Security for Cloud Native Applications

The practical guide for securing modern applications using AWS, Azure, and GCP

Eyal Estrin

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55518-903

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

The one and only, my beloved wife:

Diana

About the Author

Eyal Estrin is a cloud security architect working with cloud services since 2015. He has been involved in designing and implementing cloud environments from both the IT and security aspects. He has worked with AWS, Azure, and Google Cloud in many different organizations (in the banking, academia, and healthcare sectors). He has attained several top cloud security certifications – CCSP, CCSK, and AWS. He shares his knowledge about cloud security and adoption through social media (LinkedIn, X, Medium, and more) for the benefit of cloud experts worldwide.

Disclaimer: Opinions are his own and not the views of his employer.

About the Reviewer

Israel Chorzevski is a cybersecurity expert and professional white-hat hacker. With wide-ranging experience as VP of Cybersecurity, CTO, Tech-leader, Trainer, Consultant, Red-team, and Software Engineer, Israel ensures that cybersecurity projects are feasible from business and technology perspectives and communicates with all stakeholders in their language.

Over the past 15 years, Israel has gained expertise with multiple technologies, including cloud-native, web, mobile, client-server applications, and IoT/embedded devices. He has worked with various industries, including tech giants, financial institutions, gaming companies, and intelligence agencies.

He dedicates this book to his wife, who consistently encourages him to move forward.

Acknowledgement

I want to express my deepest gratitude to my family and friends for their unwavering support and encouragement throughout this book's writing, especially my wife, Diana, who pushed me to achieve my dream of becoming an author.

I am also grateful to BPB Publications for their guidance and expertise in bringing this book to fruition. It was an exciting journey revising this book, with the valuable participation and collaboration of reviewers, technical experts, and editors.

I would also like to acknowledge the valuable contributions of my colleagues, co-workers, and especially my technical reviewer, who have taught me so much and provided valuable feedback on my work during many years of working in the tech industry.

Finally, I would like to thank all the readers who have taken an interest in my book and for their support in making it a reality. Your encouragement has been invaluable

Preface

Cloud is an evolution of IT services, allowing organizations to build highly scalable and secure modern applications.

This book is designed to provide a comprehensive guide to building cloud-native applications. It covers various topics, including using APIs, event-driven architectures, containerization, serverless, CI/CD, and the 12-factor application methodology.

Throughout the book, you will learn about the key features of cloud-native applications and how to use them to build secure modern applications on top of AWS, Azure, and GCP infrastructure.

This book is intended for security professionals, software developers, DevOps, cloud architects, and all those designing, maintaining, and securing cloud-native applications.

This book will give you the knowledge and skills to secure cloud-native applications daily. Parte superior do formulárioParte inferior do formulário

Chapter 1: Introduction to Cloud Native Applications - It provides a quick recap of cloud services, an understanding of cloud-native services, and the characteristics of cloud-native applications.

Chapter 2: Securing Modern Design Architectures - It provides a deep understanding of securing modern design architectures from APIs, Event-Driven architectures, and Microservices.

Chapter 3: Containers and Kubernetes for Cloud Native Applications - It provides a deep understanding of securing applications using containers and the Kubernetes platform.

Chapter 4: Serverless for Cloud Native Applications - It explains how Serverless technology can be embedded in cloud-native applications, with recommendations for securing common Serverless technologies from the three major cloud providers.

Chapter 5: Building Secure CI/CD Pipelines - This provides an understanding of the various steps of a CI/CD pipeline and how to embed security controls in each step of the development process.

Chapter 6: The 12-Factor Application Methodology - It provides an understanding of the characteristics of the 12-factor app methodology and how to implement security using containers and Serverless technologies.

Chapter 7: Using Infrastructure as Code - It provides an understanding of IaC for deploying modern infrastructure and explains how to secure common IaC technologies (AWS CloudFormation and HashiCorp Terraform).

Chapter 8: Authorization and Policy as Code - It provides an understanding of Policy as Code and how to implement it as guardrails to enforce settings and implement the authorization decision process.

Chapter 9: Implementing Immutable Infrastructure - It provides a deep understanding of how to implement immutable infrastructure based on the infrastructure of the three major cloud providers.

Chapter 10: Encryption and Secrets Management - It explains how to use key management services and secrets management services to embed encryption and key management as part of cloud-native applications.

Chapter 11: Threat Management in Cloud Native Applications - It provides information on implementing vulnerability management and detecting threats on cloud-native applications at scale.

Chapter 12: Summary and Key Takeaways - It summarizes the topics learned in this book by presenting a sample cloud-native application, how to implement security for this application, and key takeaways from the book.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/pjwnkuq

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Security-for-Cloud-Native-Applications.
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Introduction to Cloud Native Applications

Introduction

This chapter will provide you with a quick recap of cloud services, an understanding of cloud-native services, and the characteristics of cloud-native applications.

Note: In various chapters of the book, we will mention services from AWS, Azure, and GCP and provide best practices for securing those services. The services will be ordered alphabetically according to the cloud providers' names.

Structure

The chapter covers the following topics:

- Recap of cloud services
- Cloud-native services
- Cloud-native applications

Objectives

At the end of this chapter, you will be able to understand the different cloud service models and cloud-native services, and you will be able to recognize cloud-native applications.

Recap of cloud services

Before we dive into cloud-native applications, let us have a short recap of what the cloud service models and how they relate to cloud-native applications.

The **National Institute of Standards and Technology** (**NIST**) provides us with the following definitions:

- **Infrastructure as a Service (IaaS)**

  The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications.

- **Platform as a Service (PaaS)**

  The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

- **Software as a Service (SaaS)**

  The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface.

(*Source*: NIST Special Publication 800-145: **https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf**)

The shared responsibility model is a concept that tries to set the boundaries of responsibility between the **cloud service provider** (**CSP**) and the cloud consumer (or customer) in various topics such as security, availability, and even sustainability. The CSP is responsible for the infrastructure layers from physical data centers to computing, storage, network, and virtualization. When customers choose IaaS, they are responsible for everything within operating systems, such as runtime and application configuration. When customers choose PaaS, they may have the option to select the runtime version and import their code into a managed service environment, depending on the service offered by the CSP. When customers choose SaaS, they only control their data. In all service models, the customers are always responsible for deciding which data to store in the cloud and who has access to their data.

Refer to *Figure 1.1*: