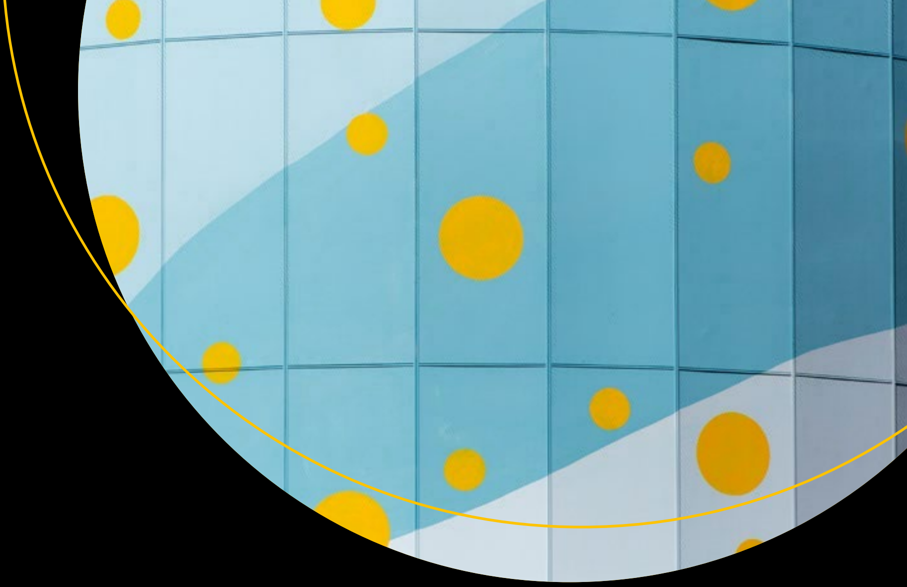

Azure Security Handbook

A Comprehensive Guide for Defending Your Enterprise Environment

Karl Ots

Apress®

Azure Security Handbook

A Comprehensive Guide for Defending Your Enterprise Environment

Karl Ots

Apress®

Azure Security Handbook: A Comprehensive Guide for Defending Your Enterprise Environment

Karl Ots
Zürich, Zürich, Switzerland

ISBN-13 (pbk): 978-1-4842-7291-6 ISBN-13 (electronic): 978-1-4842-7292-3
https://doi.org/10.1007/978-1-4842-7292-3

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Joan Murray
Development Editor: Laura Berendson
Coordinating Editor: Jill Balzano

Cover photo courtesy of Gratisography

Distributed to the book trade worldwide by Springer Science+Business Media LLC, 1 New York Plaza, Suite 4600, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484272916. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

For my wife Annie.

Table of Contents

About the Author

Karl Ots is a cloud and cybersecurity leader with a decade of experience in Microsoft Azure security with large enterprises in fields such as technology, manufacturing, and finance. Karl is recognized as the global top technology visionary with the Microsoft Regional Director award. He is a patented inventor, a LinkedIn Learning instructor, and a Microsoft Azure MVP. He holds the Azure Security Engineer, SABSA Foundation SCF, and CISSP certifications.

Karl is a frequent speaker on cloud security topics at global conferences such as Microsoft Ignite or (ISC)^2 Security Congress. In his current role, he serves as Head of Cloud Security at EPAM Systems, a global engineering and consulting company. He hosts the Cloud Gossip podcast.

About the Technical Reviewer

As a Microsoft Technical Evangelist/Cloud Solutions Architect, **Mike Martin** is an Azure go-to for ISVs (independent software vendors). He's been active in the IT industry for more than 20 years and has performed work in almost all types of job profiles, going from coaching and leading a team to architecting and systems design and training. Today, he's primarily into the Microsoft Cloud Platform and Application Life cycle Management/DevOps, with an emphasis on security domains. He's not a stranger to both Dev and IT Pro topics; they even call him the perfect hybrid solution.

In January 2012, he became a crew member of AZUG, the Belgian Microsoft Azure User Group. As an active member, he's both involved in giving presentations and organizing events (like ITProceed, Techorama, and Global Azure Bootcamp, a.k.a. GAB). Mike was also a Microsoft Azure MVP (awarded five times since 2013, receiving his fifth in July 2017!) and Microsoft Azure Advisor.

Helping out in the community and introducing new and young people to the world of Microsoft and technology is also one of his passions.

Acknowledgments

There is never a perfect time to write a book. Yet, I found it oddly calming to write this book during one of the largest turmoils of my lifetime.

I want to thank my awesome wife Annie for giving me the motivation to always reach for the next level in my professional and personal endeavors.

I want to thank Jill and Joan from Apress for keeping me accountable yet giving me the time I needed to find my voice. I also want to thank Mike and Pablo from Microsoft for their efforts on making this book better.

I want to thank my colleagues, customers, and partners I have had the pleasure of working, failing, and learning alongside with.

Finally, I want to thank the grumpy old geezers at the chat group for never resisting a good pun.

Foreword

At Microsoft, we invest more than a billion dollars each year in research and development to help our customers secure their organizations' digital transformations. For us and many other technology providers, this is one of the fastest-growing technology areas. And while in the IT industry, we usually associate growth as something positive, the case of cloud security is bittersweet. On the one hand, implementing a secure cloud or hybrid footprint is a fundamental best practice. But this fast growth is fueled largely by the need to respond to, and to be one step ahead of, the growing number of malicious actors, including many private-sector offensive actors that are helping democratize cyber threats with their new hacking-as-a-service model.

