

# Cloud WAF Demo Guide for Partners

*Written by Tal Yerushalmi*

*Advanced Solutions, Application Security Expert*

*Version 1.0*

October, 2023

## TABLE OF CONTEXT

Introduction .....	3
Key Presentation Messages .....	4
Prerequisites .....	5
Demo Summary .....	6
Detailed Guide – Core Demo .....	9
Overview Page - General .....	9
Overview Page - Widgets .....	10
Assets Page .....	11
Asset Settings Details Page .....	12
Security Events .....	13
Analytics .....	14
Drill Down to Security Events .....	15
Source Blocking .....	16
Bot Manager Demo .....	17
Bot Analytics .....	17
Bot Events .....	18
Bot Settings .....	19
API Protection Demo .....	20
API Protection .....	20
Client-Side Protection Demo .....	21
Client-Side Protection .....	21
Portal Management Demo .....	22
Notifications .....	22
Reports .....	23
Activity logs .....	24

## Introduction

Welcome to Radware's Cloud WAF Demo Guide! This document is designed to help you effectively demonstrate the features of the Application Security Service Portal. You will be guided through the Service Portal's capabilities in managing application security, analytics, and mitigation for web-application attacks.

The guide is structured with three elements on each page: "Actions," "Description," and an accompanying image. The "Actions" section provides a step-by-step guide on what to do, the "Description" section details what to say, and the accompanying image illustrates the corresponding items discussed in the first two sections.

Each section is numbered, with the action numbers corresponding to the description numbers.

The guide is divided into several parts, with the first part being the core demo. This is a basic demo that is ideal for first-time presentations and suitable for all customers. The later parts of the guide are optional and should be selected based on the customer's needs, such as their type of application (e.g. API-based), security challenges (e.g. frequent bot attacks), or expressed interests (e.g. client-side protection).

The demo will use the application [CWAFDemo.radware.net](https://CWAFDemo.radware.net), which is pre-configured with the following security protections: WAF (Web Application Firewall), API Security, API Discovery, Bot Manager, and Client Side Protection. The guide provides you with all the resources and instructions you need to conduct a successful demonstration of Radware's Cloud WAF solution and to showcase how it can protect your customers' online assets from web application, API, and bot-based attacks.

## Key Presentation Messages

When delivering the demonstration, it's important to clearly communicate the following messages to potential customers. These messages will help highlight the value and benefits of the solution being presented.

**Message 1:** Protect your web, API, and mobile applications with our comprehensive suite of security solutions, including DDoS protection, WAF, API, bot protection, GEO protection, and CDN. All of these features are easily accessible and manageable from our user-friendly dashboard.

**Message 2:** Our security service is fully managed, leveraging cutting-edge AI technology to save you time and effort. Our API discovery tool highlights this benefit by reducing the time spent querying application owners to protect APIs. This message is worth reiterating twice during the demo to emphasize its value.

**Message 3:** With our security solution, you have the peace of mind that comes with the ability to set each security engine in report-only mode initially. Then, as you become more confident in our solution, you can switch to blocking mode without worrying about blocking important traffic.

**Message 4:** Dealing with security events can be overwhelming, with thousands of events to manage. Our correlation of these events into meaningful activities through application analytics dramatically reduces the workload to just a few key events that you can manage in just a few minutes a day, or even once a week.

**Message 5:** Our portal is designed for ease of use and provides significant value for your internal users. Its user-friendly interface allows for quick and efficient management of your security needs.

## Prerequisites

The purpose of this section is to ensure that you are fully prepared and equipped with the necessary tools and knowledge to effectively demonstrate the capabilities of Radware's cloud WAF solution to potential customers. Before proceeding with the demo, it is crucial to make sure that the following steps are taken to guarantee a smooth and successful demonstration:

1. In order to conduct the demo, you will need access to the [Radware Cloud Services Portal](#). If you do not have access, please contact your account manager or our support team to request access.
2. In order for the demo to be consistent please prepare the widgets dashboard to display specific widgets which appear in this guide, to do so perform the following steps:

In the Overview Widget page of the Service Portal

Remove all widgets by clicking on the Filter icon, the Clear Dashboard button and then the Remove all Widgets button.

After all widgets have been removed, click on the icon at the top-right corner of the Overview page, and select the following widgets:

- WAF Summary
- HTTP Transactions
- OWASP Top 10 Mapping
- Blocked Geographical Map
- Bot Manager Summary
- Top DDoS Attack Sources

Then click on Add.

3. Before demonstrating, please watch the video that accompanies this document.

# Demo Summary

## Core Demo:

### 1. Overview Page - General

- a. Open the Overview page.
- b. Navigate through the different widgets using your mouse cursor.
- c. Click the toggle on bottom of the left side menu to switch back and forth from Dark Mode
- d. Point to the global time filter and click the filter button to display all available widgets.

### 2. Overview Page - Widgets

- a. Take a quick tour of the widgets starting with the WAF Summary widget.
- b. Next, show the Bot Summary widgets and point out that it shows percentages compared with the previous time frame.
- c. Show the Top DDoS attack sources.
- d. Go back to the WAF summary widget and click on "applications".

### 3. Assets Page

- a. Take a tour of the assets page.
- b. Show the current state of each application on the left side in the Assets page, hover over the green indicator to display the status of the origin servers and then over the events graph to show the event number and percentage
- c. Click on the application CWAF SecureDemo

### 4. Asset Settings Details Page

- a. On the Assets settings details page, use the cursor to hover over the Event summary bar.
- b. Next, show the Origin status and Client-Side Protection status.
- c. With the mouse cursor move to the right side of the page to and move over all of the protections.
- d. Click Go to Security Events

### 5. Security Events

- a. Use the mouse cursor to display the Security Events page by hovering over the different tabs: WAF, DDoS, Bot.
- b. Show the amount of data present in the page and scroll down to show the number of events.
- c. On the left side menu, hover over the briefcase icon and click on Assets. Click on the application CWAF SecureDemo and then click "Go To Analytics."



## 6. Analytics

- With the cursor, hover over the tabs Allow List, Vulnerabilities, and Database.
- Click on the Vulnerabilities tab, expand the top event to view the detailed information, including the top URI, number of security events, top IPs, and countries.
- Click "Show HTTP Request Example" to view an example related to the grouped attacks.
- Scroll to the bottom of the expanded view and click to access security events.

## 7. Drill Down to Security Events

- Show that the security events are filtered by the rule ID observed in the Analytics page.
- Expand the first event and use the mouse cursor to display all the data in the expanded view.
- Hover over the "Allow" button with the mouse cursor.

## 8. Source Blocking

- Click on the filter button, click Clear All, click on the filter again, select "Security protection type" as "source blocking" and click "apply."
- Expand the top event and click on the "Show Source Blocking Attack Story" button.
- Hover over the security details, the penalty score, and the attack story.
- Hover over the shield icon and click on the Analytics option. In the Analytics page, click on the Bot tab. Click on the filter to select the application "CWAF SecureDemo".

## Bot Manager Demo:

### 9. Bot Analytics

- Open the Analytics page, switch to the Bot tab and select CWAF SecureDemo
- Click on the Bad Bots tab in the Bot Analytics page.
- Expand the top event to view its details
- Click on the number of hits.

### 10. Bot Events

- Take a tour of the Bot Events Page
- Click on the top bot event to expand the view and view the request details and security details.
- Hover over the "Allow" button and the "Add Exception to Custom Policy" link.
- Go back to the Assets page by hovering over the briefcase icon in the left side menu, click assets, click on "CWAF SecureDemo" and switch to the Bot Manager tab.

### 11. Bot Settings

- Click to expand the Bot response section, Scroll through the all the generations of bots.
- Open one of the responses of a fourth generation Bot and scroll through the options.
- Expand the legitimate bot section and display the response options.
- Click on the API Security Tab.

## API Protection Demo:

### 12. API Protection

- a. Click and expand the API settings section.
- b. Click and expand the API Endpoints section.
- c. Scroll through the different endpoints and point out the sections of the right side indicating the endpoint allowed method and origin.
- d. Afterwards, click on the Client Side Protection tab.

## Client-Side Protection Demo:

### 13. Client-Side Protection

- a. Take a tour of the Client-Side Protection settings page, click and expand the settings section, and click on to expand the notifications section.
- b. Click and expand the Domains section. Scroll through the different discovered domains, the threat level assigned to them, and the action they are configured with.

