Radware Cloud Application Protection Services

Cloud WAF, Bot, ATO, API, DDoS, LLM Firewall, and Client-Side Protection

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. They're more than your primary revenue generators, growth leaders and retention engines—they're your main customer engagement platform.

The application perimeter is expanding and becoming harder to define. Whether on-premises or in the cloud, applications are now scattered across different platforms and frameworks. They rely on third-party JavaScript services, integrated LLM modules and AI agents, and the availability of information from other third-party services that they interact with via APIs. As a result, the attack surface targeting these applications grows and their risk exposure increases. Applications constantly change and update, and security policies must adapt accordingly to safeguard them and the data they host while complying with information security policies. Along with that, the democratization of generative AI tools at the hands of hackers has brought a new generation of zero-day attacks that are persistent, sophisticated and aggressive. 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 legitimate 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, layer 7 (L7) DDoS mitigation, LLM Firewall for AI Prompt protection, ATO, 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

AI-powered and 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, business logic protection, AI-driven cross-engine correlation, AI-driven incident management

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 360° 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. It also ensures compliance with new and existing such as PCI DSS 4.0, NIS2, GDPR, HIPAA, DORA and more.

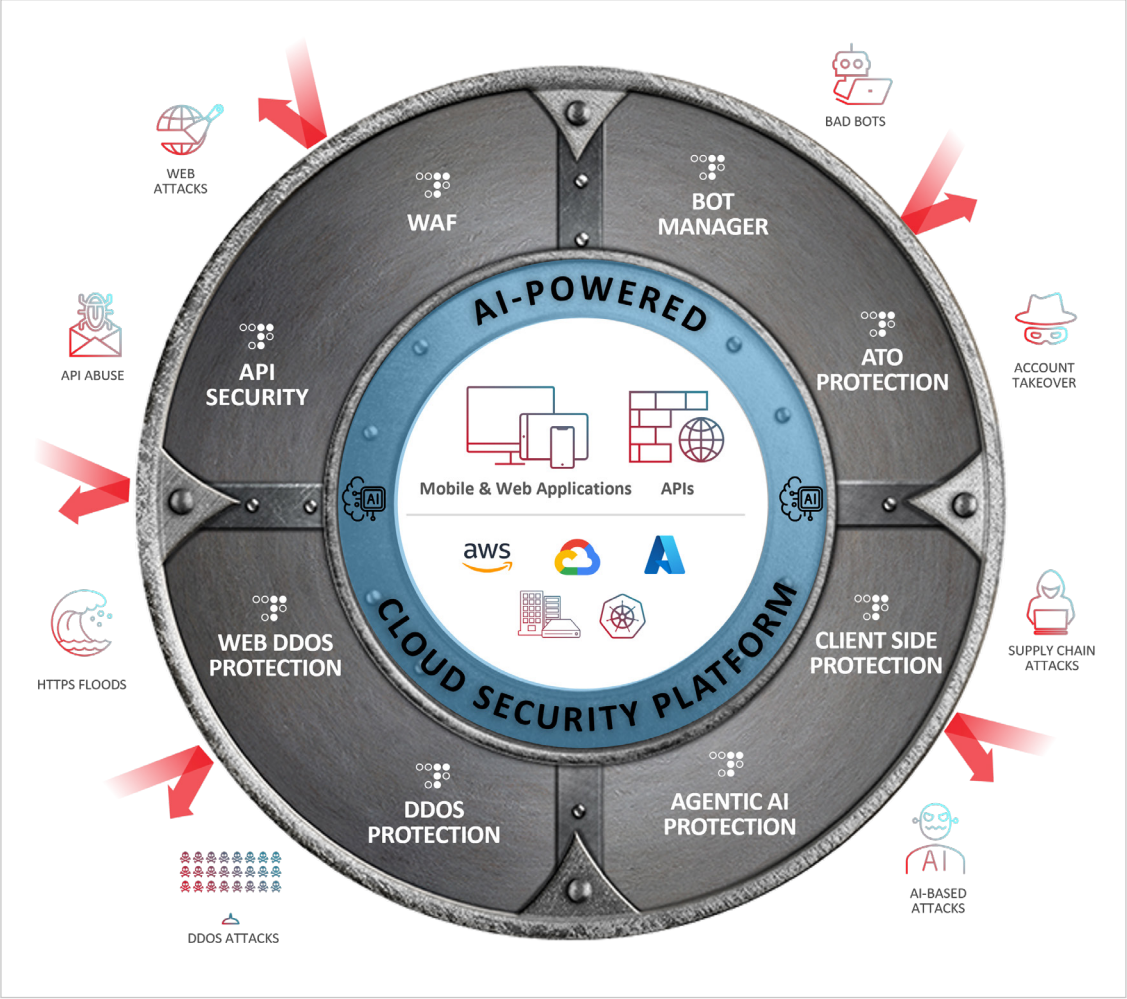


Figure 1:

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-premises, 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, Top 10 for LLM Apps 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 and business logic attacks.

