radware

RADWARE WAF

WEB APPLICATION FIREWALL

SHARE THIS BROCHURE

APPLICATION SECURITY – THE FULL STORY

ADVANCED THREATS GO BEYOND THE OWASP TOP 10 TO DISRUPT APPLICATIONS AND STEAL DATA

CHALLENGES OF KEEPING MODERN APPLICATIONS SECURE

Modern applications are difficult to secure. Whether they are custom developed and housed on-premise or cloud based, applications are now scattered across different platforms and frameworks. All applications require updating and must comply with information security policies. In addition, they rely on the availability of information from third-party services which they interact with via APIs. As a result, the attack surface targeting applications is greater, and their exposure to risk is increasing. Lastly, applications constantly change, and security policies must adopt accordingly. Applications must be protected against an expanding variety of attack methods and must be able to make educated decisions in real time to mitigate automated attacks. The result is increased manual labor and operational costs to safeguard applications and the data they host.

RADWARE APPLICATION SECURITY TECHNOLOGY OVERVIEW

AppWall, Radware's web application firewall (WAF), ensures fast and secure delivery of mission-critical web applications for corporate networks and in the cloud. Recommended by NSS Labs, AppWall is an ICSA Labs-certified and PCI-compliant WAF that combines positive and negative security models to provide complete protection against web application attacks, web application attacks behind CDNs, API manipulations, advanced HTTP attacks (Slowloris, dynamic floods), Brute Force attacks on login pages and more.

AppWall is an integrated component of Radware's attack mitigation solution. Machine-learning algorithms create and maintain security policies in real time to provide comprehensive security coverage without generating false positives. Advanced automation capabilities facilitate onboarding of new application services. Radware's WAF technology features a variety of deployment modes, including as a stand-alone deployment or integrated as part of an ADC.

FUNDAMENTAL APPLICATION PROTECTION

The OWASP Top 10 list provides a starting point for ensuring protection from the most common and virulent threats, application misconfigurations that can lead to vulnerabilities, and detection tactics and mitigations. This list serves as an industry benchmark for the application security community and defines the basic capabilities required from a WAF. In addition, there are other common attacks against web applications like CSRF, clickjacking, web scraping and file inclusions (RFI/LFI).

OWASP TOP 10 – 2013	OWASP TOP 10 – 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication
A3 – Cross-Site Scripting (XSS)	A3 – Sensitive Data Exposure
A4 – Insecure Direct Object References **[Merged + A7]**	A4 – XML External Entities (XXE) **[NEW]**
A5 – Security Misconfiguration	A5 – Broken Access Control **[MERGED]**
A6 – Sensitive Data Exposure	A6 – Security Misconfiguration
A7 – Missing Function Level Access Control **[Merged + A4]**	A7 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Insecure Deserialization **[NEW, COMMUNITY]**
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Insufficient Logging & Monitoring **[NEW, COMMUNITY]**

Source: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

However, new technologies and frameworks bring new challenges to the application life cycle. This includes DevOps, containers, the internet of things (IoT), open-source tools, APIs and others.

CHALLENGE 1: BOT MANAGEMENT

According to Radware's web application security report, almost 60% of internet traffic is bot generated, half of which is attributed to "bad" bots. Organizations are forced to increase network capacity to accommodate this malicious traffic. Therefore, they must be able to make an accurate distinction between human traffic and bot-based traffic. They must also distinguish between "good" bots (like search engines and price-comparison services) and "bad" bots. Bots can mimic human behavior and bypass CAPTCHA and other challenges. In addition, dynamic IP attacks render IP-based protection ineffective.

Radware's WAF features advanced device fingerprinting algorithms to identify a web tool's entity via a combination of the operating system and the browser's attributes. Uniquely identifying each source allows tracking activity over time and the ability to manage flexible violation scoring to distinguish between "good" and "bad" bots. Correlating the source's violations across different sessions yields high detection accuracy and minimum false positives.

