radware

Whitepaper: **Application Protection Solutions**

The Technology Behind Radware Cloud Application Protection Service

Table of Contents

The Web Application Security Space

Applications are at the core of every organization – from sophisticated e-commerce engines to cloud-based productivity solutions and personal tools on mobile phones. Applications are your primary revenue generators, growth and retention engines, and your main customer engagement platform.

The web application attack landscape is evolving in conjunction with ongoing changes around application development, hosting and maintenance. Whether on-premise or cloud based, applications are now scattered across different platforms and frameworks. Applications require updating and must comply with information security policies. In addition, they rely on the availability of information from third-party services that they interact with via APIs. As a result, the attack surface targeting applications is greater and their exposure to risk is increasing.

Applications constantly change and security policies must adapt accordingly to safeguard applications and the data they host. Protecting against an expanding variety of attack methods and real-time mitigation to automated attacks while minimizing false positives can be difficult. It often necessitates manual labor, operational costs and expertise that many organizations can't sustain by themselves. DevOps methodologies, modern app architectures 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.

This solution brief reviews the security requirements for web application and API protection and discusses Radware's holistic application protection solution.

Assessing the Application and API Attack Landscape

Application Vulnerabilities

The top issues challenging application security are 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.

OWASP Top 10 (2021)

- **A01:** Broken Access Control
- **A02:** Cryptographic Failures
- **A03:** Injection
- **A04:** Insecure Design
- **A05:** Security Misconfiguration
- **A06:** Vulnerable and Outdated Components
- **A07:** Identification and Authentication Failures
- **A08:** Software and Data Integrity Failures
- **A09:** Security Logging and Monitoring Failures
- **A10:** Server-Side Request Forgery (SSRF)

Figure 1: OWASP Top 10 Application Security Risks

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.

API-Related Risks

As the popularity of applications continues to grow, the adoption of APIs is increasing. APIs enable applications to interoperate with other services by integrating different clients and applications across multiple services.

APIs are used in a variety of modern applications, and the number of use cases is continuously growing. The most common examples are:

- Web APIs, mostly in single-page applications
- Mobile applications
- Embedding public and third-party APIs as external services into an existing application (such as Google Maps APIs)

APIs are also used to save time and facilitate the flexible development of microservices architecture apps, agile development methodologies and continuous delivery.

DevOps environments—with the ever-increasing demand for continuous delivery—require complete process automation utilizing APIs across the board:

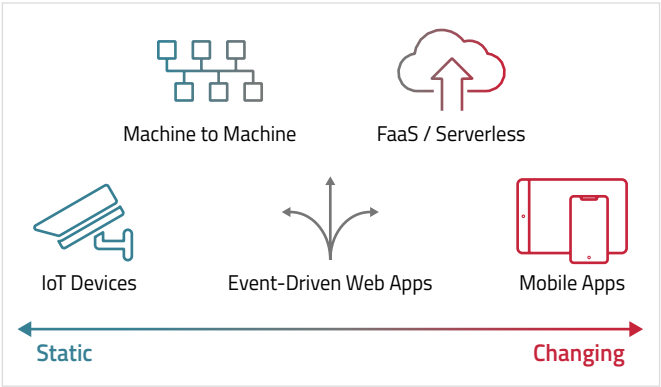


Figure 2: The API economy and use cases

- Service provisioning and management (for example, Amazon Web Services API)
- Platform management apps
- Continuous delivery process automation

The API Security Problem

While APIs bring tremendous benefits, they also introduce new security risks, including service disruption and data theft.

APIs are vulnerable to all types of attacks and threats against web applications. Most of the APIs are REST APIs with JSON bodies (REST-JSON), which run on top of the HTTP protocol. As such, most of the web application security risks are just as relevant for APIs. Additionally, APIs introduce other security challenges mostly around access control, as the APIs may be served independently and not only as a whole set of web application resources.

Figure 3

Top 10 API Security Vulnerabilities

OWASP API Security Top 10

API1 - 2019 Broken Object Level Authorization
API2 - 2019 Broken user Authentication
API3 - 2019 Excessive Data Exposure
API4 - 2019 Lack of Resources & Rate Limiting
API5 - 2019 Broken Function Level Authorization
API6 - 2019 Mass Assignment
API7 - 2019 Security Misconfiguration
API8 - 2019 Injection
API9 - 2019 Improper Assets Management
API10- 2019 insufficient Logging & Monitoring

APIs submit and retrieve data and may expose application architecture and potentially sensitive data. As a result, they have increasingly become a target for attackers trying to find easier ways into applications.

API Protection Considerations

Because of the wide variety of API threats, API protection requires a combination of access controls (such as authentication and authorization mechanisms), injection prevention, bot management, DoS mitigation and more. Hackers may also try some API-specific attacks, such as using invalid schemas, parameter tampering or token manipulations. In addition to supporting OpenAPI, an API protection solution should also cover unknown, undocumented APIs.

