radware

The Technology Behind Radware's Web Application Security Solutions

WHITEPAPER

SHARE THIS WHITEPAPER

TABLE OF CONTENTS

THE WEB APPLICATION SECURITY SPACE

The Web application attack landscape is evolving quickly in conjunction with the ongoing changes around application development, hosting and maintenance. Trends such as DevOps and cloud migration are forcing application security teams to investigate new ways to keep up with new vulnerabilities and to manage policies across disparate hosting environments. One of the most commonly used products and services for web application security is the Web Application Firewall (WAF) that sits in front of the application server and inspects inbound and outbound requests/responses to ensure they comply with various policies.
The migration of applications and security functions to the cloud has made cloud-based WAF a popular deployment option, and is now offered by a variety of vendors. The following document reviews the security requirements for web application protection and analyzes Radware's Web application security offering against these requirements.

ASSESSING THE WEB APPLICATION ATTACK LANDSCAPE

OWASP Top 10

The top issues challenging application security are to a large degree defined by the Open Web Application Security Project (OWASP) Top 10 application threats. Organizations that seek effective application protection use the OWASP Top 10 as a starting point for ensuring protection from the most common and virulent threats or application misconfigurations that can lead to vulnerabilities.[1]

OWASP Top 10 — 2017

- **A1 — 2017-Injection**
- **A2 — 2017-Broken Authentication**
- **A3 — 2017-Sensitive Data Exposure**
- **A4 — 2017-XML External Entities (XXE)**
- **A5 — 2017-Broken Access Control**
- **A6 — 2017-Security Misconfiguration**
- **A7 — 2017-Cross-Site Scripting (XSS)**
- **A8 — 2017-Insecure Deserialization**
- **A9 — 2017-Using Components with Known Vulnerabilities**
- **A10 — 2017-Insufficient Logging & Monitoring**

Figure 1: OWASP Top 10 List

In addition to the OWASP Top 10 project, other threat classifications broaden the discussion analyzing and enumerating additional threats in the web app space listing more than 100 attack categories. These attack vectors may involve HTTP protocol manipulation leading to HTTP Request Splitting and HTTP Response Splitting attacks. They can also include various traffic processing weaknesses which may result with a denial of service, and other application-based attacks such as Buffer Overflow, Directory Traversal, OS Commanding, Path traversal and others.

False Positives vs. False Negatives

Web applications are 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.

A false negative is caused when an attack is not detected or blocked by the WAF. False positives are the opposite problem, i.e., heightened security policies that cannot effectively differentiate legitimate users from attacks and as a result block traffic from legitimate users. Typically, organizations are more sensitive to false positives to the point of lowering their overall security posture to the level of not blocking any legitimate traffic, at the risk of introducing false negatives.

1 Additional information about the OWASP Top 10 project can be found in the next document.

Protection Quality – Negative Security Model

The most common protection includes a negative security model, which defines what is disallowed, while implicitly allowing everything else. Most Web application security solutions leverage a negative security model that utilizes few signatures for specific, previously seen attacks. Since attack signatures may generate false positives by detecting legitimate traffic as attack traffic, such rules tend to be simplistic, trying to detect the obvious attacks. The result of this signature-based protection is protection against the lowest common denominator attacks with low protection quality.

Relying solely on negative security models, as is the case with most cloud WAF services, offers only partial protection against OWASP Top 10 risks. In most of the cases different risk categories will not be covered at all. Out of the OWASP Top 10 list, A2 — Broken Authentication, and A5 — Broken access control — and even common attacks such as CSRF are not covered by most cloud WAF services. Even for those risk categories which are addressed such as A1 — Injections, different application security services offer protection at a differing depth.

Protection Quality – Positive Security Model

Blocking Zero-day attacks, which are previously unseen attacks, requires a different approach rather than signature-based protection. A positive security model, which defines the set of allowed types and values, is required to provide a proper protection where signature-based protection cannot fill the gap. In the scenario where a parameter is defined in the Positive Security Model Policy to accept only Integer values, no SQL Injection can risk the application, even if there is no signature for that attack.

Most cloud WAF services do not offer proper positive security model policy capabilities. Usually these capabilities are limited to whitelisting URLs and source IP addresses. Even when these services offer some level of positive security model capabilities, there is a significant effort involved with creating such rules manually, directly impacting the cost of ownership. This tedious process is also prone to human errors where these rules may generate false positives of their own.

