

פתרונות אבטחת מידע לאפליקציות ארגוניות מרמת הקוד עד רמת הלקוח.

BIG IP

פלטפורמה להגנה והנגשת אפליקציות Web באופן מאובטח ומהיר. אפשרויות פריסה: On Prem, בענן וכשירות SaaS

עומס משתמשים באפליקציה/שרתים פוגע בחוויית המשתמש וגוזל משאבים.



Local Traffic Manger (LTM)

פתרון לאיזון עומסים חכם לרשתות פנימיות וחיצוניות במגוון פרוטוקולים, כולל טיפול ב SSL ואופטימיזציה של תעבורה לשרתים. ה LTM מספק זמינות מלאה של האפליקציות, האצת ביצועים לאפליקציות נבחרות, תוך שיפור חוויית המשתמש, באמצעות שימוש בממשק ניהול חכם ומתקדם. גישת משתמשים מחוץ לארגון חייבת להיות מאובטחת על מנת לשמור על נכסי הארגון וההמשכיות העסקית.

Access Policy Manager (APM)



פתרון עבור גישה מאובטחת ומהירה לרשת ולאפליקציות של הארגון (SSL VPN) מכל מקום ובכל עת. ה APM מספק גישה מיידית מבוססת מדיניות (Policy) ומאפשר תהליך אימות יחיד (SSO), רב שלבי (MFA) וכן אפשרות לחולל סיסמה חד פעמית (OTP). הפתרון עובד בתצורת Clientless, ומספק חיבור מרחוק מהדפדפן באמצעות פורטל יעודי מותאם אישית.

מתקפות אפליקטיביות עלולות לשבש את פעילות הארגון ואף להביא לעצירת הפעילות העסקית.

Web Application Firewall Advanced (AWAF)



הגנה מתקדמת על שרתי אפליקציות וממשקי API. ה AWAF מגן מפני תקיפות ווליומטריות, DDoS ב Layer 7 תקיפות ע"י בוטים, שליפת מידע, גישה למסדי נתונים, גניבת תעודות (Certificate), הגנה בפני סיכוני OWASP TOP10 ומתקפות Zero day. ה AWAF מקנה יכולת לבצע עדכון אבטחתי ממקום אחד לסוגים שונים של CVE's עם מנגנוני למידה מתקדמים.

NGINX

פתרונות מתקדמים לניהול אפליקציות בסביבת Kubernetes

המעבר לפיתוח אפליקציות בסביבת ענן מציב אתגר מרכזי בפני ארגונים שצריכים למצוא את האיזון בין גמישות אפליקטיבית והצורך בסביבה מאובטחת. באמצעות כלי אוטומציה, ויזביליות וניהול יכולים צוותי אבטחת המידע וצוותי הפיתוח להנות מפתרון הוליסטי המאפשר גמישות מקסימלית עבור אפליקציות מסורתיות ומודרניות.

NGINX Plus



תשתית פיתוח אפליקציות מודרנית המספקת יכולות מורחבות של איזון עומסים, High availability, Caching ופתרונות אבטחה מתקדמים נוספים. ה NGINX Plus מפשט את הארכיטקטורה ומספק הגנה הוליסטית לאפליקציות וממשקי API באופן מהיר ויעיל תוך שמירה על מדיניות אבטחת המידע של הארגון. ה NGINX Plus מספק יכולות תכנות מתקדמות, Streaming media והתממשקות למודולי צד שלישי של מגוון יצרנים. הפתרון כולל תמיכה טכנית ומסחרית כדי למקסם את יכולות המוצר.

API Gateway



פתרון המציע ממשקים רבים לתכנות, הרצת סקריפטים וביצוע מניפולציות על תעבורת נתונים בזמן אמת. רכיב מרכזי המנתב תעבורת API לשירות המתאים, מפעיל מנגנוני הזדהות ואבטחת מידע מתקדמים על ממשקי API.

Ingress Controller



פתרונות עבור שירותים בסביבת Kubernetes:

- אבטחה מובנית להגנה מפני איומי סייבר ברחבי ה Cluster.
- יכולות מתקדמות של ניתוב מבוסס תוכן.
- בקרת משאבים וייעול תעבורה ברשת (בשכבות 4-7).

בנוסף, ה Ingress Controller מספק יכולות איזון עומסים עבור סביבת Kubernetes, הפצת שירותים וניתוב תעבורת משתמשים ל pod המתאים.

