Zero Trust Security

An Enterprise Guide

Jason Garbis
Jerry W. Chapman

Apress®

Zero Trust Security

An Enterprise Guide

Jason Garbis
Jerry W. Chapman

Apress®

Zero Trust Security: An Enterprise Guide

Jason Garbis
Boston, MA, USA

Jerry W. Chapman
Atlanta, GA, USA

ISBN-13 (pbk): 978-1-4842-6701-1
ISBN-13 (electronic): 978-1-4842-6702-8
https://doi.org/10.1007/978-1-4842-6702-8

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Pixabay

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, 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/9781484267011. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

For Amy, Shira, and Shelly
—J.G.

For my beautiful and loving wife, Suzette—Thank you!
To our cherished daughters, Nena and Alex—You are loved!
—J.W.C.

Table of Contents

About the Authors

Jason Garbis is Senior Vice President of Products at Appgate, a leading provider of Zero Trust secure access solutions. At Appgate, he's responsible for the company's security product strategy and product management. He has over 30 years of product management, engineering, and consulting experience at security and technology firms. He's also Co-chair of the SDP Zero Trust Working Group at the Cloud Security Alliance, leading research and publication initiatives. Jason holds a CISSP certification, a BS in computer science from Cornell University, and an MBA from Northeastern University.

Jerry W. Chapman is Engineering Fellow, Identity Management, at Optiv Security. With over 25 years of industry experience, Jerry has successfully guided numerous clients in the design and implementation of their enterprise IAM strategies, in ways that align with both security and business objectives. His job roles have spanned enterprise architecture, solution engineering, and software architecture and development. As an IAM industry expert, Jerry provides guidance, support, and thought leadership across Optiv cybersecurity practice areas, with a focus on positioning Identity and Data as a core component within enterprise security architectures. He is a key spokesperson for Optiv's Zero Trust strategy and frequently speaks at conferences and other industry events. Jerry is active in the technical working group at the Identity Defined Security Alliance (IDSA), where he was the group's original Technical Architect. Jerry is a certified Forrester Zero Trust Strategist, has a BS in computer information systems from DeVry University, and is currently pursuing a degree in applied mathematics from Southern New Hampshire University.

About the Technical Reviewer

Christopher Steffen brings over 20 years of industry experience as a noted information security executive, researcher, and presenter, focusing on IT management/leadership, cloud security, and regulatory compliance.

Chris has had a variety of roles as a professional and/or executive, from Camping Director for the Boy Scouts to Press Secretary for the Colorado Speaker of the House. His technical career started in the financial services vertical in systems administration for a credit reporting company, eventually building the Network Operations group, as well as the Information Security practice and Technical Compliance practice for the company before leaving as the Principal Technical Architect. He has been the Director of Information for a manufacturing company and the Chief Evangelist for several technical companies, focusing on cloud security and cloud application transformation, and has also held the position of CIO of a financial services company, overseeing the technology-related functions of the enterprise.

Chris is currently the lead information security, risk, and compliance management researcher for Enterprise Management Associates (EMA), a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies.

Chris holds several technical certifications, including Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA), and was awarded the Microsoft Most Valuable Professional Award five times for virtualization and Cloud and Data Center Management (CDM). He holds a Bachelor of Arts (Summa Cum Laude) from the Metropolitan State College of Denver.

Acknowledgments

Zero Trust security covers a very broad area, and the process we went through to explore, learn, and weave together technical, nontechnical, and architectural concepts was often challenging. We were fortunate to have many people willing to spend time speaking with us, educating us, answering our questions, and providing feedback and guidance. Some folks helped us by reading and commenting on our planned outline or work-in-progress, some contributed by brainstorming with us in videoconferences (a hallmark of 2020, we suppose), while others helped (whether they know it or not) by being part of the information security industry, and as part of their regular professional interactions with us.