Auto Policy Generation

Clearly we want to avoid the risks for human errors involved with defining the positive security model rules and to reduce the cost of ownership involved with manual process of rules definition. Auto policy generation technology introduces machine-learning capabilities for automatic rule definition and maintenance. Different methodologies may be involved with the automation, where the idea is to identify the legitimate traffic to the application and profile the application based on that traffic.

Most WAF solutions, especially cloud services, do not offer any auto policy generation capabilities, while those who do offer such tools, are focused on very specific attack categories such as DDoS attacks.

Anti-Bot Protection

Bot-generated attacks targeting web application infrastructure are increasing in both volume and scope, with the list of attack vectors growing in support of a variety of objectives. Among the most common: web attacks, such as SQL injections and Cross-Site Request Forgery (CSRF), web scraping, web application DDoS, brute-force attacks on login pages for password cracking, comment spammers, clickjacking and fraud.

Some bot-generated attacks are static; others are dynamic over time. Simple, script-based bots are not much of a challenge to detect and block. The same cannot be said of more advanced bots. Those based on headless browser technology, such as PhantomJS, dramatically complicate the detection process by mimicking user behavior, passing challenges (such as CAPTCHA) and serving up dynamic IP addresses.

One of the most important weapons in the bot battle is IP-agnostic bot detection. Successful detection of attack source requires correlation across sessions. That is because bot-generated traffic may seem harmless— even legitimate—at a discrete, HTTP transaction level. However, the continuous nature of these attacks makes them a clear risk.

Managed Services and Support

Customers are increasingly requesting, if not requiring, a fully managed service options for security elements, including Web Application Firewalls. Beyond the obvious complexity of managing the positive and negative security model rules, today's attacks are dynamic and evolving, as evidenced by Radware's 2016-2017 Global Network and Application Security Report that highlights over 50% of attacks last more than one day, yet fewer than half of security teams are staffed to support attacks of this length. Additionally, teams managing application security are stressed by the rapid pace of new application development and application changes, all of which require vulnerability assessment and remediation in the form of security policies. Security service providers, including several in the cloud WAF space, have been adding some levels of managed service capabilities. However, relatively few of these come from teams with extensive real-world experience providing protection form advanced cyber-attacks and non are offering a fully managed services. Additionally, many require customers to purchase additional professional services in order to configure and manage policies on the WAF.

RADWARE'S WEB APPLICATION SECURITY OFFERINGS

Providing protection for web applications is a core part of Radware's security offering. Through its ICSA Labs certified Web Application Firewall – AppWall – and its Enterprise-grade Cloud WAF Service, Radware offers full web security protection including OWASP Top-10 coverage, advanced attack protection and Zero-day attack protection that automatically adapts your protections to evolving threats and protected assets. Web assets are always protected, even while applications constantly change and threats rapidly evolve, assuring web security is future proof.

- Radware's WAF provides complete protection against web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages and more. It is the only WAF that provides complete web application security with the ability to block attacks at the perimeter and ensuring fast, reliable and secure delivery of mission-critical web applications.

- Radware's Cloud WAF Service is based on Radware's WAF and is part of Radware's full suite of enterprise-grade cloud security services. Radware Cloud Security Services provide continuously adaptive, real-time protection for the most sophisticated DDoS and web security threats via best-in-class cloud WAF and DDoS protection services with the widest security coverage supporting both negative and positive security models.

Radware understands enterprises often face challenges in deploying and managing additional security products. In response, Radware offers its attack mitigation solution in a managed cloud service model that eliminates the need for internal security resources to provision, manage or maintain incremental technology in order to achieve optimal protection from today's cyber-security threats.

COMPREHENSIVE AND ACCURATE SECURITY COVERAGE

OWASP Top 10 Coverage

Radware's Web application security offerings 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, as listed in the previous section, including injections, cross site scripting (XSS), 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.