Protect your LLMs

Radware's LLM Firewall stops prompt attacks and misuse before they even reach the organization’s origin servers. It detects risks like prompt injection, data leaks, harmful content, brand safety, and token abuse in real time and automatically stops them at the prompt level.

Block AI-Driven Zero-Day Attacks

Radware's unique behavioral-based positive security model stops unknown threats in their tracks. Our AI-driven multi-layered analysis engines continuously study application traffic and end-user behavior to establish accurate baselines and automatically fine-tune security policies. This allows users to detect and accurately block any anomalous behavior.

Protect Your Client-Side From Supply Chain Attacks

As server-side security improves, more hackers target the less protected and rarely monitored client side. Radware’s client-side protection ensures the protection of end users' data when interacting with any third-party services in the application supply chain and provides the necessary controls required for PCI DSS 4 compliance.

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, AI-based engines, alongside its global and robust cloud application protection network, Radware can stop the most sophisticated and high throughput HTTP DDoS attacks, no matter their type - web or API based.

Empower Your SecOps Team With Threat Intelligence Services

Get real-time actionable insights from real global cyberattack intelligence to analyze attack traffic, make educated decisions and defend against threats before they escalate. As well, get reputation alerts on attacks on the web originating from your own network.

AI-Powered Intelligent Cloud Application Protection as a Service

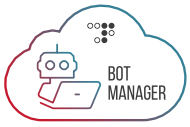
Web Application Firewall

Radware's adaptive and automated WAF protects against web application attacks, hacking and other vulnerabilities. Our WAF technology uses an AI-powered positive security model that automatically learns the behavior patterns of legitimate user activities and continuously refines security policies to avoid false positives and accurately block any action that deviates from these patterns of legitimate behavior.

The 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. This 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 API endpoints and their full structure and then generates tailored security policies to detect and block API-focused attacks in real time. As well by automatically and continuously learning and mapping the application API business logic, it can create an alert and block any business logic attacks on APIs. 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 sophisticated AI-driven automated threats and bots as well as GenAI crawlers and AI Agents.

It provides a robust and precise bot management across web, mobile and API traffic by applying an AI-based proactive protection approach comprised of three layers: preemptive protection, behavioral-based detection and advanced mitigation.

Radware Bot Manager preemptively blocks unwanted identities, utilizing unique capabilities such as AI-based cross-correlation, JavaScript validation, as well as mobile attestation for Android and iOS devices. This, along with its proprietary secure identity engine, stop bot attacks on web and mobile apps before they materialize and take a toll on your infrastructure.

The solution employs advanced AI-based technologies such as behavioral modeling (granular intent analysis), behavioral-based detection (discovery of sophisticated bot evasion behavior like rotating IPs and identities), distributed attack detection, machine-learning-based anomaly detection, and browser and device fingerprinting. It is also capable of detecting third-party CAPTCHA-farm services.

It protects against all OWASP 21 Top 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.

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.

Web DDoS Protection

Industry-leading application-layer (L7) protection against DDoS attacks, based on Radware's unique AI-based behavioral detection that distinguishes between legitimate and malicious traffic, and automatically generates granular signatures in real-time to protect against zero-day attacks. The unique solution can generate signatures to any type of attack requests, including API DDoS attacks which have become the majority of attacks. With unique hybrid, always-on and on-demand cloud DDoS service deployment options, Radware's Web 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 compliance with PCI DSS 4 and 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 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 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.

LLM Firewall

Radware LLM Firewall secures generative AI use with real-time AI-based protection at the prompt level – stopping threats before they even reach the organization's origin servers. The solution enforces enterprise-grade security and compliance by detecting risks like prompt injection, data leaks, harmful content, brand safety, and usage policies in real time. The Radware solution is fully model-agnostic and easy to onboard, and secures AI use across platforms without disrupting workflows or innovation.

