Radware Cloud Application Protection Service Plans

Radware's Cloud Application Protection Service provides state-of-the-art security capabilities alongside advanced automation and industry-leading security services provided by Radware's industry-known ERT (Emergency Response Team).

The service is offered in three service plans. Each plan is designed to cater to different cybersecurity needs and risk exposure, as well as different levels of managed services.

Cloud Application Protection

Standard Plan

Radware's Standard plan offers the industry benchmark protection level with extra unique features and capabilities. It includes Radware's Cloud WAF, API protection, zero-day attack protection, and 1Gbps of network DDoS protection, as well as Radware's outstanding SLA.

Cloud Application Protection

Advanced Plan

Radware's Advanced plan takes application security to the next level by offering advanced protection capabilities for those that want to ensure they are well protected from more sophisticated and unknown attacks. The plan includes, on top of the Standard plan, Radware's Advanced WAF with its path access protection engine that protects against more sophisticated unknown and zero-day attacks, Source Blocking engine, 10Gbps of network DDoS Protection, as well as JS supply chain mapping, monitoring, and attack detection for client-side protection. It also includes Radware's intelligence feed – the ERT Active Attackers Feed (EAAF), and further support for onboarding and policy reviewing.

Cloud Application Protection

Complete Plan

Radware's Complete plan provides a security blanket for your entire application environment. From client-side to server-side and everything in between. This plan includes everything the Advanced plan has to offer, with the addition of Radware's advanced Bot Manager and its behavioral-based multi-layered detection and mitigation, automated API discovery and API security policy generation, and client-side protection enforcement.

	Radware Cloud Application Protection Service		
	Standard	Advanced	Complete
WAF	✓	✓	✓
API Protection	✓	✓	✓
Advanced Rules	✓	✓	✓
Rate Limit	✓	✓	✓
Access Control & IP Geo Rules	✓	✓	✓
Reporting & Analytics	✓	✓	✓
DDoS Protection	1Gbps	10Gbps	10Gbps
Standard Support	✓	✓	✓
Advanced Support	✗	✓	✓
Advanced WAF (Path Access Protection and AI-based Correlation Engine)	✗	✓	✓
EAAF	✗	✓	✓
Client Side Protection – Detection	✗	✓	✓
Client Side Protection – Mitigation	✗	✗	✓
API Discovery	✗	✗	✓
Bot Manager	✗	✗	✓
Web DDoS Protection	Add-on	Add-on	Add-on
Load Balancer as a Service*	Failover	Basic	Advanced
Data Retention	30 Days	60 Days	90 Days
Unlimited DDoS	Add-on	Add-on	Add-on
CDN	Add-on	Add-on	Add-on
Premium Support	Add-on	Add-on	Add-on

*See detailed LBaaS SLA on page 4

Add-Ons

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 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.

ERT Premium Managed Service

For organizations lacking the cyber-security expertise in-house or those who simply cut their security overheads even further, Radware offers the invaluable ERT Premium managed service:

- 10-minute response SLA via "Hot-line" access
- On-demand emergency response attack mitigation
- Designated Customer Success Manager
- Post-attack forensics and recommendations
- Periodic security status reports
- Priority service case handling
- Policy tuning and application security insights
- Access logs

CDN

For enterprises that wish to combine website delivery with their web application security, Radware offers a content delivery network (CDN) solution integrated directly into Radware's application protection portal. Radware's CDN solution is based on the Amazon CloudFront CDN for a massive, globally distributed footprint, enhanced performance, and DevOps-friendly usability.

Unlimited DDoS Protection

For enterprises that suffer from high-volume DDoS attacks and 1G or 10G of mitigation capacity is not enough, Radware offers unlimited protection with its industry's top-rated DDoS protection solution. Defend your organization against today's most advanced DDoS attacks – no matter their frequency or volume.

Talk to a Radware Cyber Security advisor to find out which plan best suits your organization's security needs.

Load Balancer as a Service

Radware Load Balancer as a Service (LBaaS) complements cloud application protection services with improved SLA and scalability while maintaining high availability and protecting all origin sites. It provides Active/Active traffic and user load balancing between origin sites.

	Radware Cloud Application Protection Service		
	Standard	Advanced	Complete
Failover (Active-Standby)	✓	✓	✓
Number of Active Real Servers (Origins)	1	8	8
Active-Active Load Balancing – Round Robin	✗	✓	✓
IP-Based Persistency	✗	✓	✓
URL-based Load Balancing	✗	✗	✓
Active-Active Load Balancing – Least Connection	✗	✗	✓
Cookie-Based Persistency	✗	✗	✓

Managed Services Support Levels

	Risk/Impact-based Priority	Standard Support	Advanced Support	ERT Premium Service (Add-On)
Response SLA	P1 (Phone)	40 Min	30 Min	10 Min
	P1 (Ticket)	3 Hours	2 Hours	60 Min
	P2	6 Hours	4 Hours	2 Hours
	P3	16 Hours	12 Hours	4 Hours
	P4	24 Hours	24 Hours	12 Hours
Ticket Updates	P1	48 Hours	48 Hours	24 Hours
	P2	96 Hours	72 Hours	48 Hours
	P3	120 Hours	96 Hours	72 Hours
	P4	144 Hours	120 Hours	96 Hours
Managed Services	Certificate Management & Notifications	✗	✓	✓
	Onboarding & Policy Review	✗	✓	✓
	Post-attack Analysis	✗	✓	✓
	Chat Support	✗	✓	✓
	Access Logs	✗	✗	✓
	Quarterly Premium Security Report	✗	✗	✓
	Annual Special Event Preparation	✗	✗	✓
	Annual Attack Test (DDoS L3-7)	✗	✗	✓
	Proactive Security Recommendations	✗	✗	✓
	Security Configuration Review	✗	6 Months	3 Months
	Extended Monitoring	✗	External Monitoring on Top 5 Apps	External Monitoring on All Apps