

JUST TELL ME WHAT I NEED TO KNOW...

CLOUD SECURITY

CLEAR ANSWERS. PRACTICAL INSIGHTS.
ESSENTIALS ONLY.



SECURE YOUR
CLOUD
FOUNDATION



IDENTITY & ACCESS
MANAGEMENT



DATA PROTECTION
& PRIVACY



DETECT THREATS.
RESPOND FAST.



COMPLIANCE
& GOVERNANCE

Just Tell Me What I Need To Know

Cloud Security

A Security Architect's Practical Guide

Belshaw Consulting

Copyright Notice

This book is an independent educational work. Any company names, product names, trademarks, service marks, technologies, standards, frameworks, methodologies, or registered trademarks mentioned in this publication are the property of their respective owners. Their inclusion is for identification, educational, and illustrative purposes only and does not imply any affiliation with, endorsement by, or sponsorship from the respective owners.

Technology, products, standards, regulations, certifications, security guidance, and industry best practices evolve over time. Readers should consult current vendor documentation, official standards publications, applicable regulations, and their organization's policies and procedures before implementing any recommendations or making technical, security, or business decisions.

Copyright © 2026 Belshaw Consulting

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, transmitted, or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher, except for brief quotations used in reviews or scholarly works as permitted by applicable copyright law.

Table of Contents

Introduction	5
Part I — Cloud Security Foundations	9
Chapter 1 - Understanding Cloud Computing.....	9
Chapter 2 - Cloud Security Principles.....	18
Chapter 3 - Cloud Architecture	28
Chapter 4 - Identity and Access Management.....	39
Chapter 5 - Protecting Cloud Data	49
Chapter 6 - Cloud Network Security	60
Chapter 7 - Securing Compute Platforms	71
Part II — Building Secure Cloud Applications	82
Chapter 8 - Secure Application Development.....	82
Chapter 9 - DevSecOps.....	92
Part III — Operating Secure Cloud Environments	104
Chapter 10 - Cloud Security Operations	104
Chapter 11 - Cloud Governance.....	142
Chapter 12 - Cloud Risk Management	180
Part IV — Cloud Compliance	223
Chapter 13 - Cloud Compliance Frameworks	223
Chapter 14 - FedRAMP: Traditional and FedRAMP 20x	234
Part V — Cloud Platforms.....	284
Chapter 15 - AWS Security	284
Chapter 16 — Microsoft Azure Security	295
Chapter 17 — Google Cloud Security	311
Part VI — Emerging Technologies	327
Chapter 18 — Artificial Intelligence and Cloud Security.....	327
Part VII — Secure Cloud Architecture	347
Chapter 19 — Designing Secure Cloud Architectures.....	347

APPENDICES	372
Appendix A - Cloud Security Quick Reference	372
Appendix B - Cloud Security Design Checklists	378
Appendix C - Cloud Security Assessment Checklists	384
Appendix D - Cloud Security Interview Questions	391
Appendix E - Cloud Security Tool Reference	402
Appendix F - Cloud Acronyms and Terminology	410
Appendix G - Common Cloud Security Mistakes	417
Appendix H - Quick Reference Guides	423

Introduction

Cloud computing has fundamentally changed the way organizations design, build, secure, and operate information systems. Applications that once lived inside carefully protected data centers now run across multiple cloud providers, containers, serverless platforms, and globally distributed infrastructures. Security professionals are expected to understand not only traditional cybersecurity concepts but also identity, networking, automation, DevSecOps, compliance, governance, and the unique challenges of securing cloud-native technologies.

The problem is that cloud security has become overwhelming.

There are countless books dedicated to Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Kubernetes, Zero Trust, DevSecOps, encryption, identity management, cloud networking, compliance frameworks, and countless security products. Certification guides teach you how to pass an exam. Vendor documentation teaches you how to configure individual services. Academic textbooks often explain the theory in great detail but rarely focus on how everything fits together in the real world.

Most professionals don't need another 800-page technical reference.

They need someone to simply tell them what they need to know.

That is the purpose of this book.

Who This Book Is For

This book is written for professionals who need to understand cloud security from a practical, architectural, and operational perspective.

It is intended for:

- Security Architects
- Cloud Security Engineers
- Cloud Architects
- Cybersecurity Engineers
- DevSecOps Engineers
- System Engineers
- Security Consultants
- Information System Security Officers (ISSOs)
- Project Managers
- Technical Managers
- IT Leaders

- Students entering cloud security

Whether you're designing a secure cloud environment, preparing for a technical interview, participating in an architecture review, leading a migration project, or simply expanding your knowledge, this book is designed to provide the foundation you need.

