radware **AppWall** Data Sheet

# AppWall – More Than Just a WAF

As cyber attacks 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. 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 the speed in which new mitigation tools and techniques are being bypassed require a more robust and comprehensive solution that provides faster protection and  reduced maintenance costs.

By targeting the application layer, attackers exhaust server and application resources using stealth attack techniques that go undetected by traditional security tools. It is no longer just about http floods and downtime. Advanced methods and the use of multiple vectors during attacks present new challenges in securing an organization.

## AppWall – Faster to Deploy. Easier to Maintain.

AppWall is the only web application firewall that provides complete web application security. It blocks attacks at the perimeter and ensures fast, reliable and secure delivery of mission-critical web applications. It is the best performing application security solution for web security, mitigation and compliance.

## Detect. Signal. Block.

Once AppWall detects a web or application based availability attack, its new Defense Signaling feature automatically signals DefensePro which is deployed at the perimeter to mitigate and block attacks in real-time.

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

- Line speed mitigation:
  - 40Gbps
  - 25M DDoS pps
  - 60 micro seconds latency
- Mitigating cyber attacks targeting web applications behind CDNs
- Blocking the following attacks:
  - Advanced http DDoS attacks (Slowloris, Http Dynamic Floods)
  - Brute force attacks on login pages
  - SSL attacks
- Blocking the attack source at the perimeter, securing other applications and services
- Enabling multi-layer detection and mitigation

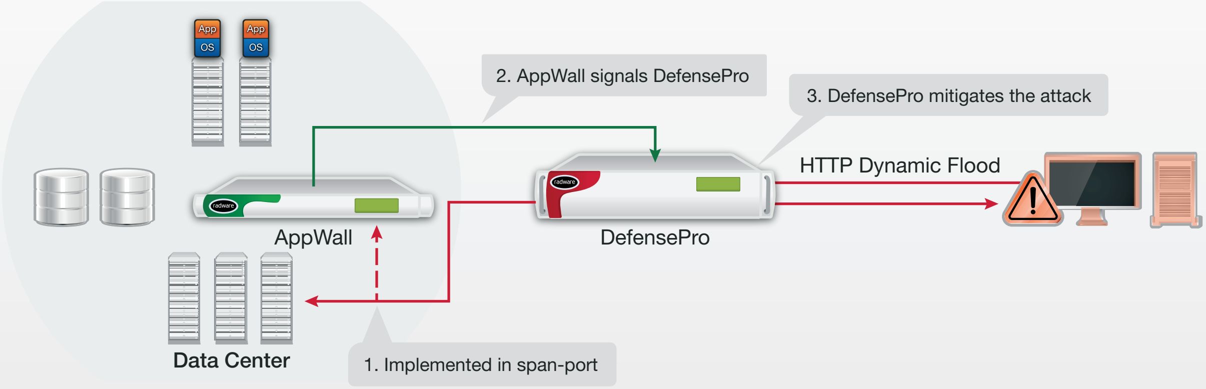

App
OS
App
OS
2. AppWall signals DefensePro
3. DefensePro mitigates the attack
HTTP Dynamic Flood
AppWall
DefensePro
Data Center
1. Implemented in span-port