"BOTS DYNAMICALLY CHANGING SOURCE IP HAVE BEEN ACTING AS FAUX BUYERS SCRAPING FLIGHT INFORMATION FROM OUR E-COMMERCE PLATFORM, IMMEDIATELY CAUSING REVENUE LOSSES. RADWARE WAF FINGERPRINTING TECHNOLOGY MITIGATED THE ATTACKS AND HELPED US MAKE A DISTINCTION BETWEEN ATTACKERS AND LEGITIMATE PRICING SCRAPERS."

PROJECT ARCHITECT, MAJOR U.S. AIRLINE

CHALLENGE 2: SECURING APIs

Many applications gather information and data from services with which they interact via APIs. When transferring sensitive data via APIs, more than 50% of organizations neither inspect nor protect APIs to detect cyberattacks. Common APIs are IoT integration, machine-to-machine communication, serverless environments, mobile applications and event-driven applications. Threats to API vulnerabilities can include injections, protocol attacks, parameter manipulations, invalidated redirects and bot-based attacks. Radware's API security controls include HTTP parsing, Layer 7 ACL management, parsing and validation of JSON/XML payload and schema enforcement and full coverage of the OWASP Top 10 vulnerabilities. This is accomplished by extracting and inspecting key API values using both positive and negative security models.

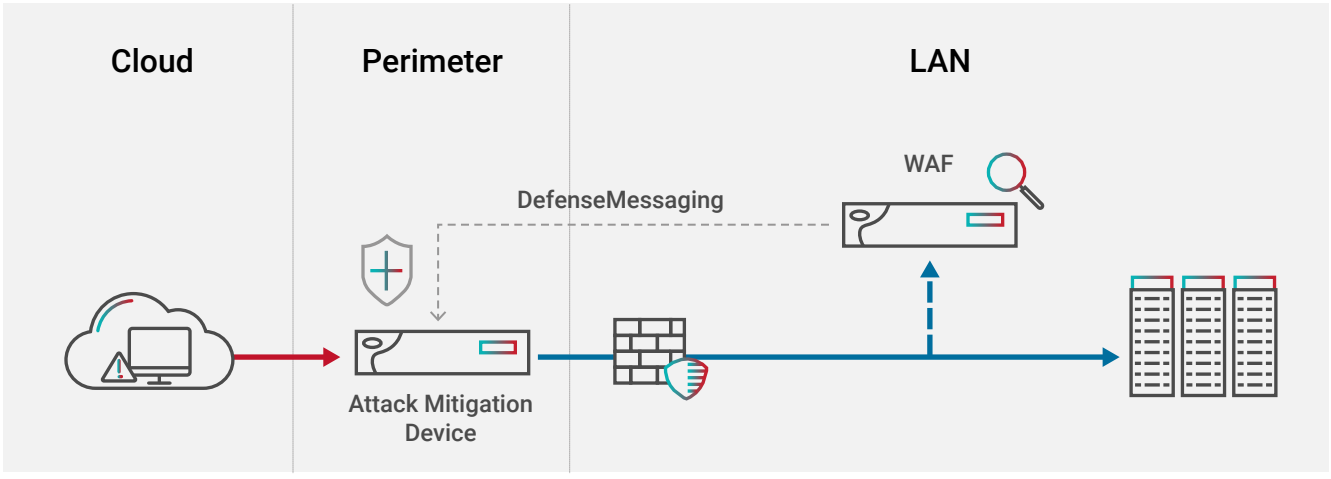
"LOW AND SLOW ATTACKS CONSTANTLY DISRUPTED THE AVAILABILITY OF OUR SERVICE. WITH RADWARE'S ATTACK MITIGATION SERVICE, WE WERE ABLE TO CREATE A DEFENSE ARCHITECTURE WITH PREDEFINED MITIGATION WORK-FLOWS AND NO PERFORMANCE IMPACT."

SR. SECURITY ENGINEER, GLOBAL SAAS

CHALLENGE 3: DENIAL OF SERVICE

DoS is an older attack vector which is still very efficient at attacking applications. There are different forms of application-layer DoS attacks, including HTTP/S floods, low and slow attacks (Slowloris, LOIC, Torshammer), dynamic IP attacks, buffer overflow, Brute Force attacks and more. Driven by IoT botnets, application-layer attacks have become the preferred DDoS attack vector.