## Portal Management Demo:

### 14. Notifications

- a. On the left side menu hover over the shield icon and click on notifications.
- b. Click on the Alert-Example.

### 15. Reports

- a. On the left side menu, hover over the shield icon and click on Reports.
- b. Click on the Report Example.

### 16. Activity Logs

- a. Go to the Activity logs page by hovering over the person icon on the left side menu and clicking on Activity log.
- b. Click on one of the reports to open the expanded view.



# Detailed Guide – Core Demo

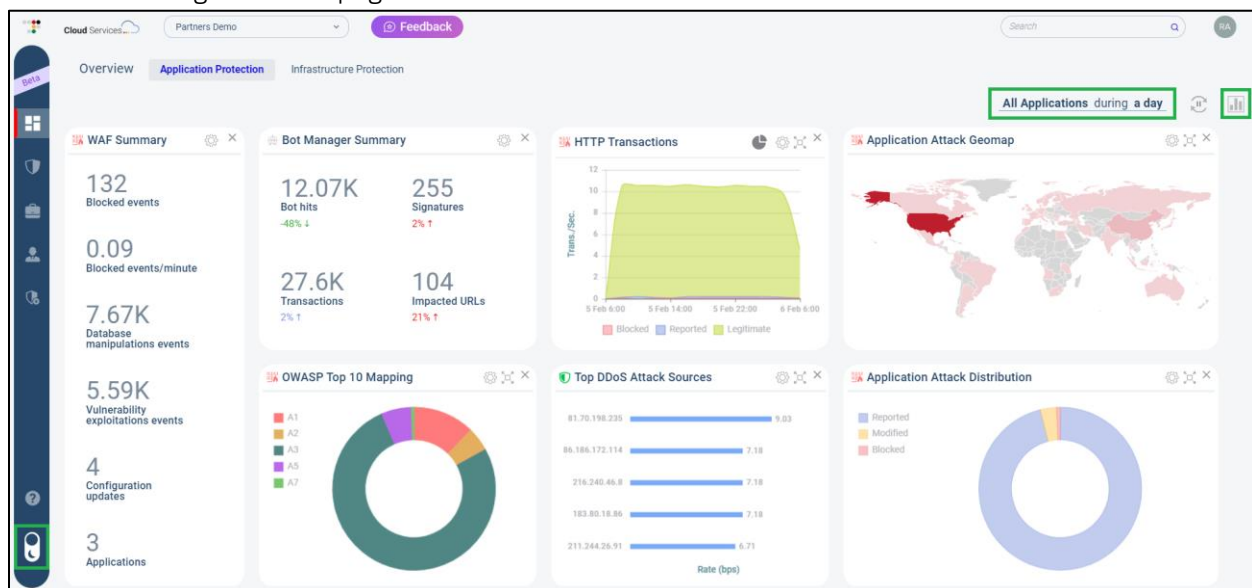
## Overview Page - General

### Actions:

1. Open the Overview page.
2. Navigate through the different widgets using your mouse cursor.
3. Click on the toggle on bottom of the left side menu to switch back and forth from Dark Mode
4. Point to the global time filter and click the filter button to display all available widgets.

### Description:

1. We are now viewing the Overview page of Radware's web-based customer service portal, which provides a comprehensive view of all the protections your APIs, web, and mobile applications needs
2. This page serves as a centralized location, allowing you to quickly check the status of various services, including DDoS, WAF, API, BOT, GEO, and CDN. This one-stop-shop of managed services simplifies your security management process and provides insightful information to keep your applications secure.
3. Before we get started you can use the Light/Dark mode toggle to switch to the mode preferable to you
4. Here you can use the this button to change the scope and time frame of the information displayed by the widgets and the widgets button allows you to add / remove and customize the widgets on the page.



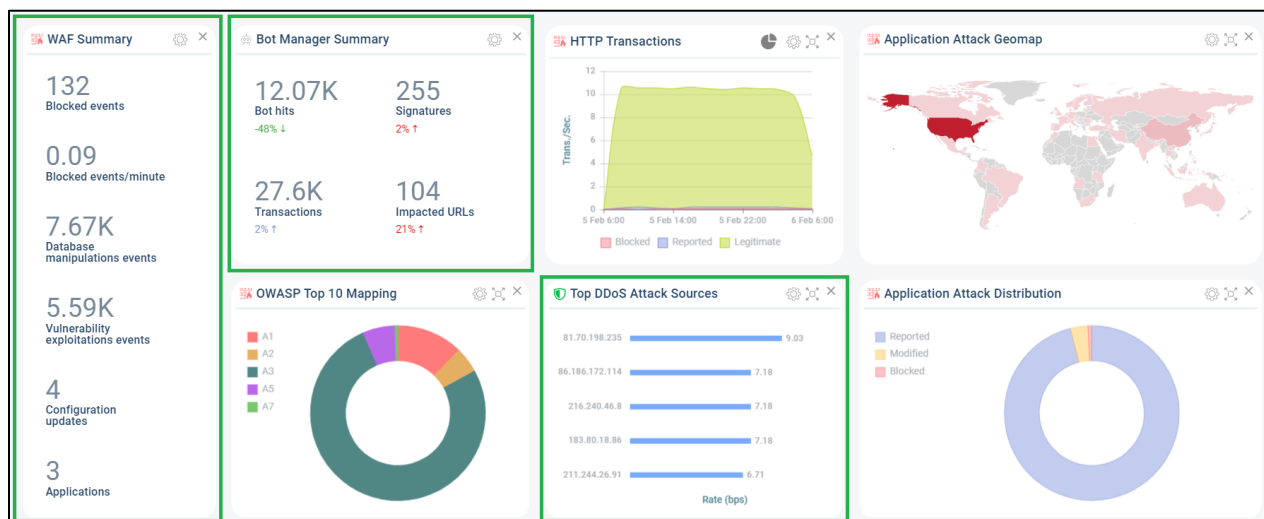
## Overview Page – Widgets

### Actions:

1. Take a quick tour of the widgets starting with the WAF Summary widget.
2. Next, show the Bot Summary widgets and point out that it shows percentages compared with the previous time frame.
3. Show the Top DDoS attack sources.
4. Go back to the WAF summary widget and click on "applications".

### Description:

1. The Overview page's widgets are interactive, customizable, and provide valuable insights at a glance. The WAF Summary widget provides clear information on event counts and rates, event types, and application count.
2. The Bot Summary widget gives us details on bot activity and relative data compared to the previous time frame. For example, it compares this week to the previous week, allowing us to quickly identify any anomalous bot activities in the applications.
3. The Top DDoS Attack Sources widget displays the top source IP addresses responsible for Layer 3/4 DDoS attacks on your application. This information is made available thanks to the built-in Layer 3/4 DDoS protection that is deployed by default with every application protected by our Cloud Application protection (CWAF)
4. Let's return to the WAF summary widget and click on "applications" to go straight to the Assets page.



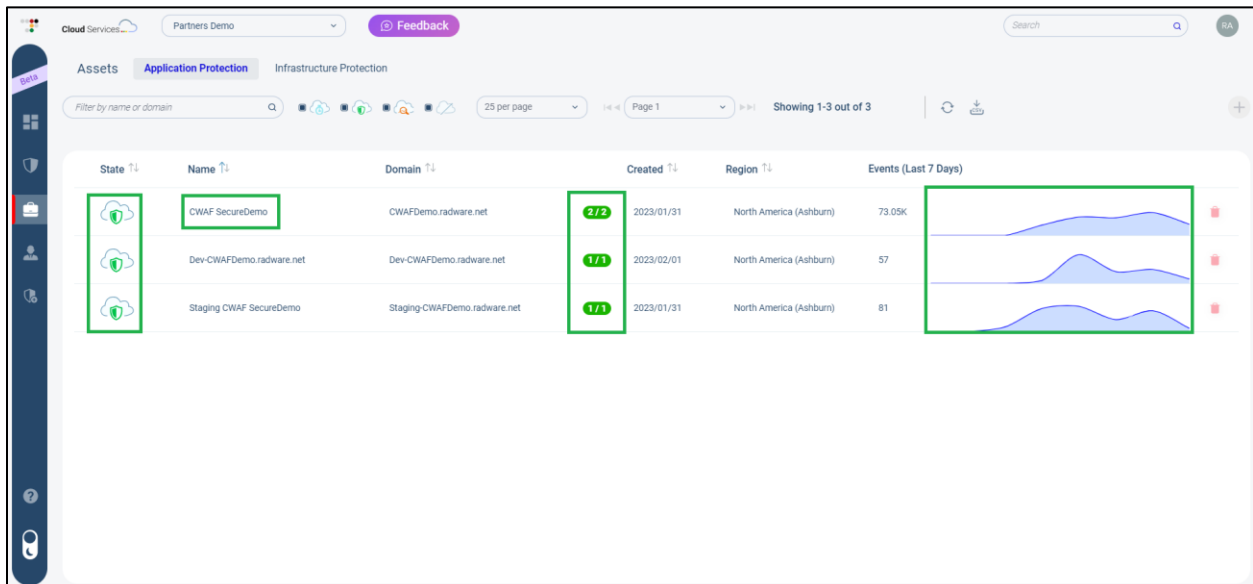
## Assets Page

### Actions:

1. Take a tour of the assets page.
2. Show the current state of each application on the left side in the Assets page, hover over the green indicator to display the status of the origin servers and then over the events graph to show the event number and percentage
3. Click on the application CWAF SecureDemo