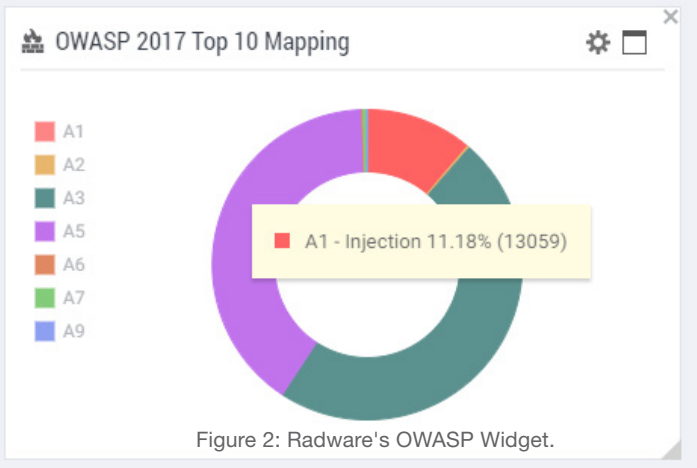


Figure 2: Radware's OWASP Widget.

By effectively providing defenses against those threats, Radware improves and maximizes the web applications security, blocking or diverting future attacks. In addition, Radware's Cloud WAF Service Portal provides complete visibility including the distribution of WAF events that are mapped to OWASP (Open Web Application Security Project) Top 10 categories.

Parsing and Normalization

Radware's WAF technology terminates the client TCP connection to detect different evasion techniques such as TCP packet reply attack. It then applies the HTTP RFC inspections to detect HTTP protocol manipulations such as HTTP Request Splitting attacks. Next it decodes and normalizes the client inputs to bring them to their basic ASCII representation, similarly to what the web server would do.

XML and JSON

A key element in the parsing of HTTP requests is the processing of XML and JSON inputs to extract the key/values pairs for proper inspection. XML and JSON key values are processed by web servers and can be used like any other client input to generate various attacks such as XML Injection attack.

Radware's WAF technology parses XML and JSON structures, allows definition of schema and structure restrictions and extracts key value pairs for detailed parameter inspection by all signatures and rules defined by Positive and Negative security model in the policy.

Security Filters

Once the parsing of the traffic is accomplished, the application security rules are applied through a set of security filters. To a large extent, these are the security policy building blocks applying the protection rules and signatures. There is a list of more than a dozen security filters focusing on different aspects and dimensions of web application security. Some are targeted to detect and block Injection attacks while others are defining restrictions on parameter values.

For instance, one such filter is protecting 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 Radware's WAF and Cloud WAF Service without an application modification.

Another example is a security filter which addresses session management attacks such as session fixation, cookie poisoning and session hijacking through encryption or signing of cookies to avoid manipulation on the client side.

Positive and Negative Security Model

The best security coverage with minimal impact on legitimate traffic is made possible by Radware's 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.

The negative security model protection is based on up to date signatures against known vulnerabilities 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. The positive security rules and mechanisms allow definition of value types and value ranges for all client side inputs, included encoded inputs and within structured formats as XMLs and JSONs. The positive security profiles, limiting the user input to only the level required by the application to properly function, thus blocking devastating Zero-day attacks.

LEVERAGING MACHINE-LEARNING ALGORITHMS TO AUTOMATE THE PROCESS OF SECURITY POLICY GENERATION

Auto Policy Generation Technology

Radware's WAF technology 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.

The Auto Policy Generation mechanism provides the best tool for automatically generating security policy for the secured Web application. 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. Building a security policy usually demands intensive work on the part of the administrator, while still leaving a system potentially open to attack due to inherent human error.

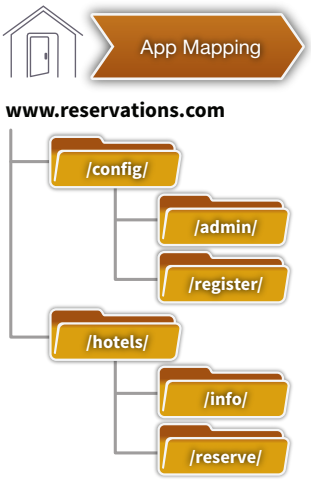
By leveraging machine-learning algorithms, Auto Policy Generation is designed to secure a web application as automatically as possible with little or limited user interaction. There are different attributes of the secured application, the environment needs that impact the process of policy generation. The system automatically discovers the structure of a web application, while at the same time, Auto Policy Generation sets the relevant security filters, analyzes traffic properties from the production environment and builds a dynamic network profile for a specific site according to which the Auto Policy Generation module automatically builds the policy.

Auto Policy Generation generates rules for different security filters. For example, when enabled, the Parameters security filter rules are automatically generated by the Auto Policy Generation module. When enabled, the Allow List security filter will automatically white list the allowed URLs to be accessed.

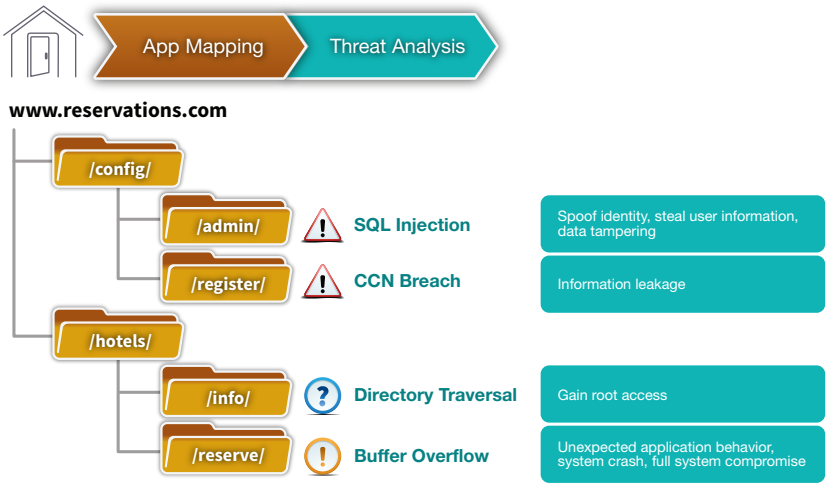
At the HTTP parsing module, various settings can be automatically optimized and modified by the systems. Examples for such automatic modification include message size settings for the request and HTTP parsing properties exceptions such as allowing High ASCII chars in the HTTP parameter value. Such HTTP RFC violation exceptions will be defined automatically either on specific URLs, or globally if required across many resources in the application.

FOUR STEPS OF AUTO POLICY GENERATION

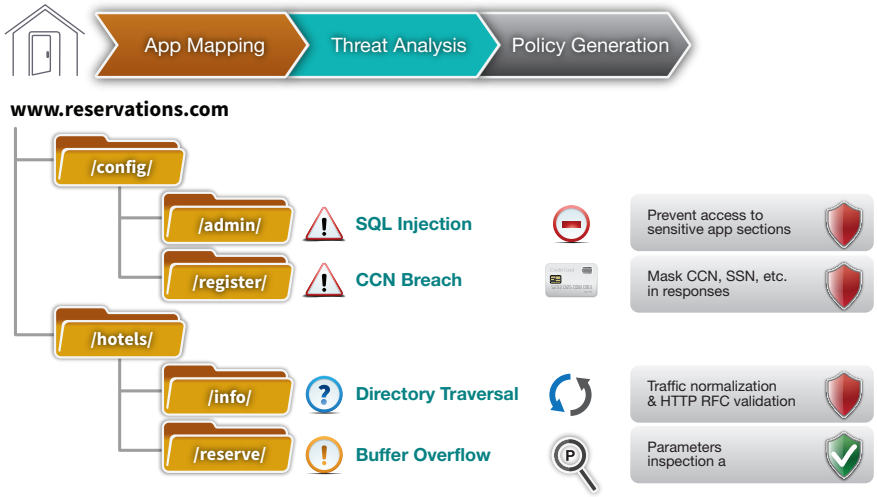
Step #1: Application Mapping



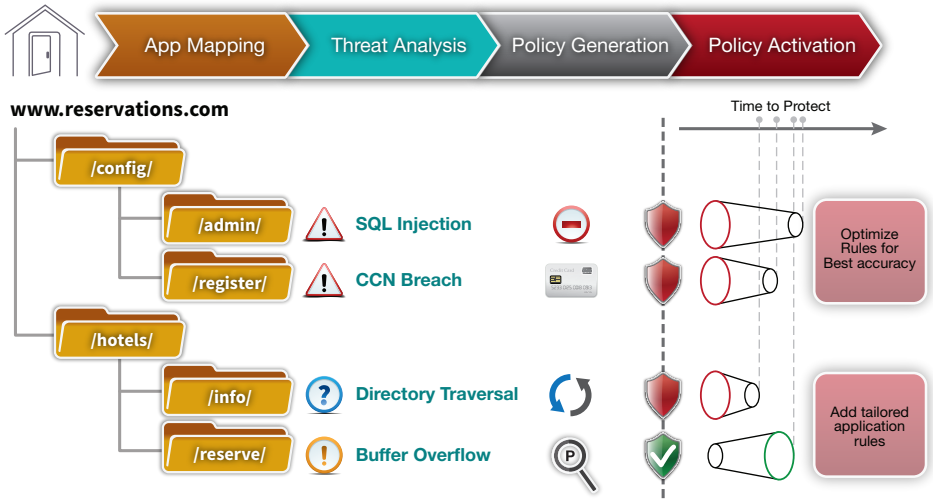
Step #2: Threat Analysis – covering over 150 attack vectors



