



Course Code: 100-102

Cloud Application Security

Training Course

Outline

1 Introduction

Applications are at the core of your business – from sophisticated e-commerce engines to cloud-based productivity solutions and personal tools on mobile phones. Applications are your primary revenue generators, growth and retention engines, and your main customer engagement platform.

Radware's industry-leading WAF, bot management, API protection, and application DDoS protection services are a one-stop-shop for all your application security needs, providing you with state-of-the-art application and API protection (WAAP) that doesn't roadblock business agility and growth.

No matter how many different environments your applications are deployed on, Radware SecurePath™, an innovative API-based cloud architecture, will maintain a consistent, top-grade, comprehensive application security across any cloud with centralized visibility and management.

This document is protected by United States and International copyright laws. Neither this document nor any material contained within it may be duplicated, copied, or reproduced, in whole or part, without the expressed written consent of Radware, Inc.

2 Purpose and Scope

This course, **CloudApplicationSecurity**, is a structured 2-day training.

It consists of a *practical* and a *theoretical* part.

In this course, you will learn how to access and set up the CloudWAAP solution and its features like BOT manager and API protection.

This training begins with an overview of the features and capabilities of Radware's CloudWAAP solution. You will learn how to request a cloud access account. We explain from the initial setup of a new application to setting up the various protection options. We use a penetration testing tool to attack this protected application and observe the security web page that is displayed on the attacker's screen. The CloudWAAP dashboard and Analytics show the admin view. We also cover setting up and configuring alerts and reports.

3 Target Audience and Prerequisites

This course is designed for technicians designing or implementing cloud-based application protection with Radware CloudWAAP. A solid knowledge of how applications are working and network protocols (like TCP, HTTP, HTTPS) is a key asset for setting up protection options.

4 Objectives

- Understand CloudWAAP main capabilities and how they work
- Install and deploy CloudWAAP applications in inline and out of path mode
- Understand how to monitor the CloudWAAP protections

5 Presentations and Hands-On Labs

Day 1:

Presentations:

- Introduction to CloudWAF
- Using CloudWAF
- Cloud WAF Monitoring and Reporting
- Security Management
- Integrated CDN

Hands-On Labs:

- Get Your Cloud Access
- Set Your Password
- Initial CloudWAF Setup
- Create your inline Application
- Enable Blocking On The Application
- Configure Kali To Access Application
- Run Attacks
- Monitoring And Reporting With OWASP-ZAP
- Configure Alerts
- Configure Reports

Day 2:

Presentations:

- API Protection and Discovery
- Introduction to BOT Manager
- BOT Manager in CWAf
- Introduction to SecurePath
- Client Side Protection

Hands-On Labs:

- API Protection
- BOT Protection
- Create a SecurePath application and run attacks on it

6 Certification

This course is the certification course to get recognized as:

Radware Certified Cloud Application Security

To be certified students need to pass a theoretical.

The exam is available from any location, only internet access is required.

The first attempt is included free of charge as part of the course.

Additional attempts require a fee.

For both exams the minimum passing grade is 75%.

6.1 Online Certification Exam

The online exam consists of Multiple-Choice-Questions based on the content presented in the theoretical part and test student's understanding of the solution.

North America
Radware Inc.
575 Corporate Drive, Lobby 1
Mahwah, NJ 07430
Tel: +1-888-234-5763

International
Radware Ltd.
22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: +972 3 766 8666