### Descriptions:

1. Welcome to the Assets Application Protection section of the Service Portal, where you can manage and configure the protection settings for your assets. In this page, you can add new assets or remove existing ones.
2. This view provides an at-a-glance view of the asset status, the status of the origin servers, and a 7-day graph of the application-related events.
3. To edit an application, simply click on it. Let's go ahead and click on the CWAF SecureDemo application.



The screenshot shows the 'Assets' page in the Cloud Services portal. The page has a sidebar with navigation icons and a main content area. The main content area has tabs for 'Assets', 'Application Protection', and 'Infrastructure Protection'. The 'Assets' tab is active, showing a table of applications. The table has columns for State, Name, Domain, Created, Region, and Events (Last 7 Days). There are three applications listed: 'CWAF SecureDemo', 'Dev-CWAFDemo.radware.net', and 'Staging CWAF SecureDemo'. Each application has a green status indicator in the 'State' column. The 'CWAF SecureDemo' application is highlighted with a green box. The 'Events (Last 7 Days)' column shows a line graph for each application. The 'CWAF SecureDemo' application has 73,09K events, 'Dev-CWAFDemo.radware.net' has 57 events, and 'Staging CWAF SecureDemo' has 81 events.

State	Name	Domain	Created	Region	Events (Last 7 Days)
	CWAF SecureDemo	CWAFDemo.radware.net	2023/01/31	North America (Ashburn)	73,09K
	Dev-CWAFDemo.radware.net	Dev-CWAFDemo.radware.net	2023/02/01	North America (Ashburn)	57
	Staging CWAF SecureDemo	Staging-CWAFDemo.radware.net	2023/01/31	North America (Ashburn)	81

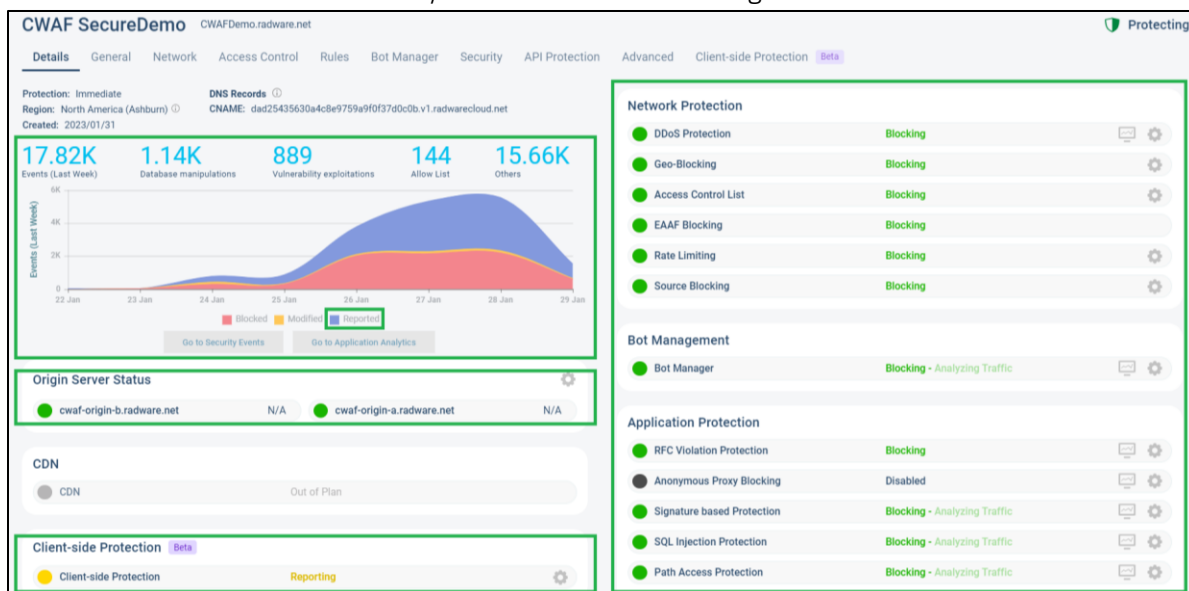
## Asset Settings Details Page

### Actions:

1. On the Assets settings details page, use the cursor to hover over the Event summary bar.
2. Next, show the Origin status and Client side protection status.
3. With the mouse cursor move to the right side of the page to and move over all of the protections.
4. Click Go to Security Events

### Descriptions:

1. Welcome to the Asset Settings Details page. Here we can get a closer look at the status of the application and its protection settings here we can see an event summary bar
2. We can see the status of our origin servers and Client Side Protection.
3. On the right side, you'll find a small dashboard that displays all the available protections and their current status. A yellow light indicator for a protection means it is in Report Only mode, allowing you to test the policy until you have the confidence to set it to Block. This section is divided into Network Protection, Bot Management, and Application Protection.
4. Now let's move on to Security events to see attack mitigation in action.



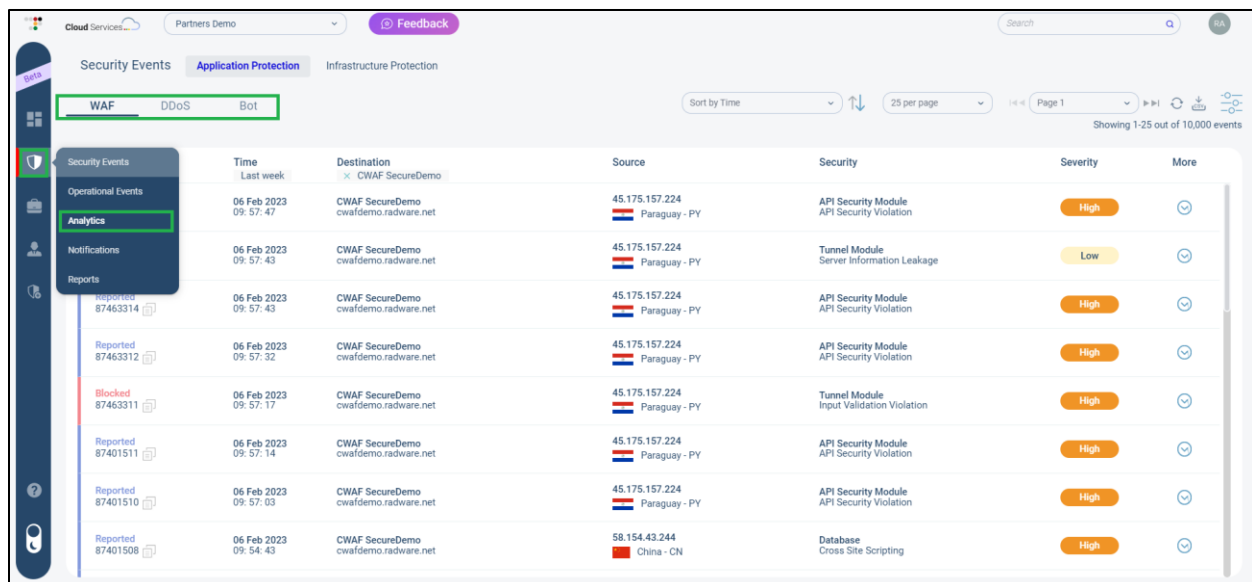
## Security Events

### Actions:

1. Use the mouse cursor to display the Security Events page by hovering over the different tabs: WAF, DDoS, Bot.
2. Show the amount of data present in the page and scroll down to show the number of events.
3. On the left side menu, hover over the briefcase icon and click on Assets. Click on the application CWAF SecureDemo and then click "Go To Analytics."