Step #3: Policy Generation with auto-optimization for out-of-the-box rules to minimize false positives



Step #4: Policy Activation



The Human Factor behind the Automation

In the case of Radware's Cloud WAF Service, once a policy is generated automatically, it is reviewed by Radware's security experts to validate the quality of the generated policy. It will be reviewed to ensure validity of the policy, integrity, false positive risks, and false negative risks. This is also available to Radware's WAF customers who chose to add the ERT Premium managed service (more on that below).
Radware's security and cloud experts have extensive real-world experience providing protection form advanced cyber-attacks with deep knowledge of Radware's WAF technology.

How Auto Policy Impacts the Quality of Protection

Beyond the obvious value of reducing the risk of human errors when expecting the customer to generate the security policy rules and the cost of ownership involved with such activities, the most important value involved with Radware's Auto Policy Generation capabilities has to do with the quality of protection!

The fact that different levels of protection can be automatically learned and optimized by the auto policy generation system allows enabling ALL RULES and activate various security filters. With this capability, the rules and filters are being optimized and updated automatically, thereby removing the risk of generating false positives.

If we take a simple example of the Always True Expression type of SQL Injection such as "OR 1 = 1," we can easily understand that rules which are aimed to block such inputs will have a high tendency to generate false positives. If there is no automatic mechanism to create such policy exceptions, it will not be reasonable to define such rules which may block legitimate traffic. As so, most cloud WAF vendors do not define such risky rules.

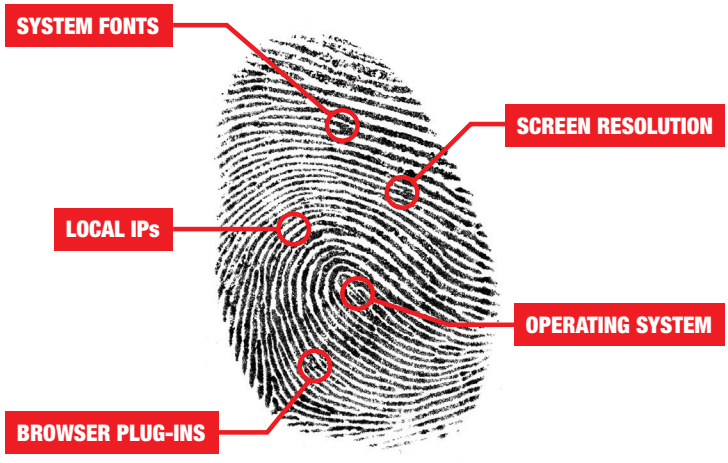
Radware's auto policy generation technology allows enabling all rules, while automatically creating the exceptions for these rules in those areas where these rules generate false positives, while properly securing the rest of the application. All HTTP RFC rules are enabled, all Injections rules are applied and being optimized automatically. This alone offers a dramatically higher quality of protection even if positive security model is not involved.

PROTECTING FROM BAD BOTS

IP-Agnostic Device Fingerprinting

Radware's Device Fingerprinting technology offers 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. Radware's WAF can detect sources operating in a dynamic IP environment and activity behind a sNAT (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. Radware can track the device activity and correlate the source security violations across different sessions over time.

Device fingerprinting implemented in Radware's WAF offerings uses dozens of characteristics of the device in a unique way to identify and distinguish it from all others. Using proprietary tracking, Radware can generate device reputational profiles that combine both historical behavioral information aiding in the detection and mitigation of threats such as DDoS, intrusions and fraudsters alike. By correlating past security violations of specific devices over time and across visits regardless of changing IP address, Radware can consistently and accurately profile legitimate and illegitimate users.



