AppWall – More Than Just a WAF

As cyberattacks and mitigation techniques continue to evolve, enterprises need to be on alert and keep time to protection as short as possible.

Enterprises are migrating business-critical functions to web applications in an effort to increase productivity, improve business agility and reduce costs. Furthermore, APIs allow applications to interoperate with other services and save development time. While the migration to web applications provides economic advantages and enables increased business agility, it also creates new security risks and compliance requirements that need to be addressed. The complexity of attacks and blind spots created due to dispersed networks make traditional solutions obsolete and call for a more robust and comprehensive solution that provides faster protection and reduced maintenance costs.

By targeting the application layer, attackers steal sensitive data or exhaust server and application resources using stealth attack techniques that go undetected by traditional security tools. Advanced methods exploit application and API vulnerabilities that present new challenges to web application firewalls (WAFs) in securing an organization.

AppWall – Advanced Web Application Security

AppWall, Radware's WAF, ensures fast, reliable and secure delivery of mission-critical web applications and APIs. AppWall is an NSS labs recommended, ICSA Labs certified and PCI compliant WAF that provides complete protection against attacks targeting web applications and APIs, access violations, injections, attacks disguised behind CDNs, advanced HTTP/S attacks (slowloris, dynamic floods), brute force attacks on login pages and more.

AppWall provides complete web application and API security, combining both negative and positive security models. It blocks attacks at the perimeter and ensures fast, reliable and secure application development and delivery.

Comprehensive and Accurate Security Coverage

AppWall delivers comprehensive and accurate security coverage of known and unknown web application threats. It provides full security coverage out-of-the-box of OWASP Top-10 threats, including injections, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication, leakage of sensitive information and session management. It offers security coverage for additional attacks and threats beyond the OWASP Top-10 list such as Web Application Security Consortium (WASC) threats.

In addition, Appwall protects APIs from targeted attacks such as parameter & token manipulations, invalid schemas, various forms of data leakage and more.

AppWall terminates TCP connections and normalizes client encoded traffic to block various evasion techniques and guarantees that out of the box negative security is much more efficient, accurate and difficult to evade.

Automated Protection from Zero-Day Web Attacks

The best security coverage with minimal impact on legitimate traffic is made possible by Radware's combination of negative (defining what is forbidden and accepting the rest) and positive security models (defining what is allowed and rejecting the rest). Combining the two models allow granular and accurate policy definitions, therefore avoiding false positives and false negatives.

By using both negative and positive security models - AppWall features not only the lowest false positives and minimal operational effort, but also robust protection against known and unknown (Zero-day) threats.

Leveraging Machine-Learning Algorithms for Auto Policy Generation

AppWall incorporates machine-learning algorithms to keep Web assets protected always, even while applications constantly change and threats rapidly evolve, assuring web security is future proof. AppWall's unique auto policy generation mechanism provides the best tool for automatically generating security policy for the protected web application and APIs.

The auto policy generation module will automatically utilize the required security filter, create security filter rules and switch the security filters into active mode. These operations would normally require many manual refinements.

By leveraging machine-learning algorithms, auto policy generation is designed to secure a web application as automatically as possible with little or limited user interaction and offers the following benefits:

- Shortest time to protection, requiring only one week for known attacks – **50% faster than other leading WAFs**
- Best security coverage by performing auto threat analysis, with no admin intervention – **covering over 150 attack vectors**
- Lowest false-positives achieved through auto-optimization of out-of-the-box rules – **close to zero false positives**
- Automatic detection of web application changes assuring security throughout the application's development lifecycle – **post deployment peace of mind**