### Descriptions:

1. This is the Security Events page where you can switch between different types of events, such as WAF, DDoS, and Bot.
2. With so many events displayed, it can be challenging to navigate and understand the data. To make things easier and help you manage the ever-growing amount of data an Application Analytics page was created.
3. In the Application Analytics page we will find the events grouped by pattern and type, making it easier to understand and act on them. Let's go ahead and take a look at the Application Analytics page for the CWAF SecureDemo application.



Time	Destination	Source	Security	Severity	More
06 Feb 2023 09: 57: 47	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	API Security Module API Security Violation	High	
06 Feb 2023 09: 57: 43	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	Tunnel Module Server Information Leakage	Low	
06 Feb 2023 09: 57: 43	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	API Security Module API Security Violation	High	
06 Feb 2023 09: 57: 32	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	API Security Module API Security Violation	High	
06 Feb 2023 09: 57: 17	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	Tunnel Module Input Validation Violation	High	
06 Feb 2023 09: 57: 14	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	API Security Module API Security Violation	High	
06 Feb 2023 09: 57: 03	CWAF SecureDemo cwfademo.radware.net	45.175.157.224 Paraguay - PY	API Security Module API Security Violation	High	
06 Feb 2023 09: 54: 43	CWAF SecureDemo cwfademo.radware.net	58.154.43.244 China - CN	Database Cross Site Scripting	High	



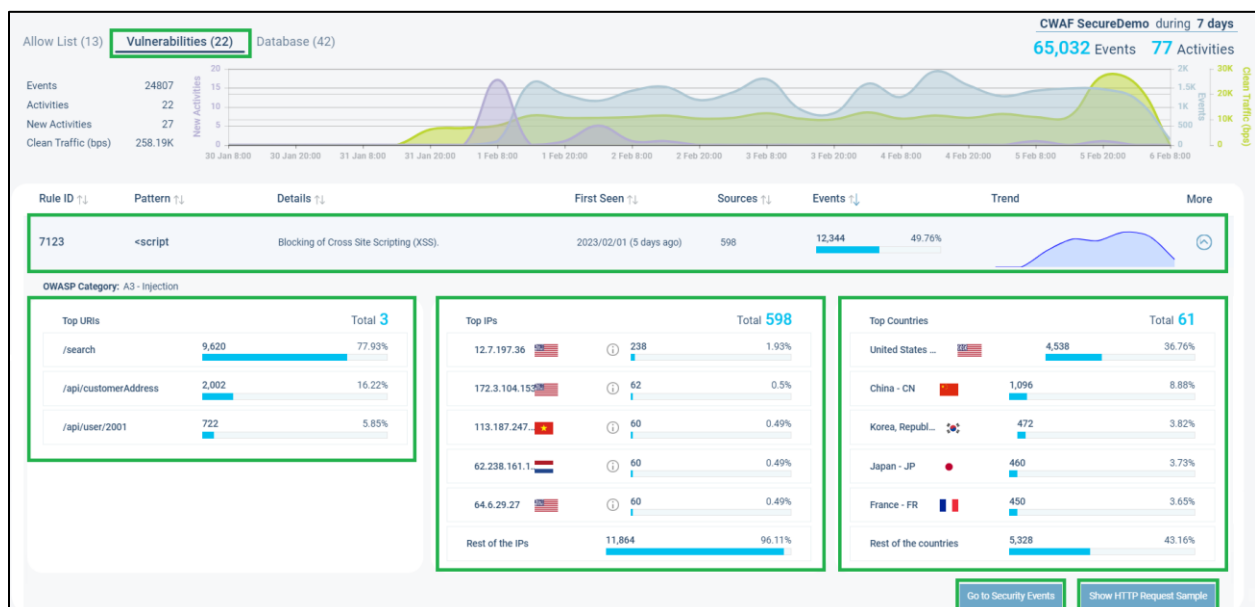
## Analytics

### Actions:

1. With the cursor, hover over the tabs Allow List, Vulnerabilities, and Database.
2. Click on the Vulnerabilities tab, expand the top event to view the detailed information, including the top URI, number of security events, top IPs, and countries.
3. Click "Show HTTP Request Example" to view an example related to the grouped attacks.
4. Scroll to the bottom of the expanded view and click to access security events.

### Descriptions:

1. The Application Analytics page provides you with an easy-to-use interface to view and analyze security events. It takes a massive amount of information, correlating hundreds of thousands of events, and distills them into an easily manageable number of activities that you can understand and analyze. With its three tabs: Allow List, Vulnerabilities, and Database you can cut through the noise and quickly identify high-priority alerts and troubleshoot issues.
2. When you click on the Vulnerabilities tab and expand the top event, you will see detailed information about the attack, such as the top URI targeted, the number of security events, the top IPs and countries involved.
3. The "Show HTTP Request Example" feature allows you to view a related example of the grouped attacks.
4. From here, you can drill down further by clicking "Go To Security Events."





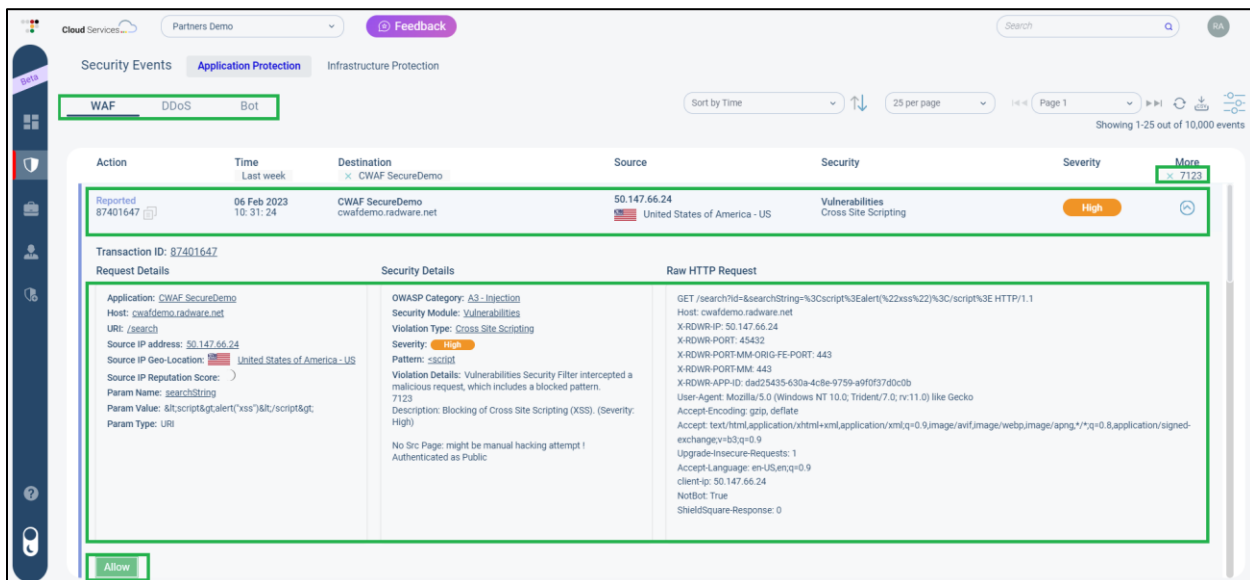
## Drill Down to Security Events

### Actions:

1. Show that the security events are filtered by the rule ID observed in the Analytics page.
2. Expand the first event and use the mouse cursor to display all the data in the expanded view.
3. Hover over the "Allow" button with the mouse cursor.