Plugins Info	version=1.7.0_51;); (; application/x-java-bean;jpi-version=1.7.0_51;); (; application/x-java-vm-npruntime;); (; application/x-java-applet;deploy=10.51.2;); (application/x-java-applet;javafx=2.2.51;). Plugin 10: Microsoft® DRM; DRM Netscape Network Object; npdrmv2.dll; (Network Interface Plugin; application/x-drm-v2; nip). Plugin 11: Microsoft® DRM; DRM Store Netscape Plugin; npwmsdrm.dll; (Network Interface Plugin; application/x-drm; nip). Plugin 12: Native Client; ; ppGoogleNaClPluginChrome.dll; (Native Client Executable; application/x-nacl;) (Portable Native Client Executable; application/x-pnacl;). Plugin 13: Picasa; Picasa plugin; npPicasa3.dll; (3.1; application/x-picasa-detect; pinstall). Plugin 14: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin.dll; (SDP stream descriptor; application/sdp; sdp) (SDP stream descriptor; application/x-sdp; sdp) (RTSP stream descriptor; application/x-rtsp; rtsp,rts) (QuickTime Movie; video/quicktime; mov,qt,mqv) (AutoDesk Animator (FLC); video/flc; flc,fli,cel) (WAVE audio; audio/x-wav; wav,bwf) (WAVE audio; audio/wav; wav,bwf). Plugin 15: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin2.dll; (AIFF audio; audio/aiff; aiff,aif,aifc,cdda) (AIFF audio; audio/x-aiff; aiff,aif,aifc,cdda) (uLaw/AU audio; audio/basic; au,snd,ulw) (MIDI; audio/mid; mid,midi,smf,kar) (MIDI; audio/x-midi; mid,midi,smf,kar) (MIDI; audio/midi; mid,midi,smf,kar) (QUALCOMM PureVoice audio; audio/vnd.qcelp; qcp). Plugin 16: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin3.dll; (GSM audio; audio/x-gsm; gsm) (AMR audio; audio/amr; AMR) (AAC audio; audio/aac; aac,adts) (AAC audio; audio/x-aac; aac,adts) (CAF audio; audio/x-caf; caf) (AC3 audio; audio/ac3; ac3) (AC3 audio; audio/x-ac3; ac3) (MPEG media; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa). Plugin 17: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin4.dll; (MPEG media; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (MPEG audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a) (MPEG audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a) (3GPP media; video/3gpp; 3gp,3gpp). Plugin 18: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin5.dll; (3GPP media; audio/3gpp; 3gp,3gpp) (3GPP2 media; video/3gpp2; 3g2,3gp2) (3GPP2 media; audio/3gpp2; 3g2,3gp2) (SD video; video/sd-video; sdv) (AMC media; application/x-mpeg; amc) (MPEG-4 media; video/mp4; mp4) (MPEG-4 media; audio/mp4; mp4) (AAC audio; audio/x-m4a; m4a) (AAC audio (protected); audio/x-m4p; m4p) (AAC audio book; audio/x-m4b; m4b). Plugin 19: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin6.dll; (Video (protected); video/x-m4v; m4v) (MacPaint image; image/x-macpaint; pntg,pnt,mac) (PICT image; image/pict; pict,pic,pct) (PICT image; image/x-pict; pict,pic,pct) (PNG image; image/png; png) (PNG image; image/x-png; png) (QuickTime image; image/x-quicktime; qtif,qti) (SGI image; image/x-sgi; sgi,rgb) (TGA image; image/x-targa; targa,tga). Plugin 20: QuickTime Plug-in 7.7.3; The QuickTime Plugin allows you to view a wide variety of multimedia content in Web pages. For more information, visit the <A HREF=http://www.apple.com/quicktime/>QuickTime</A> Web site.; npqtplugin7.dll; (TIFF image; image/tiff; tif,tiff) (TIFF image; image/x-tiff; tif,tiff) (JPEG2000 image; image/jp2; jp2) (JPEG2000 