Cisco Secure Cloud WAF Protection Service Plans

Secure Cloud Web Application Firewall (WAF) Protection provides intelligent AI-powered security capabilities alongside advanced automation and industry-leading security services provided by Radware's[1] industry-recognized Emergency Response Team (ERT).

The service is offered in three convenient service plans. Each plan is designed to meet different security needs and risk exposures and to provide different levels of managed services.

Cloud Application Protection Service Plans

Essentials Plan

The Essentials plan offers industry benchmark protection with additional unique features and capabilities. It includes Cisco® Cloud WAF, API protection, zero-day attack protection, Basic bot protection, and 1Gbps of network DDoS protection, as well as an industry-leading Service Level Agreement (SLA).

Advantage Plan

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

Premier Plan

The Premier plan provides a comprehensive security blanket for your entire application environment—from client-side to server-side and everything in between. This plan includes everything in the Advantage plan in addition to Bot Manager, behavioral-based multilayered detection and mitigation, automated API discovery and API security policy generation, and client-side protection enforcement.

1 Cisco Secure WAF and Bot Protection solutions are sold by Cisco through its global OEM partnership with Radware.

	Cisco Cloud WAF Protection Service		
	Essential	Advantage	Premier
Web Application Firewall (WAF)	✓	✓	✓
API Protection	✓	✓	✓
Basic Bot 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)	×	✓	✓
ERT Active Attackers Feed (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
DNS as a Service	Add-on	Add-on	Add-on
PCI DSS 4 Compliance Extension	×	Add-on	Add-on
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

Add-Ons

Web DDoS Protection

Secure Cloud WAF provides industry-leading application-layer (L7) protection against DDoS attacks. Advanced machine learning – behavioral detection accurately distinguishes between legitimate and malicious traffic and automatically generates granular signatures in real time to protect against zero-day attacks. With hybrid, always-on, and on-demand cloud DDoS service deployment options, Cloud Web DDoS Protection 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.

Emergency Response Team (ERT) Premier Managed Service

For organizations lacking in-house cybersecurity expertise or those who need to reduce security overheads, Cisco offers ERT Premier managed services through its OEM partner Radware:

- 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
- NoKey – SSL/TLS certificate private key storage service through HSM integration

Content Delivery Network

For enterprises that wish to combine website delivery with web application security, Secure Cloud WAF offers a content delivery network (CDN) solution integrated directly into our application protection portal. The CDN solution, which is based on the Amazon CloudFront CDN, provides a massive and globally distributed footprint, enhanced performance, and DevOps-friendly usability.

Unlimited DDoS Protection

For enterprises that suffer from high-volume DDoS attacks where 1G or 10G of mitigation capacity is insufficient, Cisco offers unlimited protection with the 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 your Cisco sales representative about which plan best suits your organization’s security needs.

PCI DSS 4 Compliance

In addition to WAF and API protection against business logic attacks, which are necessary for PCI DSS 4 compliance and included in the Secure Cloud WAF Protection service plans, the PCI DSS 4 add-on offers extended, specific client-side protection controls as required by PCI DSS 4 Sections 6.4.3 and 11.6.1:

- The PCI DSS 4 add-on provides complete visibility of all third-party scripts running on the client side of your application, along with a detailed inventory of all scripts. This includes real-time activity tracking alerts and threat-level assessments, as well as information about the script, such as whether the scrip is authorized and details about the script source and destination domain.
- The add-on notifies the user of any attempts to manipulate HTTP headers and form and payment pages and any attempts at DOM XSS.

Load Balancer as a Service

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.

	Cloud WAF Protection Service		
	Essential	Advantage	Premier
Failover (Active-Standby)	✓	✓	✓
Number of Active Real Servers (Origins)	1	8	8
Multi-port Support	×	✓	✓
Active-Active Load Balancing – Round Robin	×	✓	✓
IP-Based Persistency	×	✓	✓
URL-based Load Balancing	×	×	✓
Active-Active Load Balancing – Least Connection	×	×	✓
Cookie-Based Persistency	×	×	✓

DNS as a Service

DNS as a Service (DNSaaS) provides comprehensive Domain Name System (DNS) management, which is essential for the seamless functioning of all online applications. An integral component for any business that prioritizes application availability, security, and performance, investing in DNSaaS is more than just managing domain names; it's about safeguarding your business's digital presence and ensuring end users have a seamless experience. DNSaaS includes:

- A centralized management console with an easy-to-use interface for managing all DNS hosts, records, and health check configurations in one place.
- Customizable health checks for continuous monitoring of application sources status.
- Flexible record routing options for high availability based on Geo and Failover policies.
- Control over traffic distribution to specific resources or endpoints so end users can be served from the closest or most appropriate data center, improving latency and user experience.
- Real-time analytics that monitor the number of queries per hosted zone.

DNS as a Service is offered in three distinct packages, each priced based on the number of hosted zones, the volume of monthly DNS queries, and the quantity of health check objects.

Managed Services Support Levels

	Risk/Impact-based Priority	Essentials Support	Advantage Support	ERT Premier 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	×	✓	✓
	Chart 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
	NoKey- HSM Integration	×	×	✓ Limited Availability

DefensePro is a registered trademark of Radware, Inc.
DefensePro X and other industry-leading DDoS protection solutions are sold by Cisco through its global OEM partnership with Radware.