### Descriptions:

1. We are now back in the Security Events page, and the events are filtered by the rule ID that was viewed in the Application Analytics page.
2. By expanding the first event, you can see the Transaction ID, request details, and security details, which provide in-depth information about the event type and raw HTTP data.
3. The "Allow" button, located at the bottom, offers a simple and flexible solution for managing false positives and keeping them down to near-zero by allowing you to refine your security policy with just one click. This feature, among many others, is what makes for Radware's ability to provide ultra high level of security that doesn't stand in the way of your business – what we call state-of-the-art security that is frictionless. (user-friendly and manageable with the lowest level of false positives in the industry)



The screenshot displays the Radware Cloud WAF Security Events interface. The top navigation bar includes 'Cloud Services', 'Partners Demo', and a 'Feedback' button. The main header shows 'Security Events' with tabs for 'Application Protection' and 'Infrastructure Protection'. Below this, there are filters for 'WAF', 'DDoS', and 'Bot'. The event list is sorted by time, showing 25 events per page. The first event is highlighted, showing a 'Reported' status, a time of '06 Feb 2023 10:31:24', a destination of 'CWAF SecureDemo', a source IP of '50.147.66.24', and a security type of 'Vulnerabilities Cross Site Scripting' with a 'High' severity. The event is expanded, showing the transaction ID '87401647'. The expanded view is divided into three sections: 'Request Details', 'Security Details', and 'Raw HTTP Request'. The 'Request Details' section shows the application 'CWAF SecureDemo', host 'cwfademo.radware.net', URI '/search', and source IP address '50.147.66.24'. The 'Security Details' section shows the OWASP Category 'A3-Injection', Security Module 'Vulnerabilities', Violation Type 'Cross Site Scripting', and Severity 'High'. The 'Raw HTTP Request' section shows the GET request for '/search?Id=ResearchString=%3Cscript%3Ealert(%22xss%22)%3C/script%3E HTTP/1.1'. At the bottom of the expanded event view, there is an 'Allow' button.

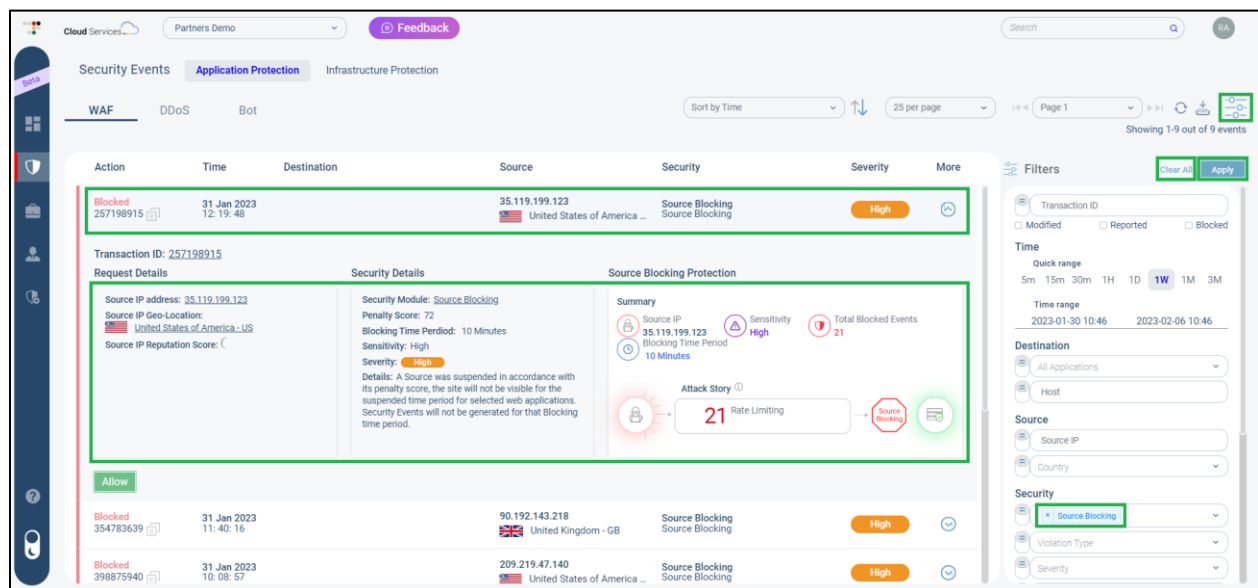
## Source Blocking

### Actions:

1. Click on the filter button, click Clear All, click on the filter again, select "Security protection type" as "source blocking" and click "apply."
2. Expand the top event and click on the "Show Source Blocking Attack Story" button.
3. Hover over the security details, the penalty score, and the attack story.

### Descriptions:

1. This is an example of an event generated by the source-blocking feature.
2. This feature assigns a penalty score to attackers, with different scores assigned for different types of attacks. If an attacker accumulates a certain score over a short period of time, they are blocked for a configurable amount of time.
3. In the expanded view, you can see all the details of the attack story, including the total number of blocked events, sensitivity, source IP, and more.



The screenshot displays the Cloud WAF Security Events interface. The top navigation bar includes 'Security Events', 'Application Protection', and 'Infrastructure Protection'. The 'Application Protection' tab is active, showing a list of events under 'WAF', 'DDoS', and 'Bot' categories. The 'WAF' category is selected, and the 'Source Blocking' event is highlighted. The event details are expanded, showing the following information:

- Transaction ID:** 257198915
- Request Details:** Source IP address: 35.119.199.123, Source IP Geo-Location: United States of America - US, Source IP Reputation Score: (C)
- Security Details:** Security Module: Source Blocking, Penalty Score: 72, Blocking Time Period: 10 Minutes, Sensitivity: High, Severity: High. Details: A Source was suspended in accordance with its penalty score, the site will not be visible for the suspended time period for selected web applications. Security Events will not be generated for that Blocking time period.
- Source Blocking Protection:** Summary: Source IP 35.119.199.123, Sensitivity High, Total Blocked Events 21, Blocking Time Period 10 Minutes. Attack Story: 21 Rate Limiting, Source Blocking.

The interface also includes a 'Filters' panel on the right with options for Transaction ID, Time range (Quick range: 5m, 15m, 30m, 1H, 1D, 1W, 1M, 3M; Time range: 2023-01-30 10:46 to 2023-02-06 10:46), Destination (All Applications, Host), Source (Source IP, Country), and Security (Source Blocking, Violation Type, Severity).

# Bot Manager Demo

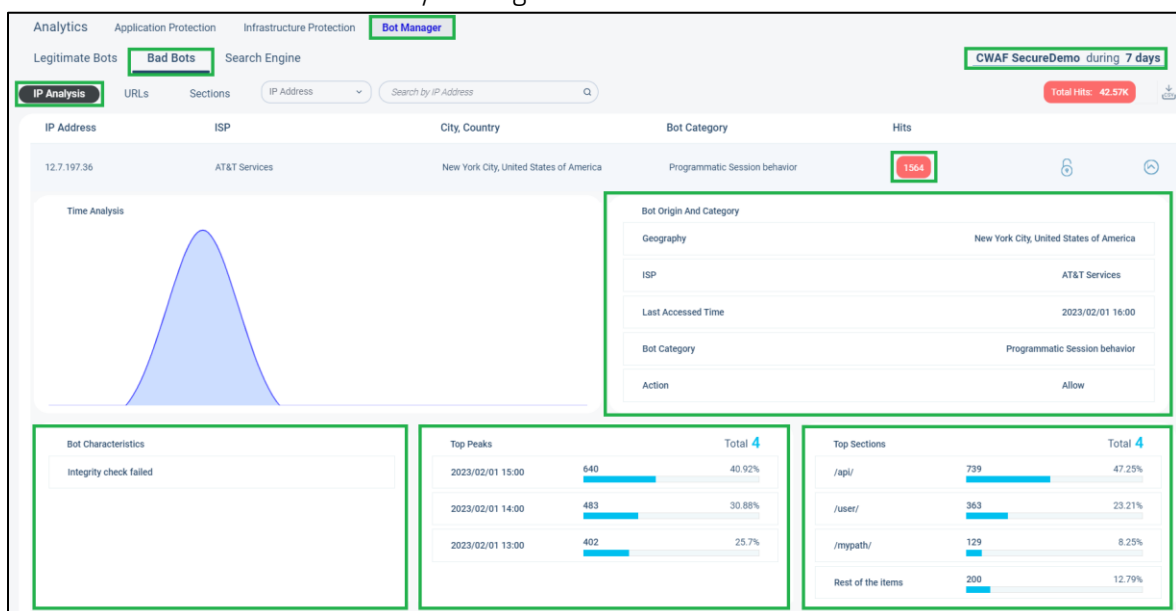
## Bot Analytics

### Actions:

1. Open the Analytics page, switch to the Bot tab and select CWAF SecureDemo
2. Click on the Bad Bots tab in the Bot Analytics page.
3. Expand the top event to view its details
4. Click on the number of hits.