F5 Distributed Cloud (xc)

Multi Cloud Networking



פתרון הוליסטי בענן - הדרך המהירה והבטוחה ביותר לאספקת אפליקציות בפריסה רחבה, מאובטחת, מהירה וזמינה - על פני Multi Cloud | Edge.

הפלטפורמה מבוססת SaaS ומספקת תשתית בעלת ביצועים גבוהים ואבטחה ברמת Zero-Trust. ממשק ניהול אחיד, מאפשר ניהול Policy ברמת אפליקציות ומשתמשים על פני כל ה Deployments בעננים השונים.

באמצעות ה Multi Cloud Networking צוותי הפיתוח יכולים להעביר בצורה חלקה עומסי עבודה בין עננים | Data Centers ללא יישום או עיבוד מחדש, יכולת זו מאפשרת גמישות בפריסה וביצועים ברמה גבוהה.

ה Multi Cloud הינו פתרון חדשני לאספקת יישומים אדפטיביים המאפשר לארגון:

- צמצום המורכבות והעלויות (TCO) התפעולית: הקלה על הפריסה, הרחבה ותחזוקה של רכיבים ושירותים קריטיים ברשת האפליקציות
- ביצועי משתמש קצה טובים יותר
- אבטחה רובסטית בשכבות L3-L7 כולל בקרת גישה
- שירות מהיר יותר המשפר את Time To Value: יותר תוצאות בפחות זמן ומאמץ וכן את ה Time to market.

WAAP



פתרון ה-(WAAP) Distributed Cloud Web Application and API Protection של F5 מספק אבטחה מקיפה מבוססת SaaS עבור כל יישומי האינטרנט והנייד שלך - לא משנה היכן הם נפרסים.

הפתרון מספק לארגון:

- WAF
- Fire wall אפליקטיבי
- API SECURITY הגנה על ממשקי API
- API DISCOVERY מיפוי של ממשקי API
- BOT DEFENSE הגנה פרואקטיבית כנגד בוטים זדוניים
- DDOS L7 הגנה כנגד מניעת שירות בשכבה האפליקטיבית

64% מתעבורת האינטרנט הינה תעבורת בוטים, 39% מתוך תעבורה זו הינם בוטים רעים. כדי לשמור על המידע של הארגון והמשתמשים, יש צורך במערך זיהוי והגנה מפני הונאות ופעילות עוינת.

Bot Defense

פתרון מקיף לאבטחת אפליקציות, משלב יכולות A.I רבות עוצמה לטובת מניעת הונאות. **BOT Defense** מונע התקפות של בוטים, הונאות ידניות/אוטומטיות, ניצול לרעה ועוד, במטרה למנוע נזק למוניטין של הארגון ו/או שיבוש החוויה הדיגיטלית של המשתמשים.

Bot Defense עונה על 3 שאלות מרכזיות:

- האם המשתמש הוא אדם או מכונה?
- האם המשתמש הוא טוב או רע?
- האם המשתמש עושה מה שהוא טוען שהוא עושה?

BOT Defense מבטל את הצורך להזדהות מספר פעמים, הוא מונע שבירה של האפליקציה ע"י מנגנונים כמו MFA | CAPCHA ע"י כך שהוא עושה זאת באמצעות מנגנונים פשוטים (ה SHAPE מעבד ברקע מאות אלפי סגנלים בצורה השקופה למשתמש ולפי התוצאה הוא מקבל החלטה אם התעבורה תקינה או לא).

DDOS L3/L4



שירות מיתוג מנוהל בענן, שמזדהה ומקל על התקפות רשת, **SSL** והתקפות ממוקדות יישומים בקנה מידה גדול בזמן אמת.

DDOS L3/L4 שומר על העסק שלך מקוון במהלך התקפת **DDoS** ואף יודע למנוע התקפות לפני שהן משפיעות על הרשת והיישומים שלך עם זיהוי בזמן אמת והפחתת התקפות בענן.

DDOS L3/L4 יעזור לך לשפר את היעילות התפעולית בארגון שלך ע"י צמצום הזמן המושקע בתגובה 'ידנית' להתקפות ברשת.

Gain Rich Threat Insights



קונסולה מרכזית המספקת נראות ודיווח שקוף להפחתת התקפות לפני, במהלך ואחרי התקפה להגברת המודעות למצב. בנוסף הקונסולה תסייע בצמצום עלויות תפעול באמצעות הפחתת תעבורה לא רצויה/זדונית ומקלה על עומס על תשתית קריטית וצריכת רוחב פס/עלויות תשתית.