

AppXcel Web Application Firewall Service Protects Against:

- Web, HTTPS and XML application attacks
- SQL Injection
- Session Hijacking
- Cross Site Scripting
- Form Field Tampering
- Known Worms
- Zero-Day Web Worms
- Buffer Overflow
- Cookie Poisoning
- Denial of Service
- Malicious Robots
- Parameter Tamper
- Brute Force Login
- Malicious Encoding
- Directory Traversal
- Web Server and Operating systems Attacks
- Scanning
- Command
- Illegal Encoding
- Identity Theft
- Data Theft
- Patient and Corporate Espionage
- Phishing
- Data Destruction

Defend Against Vulnerability Exploits With Award-Winning Web Application Security Software

The combination of Radware's AppDirector™ application delivery controller and AppXcel™ service platform provides a comprehensive set of application acceleration, optimization and security services to ensure the fast, reliable, and secure delivery of mission-critical web-enabled applications. AppXcel's service architecture provides a platform for best of breed integration. The most recent addition is the award-winning Imperva® SecureSphere™ Web Application Firewall (WAF) which provides Web and Web Services applications (XML) with automated plus immediate protection from a wide range of security threats to ensure secure and continuous on-line business activity.

Behavior-based Dynamic Profiling Provides Automated and Accurate Protection

AppXcel's automated web application firewall (WAF) service provides unified protection against application-specific attacks, worms, platform exploits, and network attacks. Using unique, behavior-based dynamic profiling, it creates a model of legitimate application usage and structure that self-adapts to application changes over time. Protection against attacks is provided without manual configuration or tuning. This is accomplished by closely monitoring application activity and user interactions to detect and block illegitimate activity while allowing valid application changes. With WAF deployment of applications and services on your network (either internally developed or purchased from a third-party vendor), risks are significantly mitigated through the benefits of an adaptive security layer.

Dynamic Profiling™ also allows for automated policy definition which greatly reduces operational overhead and lowers application developers' security burden. Behavior based policy definition eliminates time consuming manual rule creation and maintenance for the numerous rules that are needed to govern - thousands of constantly changing variables associated with web applications and web services like URLs, parameters, cookies, SML elements and form fields.

When needed, dynamic profiles can be modified by security administrators to enforce corporate security policies that may not align with actual usage. Custom policy rules can also be manually configured to accommodate operations that cannot be handled by profile and protocol violation rules.

Custom web application code is protected against attacks such as SQL injection. Protocol compliance validation ensures that HTTP protocols meet RFC and expected usage requirements. This prevents exploits of known as well as unknown vulnerabilities in commercial web server implementations. Zero-day worm profiling technology identifies and blocks attacks by detecting the specific combinations of attributes that uniquely characterize such attacks.

Dynamic Profiling technology also protects against attacks targeting XML, SOAP and WSDL applications, by creating a dynamic positive security model of allowed application usage and structure, including XML URLs, SOAP actions, XML elements and XML attributes. Any attempts to tamper with Web services application schemas or variables are identified and blocked.

Seamless Deploy Without Changing Existing Network

AppXcel's WAF service can be transparently activated to expand the functionality of Radware's APSolute AFE application delivery solution without making any network architecture, router or server changes.

No Need To Redesign Web Applications

Web traffic is examined for attacks and malicious activity without altering or rewriting Web content. Get complete and accurate application security without modifying Web applications or changing authentication schemes.

Automated Application Security Reduces Total Cost of Ownership

Ongoing policy maintenance is the most significant component of a security solution's total cost of ownership (TCO). Dynamic Profiling reduces TCO by eliminating the need for manual tuning through automatic adaptation to application changes. Nevertheless, administrators have full access to view and modify profiled information as well as create custom policy rules as desired. An adaptive security layer provides additional costs savings by also eliminating the need for expensive and lengthy penetration testing.

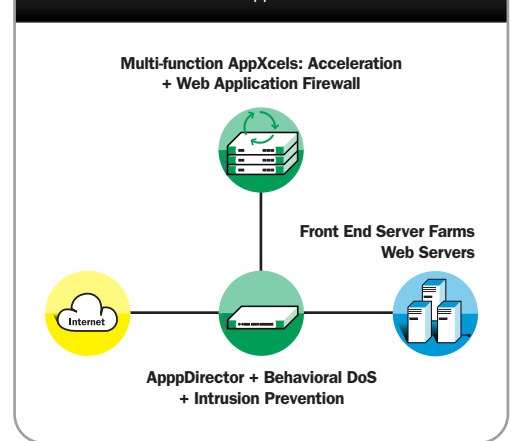
High availability – Real Time Failure Bypassing

AppDirector's extensive health monitoring capabilities enables real time identification of a faulty WAF service, automatically bypassing it and switching the traffic to a fully functional WAF in the farm.

Comprehensive Management Capabilities With Regulatory Compliance Reporting

Like all APSolute products and AppXcel services, APSolute Insite provides all of the administration and reporting capabilities needed to manage a web application firewall deployment; including profile management, status monitoring, alerting, logging and reporting activity. With APSolute Insite's rich graphical reporting capabilities, customers can easily understand security status and meet regulatory compliance requirements. APSolute Insite provides instant visibility into security, compliance (HIPAA, SOX) and content delivery concerns.

Figure 1: Typical Configuration of Radware Open Service Architecture with web application firewall service



Technical Specifications

Features	AppXcel 4000	AppXcel 8000
SSL Transactions/second	4,000	7,300
Concurrent connections	20,000	50,000
Throughput HTTP	320Mbps	
Throughput HTTPS	180Mbps	
Memory	4 GByte	
Network Interfaces	<ul style="list-style-type: none"> • One of the three options: <ul style="list-style-type: none"> – 2x 10/100/1000 BaseTX ports – 1x 10/100/1000 BaseTX & 1x 1000BaseSX port • RS-232C connector 	
Operating Environment	<ul style="list-style-type: none"> • Temperature: 0 to 40°C • Relative Humidity: 5% to 95% non-condensing 	
Weight & Dimensions:	<ul style="list-style-type: none"> • W 430.0mm x D 504.7mm x H 43.7mm • Weight: 7.25kg • Standard 19 inch EIA rack or standalone 	
Power	Auto-range supply: 100-250V 50-60Hz	
Intrusion Prevention System (IPS)	Integrated Snort®-based signature detection mechanism provides IPS protection against known infrastructure attacks targeting vulnerabilities in commercial web server, application server and operation system software (e.g. IIS, Apache, Windows 2000). Regular signature updates ensure protection against latest exploits.	

Product specifications subject to change without notice.