Figure 4

Most common attacks against APIs

*Source: Radware application security research

Access Violation	Denial of Service	Irregular Expressions	Protocol Attacks
38%	36%	33%	30%

The Challenge of False Positives and False Negatives

Web applications and API services are being accessed both by desired legitimate users and undesired attackers (malignant users whose goal is to harm the application and/or API end points). One of the biggest challenges in protecting web applications and API services is the ability to accurately differentiate between the two and identify and block malicious traffic while ensuring continuous service for legitimate users.

A false negative is caused when an attack is not detected or blocked by the WAF. False positives are the opposite problem – heightened security policies that cannot effectively differentiate legitimate users from attacks and therefore block legitimate users' transactions. 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.

Protection Quality – Negative Security Model

The most common protection scheme is based on 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 signatures for specific, previously witnessed attacks. To avoid false positives, many organizations tend to reduce the coverage of their negative security policies, focusing on known attack types and thereby resulting in a low protection quality.

While a well-tuned policy based on a negative security protection can provide reasonable protection against known attacks, it still leaves applications exposed to zero-day attacks. Certain OWASP Top 10 vulnerabilities (broken authentication, broken access control and more) can't be properly addressed with an application solution that relies solely on a negative security model.

Protection Quality – Positive Security Model

Protecting applications and APIs against zero-day attacks (previously unseen attacks) requires a positive security model that defines the set of allowed transactions, data types and values to ensure only legitimate activity is taking place. For example, if a positive security rule defines the allowed value type of a certain parameter as integer only, it will prevent SQL injection attacks even if there is no signature defined for that attack.

Most application protection solutions offering a positive security model often require significant human effort to create such rules manually, directly impacting the continuous validity of such a solution, and subsequently, its total cost of ownership. This tedious process is also prone to human errors where these rules may generate false positives.

Robust Security Policy Baselines

To reduce the effort involved in creating security policies and avoid the risks of human errors, an application protection solution should provide reliable negative and positive security policy baselines based on global network intelligence feed as well as vertical and geo big data machine-learning-based analysis.

Continuous Policy Optimization

It is critical to constantly optimize security polices to maintain high security levels and minimize false positives. To achieve both without high operational costs and manual intervention requires an application protection solution capable of automatically reviewing log files on a regular basis and artificial intelligence to refine existing policy rules or provide rule optimization recommendations.

Anti-Bot Protection

Competitors and adversaries often deploy “bad” bots that leverage different methods to achieve nefarious objectives. This includes account takeover, scraping data, denying available inventory and launching denial-of-service (DoS) attacks with the intent of stealing data or causing service disruptions. Sophisticated large-scale attacks often go undetected by conventional mitigation systems and strategies because bots have evolved from basic scripts to large-scale distributed bots with human-like interaction capabilities to evade detection mechanisms such as CAPTCHA and other challenges.

As the use of APIs increases, bot attacks targeting APIs are also becoming more common. Detecting malicious behavior on APIs is different than web and mobile applications and requires distinguishing between “good” and “bad” API calls.

To effectively stay ahead of the threats bad bots impose on web applications and APIs requires a holistic approach that can correlate several bad bot characteristics for accurate detection and apply the most effective mitigation technique without impacting legitimate users. Here are some key capabilities:

- Effective device and browser fingerprinting (for example, detecting bots with changing IP addresses)
- Intent and behavioral analysis (such as correlating of intent signatures across devices)
- Collective bot intelligence and threat research
- Dedicated protection model to safeguard APIs against bot attacks
- Identifying authentic API access patterns to pinpoint malicious access attempts

An enterprise-grade bot detection engine should have deep-learning and self- optimizing capabilities to identify and block constantly evolving bots that alter their characteristics to evade detection by basic security systems.

Managed Services and Support

As application attacks increase in complexity, so must application security solutions. Deploying a WAF or a bot protection solution often leads to false positive. The amount of human resources and expertise required to keep the application protection service updated across heterogeneous environments while constantly tuning security policies is something many organizations don’t have the resources for.

This is why buying a best-of-breed application protection solution is often not enough. One should also acquire access to professional services that support the deployment and maintenance of the solution as well as fight application attacks as they occur in real time. While a wide variety of application protection solutions exist in the market, not all vendors can offer a complementary expert services.

Radware's Application Protection Solution

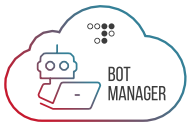
Radware Cloud Application Protection Services is a one-stop solution that provides a comprehensive set of application protection tools, including its market-leading WAF, Bot Manager, API, Client-side, and application DDoS protection, as well as a live threat intelligence feed. Radware's Cloud Application Protection portal provides a single interface for all Radware Cloud Application Protection solutions with ease of configuration, granular control options and detailed analytics into all application security events and protection metrics. This "single pane of glass" view helps you manage your security solutions in a frictionless manner with reduced overheads.

WAF

Radware's adaptive and automated WAF protects against web application attacks, hacking and other vulnerabilities. The WAF technology uses a positive security model that automatically learns the patterns of legitimate user activities, automatically builds security policies tailored to allow those activities, and blocks any action that deviates from these patterns of legitimate behavior. Radware's combination of negative and positive security models provides a complete level of protection against OWASP Top 10 threats and zero-day attacks that WAFs leveraging negative security models cannot stop because they rely on blocklists of known attack signatures.