Many thanks to Dr. Chase Cunningham for your broad industry influence, and Brigadier General (Ret.) Greg Touhill for your endorsement in the Foreword. And thanks to both of you for your careers in service to our country in military and information security roles. We'd also like to thank Evan Gilman, Doug Barth, Mario Santana, Adam Rose, George Boitano, Bridget Bratt, Leo Taddeo, Rob Black, Deryck Motielall, and Kurt Glazemakers. Also, a shout-out to the team from the Cloud Security Alliance and its SDP Zero Trust Working Group, including Shamun Mahmud, Junaid Islam, Juanita Koilpillai, Bob Flores, Michael Roza, Nya Alison Murray, John Yeoh, and Jim Reavis. And another shout-out to Julie Smith and the Identity Defined Security Alliance (IDSA) team, especially the technical working group for keeping identity in the middle of security**.** We would also like to thank our too-many-to-name colleagues for their many conversations and support, and our Apress editors Rita Fernando and Susan McDermott for their support, encouragement, and help throughout this process. And of course, a huge thanks to our technical reviewer, sounding board, and friend Chris Steffen.

Finally, we'd like to thank you—as a practitioner or leader in the information security industry, working every day to better secure your organization. We hope that this book makes your job easier. Please visit us at `https://ZeroTrustSecurity.guide` with any comments or suggestions, and to view this book's companion video series.

Foreword

> *Zero Trust wasn't born out of a need to sell another security control or solution. It was born from a desire to solve a real enterprise issue…Zero Trust is focused on simplicity and the reality of how things are now.*
>
> —Dr. Chase Cunningham, aka "Dr. Zero Trust"

I have been waiting for this book for over two decades and am delighted to introduce its arrival.

Well before the Jericho Forum's bold 2004 declaration of a new security strategy featuring "de-perimeterization," many of us in the national security community had come to the realization that the perimeter security model was no longer a viable security strategy for Internet-connected systems and enterprises. The unsatiable thirst to connect everything to the Internet, the rising cost and complexity of the layers of security tools, and the rapid pace of technological change were fracturing the perimeter security model around us. Our defense-in-depth security perimeter was a dike springing too many leaks for us to keep up with in any meaningful or fiscally responsible manner. The Jericho Forum's work pointed in a different direction, giving many of us a new hope.

Sadly, like Grand Moff Tarkin on the Death Star, many security professionals and pundits had grown comfortable with the status quo and scoffed at the notion that a new approach to securing modern enterprises was needed. One security commentator went so far as to say the Jericho Forum "missed the mark" and derisively forecast that its work would likely "end up on the scrap heap of unrealized ideas and wasted effort." I hope that he reads this book with a tinge of guilt and regret.

The work of the Jericho Forum did not go for naught, but it did not yield fruit right away either. After a little more than 5 years from the introduction of the "de-perimeterization" concept, John Kindervag, then an analyst at Forrester Research, in 2010 coined the phrase "Zero Trust" to describe the security model that organizations should not automatically trust anything outside *or* inside their perimeters, and instead must verify everything and anything before connecting them to their systems and granting access to their data.

For those of us in the military, Zero Trust was not a revolutionary security model. We had been practicing it with physical security throughout our careers. For example, every person was greeted by security personnel at the gates and had to produce proper identity credentials before being given access to the base. We practiced segmentation with protection zones around what were called priority A, B, and C resources. The flight line areas were the home of priority A assets and had tightly controlled access with armed guards. Role-based entry was tightly controlled and use of deadly force authorized against those who "broke the red line." As a lieutenant, I had to go through four levels of security before I could even get into my office. Security was ingrained in our culture, our processes, and our expectations.

Sadly, as my generation incrementally built out the Department of Defense Information Networks, while we followed a "Zero Trust" physical security model to protect our most valued facilities and weapons systems, the technology to implement a "Zero Trust" security model to protect our increasingly valuable and Internet-connected digital assets was lacking. Commercially available tools were exquisitely complex and expensive. For example, we had to contract with one noted vendor to create an "academy" just to train our already highly skilled workforce to properly use their complex networking products. Costs continued to soar as we continued our march to digitize every function we could, yet the security perimeter dike around us continued springing leaks. By the time I retired from federal service as the Chief Information Security Officer of the US government, I had come to the conclusion that the Zero Trust security strategy was our only hope to secure our digital ecosystem.

