radware

Smart Network. Smart Business.

Why a Web Application Firewall Makes Good Business Sense

How to Stay Secure with AppWall® – Whitepaper

Table of Contents

Introduction

"Now, even my cat has its own page," Bill Clinton jokingly announced in 1996 at the Next Generation Internet Initiative. Although this joke is more applicable to the consumers market, it does reflect the democratization of the internet in all the sectors and show the ease in which every company or individual can create and maintain its own web site. Generating a site, a web application, is a gateway for your business to the World Wide Web and opportunity to potentially reach millions of users. But it doesn't come for free. The internet, as a network, is a platform for data sharing and designed for openness and flexibility but with little concern for security. In addition, the web applications are developed fast, with little focus on increasing daily security risks and very little understanding of security design aspects, methods and guidelines.

This white paper discusses the threats encountered by on-line businesses constantly facing evolving security risks. It gives an overview of the challenges of web application security and introduces Radware's AppWall® , a web application firewall providing a robust solution built with security, performance and usability in mind. It answers the security needs of online businesses and complies with regulations.

Web applications are developed with limited awareness for security aspects.

Living on the Edge: Your Unprotected Business is at Risk

Your website is the face of your company and in many cases, a main revenue engine. The information provided should be accurate, safe for browsing, fast, convenient, the transactions secure and all customer and company sensitive information should be kept confidential and well protected.

Failing to secure your online applications could negatively impact your business resulting in a sensitive customer or corporate data security breach. It can lead to customer dissatisfaction and abandonment, financial losses, brand damage and even legal troubles. Companies from all industries fall victim to web applications attacks that could have been avoided with more security awareness and investment. For example, some of Sony's famous woes were caused by simple SQL injection attacks on their web applications, similar to the attacks which previously hit Fox.Com. More recently, T&T Parliament and International Police Association websites were defaced. In both cases, hackers targeted the security holes in these web applications.

Disastrous consequences for companies failing to secure their web applications

The World Wild Web Application Threats

Running an application on the World Wild Web presents risks. Threats exist, evolve and are always intimidating.

The web applications threat classifications produced by the Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC) are widely agreed upon and commonly referred to by many organizations. The two classifications overlap, but while the OWASP provides a summarized Top ten list of web application threats, WASC offers a wider classification of attacks and weaknesses and provides a detailed analysis on each of the ten OWASP categories. For example, OWASPs first item on the Top Ten list is called "Injection" and could be mapped to eight distinctive WASC items relating to "Injection" threats (SQL Injection, XML Injection, LDAP Injection, XPath Injection, XQuery Injection, Null Byte Injection, Mail Command Injection and OS commanding).

Businesses are menaced by a huge amount of web application threats

In the table below, we refer to the OWASP Top Ten classification as a limited but accurate and summarized list of threats on web applications: the "Top 10 Most Critical Web Application Security Risks".

The top ten web applications threats classification by OWASP

Injection	Untrusted data is sent to an interpreter as part of a command or a query (SQL injection). It causes the interpreter to execute unintended commands or access unauthorized data.
Cross-Site Scripting (XSS)	Untrusted data is sent to a browser without proper validation and escaping. Attackers could inject client side scripts causing user sessions to be hijacked, site defacement, etc.
Broken Authentication and Session Management	Incorrect implementation of authentication and session management functions. Attackers could compromise passwords, keys and session tokens.
Insecure Direct Object References	An internal implementation object (file, directory, database key) is exposed in the code. Attackers could manipulate those references to manipulate unauthorized data.
Cross-Site Request Forgery (CSRF)	A forged HTTP request with authentication information (session cookie) is sent to a vulnerable web application. The victim's browser unintentionally generates requests to the vulnerable application.
Security Misconfiguration	Failing to provide secure and up to date configuration of the application environment.
Insecure Cryptographic Storage	Sensitive data (CCs, SSNs, PII, etc.) are not encrypted or hashed. Attackers could steal or modify this data.
Failure to Restrict URL Access	The URL access rights are not checked when the pages are accessed. Attackers could forge URLs to access the hidden pages.
Insufficient Transport Layer Protection	Insufficient protections are implemented – weak algorithms, expired or invalid certificates, etc.
Unvalidated Redirects and Forwards	The redirect and forward pages are not validated. Attackers could redirect victims to phishing or malware sites or use forwards to access unauthorized pages.

