Radware Application Protection as a Service

Cloud WAF, Bot, API, DDoS, and Client-Side Protection Services

Challenges of Keeping Modern Applications Secure

Applications are at the core of your business – from sophisticated e-commerce platforms 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 application perimeter is expanding and becoming harder to define. Whether on-premise or in the cloud, applications are now scattered across different platforms and frameworks. They rely on third-party JS services and the availability of information from other 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 update, and security policies must adapt accordingly to safeguard them and the data they host, as well as comply with information security policies. It is increasingly difficult to protect against an expanding variety of attack methods adapt policies in real time to mitigate automated attacks, and maintain a high level of security with low levels of false positives so that no legit traffic is blocked. This often necessitates manual labor, operational costs and expertise that many organizations can't sustain by themselves.

Radware's Adaptive, Frictionless Application Protection

Radware's industry-leading web application and API protection (WAAP) suite is a one-stop shop for your application security needs, providing you with state-of-the-art WAF, API security, bot management, L7 DDoS mitigation, and client-side protection that doesn't roadblock business agility and growth.

Comprehensive

Extensive protection that covers all Open Web Application Security Project (OWASP) key vectors for web application security threats, vulnerabilities and more

Automated

Automation of resource-heavy processes for better security, minimum false positives and reduced overheads: Security policy refinements, event analytics, API discovery and schema file generation, Supply-chain JS services mapping, alerts and enforcement

Frictionless and Adaptive

Integrated with the development cycle while quickly and easily adapting to any changes made to your applications and the underlying deployment platform – with no interference to your business

Consistent

Uniform, state-of-the-art security for all apps everywhere, enabling the same level of holistic protection agnostic to where the apps are hosted (private or public clouds)

Free of Heavy Lifting

Reduced operational costs and superior protection with Radware's Emergency Response Team (ERT) 24x7 fully managed service, saving resources used for configuring security policies, mitigating attacks, and reducing false positives

In-Depth Visibility and Control

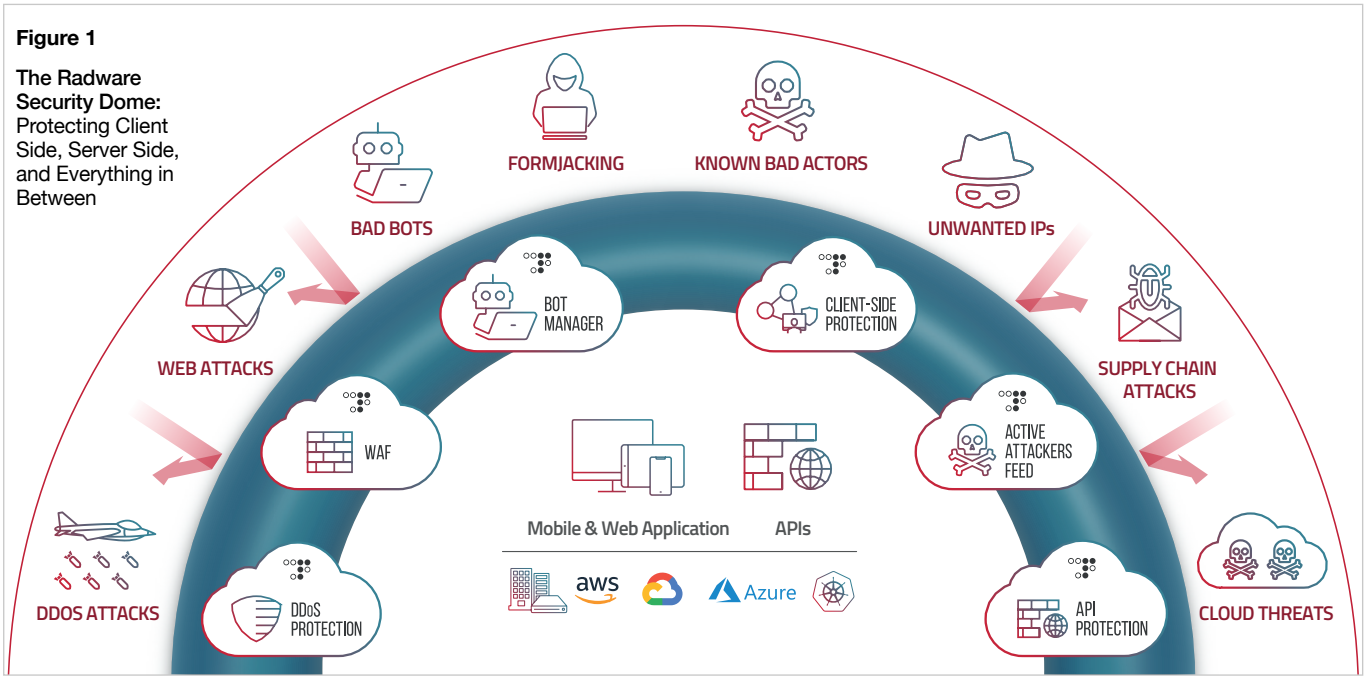
Security and development dashboards with actionable analytics, automation and customized controls, helping you to be aware of threats to your apps at all times and make educated decisions for application development