### Descriptions:

1. To view Bot manager in action lets start from Bot Analytics
2. The Bot Analytics page is where you can view and analyze all bot-related activities related to your web applications. It gives you visibility into the behavior of bots in your application and helps you identify and categorize bot activities so you can take quick action.  
The page is divided into sections for Legitimate, Bad, and Search Bots. Let's focus on the Bad Bots section.
3. In the IP analysis section, you can see detailed information on the different bot source IPs, bot categories, and number of hits generated. Expanding the top event provides more information, such as the type of bot and the ISP the source IP originated from. Additionally, the Bot Characteristics section shows the different behaviors that flagged the "user" as a bot and the Top Peaks showing when the attacks occurred and at what rate.
4. Now let's look at the Bot events by clicking on the number of Hits.



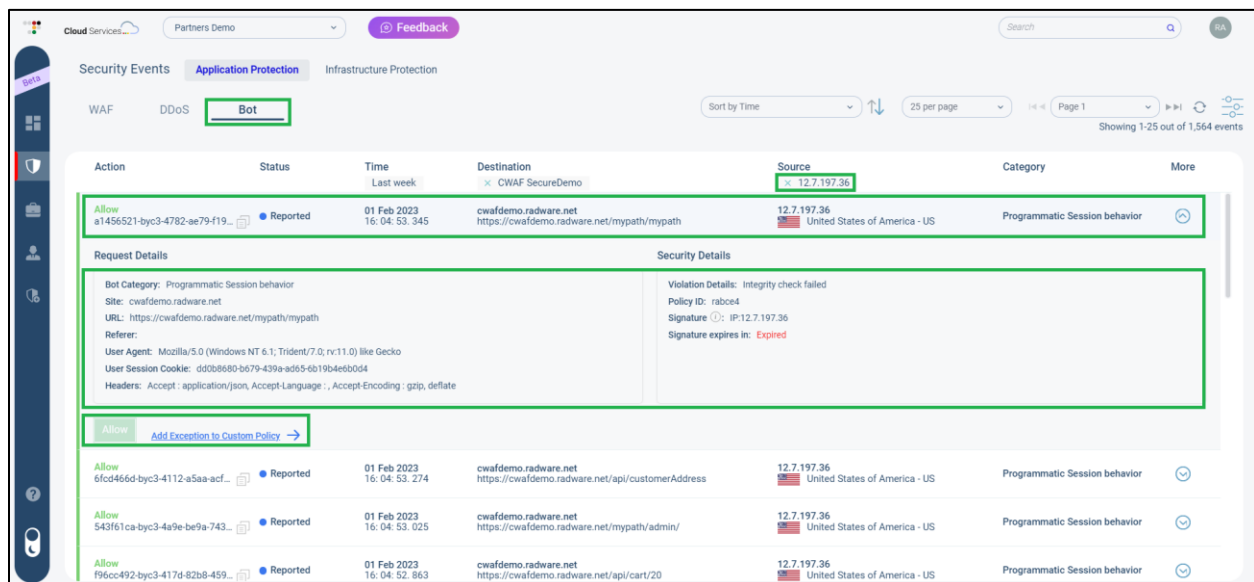
## Bot Events

### Actions:

1. Take a tour of the Bot Events Page
2. Click on the top bot event to expand the view and view the request details and security details.
3. Hover over the "Allow" button and the "Add Exception to Custom Policy" link.
4. Go back to the Assets page by hovering over the briefcase icon in the left side menu, click assets, click on "CWAF SecureDemo" and switch to the Bot Manager tab.

### Descriptions:

1. This is the Bot Events page, where you can see detailed information about each bot event detected by the Bot Manager. The chart displays the action taken, status, timestamp, source, and bot category for each event.
2. When you click on an event, you can see more information, including the request details and bot category on the left and the details of the violation, policy ID, and signature on the right.
3. At the bottom of the expanded view, you have the option to allow this specific type of event. If the event falls under a custom rule but you still consider it a violation, you can add an exception to the custom rule with just one click, making it easy to fine-tune your Bot Manager policy.
4. Let's now head over to the Bot Settings page.



Action	Status	Time	Destination	Source	Category
Allow	Reported	01 Feb 2023 16: 04: 53. 345	cwafdemo.radware.net https://cwafdemo.radware.net/mypath/mypath	12.7.197.36 United States of America - US	Programmatic Session behavior
Allow	Reported	01 Feb 2023 16: 04: 53. 274	cwafdemo.radware.net https://cwafdemo.radware.net/api/customerAddress	12.7.197.36 United States of America - US	Programmatic Session behavior
Allow	Reported	01 Feb 2023 16: 04: 53. 025	cwafdemo.radware.net https://cwafdemo.radware.net/mypath/admin/	12.7.197.36 United States of America - US	Programmatic Session behavior
Allow	Reported	01 Feb 2023 16: 04: 52. 863	cwafdemo.radware.net https://cwafdemo.radware.net/api/cart/20	12.7.197.36 United States of America - US	Programmatic Session behavior

**Request Details**

Bot Category: Programmatic Session behavior  
 Site: cwafdemo.radware.net  
 URL: https://cwafdemo.radware.net/mypath/mypath  
 Referer:  
 User Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko  
 User Session Cookie: dd0b680-b679-439a-ad55-6b19b4eeb0d4  
 Headers: Accept: application/json, Accept-Language: , Accept-Encoding: gzip, deflate

**Security Details**

Violation Details: Integrity check failed  
 Policy ID: rabce4  
 Signature: IP:12.7.197.36  
 Signature expires in: Expired

[Allow](#)
[Add Exception to Custom Policy](#)

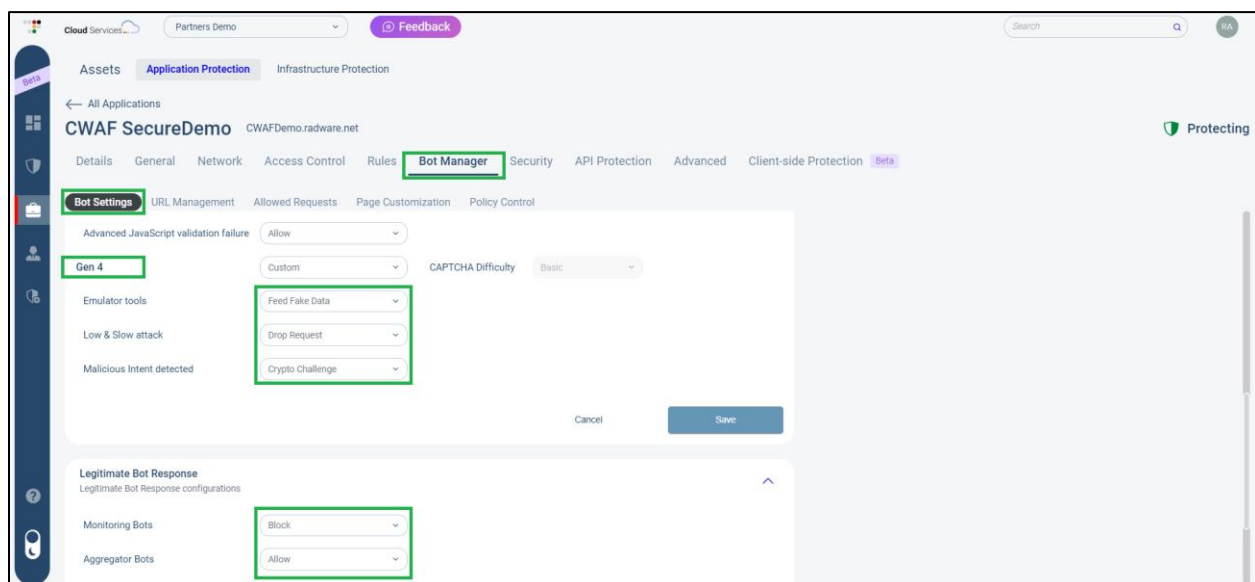
## Bot Settings

### Actions:

1. Click to expand the Bot response section, Scroll through the all the generations of bots.
2. Open one of the responses of a fourth generation Bot and scroll through the options.
3. Expand the legitimate bot section and display the response options.
4. Click on the API Security Tab.

