# Cisco Secure Cloud Web Application Firewall (WAF) Service Plans

November 2023

# Contents

## 1. Introduction

- Cisco® Secure Cloud Web Application Firewall (WAF) is a Cisco Secure OEM solution based on Radware's Cloud WAF Service that provides a fully managed, cloud-based web application firewall service.
- The service provides full protection from web application-based attacks and is based on Radware's Attack Mitigation Solution, which is comprised of Radware's AppWall[1] and, for Layer 7 distributed-denial-of-service (DDoS) protection, Radware DefensePro.[1]
- The fully managed Cloud WAF service is easy to set up and does not require the user to download or configure any software.
- The customer can fully protect web applications, mobile applications, and API endpoints by onboarding onto the Cloud WAF service. The onboarding process involves adding application information and certificates, enabling protection features, and editing their DNS records to redirect traffic to the Cloud WAF service.
- Secure Cloud WAF provides comprehensive coverage of both common and advanced web attacks as well as DDoS attacks.

## 2. Service Plans

Secure Cloud WAF Protection is available with three service plans designed to meet all customer requirements. Each service plan is also designed to meet different cybersecurity needs and risk exposures and provide a level of managed services that meets the needs of the customer.

### 2.1 Essentials Plan

The Essentials plan is an entry-level package that offers industry benchmark protection for applications. Essentials includes Cloud WAF protection, API protection, zero-day attack protection, 1 Gbps of network DDoS protection, standard support, and outstanding SLAs.

### 2.2 Advantage Plan

The Advantage plan takes application security to the next level by offering advanced protection for customers that need protection from sophisticated and unknown attacks. In addition to what's included in Essentials, the Advanced plan offers Advanced WAF (see Table 1), which utilizes a positive security model engine to protect against more sophisticated unknown and zero-day attacks. Advantage also includes 10 Gbps of network DDoS protection as well as JavaScript supply chain mapping, monitoring, and attack detection for client-side protection.

In addition, Advantage includes an intelligence feed, the ERT[2] Active Attackers Feed (EAAF), which automatically blocks known malicious active devices. Customers also benefit from the onboarding support and ongoing policy reviews that are included with the Advantage package.

[1] AppWall and DefensePro are registered trademarks of Radware, Inc.

[2] Radware Emergency Response Team (ERT)

## 2.3 Premier Plan

The Premier plan provides a comprehensive security blanket for your entire application environment. In addition to all the features and capabilities of the Essentials and Advantage plans, the Premier plan includes advanced Bot Manager with behavioral-based, multilayered detection and mitigation, automated API discovery and API security policy generation, client-side protection enforcement, and real-time automatic Web DDoS Protection.

## 2.4 Web DDoS Protection

As DDoS attacks continue to evolve, a new and more sophisticated type of DDoS attack has been developed that cannot be detected by the traditional network Layer 3, Layer 4, or even simple Layer 7 detection and mitigation solutions. The new Web DDoS attack known as a Web DDoS Tsunami attack and is often mistaken as legitimate traffic by traditional DDoS and WAF solutions as the traffic patterns are very similar.

Web DDoS attacks can easily overwhelm a system's resources by increasing the application maximum Requests Per Second (RPS) capacity, making the application unavailable to legitimate traffic. To detect a Web DDoS Tsunami attack, traffic needs to be decrypted, and the data must be parsed through new patented machine learning-based behavioral analysis in order to accurately identify valid traffic from malicious traffic and ensure the availability of the application.

**Table 1.** Secure Cloud WAF Service Plans

| Feature | Essentials | Advantage | Premier |
|---|---|---|---|
| **WAF** | • | • | • |
| **API Protection** | • | • | • |
| **Advanced Rules** | • | • | • |
| **Rate Limit** | • | • | • |
| **Access Control & IP Geo Rules** | • | • | • |
| **Reporting & Analytics** | • | • | • |
| **DDoS Protection** | 1 Gbps | 10 Gbps | 10 Gbps |
| **Standard Support** | • | • | • |
| **Advanced Support** | | • | • |
| **Advanced WAF** | | • | • |
| **ERT Active Attackers Feed (EAAF)** | | • | • |
| **Client - Side Protection - Detection** | | • | • |
| **Client - Side Protection - Mitigation** | | | • |
| **API Discovery** | | | • |
| **Bot Manager** | | | • |
| **Web DDoS Protection** | | | • |

| Feature | Essentials | Advantage | Premier |
|---|---|---|---|
| **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 |

## 2.5 Support and Premier/Enhanced Support

Enhanced support is available on any CWAF Service and offers a white glove service that provides priority support and a dedicated Customer Service Manager who will provide regular updates for policy reviews and post-threat analysis. Enhanced support is highly recommended for organizations that need professional support for WAF management and for advanced policy creating and incident forensics when the skill is not available within the customer's organization.

By default, customers who order Essentials are provided with Standard support. Customers who order Advantage or Premier are provided with Advanced support. Support levels can be seen in the table below.

**Table 2.** Support Matrix

| Category | Risk/Impact - based Priority | Standard Support | Advanced Support | Enhanced Support |
|---|---|---|---|---|
| Response SLA | P1 (Phone) | 40 Min | 30 Min | 10 Min |
| | P1 (Ticket) | 3 Hours | 2 Hours | 1 Hour |
| | 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 | No | Yes | Yes |
| | Onboarding & Policy Review | No | Yes | Yes |
| | Post - attack Analysis | No | Yes | Yes |
| | Quarterly Premium Security Report | No | No | Yes |
| | Security Configuration Review | No | 6 Months | 3 Months |
| | Extended Monitoring | No | External Monitoring on Top 5 Apps | External Monitoring on All Apps |

Cisco, through its global OEM partnership with Radware, offers industry-leading network and application protection solutions designed to meet the needs of every customer.

For more information about Cisco Secure WAF and Bot Protection, visit www.cisco.com/go/secure-waf. Contact Cisco today for more information.

For information about Cisco application security solutions, go to: https://www.cisco.com/site/us/en/products/security/cloud-application-security/index.html.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.



Printed in USA C78-xxxxxx-xx 11/23