API Protection

A dedicated, end-to-end API protection solution ensures the security of applications, APIs, development platforms and infrastructure. It maps the API attack surface by leveraging an automated discovery algorithm to discover APIs and generates tailored security policies to detect and block API-focused attacks in real time. It also uses a combination of access controls, data leakage prevention, bot management and DoS mitigation tools to protect against the growing array of API security threats listed in the OWASP TOP 10 API Security Vulnerabilities.



Bot Manager

Radware bot management and mitigation solution can accurately detect and distinguish between human traffic, good bots and malicious bots, and ensures comprehensive protection of web applications, mobile apps and APIs from automated threats and bots. It provides precise bot management across web, mobile and API traffic by combining behavioral modeling for granular intent analysis, collective bot intelligence and fingerprinting of browsers, devices and machines. It protects against the OWASP Top 21 Automated Threats, including account takeover, credential stuffing, brute force, denial of inventory, DDoS, ad and payment fraud and web scraping to help organizations safeguard and grow their online operations. Its one-of-a-kind mobile attestation for both Android and iOS (Google and Apple) devices along with its proprietary identity authentication engine stops bot attacks on native mobile apps before they materialize and take a toll on your infrastructure.

Radware Bot Manager provides the widest choice of mitigation options, including a Blockchain-based Cryptographic Challenge that exhausts malicious bot resources while making for a seamless and CAPTCHA-free user experience.

Web DDoS Protection

Industry-leading application-layer (L7) protection against DDoS attacks, based on Radware's unique machine-learning based behavioral detection that distinguishes between legitimate and malicious traffic, and automatically generates granular signatures in real-time to protect against zero-day attacks. With unique hybrid, always-on and on-demand cloud DDoS service deployment options, Radware's Cloud DDoS Protection Service provides best-in-class security against a wide variety of threats, including HTTP Floods, HTTP bombs, low- and-slow assaults, Brute Force attacks, and disruptive web DDoS Tsunamis.

Client-Side Protection

Advanced client-side protection ensures the protection of end users' data when interacting with any third-party services in the application supply chain. Easily block requests to suspicious third-party services in your supply chain and adhere to data security compliance standards. Protect against client-side attacks coming from third-party JavaScript services (Formjacking, Skimming/Magecart), automatically and continuously discover all third-party services in your supply chain with detailed activity tracking, and get alerts and threat level assessment according to multiple indicators, including script source and destination domain. Prevent data leakage by blocking unknown destinations or legitimate destinations with illegitimate parameters, as well as DOM-based XSS. Lastly, Radware Client-Side Protection's unique surgical enforcement capabilities block only nefarious scripts and don't stand in the way of vital JavaScript services.

ERT Active Attackers Feed

Radware ERT Active Attackers Feed serves as your very own network intelligence agency. It enhances the protection of applications and data centers by introducing a preemptive protective layer on top of Radware's attack mitigation solutions. The feed supplies Radware devices and Radware cloud security services with a list of attackers that were recently involved in a security incident, such as a DDoS attack, an application attack, an intrusion, or a scanning attack. This enables the platform or service to preemptively block known attackers before they come anywhere near your assets and initiate an attack.

Widest Application Vulnerability Protection with Radware's WAF Technology

Radware's web application protection solution delivers comprehensive and accurate security coverage of known and unknown web application threats. It provides full security coverage out-of-the-box against OWASP Top 10 threats. Its protection extends to the Web Application Security Consortium (WASC) threats as well as zero-day attacks.

By effectively providing defenses against those threats, Radware improves and maximizes the web application's security, blocking or diverting future attacks.

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 a credit card number (CCN) or social security number (SSN). Masking CCNs is an actual requirement of the PCI standard and is achieved with Radware's WAF Service without an application modification.

Another example is a security filter that 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 allows granular and accurate policy definitions, therefore avoiding false positives and false negatives.

The negative security model protection is based on thousands of up-to-date signatures against known vulnerabilities that provide the most accurate detection and blocking technology of application vulnerability exploits. The positive security model is useful in stopping zero-day attacks by automatically creating allow lists of path extensions and method access, API endpoints and paths, and API query parameters (types, ranges, RegEx). It also creates allow lists of specific domains/IPs to prevent SSRF/RFI attacks. When it comes to browser-side protection Radware Client-Side Protection solution utilizes positive security to create allow lists of third-party domains and IP to protect against data leakages and supply-chain attacks. It is important to mention that the positive security profiles limit the user input to only the level required by the application to function properly, thus blocking zero-day attacks.

Application Protection Policy Generation

Building an optimized, application-specific security policy covering both negative and positive security path extensions rules typically demands intensive work on the part of the administrator while still leaving a system open to attack due to inherent human error.