### Descriptions:

1. This is the Bot Manager settings page, where you can define the response for each Bot Generation and type.
2. If you click to expand the response options for a fourth-generation bot, you will many different options, some of the advanced options are "Feed Fake Data" that feeds fake product price and data to web scraper bots and "Crypto Challenge" which uses CPU intensive crypto challenges for the Bot to make the attack less viable.
3. The options for responding to legitimate bots can also be found at the bottom of the page. Although they are legitimate, you may not want to allow them access to your web applications.
4. Bot Manager has many more features that are easy to manage, but now let's move on to API Security and Discovery.





# API Protection Demo

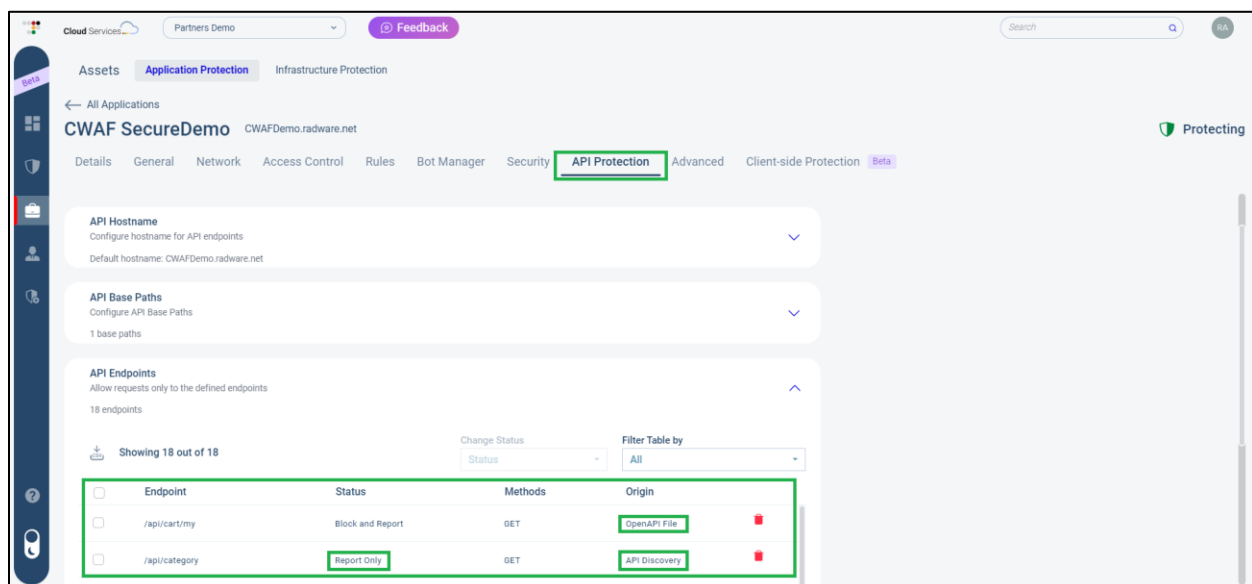
## API Protection

### Actions:

1. Click and expand the API settings section.
2. Click and expand the API Endpoints section.
3. Scroll through the different endpoints and point out the sections of the right side indicating the endpoint allowed method and origin.
4. Afterwards, click on the Client-Side Protection tab.

### Descriptions:

1. The API Security section allows you to upload an OpenAPI schema file, manually define API endpoints, or use API Discovery's machine learning engine to discover the endpoints. This includes not just the API Paths, methods, query parameters and more.
2. The API Endpoints section displays all the endpoints and indicates which endpoints have been imported using a schema file, which were added manually, and which were discovered. API Discovery can automatically generate a complete Open API schema file for the entire API.
3. It is important to note that each endpoint can be configured with quota limits which are crucial for API security and can be edited down to every detail, ultimately serving the ability to enforce the entire schema including the body
4. Next let's head over to the Client-Side Protection Tab



The screenshot shows the Radware Cloud WAF interface. The 'API Protection' tab is selected, and the 'API Endpoints' section is expanded. The table below shows the endpoints and their configurations:

Endpoint	Status	Methods	Origin
/api/cart/my	Block and Report	GET	OpenAPI File
/api/category	Report Only	GET	API Discovery



# Client-Side Protection Demo

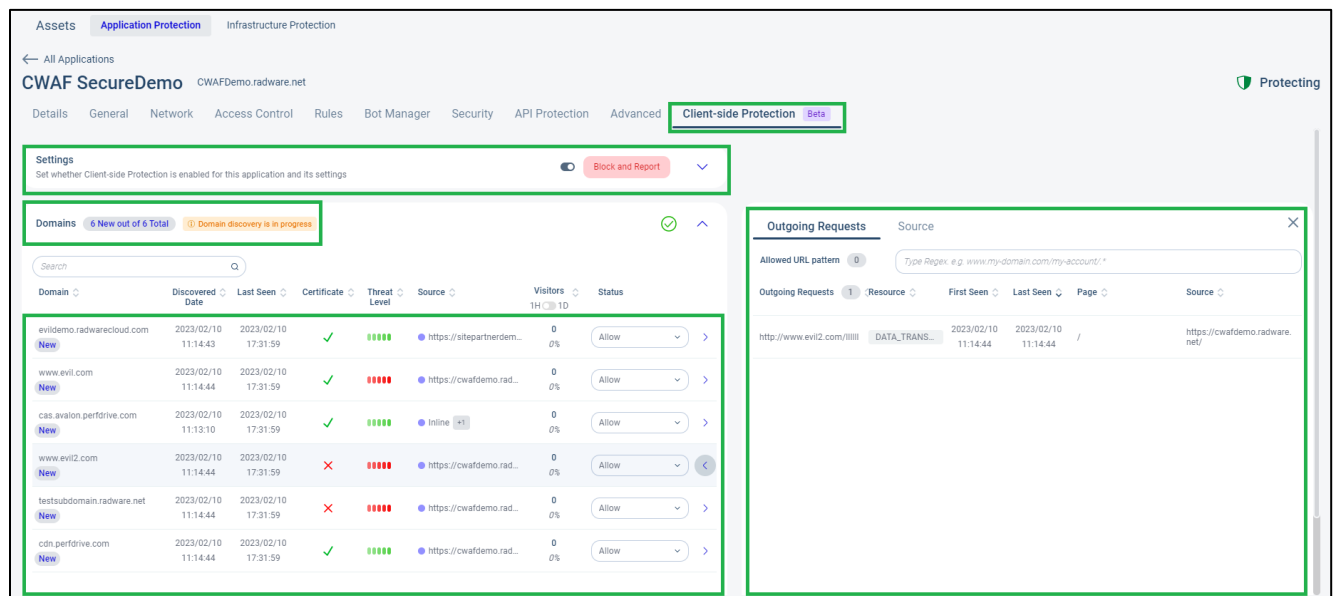
## Client-Side Protection

### Actions:

1. Take a tour of the Client-Side Protection settings page, click and expand the settings section, and click on to expand the notifications section.
2. Click and expand the Domains section. Scroll through the different discovered domains, the threat level assigned to them, and the action they are configured with.

### Descriptions:

1. This is the Client-Side Protection settings page. Here, you can enable and configure how to treat newly discovered domains and what data is considered sensitive. You can also configure different notifications regarding newly discovered domains, and view and configure all the discovered domains.
2. By clicking on the Domains section, you can view the domains already discovered. This section lists the domains with the threat level assigned to them and displays information about whether they have a valid certificate. You can easily see expected third-party domains, such as Google Analytics, and unexpected or unwanted third-party domains and configure an appropriate action related to them.



The screenshot displays the Radware Cloud WAF Demo interface, specifically the Client-Side Protection settings page. The page is divided into two main sections: Settings and Domains. The Settings section includes a toggle for 'Block and Report' and a 'Domain discovery is in progress' status. The Domains section displays a table of discovered domains with columns for Domain, Discovered Date, Last Seen, Certificate, Threat Level, Source, Visitors, and Status. The table lists several domains, including evildemo.radwarecloud.com, www.evil.com, cas.avalon.perforive.com, www.evil2.com, testsubdomain.radware.net, and cdn.perforive.com. The Threat Level column shows various indicators (green, red, orange) and the Status column shows 'Allow' or 'Deny' actions. An 'Outgoing Requests' panel on the right shows a list of requests with columns for Resource, First Seen, Last Seen, Page, and Source.