Then, the COVID 19 pandemic drove a once-in-a-lifetime acceleration in cloud adoption and digital transformation. In the last sixteen months, companies worldwide and their security teams faced new challenges in their effort to support remote and hybrid-work scenarios, all in a short window of time. These unprecedented circumstances demanded a fast response from us at Microsoft. In my role leading community programs for Azure security engineering groups and bringing the voice of our customers into our engineering roadmaps, I saw first-hand an increase in feedback and insights coming from our customers and partners. In response, we are driving a fast evolution of our Azure security services and controls embedded in many Azure components and workloads. As a result, the list of security changes across Azure services and workloads over the last year is vast.

But in parallel to technical evolution, companies face the challenge of quickly upskilling their security teams. As a direct consequence, the need for cloud security experts in all cloud areas—identity and access control, data, applications, infrastructure, and the edge—is in high demand. Our technical libraries and training at `https://docs.microsoft.com` play an essential part in this effort. My colleagues in CxE also sustain a very active calendar of Azure security webinars that help educate security professionals on the latest releases in our services. You can check them out at `https://aka.ms/SecurityCommunity`. But even with all these investments in technical readiness, we can only cover so much ground.

This is where members of the security community bring their passion for sharing knowledge with others to play. Their contributions to our technical information complement and strengthen security knowledge in Azure. Further, their contributions often add different perspectives, insights, and scenarios to those covered in our Microsoft documentation.

As both a member of our Microsoft Regional Director[1] program and our Azure Private Security Community, where he represents Swiss Re as Vice President, Cloud Security Architecture, Karl Ots has a long history of sharing valuable feedback and insights with our security engineers. The combination of community leadership and private sector responsibilities experiences gives Karl a deep understanding of cloud security and the steps that companies should take when planning and implementing security for the cloud and multi-cloud with Azure.

In his book, Karl offers much-needed guidance to help organizations that are new to Azure, or cloud security in general, in planning the security architecture for their new cloud footprint. He also provides plenty of best practices and configuration decisions that together help decrease their attack surface by explaining how to take advantage of our Azure security services and native controls and integrate our solutions and centralize security operations in Azure. Additionally, Karl shares cloud and security agnostic recommendations that go beyond user guides, sharing lessons from his vast first hand experiences. And he maps many of our Azure controls and best practices to industry security benchmarks like those from CIS and NIST and security models like Zero Trust and Shift-Left.

I appreciate that his chapters guide you through key security domains and how to secure them in Azure. From identity and access management and their fundamental role in cloud security to protecting your cloud infrastructure and workloads, he touches on security basics and configurations without shying from pointing out where integration with 3rd party providers will help with specific needs.

Through this approach, Karl also brings several conversations that, while often overlooked, are fundamental when managing security operations in the cloud. For example, decisions such as the retention time for logs used for your security monitoring and analysis can have on your company's bill and the cloud shared responsibilities matrix[2], which showcases some of the benefits of moving to the cloud and highlights the importance of defining clear roles and responsibilities that may include workload

[1] https://rd.microsoft.com/

[2] https://docs.microsoft.com/azure/security/fundamentals/shared-responsibility

owners who had little or no security ownership over on-premises implementations. Karl provides complete perspectives and hence brings clarity to architecting security in Azure.

In closing his book brings perspective to readers of all levels of expertise with security in Azure. After more than three years working in Cloud Security and learning the intimacies of our Azure security services, it has even taught me several technical and non-technical considerations of planning a move to the cloud.

I want to thank you for this book Karl. You and many others in the security community play a crucial role in communicating the benefits that our Microsoft products and services offer our customers, adding your valuable expertise. Thank you for representing the voice of our customers and for influencing the future of our Azure security services and native controls.

Pablo Chacón

Sr. Program Manager – Private Security Communities Lead
Customer Experience Engineering (CxE), Cloud Security
Microsoft

July 2021

Introduction

You are about to enter the world of cloud security and learn from the mistakes I have made when working with hundreds of Azure projects with some of the largest organizations in the world.

This is the book I wish I had on hand when I started my cloud journey. It does not cover every single knob and control for every Azure service there is. That would be overwhelming. Instead, it covers the core pillars of cloud security with a reasonable sampling of pragmatically selected Azure services.

You might be a seasoned security professional taking your first steps into the public cloud world. Or you might be a cloud-native solution architect looking at securing your applications. I hope both of you will learn about each other's mindset by reading this book and the two worlds would not be as disconnected as they still are.

I wrote this book hoping that it would keep being valuable to you over the course of your Azure projects. On the first read-through, you might struggle to unlearn some existing habits and mental models. After embracing the cloud-native security mindset, I hope that you will keep returning to this book throughout your Azure adoption life cycle.

The first half of this book, Chapters 1-4 covers the core pillars of cloud security framework development. If you are looking at the Azure cloud through the central organization's looking glass, you will find this part the most familiar to you.

The second half of the book, Chapters 5-8 covers security controls for the most archetypical workloads. If you are a cloud solution builder, you will find this part of the book to your liking.