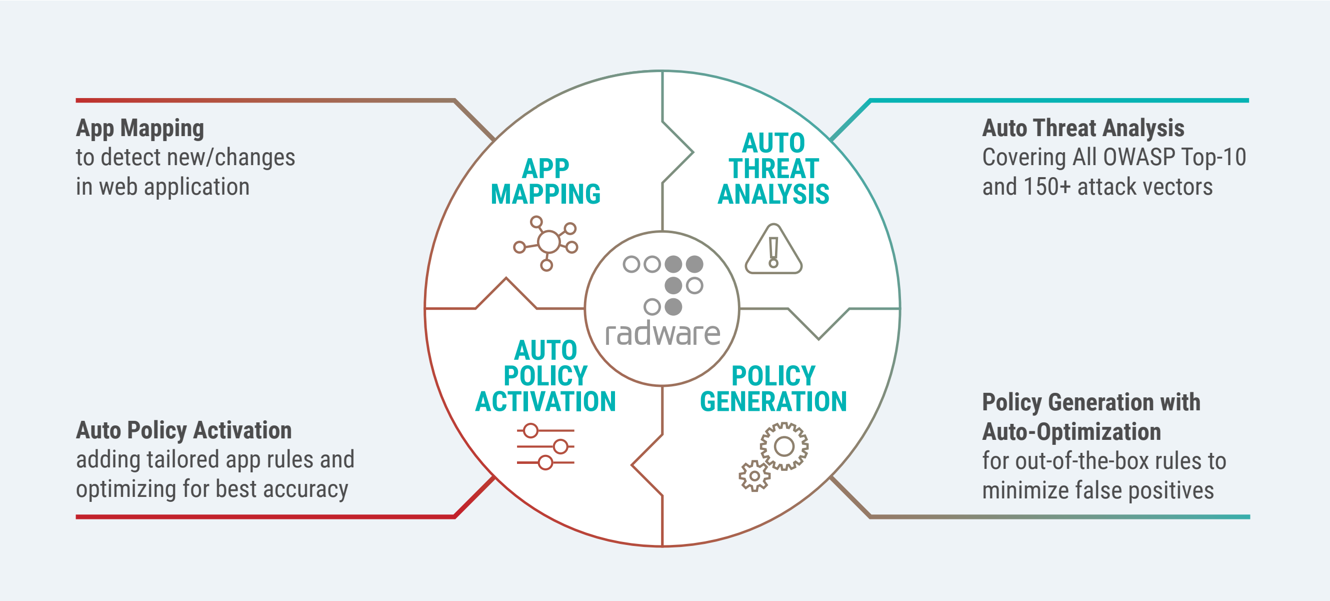
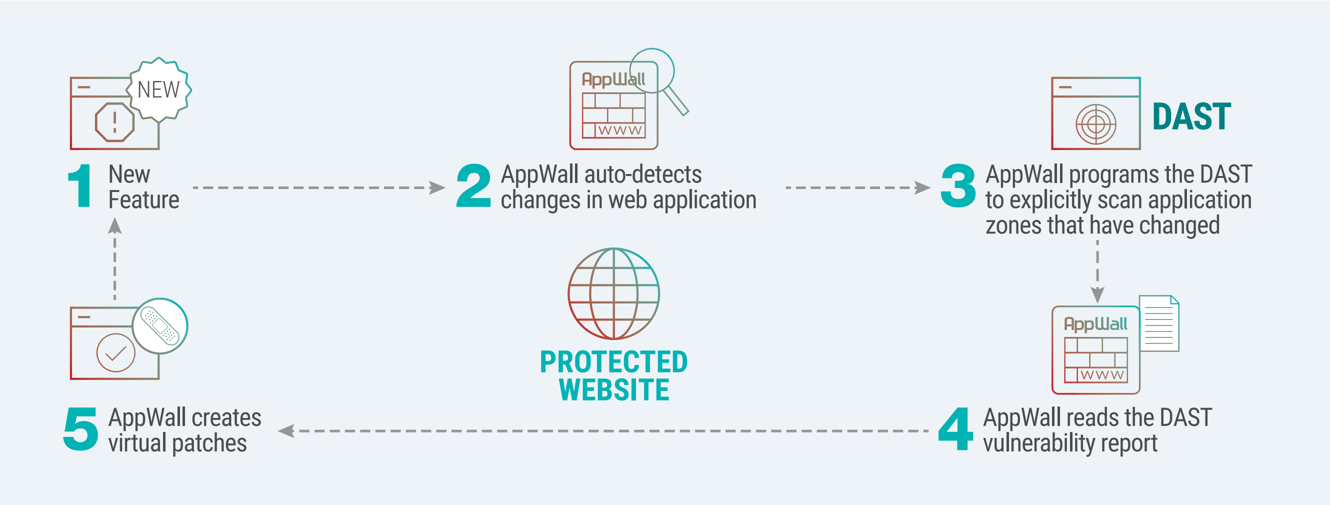