What This Book Is Not

This is not a certification guide.

Although every major topic found in professional cloud security certifications is covered throughout this book, the goal is not to prepare you for an examination. Instead, the certification bodies are used as a benchmark to ensure that the essential areas of cloud security are addressed.

Likewise, this is not a product manual.

You will not learn every button to click in AWS, Azure, or Google Cloud. Cloud platforms evolve too quickly for any printed book to remain current at that level of detail.

Instead, you will learn the concepts, architectures, security principles, and implementation approaches that remain relevant regardless of which cloud platform you use.

How This Book Is Organized

Cloud security is much more than securing virtual machines or encrypting data.

A modern cloud security professional must understand:

- Cloud architecture
- Identity and access management
- Data protection
- Network security
- Compute security
- Application security
- DevSecOps
- Cloud operations
- Monitoring and incident response
- Governance
- Risk management
- Compliance
- Artificial intelligence
- Multi-cloud environments

- Enterprise security architecture

Rather than organizing these topics around certification domains, this book follows the natural lifecycle of designing, implementing, operating, and governing secure cloud environments.

Each chapter builds upon the previous one, gradually moving from foundational concepts to enterprise architecture, operational security, and modern cloud security practices.

A Practical Approach

Throughout this book, you'll notice that the emphasis is on understanding rather than memorization.

Instead of simply defining terminology, you'll learn:

- Why technologies exist
- When they should be used
- Their strengths and weaknesses
- Common implementation approaches
- Architectural trade-offs
- Frequent design mistakes
- Real-world best practices

Where appropriate, examples from AWS, Microsoft Azure, and Google Cloud Platform are used to illustrate concepts. The focus, however, is on vendor-neutral principles that apply across modern cloud environments.

How to Use This Book

You do not need to read this book cover to cover.

If you're new to cloud security, begin with the early chapters to establish a solid foundation before progressing to more advanced topics.

If you're already working in cloud security, feel free to jump directly to the chapters most relevant to your current responsibilities.

Many readers will use this book as a desktop reference—returning to it whenever they need a refresher on a technology, security concept, or architectural decision.

That is exactly how it was designed to be used.

One Final Thought

Technology will continue to evolve.

New cloud services will appear. Security products will change. Artificial intelligence will reshape how we design and defend cloud environments. New compliance requirements and regulatory frameworks will emerge.

The underlying principles of sound security architecture, however, change far more slowly.

If you understand those principles—and know how to apply them in modern cloud environments—you'll be well equipped to design, secure, and operate cloud systems regardless of what technologies come next.

That's what this book is intended to help you do.

Welcome to Just Tell Me What I Need To Know... Cloud Security.

CLOUD SECURITY IS NO LONGER OPTIONAL— IT'S A CORE SKILL FOR EVERY IT AND CYBERSECURITY PROFESSIONAL.

Whether you're moving workloads to the cloud, designing secure architectures, managing compliance, or preparing for your next certification or job interview, you need practical knowledge you can apply immediately. This book delivers exactly that.

Just Tell Me What I Need to Know - Cloud Security cuts through the buzzwords and marketing hype to explain the technologies, principles, and best practices that matter most. Written in a clear, vendor-neutral style, it provides a solid understanding of how to secure modern cloud environments across public, private, hybrid, and multi-cloud platforms.



INSIDE YOU'LL LEARN ABOUT:

- ✓ Cloud architecture and the shared responsibility model
- ✓ Identity and access management (IAM)
- ✓ Cloud networking and secure connectivity
- ✓ Data protection, encryption, and key management
- ✓ Containers, Kubernetes, and serverless security
- ✓ Cloud-native security services and monitoring
- ✓ Zero Trust principles for cloud environments
- ✓ DevSecOps and secure software delivery
- ✓ Compliance, governance, and risk management
- ✓ Incident response, disaster recovery, and business continuity



Whether you're an engineer, architect, system administrator, manager, student, or cybersecurity professional, this book gives you the knowledge you need—without hundreds of pages of unnecessary theory.



PRACTICAL.
REAL-WORLD
SOLUTIONS.



SECURE.
PROTECT WHAT
MATTERS.



SCALABLE.
BUILT FOR THE
CLOUD ERA.



MONITOR.
DETECT AND
RESPOND FAST.



COMPLIANT.
MEET STANDARDS.
REDUCE RISK.



**LESS FLUFF.
MORE PRACTICAL KNOWLEDGE.
JUST TELL ME WHAT I NEED TO KNOW.**