Complete Application Protection – Client-Side, Server-Side, and Everything in Between

Easily manage and seamlessly scale your application security as you grow your business, evolve your application architecture and expand your cloud environments and services. The one-stop shop comprising Radware's protection services keeps you protected against threat vectors as your business grows and applications evolve.

Figure 1

The Radware Security Dome: Protecting Client Side, Server Side, and Everything in Between



Protect Digital Assets and Data

Compatible with any application architecture, Radware protects your digital assets and customer data in all environments, be it on-premise, virtual clouds, private clouds, public clouds, hybrid environments and Kubernetes.

Detect, Manage and Mitigate Bots

Detect and distinguish between "good" bots and "bad" bots to protect websites, mobile apps and APIs. Easily optimize and customize your bot management policies to provide a better user experience and drive more ROI from your application traffic.

Protect Against OWASP Vulnerabilities

Stay protected against 150+ known attack vectors, including the OWASP Top 10 Web Application Security Risks, Top 10 API Security Vulnerabilities, Top 21 Automated Threats To Web Applications, and Top 10 Client-side vulnerabilities.

Protect Application APIs

API attacks are a rapidly growing threat to business applications and customer data. Radware combines behavioral analysis and policy automation to protect your evolving API matrix from increasingly sophisticated API assaults.

Protect Against Zero-Day Attacks

Radware's unique positive security model stops unknown threats in their tracks. Radware's machine-learning analysis engine continuously studies application traffic and end-user behavior to build security policies that reduce exposure to zero-day threats.

Protect Client-Side From Supply Chain Attacks

As server-side security improves, more hackers target the less protected and rarely monitored client side. As part of Radware's one-stop-shop application protection service that protects the application data center and functionality, this solution offers advanced client side protection that ensures the protection of end users' data when interacting with any third-party services in the application supply chain.

Mitigate Application-Level DDoS Assaults

Radware's DDoS protection technologies provide the shortest time to detection and mitigation of HTTP-based DDoS assaults. Utilizing patented behavioral analysis, machine learning-based engines, alongside its global and robust cloud application protection network, Radware can stop the most advanced and high volume, high throughput HTTP DDoS attacks.

State-Of-The-Art Application Protection as a Service

Web Application Firewall

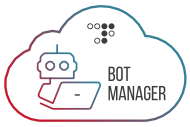
Radware's adaptive and automated WAF protects against web application attacks, hacking and other vulnerabilities. The WAF technology uses a positive security model that automatically learns the behavior patterns of legitimate user activities, automatically builds security policies tailored to allow those 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 based on negative security models cannot stop, as they rely on blocklists of known attack signatures.

API Protection

A dedicated, end-to-end API protection solution is part of Radware's comprehensive web application security architecture. The fully automated solution ensures the security of apps, APIs, development platforms and infrastructure.

It maps the API attack surface by leveraging an automated deep discovery algorithm to discover APIs endpoints and their full structure and generate 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 API Security Top 10.



Bot Manager

Radware's industry-leading bot management and mitigation solution can accurately detect and distinguish between human traffic, good bots and bad bots, and ensure 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 all OWASP 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 Google and Apple devices along with its proprietary identity authentication engine stops bot attacks on mobile apps before they materialize and take a toll on your infrastructure.

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

Application DDoS Protection

Industry-leading application-layer (L7) protection against DDoS attacks, based on Radware's unique behavioral approach that distinguishes between legitimate and malicious traffic, automatically protecting 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, and Brute Force attacks.

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 JS services (Formjacking, Skimming/Magecart), automatically and continuously discover all third-party services in your supply chain with detailed activity tracking, as well as get alerts & 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 JS services.