Radware's Cloud WAF solution leverages machine learning algorithms to automatically optimize security policies for each specific application. These algorithms enable organizations to:

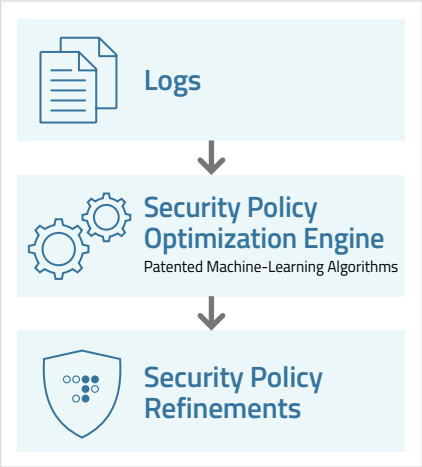
- Reduce the amount of human resources required to generate such extensive security policies
- Eliminate human errors in the process
- Leverage Radware's negative and positive protection models
- Reduce false positives and false negatives
- Remain accurate as the application evolves by automatically adjusting the policy for each new version introduced

By leveraging machine learning algorithms, Radware Cloud WAF secures a web application with as little human intervention as possible. The system automatically analyzes traffic properties from the production environment to find false positives and fix them. It does so by allowing specific parameters for specific paths, and by adding allowed extensions and methods, thus automatically creating a dynamic security profile for a specific site to effectively protect against injections and path access violations.

Automated Security Policy Refinement

A primary challenge of application protection is keeping pace with application development and new threats while achieving accurate security policies with minimum false positives. Typically it requires hands-on management of security policies by reviewing logs with thousands of entries and manually fine-tuning security rules. It is a tedious task that increases operational expenses and introduces manual errors.

Radware's automated policy optimization engine overcomes these challenges by using a frictionless policy optimization engine based on advanced machine-learning algorithms that automatically—and continuously—reviews large log files in pre-defined intervals, identifies anomalies with high level of accuracy and automatically suggests policy refinements for the ERT team to examine and prioritize, and for customers to review and approve. It is an error-proof mechanism that provides the following benefits:



- More accurate, tighter protection
- Fewer false positives
- Improved efficiency and reduced operational costs

How Auto Policy Optimization Impacts the Quality of Protection

The fact that different levels of protection can be automatically learned and optimized by the system allows enabling ALL RULES and activates various security modules. 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 that may block legitimate traffic. Many cloud WAF vendors do not define such risky rules.

Radware CWAF allows all rules to be enabled while automatically creating the exceptions for areas where these rules generate false positives while properly securing the rest of the application. 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.

Protection from Bad Bots

Over half of all internet traffic is generated by bots – some legitimate, some malicious. Competitors and adversaries alike often deploy “bad” bots that leverage different methods to achieve nefarious objectives. This includes account takeover, scraping data, denying available inventory and launching DoS attacks with the intent of stealing data or causing service disruptions. Sophisticated large-scale attacks often go undetected by conventional mitigation systems and strategies.

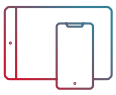
Leveraging proprietary, semisupervised machine-learning capabilities, Radware’s Bot Manager allows precise bot management across web and mobile applications and APIs, combining behavioral modeling for granular intent analysis, collective bot intelligence and device fingerprinting. Radware Bot Manager’s nonintrusive API-based approach detects and blocks highly sophisticated human-like bots in real time, which can be massively distributed or adequately “low and slow” to operate under the permissible limits of rule-based security measures. Our collective bot intelligence gathers bot signatures from across our client base to build a database of bot fingerprints and proactively stop bots from infiltrating into your internet properties.

Intent-Based Deep Behavioral Analysis (IDBA)

Identify the intent of bots with the highest precision through proprietary semisupervised machine-learning models

Full Coverage Of OWASP Automated Threats

Protect from all forms of account takeover, denial of inventory, distributed denial of service (DDoS), card fraud and web scraping



Secure All Channels: Web & Mobile Apps, APIs

Defend against bots that target various digital assets— even sophisticated bots designed to hit multiple assets

Flexible Integration Options

Nonintrusive deployment using SDK, web server or content delivery network (CDN) plug-ins, JavaScript (JS) tag or as a reverse proxy — no impact on the technology stack

Mobile SDK Capabilities

- **Integrated Device Authentication:**
  Radware Bot Manager SDK includes a one-of-a-kind attestation for Google and Apple devices, for tighter and faster protection of native mobile applications. This unique capability keeps device authenticity in check, making sure only real devices get access to resources while emulators, modified applications and applications with modified OS are prevented from accessing the resources.
- **Secure Identity:**
  This unique solution ensures the security of your client identity against identity spoofing, identity tampering, and replay attacks. Secure Identity along with Google/ Apple attestation (Integrated Device Authentication) provides enhanced protection to your mobile devices and apps and stops bot attacks on mobile apps before they materialize and take a toll on your infrastructure.
- **Analytics and Reporting:**
  Radware offers granular analytics as well as detailed reports on bot activities across your mobile app and web. The report includes highly targeted screens, global bot distribution, malicious IPs list, traffic pattern along with detailed insight on the severity of an attack.
- **Flexible Integration:**
  The SDKs are lightweight and easy to integrate with iOS and Android apps. SDKs can be embedded into native apps as well as hybrid apps, and are optimized to consume less space, memory, CPU, and battery power. Radware Bot Manager SDK can be deployed in any existing infrastructure provided by the customer through our multiple server-side integration options.
- **CAPTCHA Customization:**
  Users can customize the Captcha and Block Pages on the Mobile SDK as per their requirement. The customization options are provided across multiple elements in the CAPTCHA/Block page like text, text alignment font, color, language, image etc.