Figure 1: An overview of AppWall's machine-learning capabilities

Continuous Security Delivery

AppWall is the first WAF to provide a real-time security patching solution for Web applications in continuous application deployment environments. This is accomplished via tight integration with Dynamic Application Security Testing (DAST) solutions.

As Web applications are continuously introducing new features and resources, Radware's AppWall automatically detects any changes in the web applications (1) in real time and invokes (2) DAST tool to explicitly scan (3) the specific application zones that have been changed. This scan is accomplished in minutes versus a complete web application scan that can take hours. AppWall then reads (4) the DAST vulnerability report, and uses it to automatically update the application security policy (5) by creating the applicable virtual patches. Following that, a second vulnerability scan is invoked to test whether the application security was indeed successfully patched.



NEW
1 New Feature
AppWall
WWW
2 AppWall auto-detects changes in web application
DAST
3 AppWall programs the DAST to explicitly scan application zones that have changed
PROTECTED WEBSITE
AppWall
WWW
4 AppWall reads the DAST vulnerability report
5 AppWall creates virtual patches

Figure 2: Continuous Security Delivery – How it works

IP-Agnostic Device Fingerprinting for Bot Protection

AppWall's device fingerprinting and activity tracking modules offer IP-agnostic source tracking to help address the threats advanced bots pose to applications and APIs, such as web scraping, web application DDoS, brute force attacks for password cracking and clickjacking. AppWall can detect sources operating in a dynamic IP environment and activity behind a source NAT, such as an enterprise network or proxy. Even if the bot dynamically changes its source IP address, its device fingerprint does not change. AppWall tracks the device activity and correlates the source security violations across different sessions over time.

Unique Out-of-Path Deployment with Full, Line-Speed Mitigation

AppWall is the only WAF that can be deployed out-of-path while still providing full mitigation. As part of Radware's integrated Attack Mitigation Solution, DefenseMessaging, a unique messaging mechanism, enables AppWall to signal Radware's perimeter attack mitigation device, DefensePro, when a web application attack is detected, block it at the perimeter and protect the rest of the network.

Once AppWall detects a web-based attack, it automatically sends a message to DefensePro which is deployed at the perimeter to mitigate and block attacks in real time.

This unique Defense Messaging mechanism can be leveraged when AppWall is deployed inline as well as out-of-path to assure line speed web-based attack mitigation with no additional latency, performance impact or risk. This includes:

- Mitigating at line speed– up to 400Gbps, 330M DDoS PPS at 60 micro-seconds latency.

- Mitigating cyberattacks targeting web applications behind CDNs.
- Blocking advanced http DDoS attacks (Slowloris, HTTP Dynamic Floods), Brute Force attacks on login pages and SSL-based attacks.
- Blocking the attack source at the perimeter, before it enters the organizations' network, securing other applications and services.
- Enabling multi-layered detection and mitigation

