

Table of Contents

About the Authors	xiii
About the Technical Reviewer	xv
Acknowledgments	xvii
Foreword	xix
Part I: Overview	1
Chapter 1: Introduction	3
Chapter 2: What Is Zero Trust?	7
History and Evolution	7
Forrester's Zero Trust eXtended (ZTX) Model	9
Gartner's Approach to Zero Trust	12
Our Perspective on Zero Trust.....	13
Core Principles	13
Expanded Principles	15
A Working Definition	16
Zero Trust Platform Requirements	17
Summary.....	18
Chapter 3: Zero Trust Architectures	19
A Representative Enterprise Architecture	20
Identity and Access Management	22
Network Infrastructure (Firewalls, DNS, Load Balancers).....	22
Jump Boxes	23
Privileged Access Management	23
Network Access Control	24

TABLE OF CONTENTS

Intrusion Detection/Intrusion Prevention	24
Virtual Private Network.....	25
Next-Generation Firewalls	25
Security Information and Event Management	26
Web Server and Web Application Firewall	26
Infrastructure as a Service	27
Software as a Service and Cloud Access Security Brokers.....	28
A Zero Trust Architecture.....	28
The NIST Zero Trust Model.....	29
A Conceptual Zero Trust Architecture	30
Zero Trust Deployment Models.....	39
Resource-Based Deployment Model	39
Enclave-Based Deployment Model	43
Cloud-Routed Deployment Model.....	45
Microsegmentation Deployment Model.....	48
Summary.....	51
Chapter 4: Zero Trust in Practice	53
Google's BeyondCorp	53
PagerDuty's Zero Trust Network.....	58
The Software-Defined Perimeter and Zero Trust.....	60
Mutual TLS Communications.....	61
Single-Packet Authorization	61
SDP Case Study.....	63
Zero Trust and Your Enterprise	66
Summary.....	67
Part II: Zero Trust and Enterprise Architecture Components	69
Chapter 5: Identity and Access Management.....	71
IAM in Review	72
Identity Stores (Directories).....	72
Identity Lifecycle	75

TABLE OF CONTENTS

Access Management 78

Authorization 82

Zero Trust and IAM 85

 Authentication, Authorization, and Zero Trust Integration..... 85

 Enhancing Legacy System Authentication..... 87

 Zero Trust as Catalyst for Improving IAM..... 89

Summary..... 90

Chapter 6: Network Infrastructure 93

 Network Firewalls 94

 The Domain Name System..... 96

 Public DNS Servers..... 96

 Private DNS Servers 96

 Monitoring DNS for Security..... 98

 Wide Area Networks..... 99

 Load Balancers, Application Delivery Controllers, and API Gateways 101

 Web Application Firewalls..... 102

 Summary..... 103

Chapter 7: Network Access Control..... 105

 Introduction to Network Access Control..... 105

 Zero Trust and Network Access Control 108

 Unmanaged Guest Network Access..... 109

 Managed Guest Network Access 110

 Managed vs. Unmanaged Guest Networks: A Debate 110

 Employee BYOD 112

 Device Posture Checks..... 113

 Device Discovery and Access Controls..... 115

 Summary..... 116

TABLE OF CONTENTS

Chapter 8: Intrusion Detection and Prevention Systems	117
Types of IDPS	118
Host-Based Systems	119
Network-Based Systems	120
Network Traffic Analysis and Encryption.....	121
Zero Trust and IDPS.....	122
Summary.....	126
Chapter 9: Virtual Private Networks	127
Enterprise VPNs and Security	129
Zero Trust and VPNs	131
Summary.....	133
Chapter 10: Next-Generation Firewalls	135
History and Evolution	135
Zero Trust and NGFWs.....	136
Network Traffic Encryption: Implications.....	137
Network Architectures	139
Summary.....	141
Chapter 11: Security Operations	143
Security Information and Event Management.....	144
Security Orchestration, Automation, and Response.....	145
Zero Trust in the Security Operations Center	146
Enriched Log Data	146
Orchestration and Automation (Triggers and Events)	147
Summary.....	153
Chapter 12: Privileged Access Management	155
Password Vaulting.....	155
Secrets Management.....	156
Privileged Session Management.....	157
Zero Trust and PAM	159
Summary.....	161

Chapter 13: Data Protection 163

- Data Types and Data Classification 163
- Data Lifecycle 165
 - Data Creation..... 165
 - Data Usage 166
 - Data Destruction..... 168
- Data Security 168
- Zero Trust and Data..... 170
- Summary..... 172

Chapter 14: Infrastructure and Platform as a Service..... 173

- Definitions..... 174
- Zero Trust and Cloud Services 175
- Service Meshes..... 180
- Summary..... 183

Chapter 15: Software as a Service 185

- SaaS and Cloud Security..... 186
 - Native SaaS Controls 186
 - Secure Web Gateways 187
 - Cloud Access Security Brokers..... 188
- Zero Trust and SaaS 189
 - Zero Trust and Edge Services 189
- Summary..... 190

Chapter 16: IoT Devices and “Things” 193

- IoT Device Networking and Security Challenges 195
- Zero Trust and IoT Devices 198
- Summary..... 206

TABLE OF CONTENTS

Part III: Putting It All Together	209
Chapter 17: A Zero Trust Policy Model.....	211
Policy Components.....	212
Subject Criteria.....	213
Action	213
Target.....	216
Condition	219
Subject Criteria vs. Conditions	222
Example Policies	223
Policies, Applied.....	226
Attributes.....	226
Policy Scenarios	229
Policy Evaluation and Enforcement Flows.....	233
Summary.....	237
Chapter 18: Zero Trust Scenarios	239
VPN Replacement/VPN Alternative.....	239
Considerations.....	241
Recommendations.....	244
Third-Party Access.....	244
Considerations.....	246
Recommendations.....	247
Cloud Migration.....	248
Migration Categories	248
Considerations.....	250
Recommendations.....	251
Service-to-Service Access.....	252
Considerations.....	254
Recommendations.....	255

TABLE OF CONTENTS

DevOps..... 256

 DevOps Phases..... 257

 Considerations..... 258

 Recommendations..... 259

Mergers and Acquisitions 259

 Considerations..... 260

 Recommendations..... 260

 Divestiture 261

Full Zero Trust Network/Network Transformation 262

 Considerations..... 264

 Recommendations..... 264

Summary..... 265

Chapter 19: Making Zero Trust Successful..... 267

 Zero Trust: A Strategic Approach (Top-Down)..... 268

 Governance Board 269

 Architecture Review Board 269

 Change Management Board 270

 Value Drivers 270

 Zero Trust: A Tactical Approach (Bottom-Up)..... 272

 Sample Zero Trust Deployments 273

 Scenario 1: A Tactical Zero Trust Project..... 274

 Scenario 2: A Strategic Zero Trust Initiative..... 278

 Common Roadblocks 280

 Identity Management Immaturity 281

 Political Resistance 281

 Regulatory or Compliance Constraints 282

 Discovery and Visibility of Resources 282

 Analysis Paralysis..... 283

 Summary..... 284

TABLE OF CONTENTS

Chapter 20: Conclusion	285
Chapter 21: Afterword	287
Plan, Plan, Then Plan Some More	287
Zero Trust Is (Unfortunately) Political	288
Dream Big, Start Small.....	288
Show Me the Money	288
Digital Transformation Is Your Friend	288
Appendix A: Further Reading: An Annotated List	289
Industry Standards and Specifications	289
Books	290
Research Documents and Publications.....	291
Index	293

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

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.