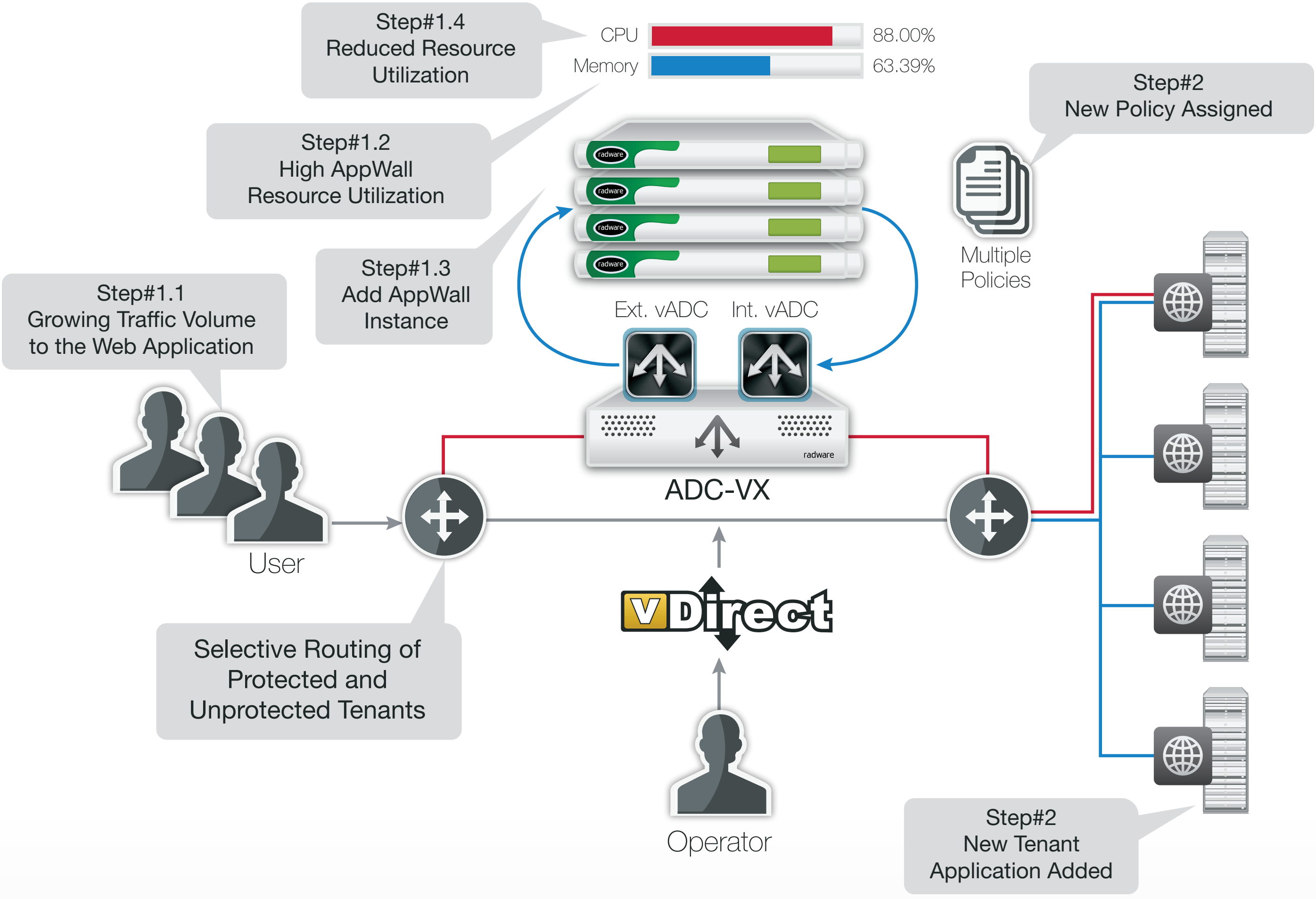
Figure 1: Out-of-path detection, signaling DefensePro at the perimeter, line speed

## All-in-One Application Delivery & Security

When AppWall is deployed as part of Alteon NG, 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.

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.



Step#1.4
Reduced Resource Utilization
CPU
88.00%
Memory
63.39%
Step#1.2
High AppWall Resource Utilization
Step#2
New Policy Assigned
Multiple Policies
Step#1.3
Add AppWall Instance
Step#1.1
Growing Traffic Volume to the Web Application
Ext. vADC
Int. vADC
radware
ADC-VX
User
vDirect
Selective Routing of Protected and Unprotected Tenants
Operator
Step#2
New Tenant Application Added

Figure 2: ADC deployment with AppWall: Fault isolation, SLA assurance and high platform density

## Shortest Time to Security

AppWall's unique Auto Policy Generation analyzes the protected application, generates granular protection rules and applies a security policy in blocking mode that 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**

## 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.

## Web Security

AppWall's complete web application protection provides full coverage of OWASP Top-10 Risks by enforcing negative & positive security models that offer the most comprehensive set of web security features. AppWall protects against over a hundred attack vectors some of which are listed in the WASC Threat Classification.