The LLM Firewall key features include:

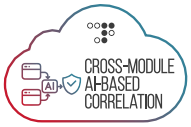
- **Model Agnostic with Zero-friction setup:** Simple configuration with no special integration - protects multiple prompts LLM models across your stack
- **Inline pre-origin protection:** Guards run before the request hits the origin server, blocking abuse early, reducing compute load, and lowering infrastructure costs
- **Flexible & Compliant Policy Controls:** Fine-grained guard settings with customizable block messaging - built to align with OWASP Top 10 for LLMs, enterprise brand rules, and regulatory requirements
- **Security visibility with tuning support:** Full security event logging with all relevant context, plus a "report

Threat Intelligence Service

Radware Threat Intelligence Service sheds light on why certain IPs are flagged, providing invaluable insights and context in real-time. The actionable intelligence will allow you to confidently assess threats, enable informed decisions and proactively defend against threats before they escalate. Whether it's blocking a suspicious IP, fine-tuning your defenses, or identifying compromised systems, we've got you covered.

Key features for Radware Threat Intelligence Service include:

- Actionable data from real cyberattacks
- Research into any suspicious IP address with IP insights, open proxies and malware data
- Reputation alert to ensure network security and integrity by proactively informing of potential cyberattacks originating from the organization's own network.
- Seamless REST API integration to any environment, existing security workflows and systems
- Telegram Claimed attacks reports - see the threats to your business, industry and country and real-time and take educated preemptive defense actions



Cross-module AI-based Correlation

Radware's AI-driven threat analysis algorithms preemptively and automatically block malicious sources across all applications within an account.

By cross-correlating security events in real-time from all active protection modules (WAF, API Protection and Bot Manager) across your account's chosen applications, Radware's AI-based Correlation Engine gives each source a penalty score based on the number, type and severity of the source IP's security events. Once a penalty score crosses a threshold, the malicious source IP becomes instantly blocked in all enabled apps for a set duration, whether it attacked one or more applications. This unique way of analyzing the source IPs' malicious behavior and blocking them as needed adds a highly accurate proactive protection layer to your security strategy. It prevents incoming bad traffic from overloading your application server and reduces overheads to your applications' infrastructure and security management costs.

Radware AI SOC Xpert

Radware AI SOC Xpert transforms SOC operations by embedding agentic AI into the workflows that matter most. Built on Radware's AI-powered framework, it provides SOC teams with guided investigation, precise remediation and continuous improvement.