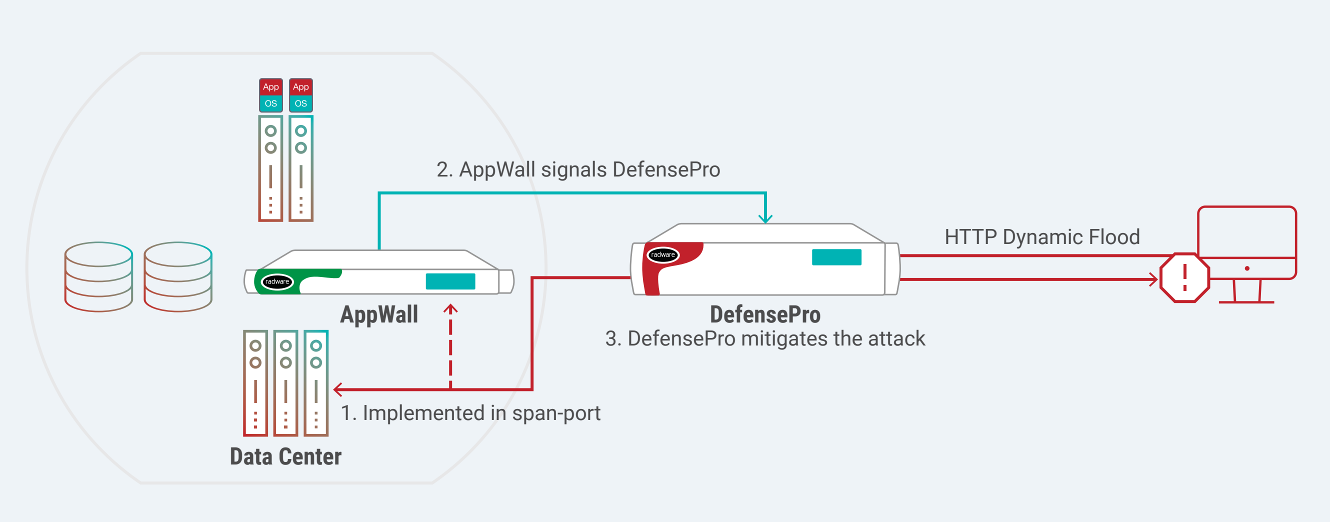

App
OS
App
OS
2. AppWall signals DefensePro
HTTP Dynamic Flood
radware
AppWall
radware
DefensePro
3. DefensePro mitigates the attack
1. Implemented in span-port
Data Center

Figure 3: Out-of-path detection, signaling DefensePro at the perimeter, line speed

All-in-One Application Delivery & Security

When AppWall is deployed as part of Radware's application delivery controller, the solution provides a comprehensive set of availability, acceleration, and security services designed to ensure fast, reliable, and secure delivery of mission- critical web applications, regardless if they run in a datacenter, private or public clouds.

Resources of AppWall instances can be dynamically allocated according to enterprise needs and deliver fault isolation, SLA assurance and high platform density.

The solution supports both out-of-path and inline deployment modes and can be delivered on a variety of platforms that support up to 80Gbps.

Fully Managed Web Application Protection

Understanding the challenges organizations face in managing and maintaining web application security solutions, and the required labor that comes with onboarding, tuning and analyzing security policies, Radware offers a fully-managed Cloud WAF Service – provided by Radware's ERT security experts, and includes the ongoing management, monitoring and configuration of the on-premise WAF device.

Authentication Gateway

AppWall's user authentication and single sign- on offering functions as an authentication tier in front of the web applications or APIs. It applies two factor authentication, authorizes and enforces web access control policy, and enables access to premise-based applications from outside the enterprise network. Various authentication schemes are supported among of which are the FBA (Form Based Authentication), NTLM, and KCD (Kerberos Constrained Delegation).

Multi-Vector Role Based Security Policy

By leveraging AppWall's authentication and SSO, application or organizational web role (employees, partners, customers etc.), and security policies (such as application access, data visibility and web security) can enforce segregation of duties that ensure access to data is based on business needs.

Compliance

AppWall enables organizations to fully comply with PCI DSS section 6.6 requirements and includes the granular event analytics to convey visibility into the application security and detected attacks. Its detailed PCI compliance report analyzes the security policies, provides automatic compliance status and a mandatory action plan for compliance.

BUSINESS VALUES

- **Best Security Coverage**
  - Attack mitigation with no performance impact or risk
  - Secure availability of web applications
  - Audit ready and visibility into application security
  - Data loss prevention
- **Fastest to Deploy**
  - Fast, reliable, and secure delivery of mission-critical web applications
- **Allows Secured, Continuous Web Application Delivery**
  - Integrated with DAST solutions for
  - real time web security patching
- **Easiest to Maintain**
  - Low maintenance costs and post deployment peace of mind
  - Improved risk management

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 that can assist customers on a professional services basis for advanced project deployments.

Learn More

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

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.