Detection and Mitigation with High Accuracy

Radware Bot Manager uses a proprietary Intent-Based Deep Behavior Analysis (IDBA) to understand the intent of highly sophisticated nonhuman traffic. It does this by collecting over 250 parameters including browsing patterns, mouse movements, keystrokes and URL traversal data points from the end user's browser and using proprietary algorithms to build a unique digital fingerprint of each visitor. IDBA uses this information to perform a behavioral analysis at a higher level of abstraction of "intent," unlike the commonly used shallow "interaction"-based behavior analysis. Capturing intent enables IDBA to provide significantly higher levels of accuracy while detecting bots with advanced human-like interaction capabilities. IDBA builds upon Bot Manager's research findings in semisupervised machine learning and leverages the latest developments in deep learning.

Ability to Handle Bot Traffic in Multiple Ways

Aggregators and competitors continuously target your web properties to scrape prices, content, and other information. Radware allows you to take custom actions based on bot signatures and types. For example, block access to resources for suspected non-human traffic with CAPTCHA or outsmart competitors using "Feed Fake Data" that enables you to feed fake pricing and product information to malicious bots. Using "Redirect Loop," bots get looped in a cycle of redirection ending with a drop page. With Radware's unique browser-based Cryptographic Challenges, bots are forced to solve puzzles that exhaust their resources, and end-users get to enjoy a CAPTCHA-free experience. "Throttle" slows down the loading time of a page request. Similarly, other Radware bot mitigation options help organizations customize their response to a bot attack. The response to these challenges allows Radware to build a closed-loop feedback system to minimize false positives down to negligible values. More than one mitigation option can be applied at the same time depending on the resource or severity of the threat.

Widest Mitigation Options

- Allow
- Challenge CAPTCHA
- Block
- Feed Fake Data
- Throttle
- Drop
- Session Termination
- Redirect Loop
- Log Only
- Custom Response
- Crypto Challenge

Crypto Challenge Mitigation

Radware Bot Manager provides the widest choice of mitigation options, including a Cryptographic Challenge based on the principles of Blockchain's 'Proof of Work' that is immune to third-party tampering and makes for a seamless and CAPTCHA-free user experience.

Crypto Challenge is a behavior-enforcing mechanism that detects anomalies against a baseline of normative behavior. When an anomaly is detected, the mitigation method challenges the user device by creating CPU-intensive browser-based challenges with increasing difficulty. The increasing difficulty of the challenge is exponential by nature, forcing the attacker's CPU to work harder every time it is challenged, effectively creating a cyber counterstrike and demotivating them from continuing their attacks.

Dedicated API Protection

Ability to control navigation flow and fingerprint machine-to-machine communications to avoid invoking APIs that are accessed or targeted by misbehaving bots.

Complete Application Bot Protection Suite

The suite includes a WAF, Bot Manager, API protection and DDoS mitigation brought together to provide the most robust application protection. 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.

Easy Integration

Flexible deployment options include integration through our JS tag, cloud connectors or web server plug-ins. Alternatively, a virtual appliance is also available for the entire web app or selected sections. Using Radware's API-based approach, Domain Name System (DNS) redirection is not mandatory, so deployment into the existing application stack is easy and seamless.

Accuracy and Scalability

Detecting advanced bots based on shallow interaction characteristics results in a high number of false positives. Radware's Intent-based Deep Behavior Analysis helps filter highly sophisticated human-like bots without causing false positives. We also ensure that website functionality and user experience remain intact. We use cutting-edge technologies such as Kubernetes container orchestration and Kafka to maintain high scalability during peak hours.

Transparent Reporting and Comprehensive Analytics

Transparency in traffic reports helps you build trust with internal stakeholders and partners. A granular classification of different types of bots such as search engine crawlers and malicious bots allows you to efficiently manage non-human traffic. Clean analytics and transparent reports offer a clear understanding of web traffic and give you a detailed picture of a bot's intent. Radware provides comprehensive analytics of non-human traffic, their source, and URL analytics. One of the key benefits of the bot detection engine is its modularity and transparency in reports — this is particularly useful for automated threats such as digital ad fraud. The analytics dashboard demonstrates the distinctive user behavior on the protected apps. The bot mitigation solution can also be seamlessly integrated with leading marketing analytics platforms.

Designing a Secure API Environment

While APIs bring tremendous benefits, they also introduce new security risks, including service disruption and data theft. Many APIs process sensitive personally identifiable information (PII). Additionally, known application security risks with HTTP/S apps are as relevant for APIs as they are for web applications. Communication with APIs usually follows known structures and protocols. The most common protocol is REST-JSON, which has a schema format definition called OpenAPI.

Because threats vary, API security requires a combination of access controls (such as authentication and authorization mechanisms), injection prevention, bot management and DoS mitigation. In addition, hackers may try certain API-specific attacks such as using invalid schemas, parameter tampering or token manipulations.

This is why providing comprehensive protection against API related attacks and a combination of several technologies are required, such as application and API vulnerability protection, bot protection and behavioral analysis, all with positive and negative security models.