Regulations and PCI-DSS compliance

Regulations as GLBA, HIPAA or FISMA all induce some level of web application security while giving organizations the freedom to choose the preferred method of threat mitigation. In all cases, a Web application firewall (WAF) could be used as an effective security enforcement solution.

Regulations and standards emphasize the need for web application security measures.

The Payment Card Industry Data Security Standard (PCI-DSS) is much more explicit on web application security guidelines. PCI-DSS is a standard which was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. It is comprised of twelve requirements which are organized in six main categories. PCI-DSS section 6 addresses the development and maintenance of secure systems and applications; it requires that organizations either submit to code audits or install a Web Application Firewall to secure their public-facing Web applications. Non- compliance could result in fines and penalties and rescind the ability to process credit card transactions.

PCI-DSS recommends protecting web applications with Web Application Firewalls.

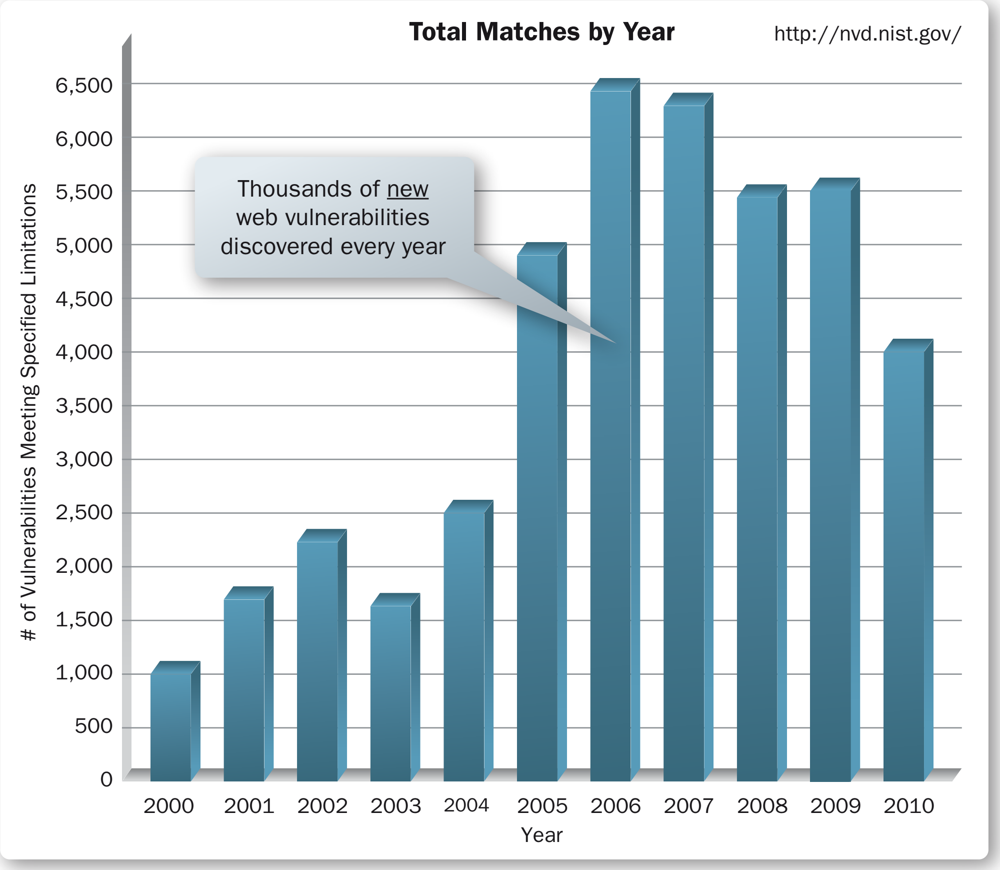
Why Existing Defenses are Not Good Enough

A common answer one could expect from organizations when referring to their web application security measures is: "we are protected by our network firewall and our IPS". While traditional defense tools can protect against a wide range of threats, they are not good enough to specific web applications needs.

Network firewalls (which operate at layers 3 – network- and 4 –transport) are not adapted to web applications protection (layer 7 –application), as they basically open and close the gate to ingoing and outgoing traffic without actually inspecting the content of the traffic.