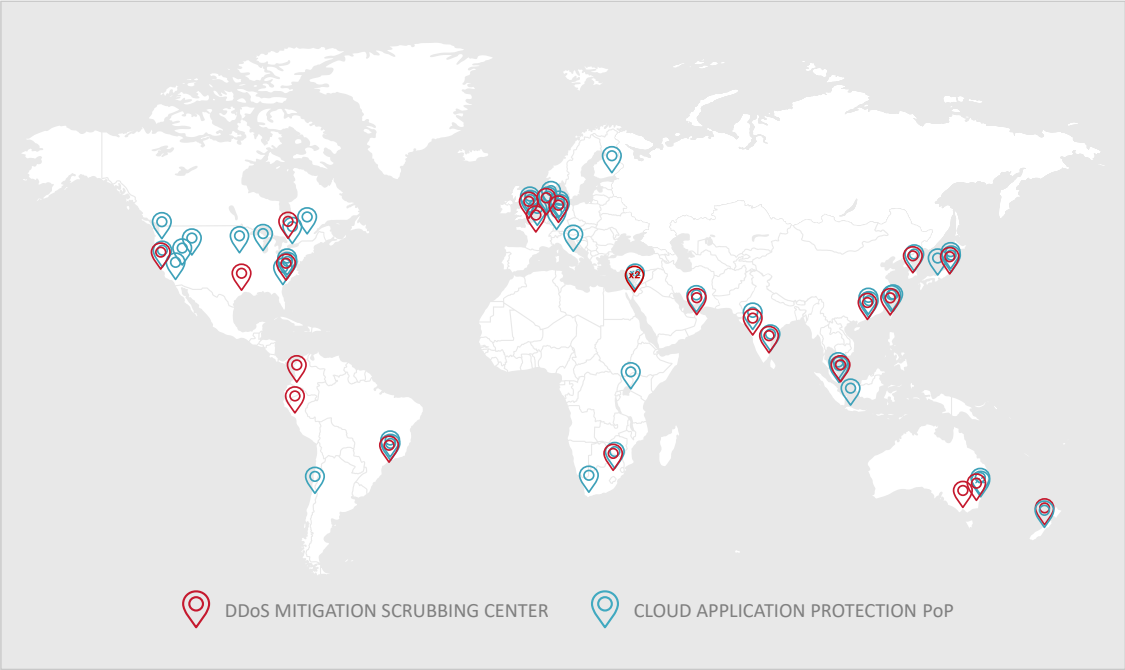
AI SOC Xpert Empowers Analysts

With AI-driven guidance built into every stage of the incident lifecycle, AI SOC Xpert gives analysts the clarity, precision and confidence they need to manage even the most complex attacks. It enables them to:

- Investigate incidents faster by delivering complete attack stories with timelines, indicators and behavioral patterns
- Pinpoint coverage gaps, traffic anomalies or vector shifts for immediate context
- Remediate with precision through AI-generated recommendations and one-click enforcement
- Gain full transparency with real-time access to structured incident data, enriched traffic insights and analyst-first forensics
- Explore incidents in plain language using built-in AI agents, reducing reliance on external teams
- Strengthen defenses over time by leveraging continuous learning from traffic, incidents and SOC actions
- Act with confidence at every skill level, reducing investigation fatigue and improving decision quality under pressure

Global Cloud Application Protection Network

Radware's Cloud Application Protection Services are 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 15 Tbps, 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®

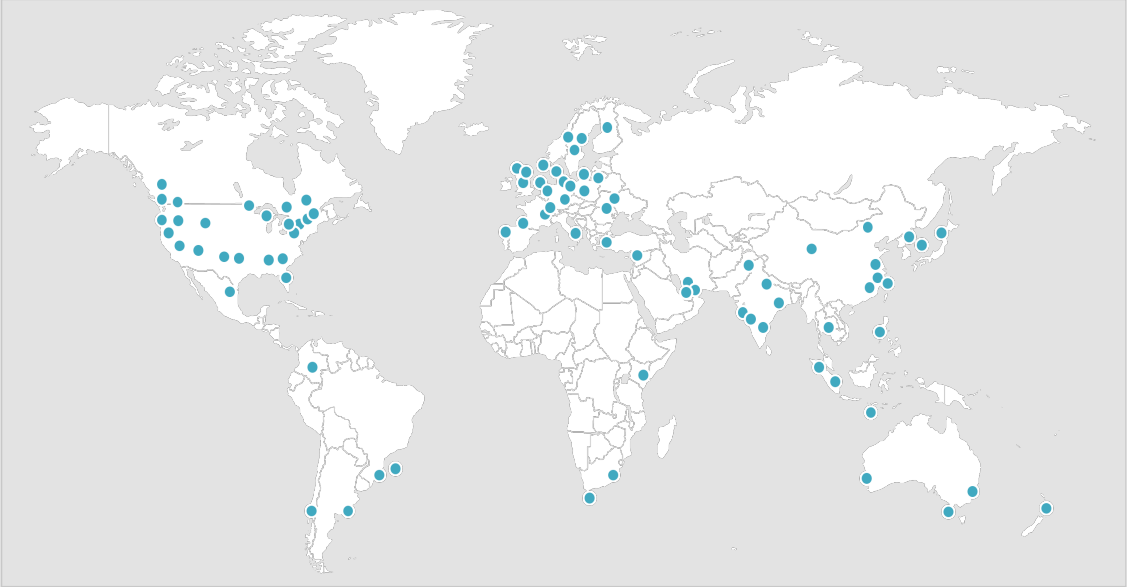
Radware SecurePath® is an innovative, API-based cloud application security architecture designed to optimally protect applications deployed across any cloud or data center—on-premises, private cloud or public cloud environments—while maintaining consistent, high-grade and comprehensive protection.

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 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 in-line, 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 600 points of presence in more than 100 cities across more than 50 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/)
- Managed services for peace of mind with lower TCO

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.