Radware's API Protection Solution

WAF, bot management solutions (with API protection algorithms) and API gateways are the primary in-line security tools for API protection. While API gateways usually offer authentication and authorization features, their HTTP traffic and payload analysis as well as their OWASP Top 10 API security risks and web protection capabilities are either limited or absent.

By combining positive and negative security models together with an auto-learning and a purpose-built bot management solution for APIs, Radware secures APIs from known and zero-day attacks as part of its web application security solution.

Attack category	Example of attacks / risks	Protection technology
API1:2019 Broken Object Level Authorization	↗ Unauthorized Access to APIs: IP / Token / Role / customer based	**WAF:** ↗ Quota ↗ API catalog
API2:2019 Broken User Authentication	↗ Authentication: OAuth2, JSON Web Token ↗ Session Hijacking (e.g. steal token) ↗ Token manipulation (e.g. privilege esc.)	**WAF:** ↗ Token Protection
API3:2019 Excessive Data Exposure	↗ Environment Fingerprinting: • 5XX Internal Server Errors • HTTP response headers	**WAF:** ↗ Data Masking ↗ Replace 500 messages
API4:2019 Lack of Resources and Rate Limiting	↗ ATO: Credential Cracking / Stuffing… ↗ Scraping / Data Harvesting ↗ Denial of Inventory ↗ Token Cracking: Coupons Enumeration	**WAF:** ↗ Quota ↗ Activity Tracking BOT Management with intent based behavioral analysis

Attack category	Example of attacks / risks	Protection technology
API5:2019 Broken Function Level Authorization	↗ Unauthorized Access to APIs IP / Token / Role / Customer based ↗ Access to restricted APIs	**WAF:** ↗ API catalogue validation ↗ IP and GEO policies
API6:2019 Mass Assignment	↗ Unauthorized Access to APIs ↗ Access to restricted APIs	**WAF:** ↗ API catalogue validation ↗ IP and GEO policies
API7:2019 Security Misconfiguration	↗ Incomplete or ad-hoc configurations ↗ Misconfigured HTTP headers ↗ Unnecessary HTTP methods	**WAF:** ↗ Data Masking ↗ Replace 500 messages ↗ Auto learning
API8:2019 Injection	↗ SQL Injections ↗ XSS ↗ Command Injection ↗ Directory Traversal	**WAF:** ↗ Positive Security model ↗ Negative Security model ↗ API catalog validation
API9:2019 Improper Assets Management	↗ Overexposed API end points	**WAF:** ↗ Positive Security model ↗ Negative Security model ↗ Auto learning
DoS, Availability	↗ Volumetric Application DDoS on APIs ↗ Low and Slow Attacks (TCP / HTTP)	**WAF:** ↗ TCP low and slow detection ↗ Behavioral low and slow detection BOT Management

Managed Application Protection

Radware's emergency response team (ERT) are security experts available 24x7, every day of the year, for proactive security support services for customers facing an array of application- and network-layer attacks. Powered by Radware's Threat Research Center, ERT engineers combat common and emerging attacks daily and provide customers with industry-leading expertise and intelligence and allow them to leverage Radware's application security solutions, even if in-house application protection skills are lacking.

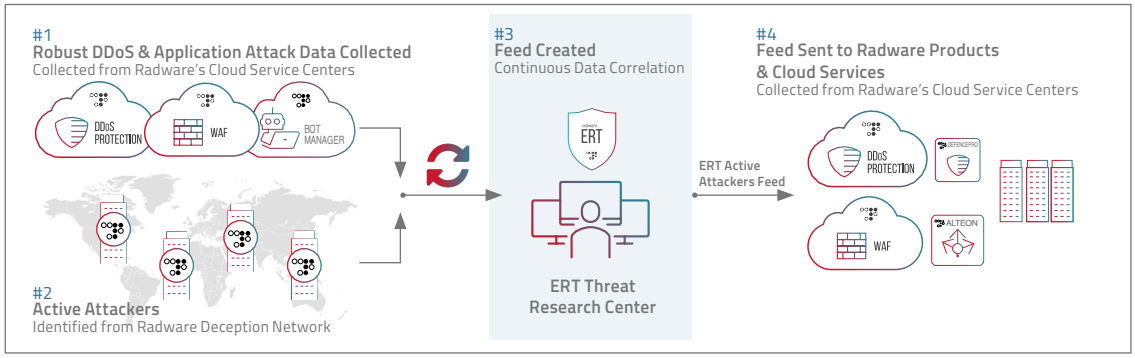
- Radware's ERT managed service assumes full responsibility to configure and update security policies as well as actively monitor, detect, alert and mitigate attacks in real time
- Fastest attack mitigation – Radware's ERT maintains a 10-minute SLA to provide organizations under attack with access to battle-proven security experts
- Preemptive Attack Intelligence allows access to threat alerts, advisories and attack reports provided by Radware's Threat Research Center
- Consulting and reporting features provide a monthly analysis of cyberattacks against your organization and others to identify attack trends, how your organization's network can be impacted and defense recommendations
- Technical account management includes a dedicated and proactive consultant who serves as a focal point for configuration, tuning, integration upgrades and attack mitigation

EAAF

The ERT Active Attackers Feed (EAAF) is an aggregation of multiple exclusive Radware data sources that are combined and correlated by Radware's ERT Threat Research Center. These include:

- DDoS and application attackers' intelligence data from Radware's cloud security services
- Attackers actively engaged in malicious activity collected via Radware's Global Deception Network
- Proprietary bot and botnet intelligence algorithms generated by Radware's ERT research that incorporates proprietary automatic botnet detection algorithms and manual research

These sources are integrated and scored in a big data cloud platform, creating a list of malicious attackers that are currently active. The list is downloaded to Radware's attack mitigation platforms and cloud services so that they can block the attackers before an assault starts.



