Table of Contents

CHAPTER 1

Introduction

Enterprise security is hard. This is due to the complexity of IT and application infrastructures, the breadth and velocity of user access, and of course the inherently adversarial nature of information security. It's also due to the far-too-open nature of most enterprise networks—by not enforcing the principle of least privilege at both the network and application levels, organizations are leaving themselves incredibly vulnerable to attacks. This is true both for internal networks and for public Internet-facing remote access services such as Virtual Private Networks (VPNs), the latter of which are exposed to every adversary on the Internet. Given today's threat landscape, you'd never choose to design a system like this. And yet, traditional security and networking systems, which remain in widespread use, continue to perpetuate this model.

Zero Trust security, the subject of this book, changes this and brings a modern approach to security which enforces the principle of least privilege for networks and applications. Unauthorized users and systems will have no access whatsoever to any enterprise resources, and authorized users will only have the minimum access necessary. The result is that enterprises are safer, more secure, and more resilient. Zero Trust also brings improvements in efficiency and effectiveness, through the automated enforcement of dynamic and identity-centric access policies.

Please note that the "zero" in Zero Trust is a bit of a misnomer—it's not about literally "zero" trust, but about zero *inherent* or *implicit* trust. Zero Trust is about carefully building a foundation of trust, and growing that trust to ultimately permit an appropriate level of access at the right time. It could perhaps have been called "earned trust" or "adaptive trust" or "zero implicit trust," and these would have suited the movement better, but "Zero Trust" has more sizzle, and it stuck. Don't take the "zero" literally, please!

Zero Trust is an important and highly visible trend in the information security industry, and while it's become a marketing buzzword, we believe there's real substance and value behind it. At its heart, Zero Trust is a philosophy and an approach, and a set of guiding principles. This means that there are as many ways to interpret Zero Trust as there are enterprises. However, there are fundamental and universal principles that

J. Garbis and J. W. Chapman, *Zero Trust Security*, https://doi.org/10.1007/978-1-4842-6702-8_1

every Zero Trust architecture will follow. Throughout this book, we'll be providing guidelines and recommendations for Zero Trust based on our experiences working with enterprises of different sizes and maturities throughout their Zero Trust journeys. Keep in mind, we use the word *journey* deliberately; this is to underscore the fact this is not a one-and-done project, but an ongoing and evolving initiative. And this is why we wrote this book—to share our thoughts and recommendations around how to best approach Zero Trust in your environment, and to be a guide along your journey.

We fundamentally believe that Zero Trust is a better and more effective way to approach and achieve enterprise security. In some ways, Zero Trust has been closely associated with network security, and while networks are a core element of Zero Trust, we're also going to be exploring the full breadth of Zero Trust security, which crosses boundaries into applications, data, identities, operations, and policies.

As a security leader, you have a responsibility to push, pull, and prod your organization into adopting this new approach, which will improve your organization's resiliency, and also help you grow professionally. This book—your guide—is divided into three parts. Part I provides an introduction to Zero Trust principles, and establishes the framework and vocabulary we'll be using to define Zero Trust and align IT and security infrastructure. These are the foundations of what we believe is required to tell the full Zero Trust story.

Part II is a deep dive into IT and security technologies, and their relationship to Zero Trust. This is where you'll begin to see how your organization can start using Zero Trust, and where you can adapt and integrate your current IT and security infrastructure into a more modern architecture. Because Zero Trust takes an identity-centric approach to security, we'll be examining how different technologies can start to incorporate and benefit from identity context to become more effective.

Part III brings everything together, building on where the first two parts of the book provided a conceptual foundation and a deep technology discussion. This part explores what a Zero Trust policy model should look like, examines specific Zero Trust scenarios (use cases), and finally discusses a strategic and tactical approach to making Zero Trust successful.

Also, it's important to note that we're deliberately not evaluating vendors or vendor products within the scope of this book. Our industry moves too quickly—the pace of innovation is high—and any such reviews would have a very short shelf life. Instead, we're focusing on exploring architectural principles from which you can draw requirements and which you can use to evaluate vendors, platforms, solution providers, and approaches.

By the time you reach the end of this book, it should be clear that there is no single right approach to Zero Trust. Security leaders will need to take into consideration existing infrastructures, priorities, staff skills, budgets, and timelines while designing their Zero Trust initiative. This may make Zero Trust seem complicated, but its breadth of scope actually helps simplify enterprise security and architecture. As an overlay security and access model, it normalizes things and gives you a centralized way to define and enforce access policies across a distributed and heterogeneous infrastructure.

Ultimately, the goal of this book is to provide you with a solid understanding of what Zero Trust is, and the knowledge to successfully steer your organization's unique journey to Zero Trust. If you come away with this, we've been successful in our efforts. Let's get started on our voyage.