Intrusion Prevention Systems offer a better protection against application threats; however their main focus is on client vulnerabilities rather than server vulnerabilities. IPSs inspect the content of network packets, match the content to a predefined set of signatures and then raise an alert or block the traffic if anomalies are detected. A typical IPS product includes several hundred signatures which still may not detect the thousands of new web application vulnerabilities discovered each year. Furthermore, IPSs could not parse the web application content so they are not capable of learning different web application components, pages, parameters, and reaction to zero-day attacks for which no signatures exist. In addition, IPSs do not have the ability to understand the web application protocol logic so they are unable to detect protocol violations (a common IPS evasion technique).

Traditional defenses are not appropriate to web application security. Web application firewalls provide the adequate solution.



Application security requires a deep understanding of the way applications work, how they request and get a resource, interpret and parse parameters, and how they normally behave. These functionalities are provided by Web Application Firewalls (WAF); defense systems adapted to web applications specificities, with the ability to understand Layer 7 (application) protocols, parse web applications parameters, pages, and define security policies as well as support XML and Web Services protection. WAFs should be smartly designed and finely tuned to provide maximum and dynamic security in the shortest time and with minimal impact on web application traffic.

Web Application Security Challenges

In previous years, attacks have evolved and become more complex with attackers using attack vectors in a single attack campaign.

The massive attacks on Sony were a mix of DDoS attacks, targeting the availability of the websites while simultaneously distracting the attention of Sony's security administrators with specifically targeted web application attacks (SQL injection). The goal of these attacks was to steal the user's accounts data. Simple correlation of security events from different sources may have thwarted this diversion technique.

Achieving good and efficient web application security is not an easy task and there are many challenges web application firewalls are up against.

A multi-dimensional problem

Due to the inherent way web applications are built, security is a complex equation with multiple variables. Web applications are based on third party web servers, legacy components, servers, operating systems and code development by the company. They contain numerous settings, pages, folders, parameters and authentication schemes. Each of these layers could be targeted and are potentially vulnerable to attacks that even the companies' best security practices can't guard against. The organization deploying the web application still relies on other companies' software which contains known, documented vulnerabilities or new vulnerabilities yet to be discovered.

Each of the layers the web application is built on could be attacked

The web application components are vulnerable

A needle in a haystack: Distinguishing between attacks and legitimate traffic

On average, a web application is being accessed both by desired legitimate users and undesired attackers (malignant users whose goal is to harm the application).

One of the biggest challenges in protecting web applications is the ability to accurately differentiate between the two and identify and block security threats while not disturbing the regular traffic. In other words, avoid **false negatives** and provide the best security coverage while maintaining a **low or inexistent percentage of false positives**. False negatives put your applications at risk and false positives not only disturb the legitimate traffic but also increase deployment operational efforts significantly. Combining multiple detection techniques and security models helps minimize both of them.

False negatives: non-blocked attacks False positives: normal behavior incorrectly identified as a security violation

Complex and time-consuming deployments

Another concern is deployment considerations. WAFs' deployments are renowned for being complex and time consuming.

How do we deploy the web application firewall in a timely and efficient manner and break the myth of the WAF complex deployments? How do we make sure the web application firewall quickly starts to effectively block attacks -without dragging the testing phases for ages?

Bringing down the myth of complex and time-consuming WAF deployments

In order to achieve web application security, the WAF has to learn the application, map its pages, parameters, and analyze its traffic in order to create and later dynamically update an application baseline. This baseline is the normal state of the application and the security tool compares this baseline to new incoming traffic. The learning and mapping processes could be timely and require a lot of manual configuration as web applications usually contain a multitude of pages, folders and a myriad of parameters. Any application change would also require full relearning and remapping of the baseline. This action slows down the security policies definition and therefore delays the actual WAF deployment.

The challenge is to provide the shortest time to protect and create a smooth deployment process and a fast and dynamic learning curve of the applications characteristics while automatically generating and effectively applying granular security policies.

Scale to growing businesses requirements

As the number and size of web applications grow, the web application firewall aimed at protecting those applications becomes busier, having to deal with more bandwidth, throughput and processing. Ill designed WAFs can't withhold the load and experience performance degradations and the inability to meet the scalability requirements of the organization which sometimes collapse. The web application firewall should therefore provide a robust, scalable infrastructure, enabling to meet the adaptive and progressive requirements for growth of the organizations.

