Table of Contents

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.