



Enterprises are migrating business-critical functions to Web applications to increase productivity, improve business agility and reduce costs. While Web applications provide significant economic advantages and enable increased operational efficiencies, they also create new security risks that need to be addressed.

Radware's AppWall is a Web application firewall (WAF) appliance that secures Web applications. It enables PCI compliance by mitigating Web application security threats and vulnerabilities to prevent data theft and manipulation of sensitive corporate and customer information. AppWall incorporates advanced, patent-protected Web application security filtering technologies to seamlessly detect threats, block attacks and report events.

AppWall improves the security and availability of business-critical Web applications and creates a higher return on investment (ROI) for Web-based applications.

Taking Web Application Security to the Next Level

AppWall is a comprehensive Web application firewall supporting small- to large-scale Web application deployments for the distributed enterprise. It secures Web applications by enforcing security policies to seamlessly detect threats, generate security events, and block both internal and external attacks on critical corporate data with minimal impact on day-to-day operations and enhanced savings on OPEX.

Maximum Web Application Threat Mitigation through Negative and Positive Security Models

AppWall supports a negative security model, ensuring that all risky Web traffic is blocked, including inspection of sensitive fields that can be defined using custom patterns such as Social Security numbers or credit card numbers. AppWall also employs a positive security model, guaranteeing that only Web traffic that complies with Web application behavior is passed through while all other traffic is blocked, without requiring continuous updates of new attack signatures.

Prevented Threats

- SQL injection
- Cross-site scripting
- Parameter tampering
- Hidden field manipulation
- Session manipulation
- Cookie poisoning
- Stealth commanding
- Backdoor and debug options
- Application buffer overflow attacks
- Brute force attacks
- Data encoding
- Unauthorized navigation
- Gateway circumvention
- Web server reconnaissance
- SOAP and Web services manipulation

Instant Protection with Out-of-the-Box Security Policies

AppWall's out-of-the-box security policies address major threat categories and provide instant protection, allowing the enterprise to deploy and secure new Web applications within hours. AppWall policies are defined based on the unique structure, characteristics, and vulnerabilities of third-party or internally developed applications. Policies developed for one deployment can be quickly replicated for other AppWall instances in other locations.

Fine Grain Security Policies Enable Flexible Deployment

AppWall enables the user to define highly granular policies and to easily refine security policies for each application, down to the page or the parameter level. This provides the flexibility to tailor the level of security based on both the needs of the business and the level of risk. This allows for precise security coverage and full enforcement while minimizing false positives.

Integral Part of Radware's Application Delivery Solution

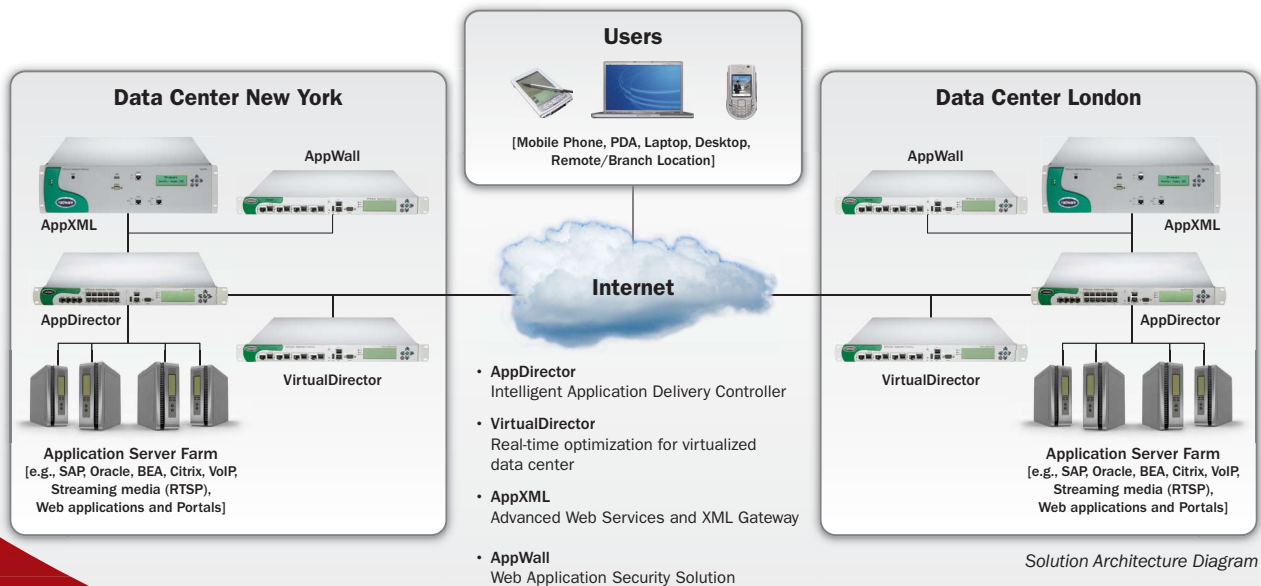
As AppWall is an integral part of Radware's suite of ADC solutions, customers can augment their Web application security protection with: local and global traffic redirection, application acceleration, bandwidth management, and other application-aware services, all while benefitting from a standardized hardware platform. Combining AppWall with AppDirector, VirtualDirector and AppXML provides a comprehensive set of availability, acceleration, and security services designed to ensure the fast, reliable, and secure delivery of mission-critical Web applications.

Highly Scalable Solution

AppWall is deployed on Radware's next-generation OnDemand Switch hardware platform, delivering breakthrough performance. As an AppWall deployment can scale to an AppWall cluster, it addresses current and future business needs and it enables business agility for distributed enterprise data centers. The AppWall cluster is easily managed with the Cluster Management component, ensuring all policies across the entire AppWall cluster are synchronized.