Radware EAAF Key Benefits

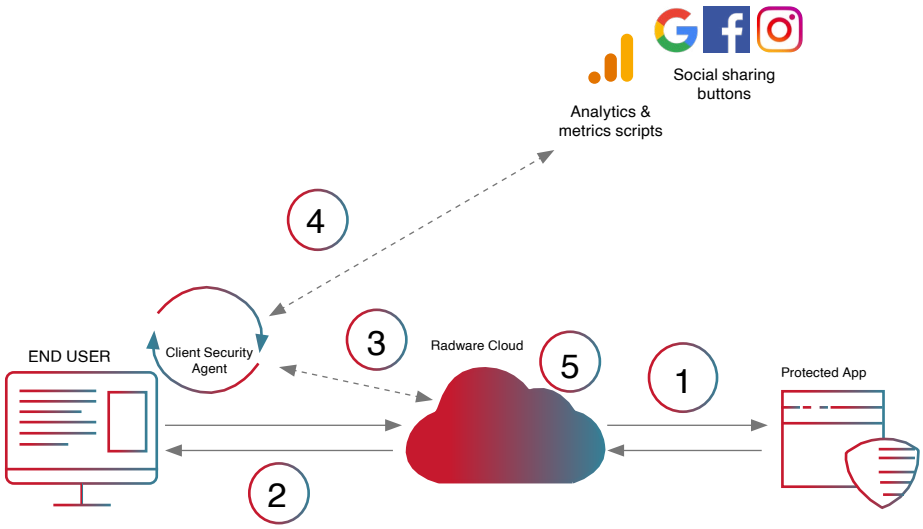
Radware EAAF key benefits include:

- **Preemptive Protection** – blocks attackers before they enter a network
- **Block Active Attackers in Real Time** – Blocks IPs actively involved in DNS and IoT botnet DDoS attacks in 24 hours
- **Real-time actionable intelligence** – Radware EAAF serves as your own network intelligence agency

Client-Side Protection Solution

The Radware client-side protection solution offers the following:

- **Protection against attacks coming from third-party JavaScript services** (Formjacking, Skimming/Magecart)
- **Visibility** – Discover, map, and assess third-party JavaScript-based services embedded in your app
- **Easily blocks requests to suspicious third-party services in the supply chain**
- **Complies with data security and liability standards** – Gain control over end-user data and PII



Radware Client-Side Protection Flow

The Radware client-side protection flow involves the following:

- First, the request is sent to the protected app via Cloud Reverse Proxy
- The Client Security Agent is sent to the browser along with the response from the protected app (JS injection)
- The agent retrieves the whitelist from the Client Security Manager
- The agent continuously monitors outgoing requests and checks them against the whitelist
- The client-side security manager in the CWAF portal provides detailed activity tracking, alerts, and threat level assessment upon which traffic can be allowed or blocked

Web DDoS Protection

New and disruptive Web DDoS Attacks

As can be seen in recent attack campaigns, attackers are leveraging multiple types and vectors of attacks as part of one campaign, combining new tools to generate new types of HTTPS Flood attacks—also referred to as Web DDoS Tsunami attacks—that are more sophisticated, more aggressive, higher in volume and throughput, and much more complex to mitigate. The attacks act at Layer 7, so most of the attack mitigation activities, specifically inspecting the traffic, must be done after terminating the connection and inspecting the content. The attack mitigation processes that are taken after the traffic is proxied and encrypted are relatively heavy and expensive to maintain, especially at scale. This makes HTTP/S floods a very attractive technique for attackers.

Why Your Current Protections Are Not Effective

Network-based DDoS protection solutions are simply not equipped to detect and accurately mitigate application-layer DDoS attacks. Since it requires decryption of the attack traffic and deeper inspection into the L7 headers, these web DDoS attacks would go undetected.

A standard WAF—whether on-prem or cloud-based—is an effective tool to protect applications from standard web-based threats but it's failing against these L7 DDoS threats for several reasons:

Scale – The rate of these attacks, measured by Requests Per Second (RPS), is reaching new heights, sometimes even millions of RPS. On-prem WAFs are maxed out under such attacks.

Attack Sophistication – These Layer 7 DDoS attacks appear as legitimate traffic requests and are constantly randomized (dynamic IPs and other parameters). Therefore, only behavioral-based algorithms with self-learning and auto-tuning can detect and mitigate these attacks.