On demand, progressive scalability is a critical element

Accurate tracking and reporting of security events

The last challenge is to provide accurate, centralized and intuitive logs, traces and reports of the Web application security state.

In-depth reporting and forensics analysis are useful to learn about the attacks, how they occurred and how they were blocked. In many cases, organizations are also looking for correlation reports on different security events which were triggered on different parts of their application infrastructure. This is not always obvious as each security tool provides its own security report which does not correlate.

Another reporting challenge is to present comprehensive, clear and useful reports for regulations and standards compliance – for example PCI reports.

Comprehensive, correlated, compliance aware reporting is a top requirement.

Protect Your Web Applications with AppWall- Radware's Web Application Firewall

Radware's AppWall is a Web Application Firewall (WAF) that secures Web applications and enables PCI compliance by mitigating web application security threats and vulnerabilities. It prevents data leakage and manipulation of sensitive corporate and customer information. AppWall addresses the multiples challenges faced by Web applications security.

Appwall features and benefits address the web application security challenges.”

Multi-layers security

No matter what software the web application is deployed on, AppWall effectively protects it. It acts as a door keeper for the web application, scanning its various elements, disregarding the pieces of software it is assembled on. AppWall protects the web applications from both known vulnerabilities and new, but not documented ones.

Full support of OWASP top 10 and WASC threats

Comprehensive and accurate security coverage

AppWall offers 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, as listed in the previous section, including injections, cross site scripting (XSS), cross site request forgery (CSRF), broken authentication, session management, security mis-configuration and security coverage for Web Application Security Consortium (WASC) threats.

Full security coverage without affecting the normal traffic

By effectively providing defenses against those threats, AppWall improves and maximizes the web applications security, blocking or diverting future attacks. For instance, AppWall protects against data leakage by identifying and then blocking or masking sensitive information transmission such as credit card numbers (CCN) and social security numbers (SSN). Masking credit cards numbers is an actual requirement of the PCI standard, requirement 3.3, and easily achieved with AppWall without an application modification.

Negative security profiles define signature-based protections to known vulnerabilities.

Data Leak Prevention	• Credit card numbers (CCN) • Social Security numbers (SSN)
Traffic Normalization & HTTP Validation	• Evasions • HTTP response splitting (HRS)
Parameters Inspection	• Buffer overflow (BO) • Zero-day attacks
Signature & Rule Protection	• Cross site scripting (XSS) • Web application vulnerabilities • SQL injection, LDAP injection, OS commanding
User Behavior	• Cross site request forgery (CSRF) • Cookie poisoning, session hijacking • Brute force

The best security coverage with minimal impact on legitimate traffic is made possible by the AppWall combination of negative (defining what's 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. For instance, to illustrate the negative security model signatures protection, AppWall negative security profiles are up to date signatures against known vulnerabilities (similar to black list) which provide the most accurate detection and blocking technology of web application vulnerability exploits. The positive security model is useful in stopping zero-day attacks. AppWall provides positive security profiles, (similar to white lists), limiting the user input to only the level required by the application to properly function, thus blocking devastating zero day attacks.

Positive security profiles effectively stop zero-day attacks targeting vulnerabilities for which there is no signature.

Fast and automatic deployments

While other web firewalls require weeks or months of testing and deployment, AppWall has concentrated its efforts on providing rapid time to market, with the patented adaptive auto policies generation feature offering fast application auto-learning and granular automatic policies generation. AppWall analyzes the security related attributes of the protected web application and derives the potential threats in the application. The web application is mapped into application zones or paths, each with its own common potential threats. AppWall then generates granular protection rules for each zone and sets local policies in blocking mode after it has completed an optimization process that minimizes false-positives while maintaining the best security coverage. This process is automatic and requires no human intervention. The learning process is fast, the deployment smooth and efficient, and moving from learning to blocking mode is straightforward. Future changes to the application (pages, parameters, etc.) are transparent and AppWall automatically adds them to the appropriate security policies. In addition, AppWall supports web application role based policies which allows the configuration of different inspection and enforcement policies on different user types, such as administrator, employee and customer.

The adaptive auto-policy generation and self-modification feature enables

How AppWall Auto-Policy generation feature works?

