

Table of Contents

- About the Authors..... ix**
- About the Technical Reviewer xi**
- Acknowledgments..... xiii**
- Introductionxv**

- Part I: Zero Trust Cloud Security..... 1**

- Chapter 1: Reduce Cyber Security Vulnerabilities: Identity Layer 3**
 - Azure Cloud Relations: Tenant, Subscription, Resources 4
 - Azure Tenant Security..... 4
 - Azure Subscription Security 5
 - Azure API Security 6
 - Azure Resource Locks 7
 - Managing Azure Active Directory: Users and Groups 8
 - Azure Users 8
 - Azure Groups 9
 - Azure Active Directory: OAuth, SAML, AD Connect 13
 - OAuth..... 13
 - SAML 14
 - AD Connect..... 16
 - Security Measures 18
 - Azure Application Permission Scopes 19
 - Configure Multi-Factor Authentication 21
 - Conditional Access Policies 24
 - Azure AD Privileged Identity Management..... 28
 - Summary..... 35

TABLE OF CONTENTS

- Chapter 2: Azure Network Security Configuration..... 37**
 - Virtual Network Overview 38
 - VNets 43
 - Network Security Group 52
 - VNet Security Best Practices 55
 - Network Peering 57
 - Application Security Groups 60
 - TCP/IP Port Vulnerability 65
 - Azure Front Door Service 66
 - Remote Access Management 74
 - Azure Bastion Host 79
 - Summary 81
- Chapter 3: Reduce Cyber Security Vulnerabilities: IaaS and Data..... 83**
 - Azure Security with IaC..... 84
 - ARM Development 85
 - Harden Azure VMs 90
 - Patching the VM Directly 94
 - VM Security and Endpoint Protection..... 95
 - Database Security..... 97
 - DB Best Practices 99
 - DB Authentication 100
 - Database Auditing 101
 - Storage Accounts 102
 - Shared Access Signatures 105
 - Key Management..... 107
 - Summary..... 108

Part II: Azure Cloud Security Operations	109
Chapter 4: Configure Azure Monitoring for Blue Team Hunting.....	111
Azure Data Platform	113
Azure Logs.....	116
Azure Metrics	118
Azure Monitor and Log Analytics Enablement.....	119
Log Analytics Workspace Security Strategy	125
Guest OS Metrics and Logs.....	130
Connecting Data Sources to Log Analytics Workspace	136
Summary.....	151
Chapter 5: Azure Security Center and Azure Sentinel	153
Cloud Security Challenges	154
Enable Security	156
Configuration Value	160
Standard Tier Advantages.....	161
Just-in-Time Access.....	162
Advanced Threat Detection.....	162
Anomaly Detection	163
Crash Analysis	164
Threat Intelligence.....	164
Behavioral Analysis	164
Configure Alerting	165
Using Security Center	166
Compute and Apps	168
Network.....	169
Data and Storage.....	170
Azure Sentinel.....	173
Connect to Data Streams.....	179

TABLE OF CONTENTS

- Using Azure Sentinel 186
 - Logs Pane 187
 - Analytics Pane 189
 - Hunting 194
- Summary..... 196
- Chapter 6: Azure Kubernetes Services: Container Security 197**
 - Microservices..... 198
 - Containers, Docker, and Kubernetes 200
 - Azure Kubernetes Services and Security..... 204
 - Authentication 213
 - Container Security 214
 - AKS Security with Security Center and Sentinel..... 217
 - Kubernetes Security with Azure Policy 221
 - Summary..... 226
- Chapter 7: Security Governance Operations 227**
 - Azure Governance Architecture..... 228
 - Management Groups 230
 - Azure Policy 234
 - Compliance Reporting 239
 - Assignments 240
 - Blueprints 244
 - Role-Based Access Control 249
 - Azure Cost Management 251
 - Data Governance..... 257
 - Classification 257
 - Data Retention 268
 - Summary..... 272
- Index..... 273**

Introduction

The first edition of this book in 2017 placed cyber security front and center to teams of IT professionals who may not have focused on cyber security. This second edition is completely rewritten and updated, with more than 70% of the book containing brand-new Azure cloud security topics. Business relies more on subject matter experts (SME), the professional resources, as they continue to secure applications and data in the cloud. This second edition goes deeper on Azure security features that did not exist a few years ago. This publication is an ambitious resource to provide readers a strong foundation to learn and deploy Azure security best practices.

This book comes from several years of lessons learned and late nights of trying to understand the what, how, and why. Having worked with several customers and organizations moving to cloud-focused technologies, this book will aid in choosing the right path for planning and moving forward with a cloud strategy. It will also empower organizations to start taking their first steps toward cloud adoption, cloud migration, and creating governance around an ever-changing technology and toolset.

This book was written for the following types of IT/cloud professionals:

- IT subject-matter experts (SMEs)
- IT professionals looking to expand their knowledge of cloud technologies
- Cyber security teams

This second edition does not repeat guidance to review current cyber security reports; that should now be part of your security practice. You expand beyond Azure Security Center and learn to use new and updated Azure native security services like Azure Sentinel, Privileged Identity Management, Azure Firewalls, and SQL Advanced Threat Protection and how best to protect Azure Kubernetes Services. Open this book and begin the deep dive into Microsoft Azure Security.

Introduction

The first edition of this book in 2017 placed cyber security front and center to teams of IT professionals who may not have focused on cyber security. This second edition is completely rewritten and updated, with more than 70% of the book containing brand-new Azure cloud security topics. Business relies more on subject matter experts (SME), the professional resources, as they continue to secure applications and data in the cloud. This second edition goes deeper on Azure security features that did not exist a few years ago. This publication is an ambitious resource to provide readers a strong foundation to learn and deploy Azure security best practices.

This book comes from several years of lessons learned and late nights of trying to understand the what, how, and why. Having worked with several customers and organizations moving to cloud-focused technologies, this book will aid in choosing the right path for planning and moving forward with a cloud strategy. It will also empower organizations to start taking their first steps toward cloud adoption, cloud migration, and creating governance around an ever-changing technology and toolset.

This book was written for the following types of IT/cloud professionals:

- IT subject-matter experts (SMEs)
- IT professionals looking to expand their knowledge of cloud technologies
- Cyber security teams

This second edition does not repeat guidance to review current cyber security reports; that should now be part of your security practice. You expand beyond Azure Security Center and learn to use new and updated Azure native security services like Azure Sentinel, Privileged Identity Management, Azure Firewalls, and SQL Advanced Threat Protection and how best to protect Azure Kubernetes Services. Open this book and begin the deep dive into Microsoft Azure Security.