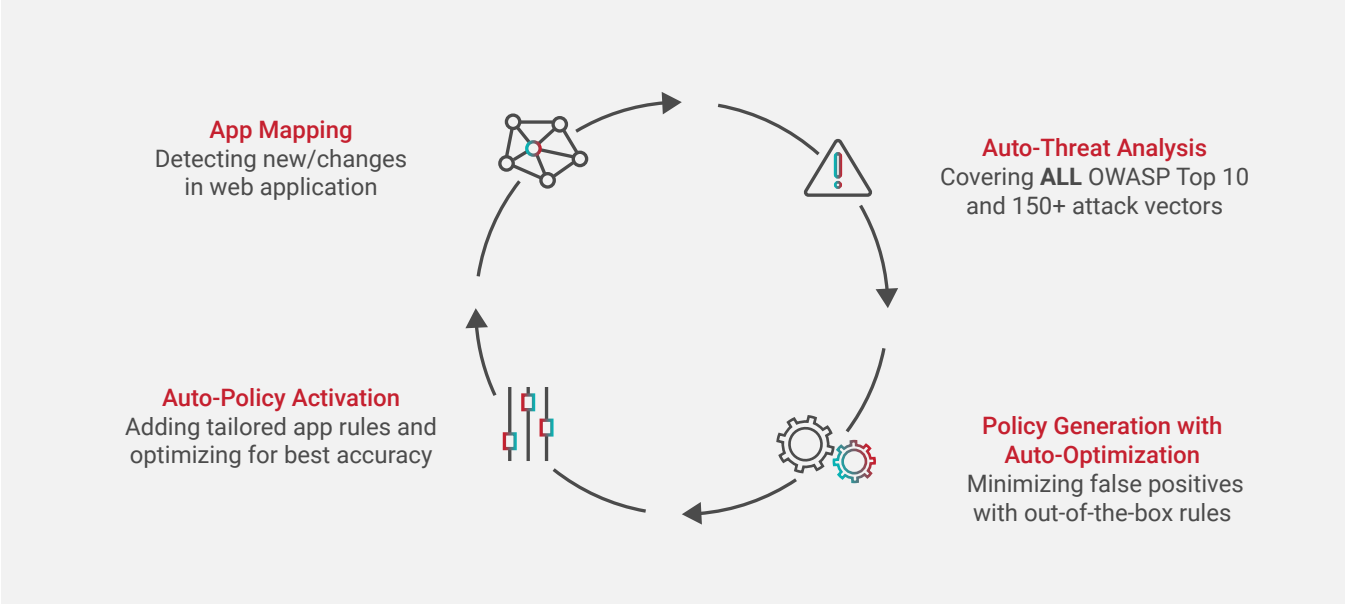
As part of an integrated attack mitigation system, AppWall can detect a web application attack and signal it to DefensePro, Radware's DDoS mitigation appliance, using DefenseMessaging, a unique signaling mechanism for unmatched mitigation capabilities (up to 400Gbps, 330M DDoS PPS at 60 microseconds of latency).



Radware's WAF signals attack information to the perimeter attack mitigation device

CHALLENGE 4: CONTINUOUS SECURITY

Applications change frequently. Development and rollout methodologies, such as continuous delivery, mean applications are continuously modified. It is extremely difficult to maintain a valid security policy to safeguard sensitive data in dynamic conditions without creating a high number of false positives. AppWall leverages machine-learning capabilities that map application resources, analyze possible threats and create and optimize security policies based on application changes (see image below).



AppWall continuously detects changes in the application and user behavior to keep protection updated

SUMMARY

Radware AppWall provides adaptive, real-time protection against the most sophisticated threats that target applications. Machine-learning algorithms update security policies automatically to safeguard applications without generating false positives. AppWall is available in multiple deployment models, including on-premise, virtual or as a cloud service, and can be deployed as a stand-alone solution or integrated either in-line or out of path. Radware's Cloud WAF Service is available to organizations that want a WAF service that is fully managed by application security experts. Radware's Cloud WAF Service is based on the same technology and provides the same robust security for cloud applications.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance and on-site support. Radware also has dedicated engineering staff members who can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery and security solutions can enable you to get the most from your business and IT investments, email us at info@radware.com or go to www.radware.com.