Load Balancer as a Service

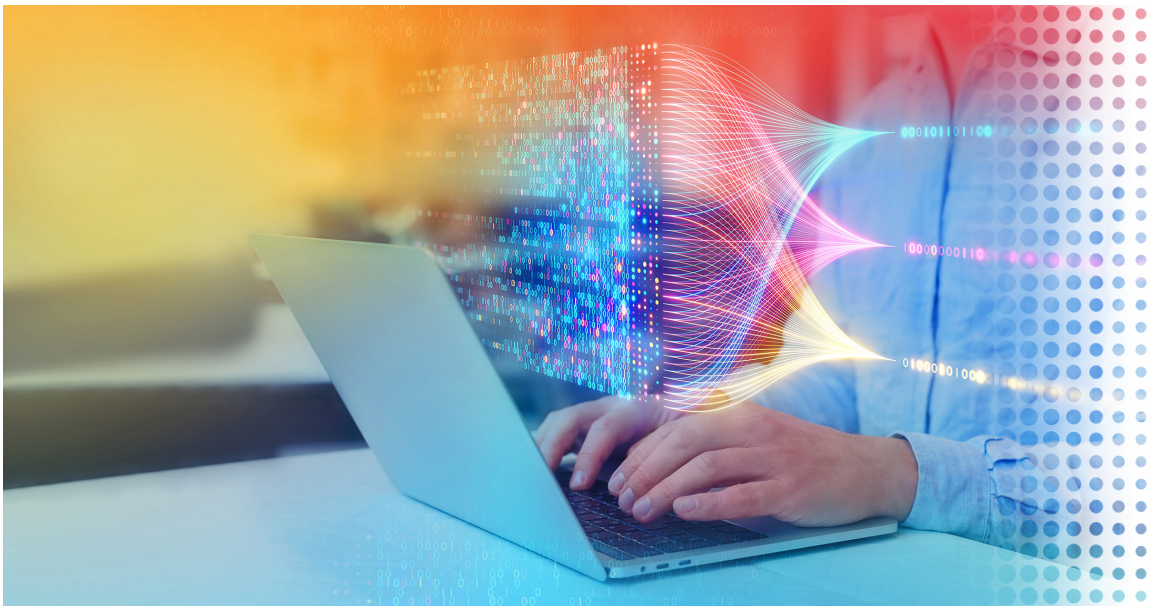
Integrated into Radware's Cloud Application Protection Services, Radware Load Balancer as a Service (LBaaS) addresses the evolving needs of modern IT infrastructures. With a range of features aimed at simplifying configuration and boosting efficiency, all Load Balancer configurations are consolidated into one central place. This gives users a seamless, convenient management experience and empowers them with more control over their load-balancing requirements.

Radware Load Balancer as a Service complements cloud application protection services with improved SLA and scalability while maintaining high availability and protecting all origin sites. It provides continuous automatic origin server status health checks, Active/Active traffic, user load balancing between origin sites, and URL-based server load balancing to optimize resource access and server performance. It also delivers advanced persistency capabilities: IP persistency to ensure consistent network connectivity by maintaining a constant IP address for the device or user, and cookie-based persistency to ensure personalized and consistent user experience across visits by retaining cookies in the user's web browser.

DNS as a Service

Radware DNSaaS (Domain Name System as a Service) provides comprehensive Domain Name System (DNS) management, which is crucial for the seamless functioning of any online application. By leveraging DNSaaS, Radware Cloud Application Protection Services Customers ensure their applications remain protected, available and performant.

Fully integrated into Radware's cloud application protection portal, the DNSaaS centralized management console provides an easy-to-use interface for managing all DNS Hosts, records and health check configurations in one place. With control over traffic distribution to specific resources or endpoints, and real-time analytics and monitoring, Radware DNSaaS improves latency and ensures your end users a seamless experience.



Summary

Radware Cloud Application Protection Services allow organizations to manage and scale application security as the business grows, evolve application architectures and expand cloud environments and services. It provides:

Comprehensive protection

A one-stop shop for application protection solutions: WAF, Bot Management, API, Client-side, and Web DDoS Protection

AI-powered intelligent security

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

Reduced overhead and lowered MTTR

AI-powered adaptive protection with automatic analytics and policy optimization, managed services, 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.

Compliance with privacy and security standards

Holistic application protection solution with specific controls, visibility and reports to comply with security standards such as PCI DSS 4, GDPR, HIPAA, NIS2 and DORA.

Enable Informed Decisions with Real-Time Threat Intelligence

Research any IP address to shed light on its origin and legitimacy and transform uncertainty into clarity.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2026 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.

RWI 153 I 05.13.2026