Morphing Attacks – To protect from such zero-day attacks, organizations need solutions that can quickly adapt in real-time to the attack campaign. An on-prem WAF cannot provide that.

The Human Factor – Sophisticated web DDoS campaigns require having security experts that can handle the complexity of attacks without compromising application security. Self-managed teams, limited in personnel, tools, and budgets, can't cope with a 24x7 attack campaign.

Radware New Advanced Web DDoS Protection Service

As part of its Cloud Application Protection Service, Radware's new Cloud Web DDoS Protection solution is uniquely designed to protect from this high-scale, newly emerging Web DDoS Tsunami attacks and provide customers with advanced protection at the scale needed to combat these threats.

- Automated, accurate, behavior-based detection and mitigation with minimum false positives
- Widest attack coverage (including zero-day attacks)
- Best protection against high-scale Web DDoS Trunami Attacks

Analysis Of Radware's Application Protection Capabilities

The table below highlights some of the key features necessary for effective application protection and analyzes Radware's WAF and Cloud WAF Service offerings.

Feature	Description	Radware's Advantage and Benefits
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 or responses using a combination of auto-policy generation and security filters. This allows Radware to maintain an effective positive security model that can help block well-known and zero-day attacks. With regards to API traffic, WAF technologies define the allowed actions while blocking all access attempts to nonlisted API end points or paths. API catalogs, definition of headers, path parameters and query parameters with a strong schema validation are all great examples of a positive security model. The value of such an approach is a tighter, more-effective security policy, including the ability to define a positive security model immediately without any learning process to effectively secure the APIs.
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 helps create a positive security model for the application and configure the negative security policy while automatically correcting false positives.	Radware WAF automatically maps the application structure, performs threat analysis process, autogenerates a tailored policy for the secured app, and automatically updates policy with application changes. With regard to the API traffic and for the undocumented approach, Radware WAFs propose the API Discovery module to automatically learn the API traffic and create the rule based on a positive security approach.
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.
Server-side request forgery (SSRF)	SSRF is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker. The attacker might cause the server to make a connection to internal-only services where they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials.	Radware host protection protects SSRF by avoiding unvalidated redirect with support of such attacks into different locations of the attack payload, including XML format.

Feature	Description	Radware's Advantage and Benefits
Tailored granular policies for custom applications and protection from session or cookie hijacking	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. Session hijacking involves the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.	Radware offers 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. The configuration can also be delivered using the management API for CI/CD integration. 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 the 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 an outage since its inception in 2013.
Data leak prevention (DLP) for sensitive data	DLP features protect against the loss of sensitive data through application attacks that exploit vulnerabilities to force applications to reply to malicious requests with sensitive data (for example, CCNs).	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	Advanced security systems are using device fingerprints as a more accurate means of attacking traffic sourcing or malicious behavior tracking. IP address-based bot or attack detection has become insufficient due to the various ways that IP addresses can be masked (for example, through anonymous proxies or global NATs) or spoofed.	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 Floods and low and slow, where the correlation across multiple sessions is essential for proper detection and mitigation.

Beyond all the required protections discussed above, including SQL injection, broken authentication, XSS, CSRF, DDoS and more, Radware's web application protection technology features additional attack correlation capabilities. These capabilities allow blocking of repetitive attack sources by managing a penalty score for security violations per source. Once an attack source reaches a predefined score threshold, it will be blocked.

Consistent Cross-Cloud Web Application Security

Modern organizations run their web applications across multiple environments, including on-premise, private or public clouds. The result is a patchwork of application security tools that require either disparate tools with limited security and no central management or external cloud services that add latency and complexity. Radware offers a unique application security architecture specifically designed for the public cloud by providing comprehensive security against application, bot and API vulnerabilities, centralized cross-cloud management, and no added latency or complexity to cloud deployments.

Application Protection for Any Cloud with Radware SecurePath™

Radware SecurePath™ is an innovative, API-based cloud application security architecture designed to optimally protect applications deployed across any cloud or data center – on-premise or in private cloud or public cloud environments – while maintaining consistent, high-grade and comprehensive protection.

Radware SecurePath™ allows Radware's application protection services to be deployed inline, where they serve as a "middleman," or an API-based, out-of-path service. The latter utilizes an API-based software detector that monitors application traffic to the origin server. The detector communicates with Radware's WAF engine, which processes its findings and alerts against any malicious traffic. Host transactions are blocked only when malicious traffic is detected. This deployment enables application requests to go directly from the client to the application server without interruption. This innovative approach provides many advantages, including:

Reduced Latency

The same level of security is provided without the inline latency

No Key Sharing

With so SSL certificate sharing, certificates are managed solely at the origin, making them more private, more efficient, faster to deploy and easier to maintain

No Traffic Redirection

There is no need for Domain Name Server (DNS) or Border Gateway Protocol (BGP) routing changes to get protection. Requests go from the client directly to the application server. Only copies of important transaction parameters are sent to Radware's application protection cloud for inspection.

Increased Uptime

As traffic is not inspected inline, customers are not impacted by overloads or outages.

No Bottlenecks

Latency thresholds can be set to avoid congestion.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity 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 and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, 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 of DDoS attack tools, trends and threats.

RW-1151 04/27/23