LEARNING MADE EASY

Netskope
Special Edition

Securing Generative AI

for dummies®
A Wiley Brand

Enable responsible use of generative AI

Discover the risks and debunk the myths of generative AI

Create a secure strategy for your data

Brought to you by

netskope

Carmine Clementelli
Krishna Narayanaswamy

About Netskope

Netskope, a global SASE leader, helps organizations apply Zero Trust principles and AI/ML innovations to protect data and defend against cyber threats. The Netskope One platform provides optimized access and real-time security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.

We would like to thank a number of individuals who, along with the authors, made this book possible:

From Netskope: Chad Berndtson, Catie Halliday, Atul Malik, Elena Matchey, Naveen Palavalli, Stephenie Pang, Bruno Raimondo, Neil Thacker

From Evolved Media: David Penick, Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Securing Generative AI

Netskope Special Edition

by Carmine Clementelli and Krishna Narayanaswamy

for dummies®
A Wiley Brand

Securing Generative AI For Dummies®, Netskope Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-26422-3 (pbk); ISBN 978-1-394-26423-0 (ebk); 978-1-394-28354-5 (epub)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Client Account Manager: Jeremith Coward

Production Editor: Saikarthick Kumarasamy

Special Help: Nicole Sholly

Introduction

Generative artificial intelligence (GenAI) exploded into the mainstream in late 2022. Since then, it has begun to transform (or promises to transform) many aspects of how businesses operate. Tools like ChatGPT and Google Gemini are more than just novel technologies — they've instigated a seismic shift in how data is managed and secured. It's estimated that at least one in four corporate employees interacts with a GenAI tool daily, mostly unseen and undetected by employers and security personnel. That's a concern because GenAI has a voracious appetite for your data, consuming the most mundane and the most sensitive data with equally aggressive greed.

GenAI has been around for years, to say nothing of the much bigger category of AI itself. But because of its mushrooming popularity, we now face a new, complex, and unexpected set of data security challenges. As these GenAI tools offer to enhance efficiency and drive innovation, they're also blurring the traditional lines of data protection and sending sensitive information beyond the safe confines of company networks into an expansive digital realm, where they may reemerge anywhere and in anyone's hands.

Effectively managing data security amidst the proliferation of GenAI is not just about risk mitigation; it's a strategic imperative. When approached correctly, effective data security enables businesses to leverage GenAI for competitive advantage. Conversely, neglecting the need for data security related to GenAI use can lead to catastrophic consequences for your business.

About This Book

This book equips your organization with the knowledge to balance the innovative potential of GenAI tools like ChatGPT and Google Gemini with robust data security practices. We emphasize the importance of understanding the unique risks posed by GenAI and advocate for advanced data loss prevention (DLP) strategies, regular risk assessments, and the integration of modern cybersecurity tools. We also underscore the necessity of cultivating a culture of responsible AI usage among employees. This book is a vital resource for navigating the complexities of data security in a landscape transformed by GenAI. It provides actionable insights for organizations to protect their data while embracing important advancements in technology and business workflows.

Foolish Assumptions

This book assumes a few things about you:

- You have basic experience and familiarity with public GenAI applications like ChatGPT or Google Gemini.
- You're familiar with cloud-based apps and their significance in enhancing a business's productivity.
- You understand the need to secure interactions with such tools, especially given the remote and mobile workforce environment.
- You're driven to enable your organization to leverage the potential of GenAI while ensuring that sensitive data is never compromised.

Icons Used in This Book

We use icons to call attention to important information.

TIP

Anything marked with the Tip icon is a shortcut to simplify a specific task.

REMEMBER

The Remember icon flags facts that are especially important to remember.

WARNING

Heed anything marked with the Warning icon to save yourself some headaches.

Beyond the Book

This book is full of detailed information, but GenAI and security are evolving rapidly. If you find yourself at the end of this book wondering, "Where can I learn more?," just go to `www.netskope.com`.