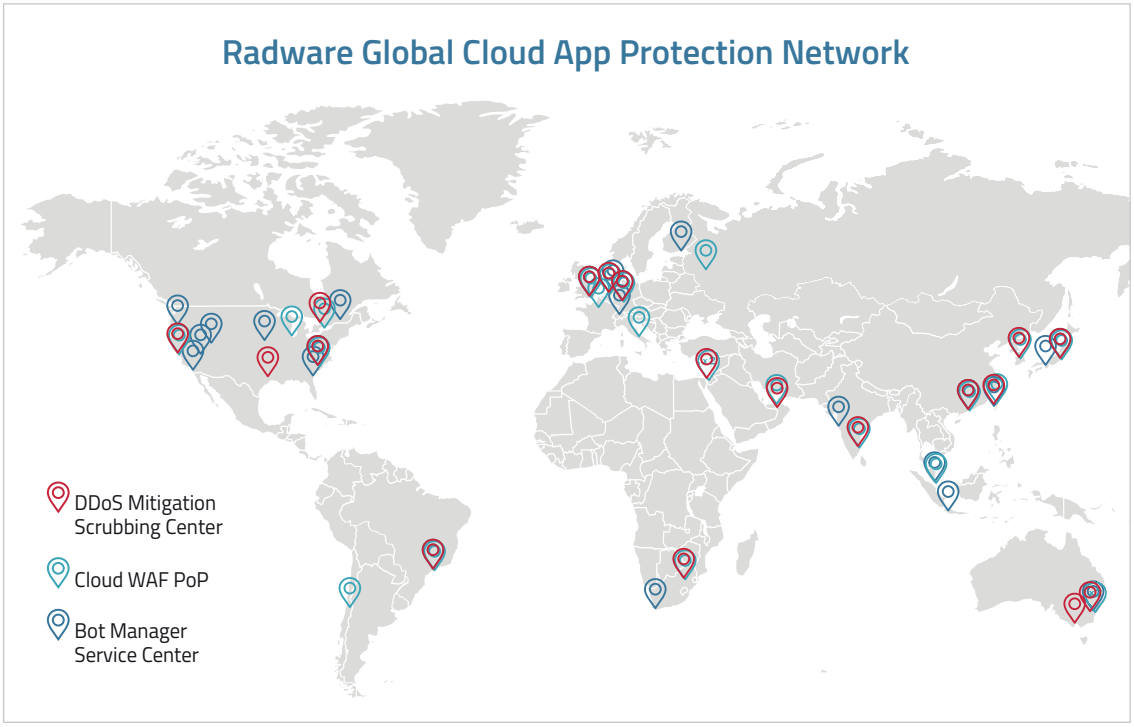
ERT Active Attackers Feed

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.

Global Cloud Application Protection Network

Radware's Application Protection as a Service is based on Radware's global network of distributed application security points of presence (POPs) and DDoS mitigation scrubbing centers.

With locations at major traffic hubs connecting to Tier 1 ISPs, and a global mitigation capacity of 12Tbps, Radware's cloud network protects you close to your origin server to ensure low latency and minimal impact on web application performance.



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, 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. 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 no 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

Application Protection and the Content Delivery Network: The Best of Both Worlds

For customers who wish to combine their web application security with their website delivery, Radware offers an integrated content delivery network (CDN) solution integrated directly into Radware's application security stack and management portal. Radware's CDN solution is based on the Amazon CloudFront CDN for a massive, globally distributed footprint, enhanced performance and DevOps-friendly usability. Radware's integrated CDN offering is built directly into the portal for Radware Cloud Security Services to unify management and reporting – all from a single dashboard. Key features include:

- Massive capacity, based on the AWS network
- Global footprint with over 300 points of presence in more than 90 cities across
- more than 47 countries
- Unified management within the portal for Radware Cloud Security Services
- Single SSL key (the same as the one used for WAF)
- Advanced metrics and reporting
- Cost-effectiveness
- Super-fast (faster than most CDN providers. See www.cdnperf.com/)

Summary

Radware's Application Protection as a Service allows organizations to manage and scale application security as the business grows, evolve application architectures and expand cloud environments and services. It includes:

Comprehensive protection

A one-stop shop for application protection solutions: WAF, API protection, L7 DDoS mitigation and bot management

State-of-the-art security

The widest coverage against known threats and zero-day attacks based on advanced, patented, machine-learning-based behavioral analysis technology

Reduced overhead

Adaptive protection with automatic policy generation and 24x7 support through Radware's ERT

Centralized management and reporting

One place to manage and monitor the security of your applications, no matter where they are deployed

Flexible deployment and compatibility

Ability to maintain the same level of protection across any environment: on premise, virtual clouds, private clouds, public clouds, multi-clouds, hybrid environments or Kubernetes