# Portal Management Demo

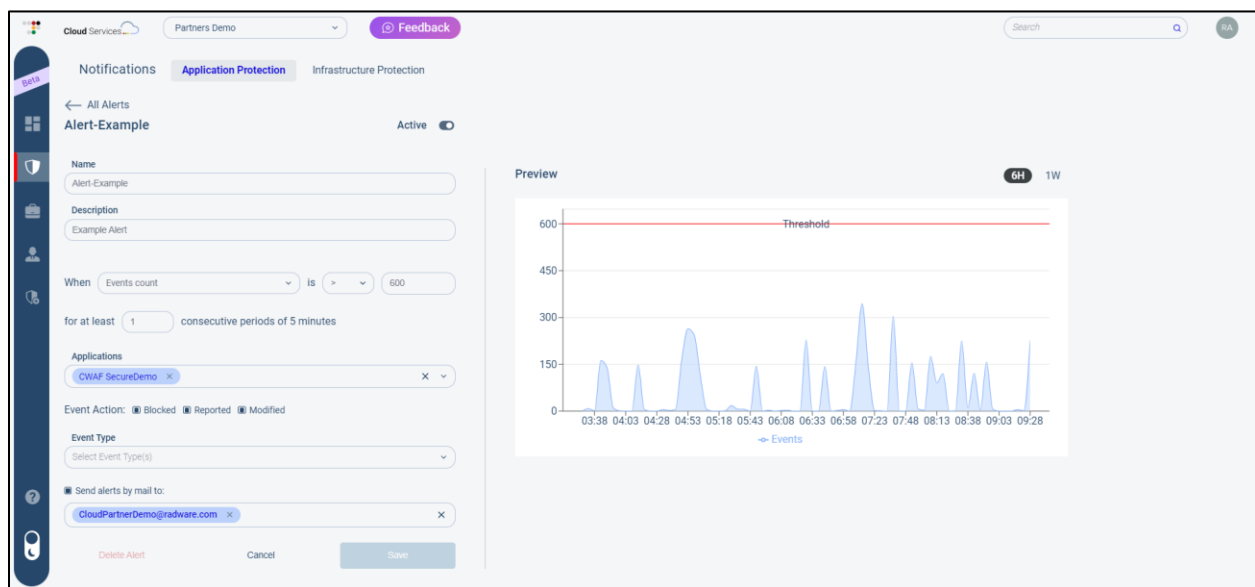
## Notifications

### Actions:

1. On the left side menu hover over the shield icon and click on notifications.
2. Click on the Alert-Example.

### Descriptions:

1. This section is called "Notifications" and is used to configure alerts that can be sent via email.
2. By clicking on the preconfigured Example Alert, you can see that an email notification can be set to trigger if an event count exceeds 600 events per minute for 5 consecutive minutes. This feature provides you with real-time information about potential security threats, and can be customized for a specific application, violation type, and action.



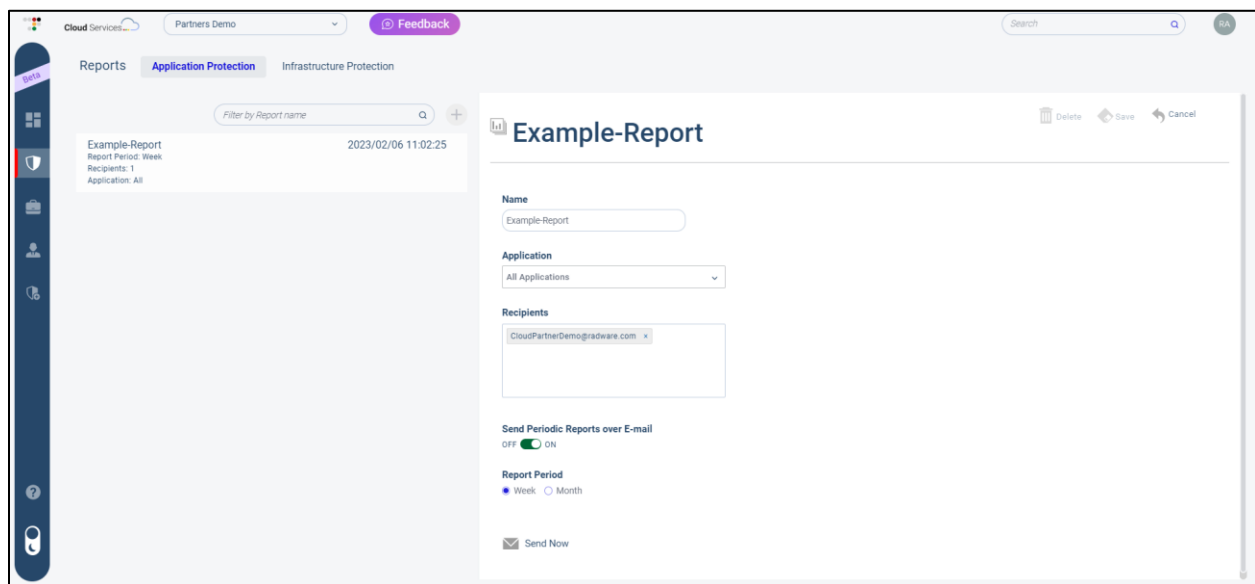
## Reports

### Actions:

1. On the left side menu, hover over the shield icon and click on Reports.
2. Click on the Report Example.

### Descriptions:

1. This section is called "Reports" and it allows you to create reports on your applications' activity.
2. Let's click on the Example Report that has been preconfigured. In this example, the report is set to be sent once a month and includes information about all applications. This feature can be configured to send reports to multiple recipients and can be customized for each individual application.



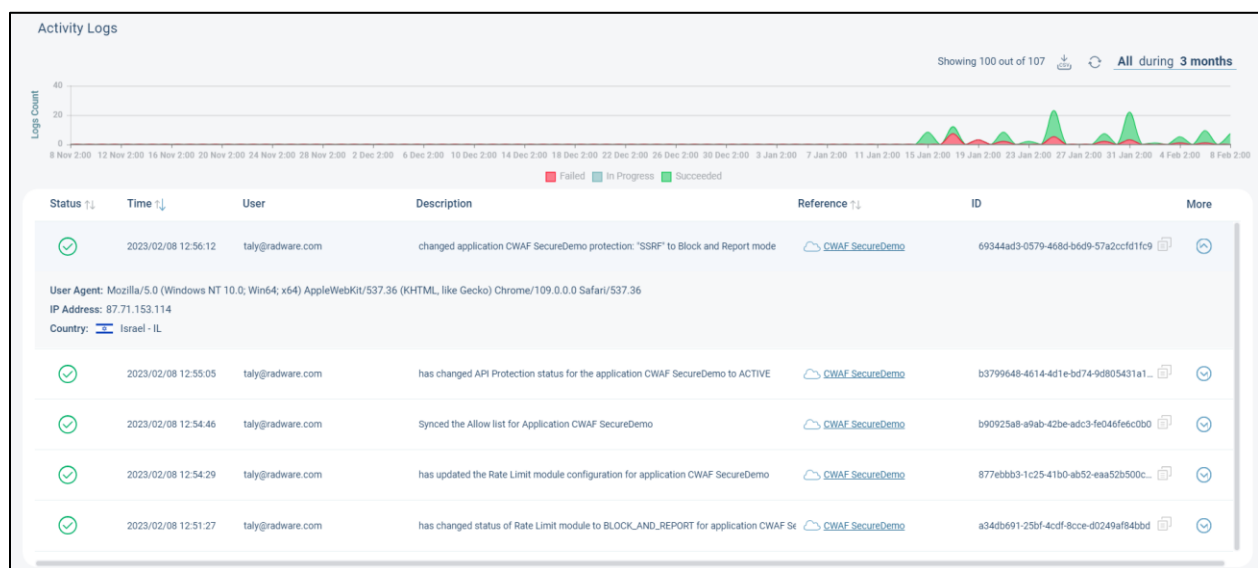
## Activity logs.

### Actions:

1. Go to the Activity logs page by hovering over the person icon on the left side menu and clicking on Activity log.
2. Click on one of the reports to open the expanded view.

### Description:

1. The Activity logs page provides a detailed overview of all actions taken within the service portal.
2. On this page, you can view events with detailed information, including configuration differences in JSON format (although this information may not be available in the current account). This allows for full monitoring of activity within the portal.



©2022 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this press release 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.