image; image/jpeg2000; jp2) (JPEG2000 image; image/jpeg2000-image; jp2) (JPEG2000 image; image/x-jpeg2000-image; jp2). Plugin 21: Shockwave Flash; Shockwave Flash 11.6 r602; NPSWF32_11_6_602_171.dll; (Adobe Flash movie; application/x-shockwave-flash; swf) (FutureSplash movie; application/futuresplash; spl). Plugin 22: Shockwave Flash; Shockwave Flash 12.0 r0; pepflashplayer.dll; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 23: Silverlight Plug-In; 5.1.20913.0; npctrl.dll; (npctrl; application/x-silverlight; scr) (; application/x-silverlight-2;). Plugin 24: VMware Remote Console Plug-in; VMware Remote Console Plug-in; np-vmware-vmrc.dll; (VMware Remote Console Plug-in; application/x-vmware-remote-console-2012;). Plugin 25: VMware Remote Console and Client Integration Plug-in; VMware Remote Console and Client Integration Plug-in; np-vmware-vmrc.dll; (VMware Remote Console and Client Integration Plug-in; application/x-vmware-remote-console-2011;). Plugin 26: Widevine Content Decryption Module; Enables Widevine licenses for playback of HTML audio/video content.; widevinecdmadapter.dll; (Widevine Content Decryption Module; application/x-ppapi-widevine-cdm;). Plugin 27: Windows Media Player Plug-in Dynamic Link Library; Npdsplay dll; npdsplay.dll; (Media Files; application/asx; *) (Media Files; video/x-ms-asf-plugin; *) (Media Files; application/x-mplayer2; *) (Media Files; video/x-ms-asf; asf,asx,*) (Media Files; video/x-ms-wm; wm,*) (Media Files; audio/x-ms-wma; wma,*) (Media Files; audio/x-ms-wax; wax,*) (Media Files; video/x-ms-wmv; wmv,*) (Media Files; video/x-ms-wvx; wvx,*). Plugin 28: Windows Presentation Foundation; Windows Presentation Foundation (WPF) plug-in for Mozilla browsers; NPWPF.dll; (XAML Browser Application; application/x-ms-xbap; xbap) (XAML Document; application/xaml+xml; xaml). Plugin 29: iTunes Application Detector; iTunes Detector Plug-in; npitunes.dll; (This plug-in detects the presence of iTunes when opening iTunes Store URLs in a web page with Firefox.; application/itunes-plugin;).
Fonts Info	Adobe Hebrew|Agency FB|Aharoni|Andalus|Angsana New|AngsanaUPC|Arabic Transparent|Arial Black|Arial|Bauhaus 93|Bell MT|Bodoni MT|Bookman Old Style|Broadway|Browallia New|BrowalliaUPC|Calibri|Californian FB|Cambria Math|Cambria|Candara|Castellar|Centaur|Century Gothic|Colonna MT|Comic Sans MS|Consolas|Constantia|Copperplate Gothic Light|Corbel|Cordia New|CordiaUPC|Courier New|David|DilleniaUPC|Engravers MT|Eras Bold ITC|EucrosiaUPC|Forte|FrankRuehl|Franklin Gothic Heavy|Franklin Gothic Medium|FreesiaUPC|French Script MT|Georgia|Gigi|Goudy Old Style|Haettenschweiler|Harrington|Impact|Informal Roman|IrisUPC|JasmineUPC|Kartika|KodchiangUPC|Levenim MT|LilyUPC|Lucida Bright|Lucida Console|Lucida Fax|Lucida Sans Unicode|MS Mincho|MS Reference Sans Serif|Magneto|Marlett|Matura MT Script Capitals|Microsoft Sans Serif|Miriam Fixed|Miriam|Narkisim|Niagara Solid|Palace Script MT|Palatino Linotype|Papyrus|Perpetua|Playbill|Rockwell|Rod|Script MT Bold|Segoe UI|Showcard Gothic|Simplified Arabic Fixed|Simplified Arabic|Snap ITC|Sylfaen|Symbol|Tahoma|Times New Roman|Traditional Arabic|Trebuchet MS|Tw Cen MT Condensed Extra Bold|Verdana|Vladimir Script|Vrinda|Webdings|Wide Latin
Canvas Info	790d501ff7a93d9003dcf73c2004bb0cadca7a8a1263a5814ef66b40f02da3d6
Local IP's	10.206.102.26

