא הוכרז בכנס RSA בפברואר 2017 ומהווה פריצת דרך טכנולוגית בשכבת נראות הרשת. יחד עם שילוב ממשקי Bypass במכונות, המאפשרים הכנסת כלים ב- Inline, ניתן לבצע שרשור שירותים עבור תעבורה מסוגים שונים ולקבל ערך אמיתי וגמישות רבה בהטמעתם.
11. תמיכה בתשתית ענן ציבורי הוכרזה גם היא לאחרונה, בכנס Amazon re:Invent בדצמבר 2016, ומאפשרת ללקוחות המעבירים שירותים ל- AWS לנטר את המידע. כך גם ב- **AZURE** ו- **GOOGLE CLOUD**.
12. ייצור רשומות Netflow, על מידע מלא ו/או סטטיסטי, המועשרים בערכים אפליקטיביים (IPFIX) ויצוא למספר מערכות ניתוח ייעודיות במקביל. כגון: Q-Radar, Plixer, Splunk, Lancope וכיו"ב.

DANET

COMMUNICATIONS



Driving your business evolution

טלפון: 074-7016070

אימייל: Office@danetcomm.co.il | **אתר:** www.danetcomm.co.il

כתובתנו: אלקטרה סיטי קומה 3 | הרכבת 58, תל אביב 6777016