It 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.

**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
- **Easiest to maintain**
  - Low maintenance costs and post deployment peace of mind
  - Improved risk management

## IP-agnostic Device Identification and Tracking

AppWall's Device Fingerprinting and Activity Tracking modules offer IP-agnostic source tracking to help address the threats posed by advanced bots, 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.

## Compliance

AppWall enables organizations to fully comply with PCI DSS section 6.6 requirements and includes the most advanced security graphical reports 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.

## Ready for the Future with Attack Mitigation Network (AMN)

AppWall is part of Radware's Attack Mitigation Network (AMN), a holistic security architecture designed to fight emerging cyber-attacks. AMN offers Defense Signaling, a unique feature deployed in Radware's solution. Every device and solution that is part of the AMN architecture provides information about traffic baselines and real time signatures to the other solutions so all systems have full visibility into available information.

Defense Signaling can automatically respond and mitigate threats where they should be mitigated. For example, it can detect attacks on the application level through AppWall, but can block it in the perimeter with DefensePro, or move volumetric attack mitigation to the cloud. This allows scaling mitigation capabilities and moving mitigation as far as possible from the application infrastructure, resulting in faster, better protected application delivery.

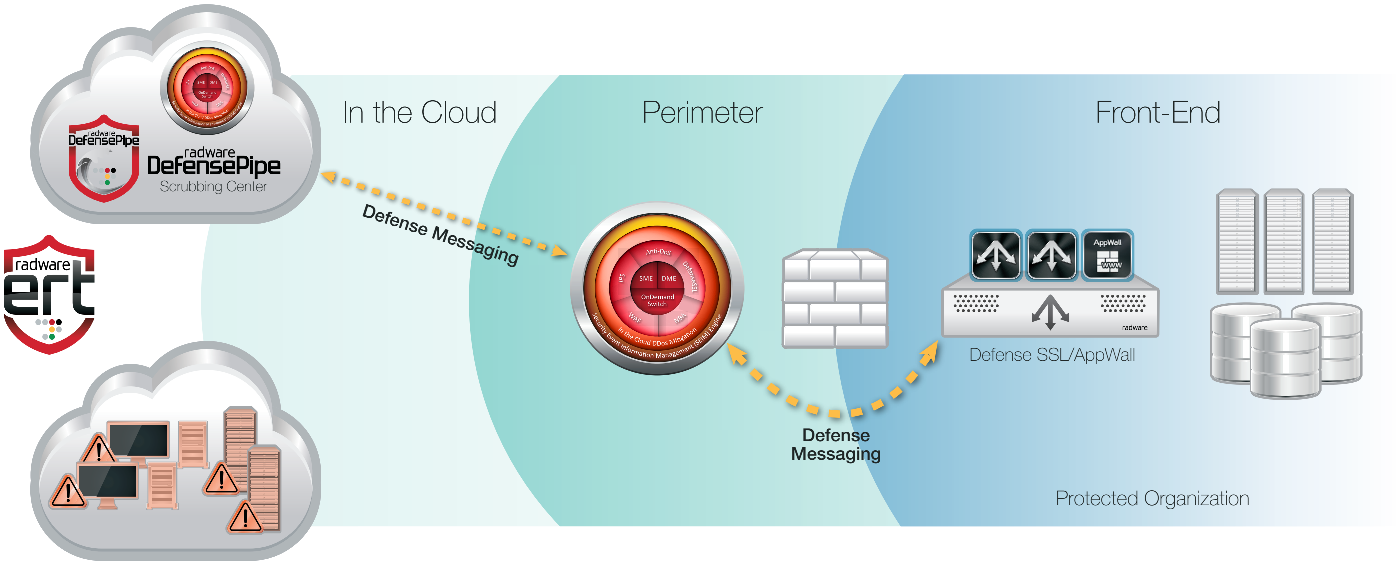


Figure 3: AMN Defense Messaging and mitigation

## About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, 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: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube and the Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on 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.