Let's take the example of an "on-line reservation" application with admin, registration, purchase and info pages. Various actions are performed on those pages – view only on the information pages, transactions on the purchase pages and customers' data manipulation on the admin pages.

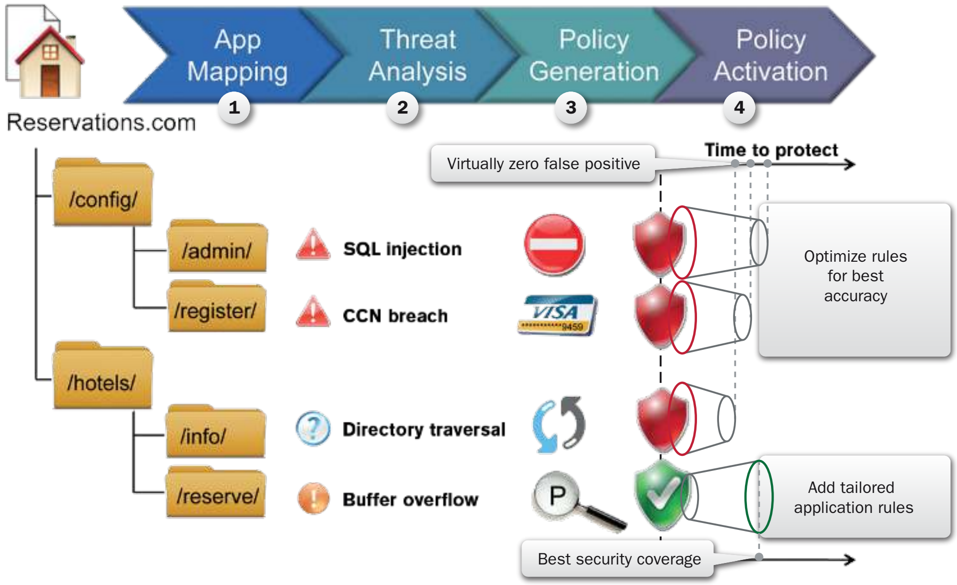
AppWall four-step auto-policy flow as follows:
1- Application pages & attributes learning and mapping to app. paths. Ex: parameters as "username", "customer number" or "transaction id" are collected and four different threat level application paths are created, /admin/, /register/, /info/ and /reserve/
2- Threat analysis per application path. Ex: /admin/ pages are sensitive to user information theft and manipulation; /reserve/ pages sensitive to credit card or SSN info.theft
3- Auto-policy generation per application path. Ex: /admin/ has static content so it's assigned negative security profile while /purchase/ and /register/ which have dynamic content, are protect with positive security profiles.
4- Policy optimization and activation: unnecessary signatures removed, values learned from parameters inspection are locked. Result: Max security coverage with low false positives and performance improvement.

Scalable platform and multi-tenant solution

AppWall infrastructure is based on Radware's on demand Switch (ODS). This platform enables a **scalable pay-as-you-grow** model providing breakthrough performance without service disruption and meeting organizations' needs for progressive, scalable growth. This way, an organization could purchase and start with a single AppWall machine and later, after additional throughput is required (application growth, new applications deployment), seamlessly add more resources.

The on-demand platform enables transparent and easy scalability.

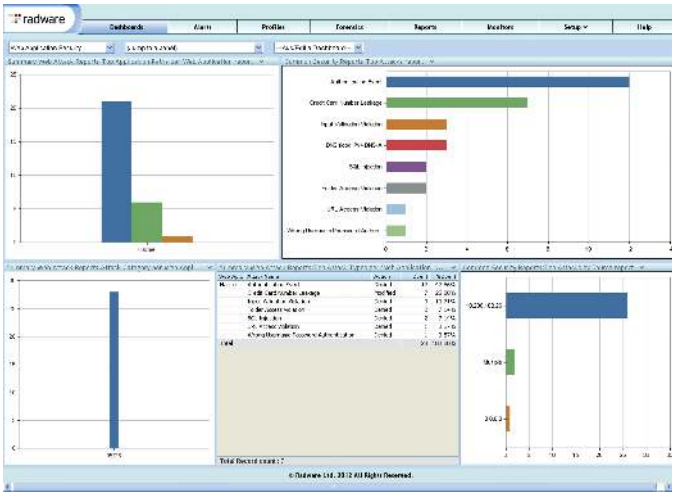
In addition, AppWall enables a complete **multi-tenancy** offering policy separation per Web Application, role-based access control per Web Application and reporting per Web Application.