Figure 3: Example of a device fingerprint created by Radware

FULLY MANAGED WEB SECURITY SOLUTIONS

Understanding the challenges organizations face in managing and maintaining web application security solutions, Radware offers solutions that are fully managed by Radware's security experts.

- Radware's Cloud WAF Service is a fully managed, 24x7 service provided by Radware's Emergency Response Team (ERT) – a dedicated group of security experts that assume full responsibility to configure and update security policies as well as actively monitor, detect, alert and mitigate attacks in real-time.

- With Radware's WAF, AppWall, customers can also get the managed service – ERT Premium – provided by Radware's ERT security experts that includes the ongoing management, monitoring and configuration of the on-premise WAF device.

ANALYSIS OF THE RADWARE'S WAF CAPABILITIES

The table below highlights some of the key features necessary for effective WAF and DDoS protection, and analyzes Radware's WAF and Cloud WAF Service offering against these required features.

Feature	Description	Radware
Positive Security Model	A positive security model is one that defines what is allowed, and rejects everything else. This should be contrasted with a negative security model, which defines what is disallowed, while implicitly allowing everything else.	Radware's WAF technology automatically learns the web application structure and appropriate requests and responses. This allows Radware to maintain an effective positive security model that can help block zero-day attacks.
Machine-learning based Auto Policy Generation	Leveraging machine-learning algorithms, auto-policy generation helps automatically generate a security policy tailored to the specific application. The auto-policy help creates a positive security model for the application and configure the negative security policy while automatically correcting false positives.	Automatically maps the application structure, performs threat analysis process, auto generates a tailored policy for the secured app, and automatically updates policy with application changes.
Cross Site Request Forgery (CSRF)	CSRF is a type of malicious website exploit where unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser	Radware offers CSRF protection based on a reference header validation. This mechanism allows robust CSRF protection by blocking requests if they are not coming from the trusted referrer.
Tailored granular policies for custom applications	Effectively protecting custom applications requires granularity in application mapping and policy development. The lack of granular policies limits the tailoring of policies for particular parts of the applications and means the entire application needs to be scanned for new policies based on changes to the application.	Radware offers very granular application mapping down to the folder or file level. This enables more tailored protection for different parts of the application and speeds up the time to protection following changes to the application.
Protection from Session or Cookie Hijacking	Session hijacking is one of the OWASP Top 10 threats, and involved the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.	Radware provides session and cookie hijacking protection by validating that users do not modify cookies and those user sensitive cookies such as session cookies are not being sent by different devices.
Mitigation Platform Stability	The ability of a cloud-based DDoS provider to deliver service is only as reliable as the availability of its mitigation platform. Outages of these platforms result in performance impacts or event unavailability of customers' websites.	Radware maintains a separate infrastructure for handling large volumetric DDoS attacks. This eliminates impact on legitimate traffic running through Radware's cloud services when there is an attack. Additionally, Radware has maintained its cloud DDoS mitigation platform without outage since its inception in 2013.
Data Leak Prevention (DLP) for Sensitive Data	DLP features protect against the loss of sensitive data via application attacks that exploit vulnerabilities to force applications to reply to malicious requests with sensitive data (e.g., credit card numbers)	Radware offers DLP features that mask or block sensitive information in application replies including CCN, SSN and server error messages. Policies for specific data can be applied globally to the application or on specific folders.
Device Fingerprinting	IP address-based bot or attack detection has become insufficient due to the various ways that IP addresses can be masked (e.g., through anonymous proxies, global NATs) or spoofed. Advanced security systems are using device fingerprints as a more accurate means of attack traffic sourcing or malicious behavior tracking.	Radware WAF offers a web client fingerprint being generated on every new session to allow IP agnostic attack source detection and mitigation. This delivers unique protection from continuous attack vectors such as web scraping, brute force attacks on login pages and Advanced Availability threats such as HTTP Dynamic Flood and Low & Slow, where the correlation across multiple sessions is essential for proper detection and mitigation.

UNMATCHED, ADAPTIVE WEB SECURITY PROTECTION

The rapidly evolving threat landscape poses a daunting challenge for the protection of web applications. Attacks on web assets are continuously growing in complexity and persistency. Zero-day attacks exploit newly discovered vulnerabilities as soon as they are discovered while attackers frequently hide their real IP addresses behind CDNs, or commonly spoof IP addresses in order to obfuscate their identity, thus rendering invaluable all IP blacklisting techniques. Bots, crawlers and spammers keep crowding web assets, evolving their techniques to disguise their nonproductive traffic as legitimate.

Radware provides adaptive web security protection through its Web Application Firewall and Cloud WAF Service that go beyond signature-based protection and blacklisted IP addresses, to provide hassle-free, automated protection for today's dynamic landscape.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of cyber security 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 services to enterprises globally. Radware's solutions empower more than 12,500 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: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, 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.