Automatic Protection Level Escalation

AppWall can dynamically change its protection level whenever an attack is detected by one of the devices in the environment. Consequentially, organizations can establish security policies that trigger the escalation of the AppWall protection level across the enterprise. This unprecedented intelligence provides organizations with the flexibility to weigh the tradeoffs between business needs, operational performance, and security information risk. The escalation automation ensures that an attack against a single location triggers a rapid and appropriate response throughout the enterprise, increasing compliance and savings on OPEX.



Integration with Enterprise Management Systems

AppWall provides centralized reporting of security events through integration with leading enterprise management systems. Using the AppWall Publisher module, security events can be exported via SNMP, SMTP, SysLog, ODBC and other industry-standard formats to meet auditing and regulatory compliance requirements, save time and increase productivity.

Simplified, Centralized Management and Control

AppWall's management application provides simplified and centralized management, fast-and-efficient policy refinement, and detailed dashboard and server statistics across the entire enterprise. The Auto Discovery feature delivers a graphical view of the application structure with links to security policies. As a result, operations are simplified to increase OPEX savings.



AppWall Management Application Forensics View

Feature	Business Benefits
Out-of-the-box security policies based on negative security model addressing a wide range of security threats	<ul style="list-style-type: none"> Comprehensive Web application attack protection and risk mitigation Rapid deployment Instant protection Simple operation Increased savings on OPEX
Positive security model delivering automatic applications learning capability	<ul style="list-style-type: none"> On-the-fly, secure new application deployment Reduced operations complexity due to automatic learning capability Assured, uninterrupted business continuity
Highly granular policy control based on application path	<ul style="list-style-type: none"> Flexible deployment Precise security coverage enforcement enhancing performance Increased savings on OPEX via elimination of redundant security checks
One-click policy refinement for every security event	
Integral part of Radware's ADC solution	<ul style="list-style-type: none"> Extract more value from investments in ADC - maximum availability, best performance and bulletproof security through the most comprehensive ADC solution Increase savings on OPEX through standardization on the OnDemand Switch platform Less spare parts, less training, simplified operations Enhanced manageability for administering the entire ADC solution
Scalable solution by device supporting distributed enterprise data center	<ul style="list-style-type: none"> Address business growth needs Support current and future requirements Enable business agility
Automatic protection level escalation based on attack detection	<ul style="list-style-type: none"> Enable enforcement of security policies across the entire enterprise more easily Increased savings on OPEX due to escalation automation
Centralized reporting of security events through integration with leading enterprise management systems	<ul style="list-style-type: none"> No customization needed for interoperability with other IT systems Increased productivity Increased savings on OPEX Enhanced auditing and regulatory compliance
Simplified management and control enabling to centrally synchronize the configuration and learned data to all devices	<ul style="list-style-type: none"> Improved manageability and usability Increased savings on OPEX

Technical Specifications

Platform	OnDemand Switch 1 XL
Processor	2 AMD Opteron dual-core 2.2 GHz
Memory	6 GB
Gigabit/GBIC Ports	4 Gigabit Ethernet Ports (Copper or Fiber)
1000Base-SX/LX/ZX Ports	All Gigabit Fiber ports deliver SX/LX/ZX interfaces depending on GBIC
1000Base-SX (850 nm) Operating Distance	<ul style="list-style-type: none"> • 62.5 micron MM fiber .2 m to 275 m • 50 micron MM fiber .2 m to 550 m
1000Base-LX/ZX Operating Distance	<ul style="list-style-type: none"> • LX: Up to 10 km (6.2 mi) • ZX: Up to 80 km (49.7 mi)
USB Port	On front panel
LCD Screen	On front panel
RS-232C Console	<ul style="list-style-type: none"> • DB-9 serial connection • Female DCE interface for out-of-band management
Dimensions	<ul style="list-style-type: none"> • 1U: <ul style="list-style-type: none"> o Width: 424 mm (17 in.) o Depth: 600 mm (24 in.) o Height: 44 mm (1.7 in.) • 2U (dual Power Supply Option): <ul style="list-style-type: none"> o Width: 424 mm (17 in.) o Depth: 600 mm (24 in.) o Height: 88 mm (3.4 in.) <p>EIA Rack or Standalone: 482 mm (19 in.)</p>
Weight	<ul style="list-style-type: none"> • 1U: 9.5 kg (20 lbs) • 2U: 10.9 kg (23 lbs)
Environmental	<ul style="list-style-type: none"> • Operating temperature: 0°C to 40°C (32°F to 104°F) • Humidity: 5% to 95% non-condensing
Power	<ul style="list-style-type: none"> • Auto-range supply: • AC: 100-240V 50-60Hz • DC: -42~72V • Frequency: 47Hz - 63Hz • Power consumption: 150 W • Heat dissipation: 511.5 BTU/h • Dual power supply (AC/DC) in 2U form
Certifications	<ul style="list-style-type: none"> • Safety: EN, UL, CSA, IEC #60950-1 • EMC: EN 55022, EN 55024, FCC Part 15B Class A • CE, FCC, VCCI, CB, TUV, UL/cUL, CCC, C-Tick, RoHS

Technical specifications and product information are subject to change without prior notice.

Radware APSolute™ Product Suite

Radware, the global leader in integrated application delivery solutions, assures the complete availability, performance and security of business-critical applications for more than 6,000 enterprises and carriers worldwide. With Radware's comprehensive APSolute suite of application delivery and network security products, companies can drive business productivity, improve profitability, and reduce IT operating and infrastructure costs by making their networks "business-smart."

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

Learn More

To learn more about how Radware's integrated application delivery 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.