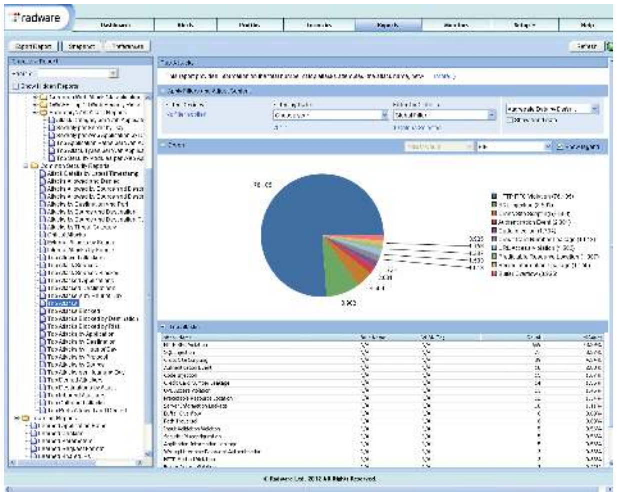


Detailed security and compliance reporting

AppWall reporting module offers dashboards, comprehensive security and compliance reports with the ability to drilldown to the security events, policies and statistics. Reports showing the correlation between network and application security events are also available offering an overall status at a glance.

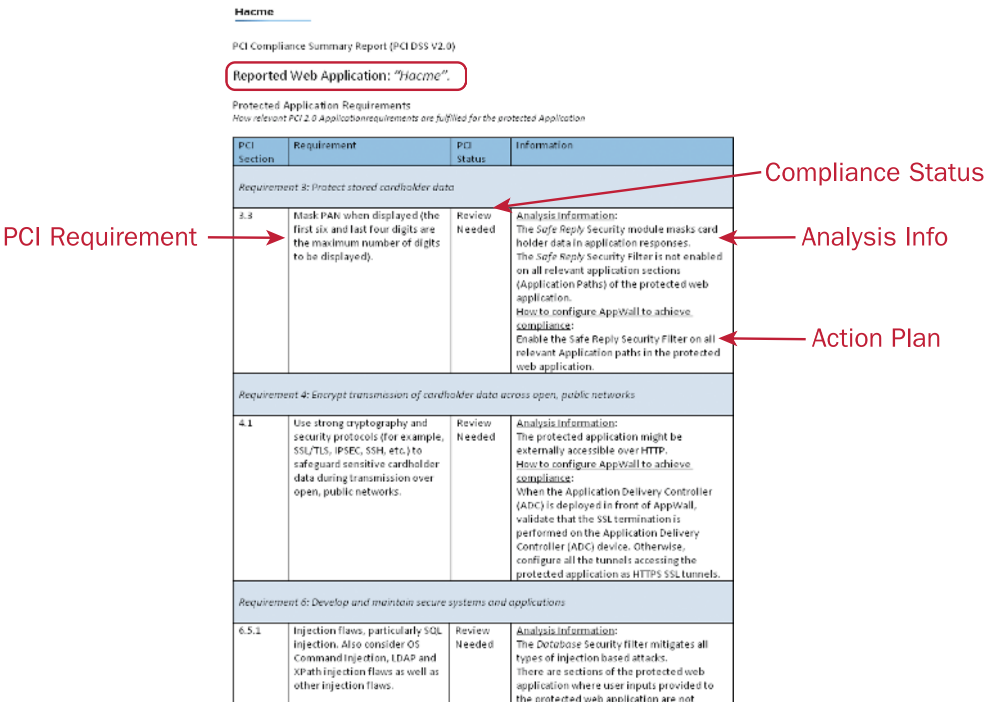
Centralized, comprehensive and correlated reports are available.





AppWall is the only solution with **tailored reports** addressing customers' applications requirements for **PCI-DSS compliance**, by providing detailed **step by step** per-application customized instructions.

Only solution with PCI-DSS tailored reports.



Hacme

PCI Compliance Summary Report (PCI DSS V2.0)

Reported Web Application: *"Hacme".*

Protected Application Requirements

How relevant PCI 2.0 Applicationrequirements are fulfilled for the protected Application

PCI Section	Requirement	PCI Status	Information
Requirement 3: Protect stored cardholder data			
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Review Needed	Analysis Information: The *Safe Reply* Security module masks card holder data in application responses. The *Safe Reply* Security Filter is not enabled on all relevant application sections (Application Paths) of the protected web application. How to configure AppWall to achieve compliance: Enable the Safe Reply Security Filter on all relevant Application paths in the protected web application.
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	Review Needed	Analysis Information: The protected application might be externally accessible over HTTP. How to configure AppWall to achieve compliance: When the Application Delivery Controller (ADC) is deployed in front of AppWall, validate that the SSL termination is performed on the Application Delivery Controller (ADC) device. Otherwise, configure all the tunnels accessing the protected application as HTTPS SSL tunnels.
Requirement 6: Develop and maintain secure systems and applications			
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Review Needed	Analysis Information: The *Database* Security filter mitigates all types of injection based attacks. There are sections of the protected web application where user inputs provided to the protected web application are not

The Unique AppWall Differentiators

After reviewing how AppWall answers the web applications security challenges, it's important to look at some business values and key differentiators it brings to your business.

Best and granular security coverage

Radware's AppWall protects Web applications from existing and emerging threats providing the best security coverage to your applications. Due to its support for both positive and negative security models, as well as, policies definition per application path, user or group of users (RBAC-role based access control), AppWall offers a full protection of on-line revenue generating web applications against known and zero-day web attacks.

Best security coverage

Fast, non-disruptive deployment and shortest time to protect

A truly unique value and key differentiator of AppWall is its capacity to provide fast and non-disruptive deployment attributed to its patented auto-policy generation and activation. With one click you can change from learning to active protection mode to apply immediate policy modifications upon application changes.

Shortest time to protect with minimal impact to businesses

AppWall support for policies is based on users' application roles and on application paths. It is provided by granular policies defined with adapted inspection and enforcement rules on different users and different zones of the application. These policy definition levels enable focused scanning and protection of the application, generating local independent policies and ultimately avoiding the disrupting consequences of global policies.

Scalable solutions

Scalable, pay as you grow model
AppWall is built on top of Radware's on demand architecture. This model allows the organizations to build their Web application security infrastructure progressively and extend as they grow. Organizations transparently purchase and add more resources thus allowing to scale to their progressive needs.

Best solution for online businesses

Best security solution for online businesses – the Attack Mitigation System
Radware's AppWall is part of the Radware's Attack Mitigation System (AMS) solution which covers the full range of security solutions for integrated application, network security and security tool management. In addition to its WAF, AppWall AMS provides a best of breed anti-DOS solution, an IPS, an NBA and a Reputation Engine. All the components are centrally managed and correlated reporting is available in Radware's Vision Security Information and Event Management (VSIEM) system. In addition, Radware offers the service of the ERT, Emergency Response Team, who are available 24/7 to help customers under attack. AMS lets its customers benefit from top of the line security solutions as well as the ability to correlate security events in a single dashboard and reporting tool.

Comprehensive reporting and best PCI-DSS compliance tailored report

Comprehensive PCI-DSS compliance solution and security reporting
AppWall fully complies with PCI-DSS 2.0 section 6.6 requirements and helps with section 3.3 requirement (masking of CC numbers). It provides the most advanced PCI compliance reports with a detailed step by step plan and application-customized configuration to achieve compliance. It also offers comprehensive centralization, correlated reporting and an events correlation engine for historical forensics.

Reduces TCO of security management

Reduces total cost of ownership (TCO) of security management
Due to Radware's AppWall auto-policy generation and ongoing learning, it can provide automatic real-time attach protection without human intervention thus reducing the total cost of ownership (TCO) of the solution.

Summary

With AppWall available both as a standalone and as part of its holistic AMS – Attack Mitigation System – solution, Radware is the only vendor to provide 360 degrees security coverage and reporting correlation for your applications.

AppWall is the most comprehensive, PCI-aware web application firewall built with deep expertise on web application threats and security. It understands the challenges organizations encounter when implementing a WAF solution. Its patented technology makes creating, maintaining and applying security policies fast and automated reducing the total cost of ownership by not requiring human intervention. Radware AppWall provides the widest security coverage, acting as a kind of virtual patch against zero-day attacks with the lowest false positives and minimal performance impact.