The COVID-19 pandemic spurred a massive pivot from traditional office environments to a work-from-home model that has accelerated the long-anticipated move to the Zero Trust security strategy. The illusion of the security perimeter has been shattered by massive mobility, cloud computing, Software-as-a-Service, and unparalleled Bring-Your-Own-Device implementation as organizations everywhere pivoted from traditional enterprise environments to today's modern digital reality. Today's reality is that the traditional network security perimeter is dead; there is no "outside" or "inside" anymore.

Sadly, many people and organizations, including that naysayer who scoffed at the Jericho Forum's vision, have jumped on the Zero Trust bandwagon. Many declare allegiance to "Zero Trust" yet don't know what it really is or how to practice it. Organizations whose legacy networking gear and methodologies have proven exceedingly complex and vulnerable have their marketing teams miraculously declare

their vulnerable capabilities to be "Zero Trust." Despite the great Zero Trust research conducted by Forrester's Dr. Chase Cunningham and Gartner's Neil MacDonald, until this book, there wasn't a practical definitive guide to Zero Trust.

Fortunately, authors Jason Garbis and Jerry Chapman are highly experienced technologists and practitioners who are recognized experts in Zero Trust, enterprise network operations, cybersecurity, and business operations. I encourage you to read their biographies as their credentials are impressive and uninflated. To use military jargon, they've "Been There, Done That."

In the chapters that follow, Jason and Jerry deliver an outstanding book that presents an invaluable explanation of Zero Trust that I believe ought to be used as the definitive reference for students and practitioners everywhere.

The organization of the content is superb. Those who are not familiar with the concept of Zero Trust, and even those who are, will benefit from the first four chapters, which provide a strategic overview of the Zero Trust journey. Chapter 1 provides an insightful discussion that answers the question, "Why is Zero Trust needed?" Those who are just starting their Zero Trust journey will find Chapter 2 invaluable as the authors provide an excellent chronicle of how we got to today's Zero Trust environment and clearly define what Zero Trust is, and isn't. Those seeking to see how to incorporate Zero Trust into their operational architectures will appreciate the practical advice and vivid descriptions presented in Chapter 3. Many people, myself included, prefer to have others "flight test" capabilities before making significant investments or major strategic changes. We're rewarded in Chapter 4 with a fulsome discussion of how organizations such as Google have incorporated Zero Trust into their operations.

The second part of the book provides an outstanding overview of the essential components of Zero Trust, starting with Chapter 5's exceptional discussion on Identity. I contend that Identity is the core component of any successful Zero Trust implementation and was pleased to see Jason and Jerry starting this section of the book with this chapter. The next three chapters provide an important discussion on the impact of Zero Trust on network infrastructure, network access control, and intrusion detection and protection systems. If you find those three chapters provocative, Chapter 9's discussion on virtual private networks in a Zero Trust world likely will change the way you view today's environment and the ongoing movement to a work-from-anywhere future.

Chapter 10's discussion on Next-Generation Firewalls (NGFWs) likewise is provocative as the authors discuss the history and evolution of the subject capabilities and forecast their future in a Zero Trust world. Chapter 11's discussion on Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) in a Zero Trust model is a must-read for those focused on identifying, managing, and controlling risk. Those who find Chapter 5's discussion on Identity exceptional won't be disappointed with Chapter 12's discussion on Privileged Access Management. Those organizations that are keen to reduce their risk of insider threats ought to pay close attention to it as well!

The next four chapters provide practical analysis and guidance on contemporary technical issues many organizations are wrestling with today. Chapter 13's discussion on Data Protection is exceptional and one my students at Carnegie Mellon University's Heinz College ought to pay close attention to (that's a not-too-subtle hint from the professor!). Chapter 14's discussion on Cloud Resources provides straightforward practical advice on how to properly apply Zero Trust when operating in cloud-based environments. As many organizations embrace technologies such as Software as a Service, Secure Web Gateways, and Cloud Access Security Brokers, Chapter 15 provides an outstanding discussion on how these technologies can integrate into your Zero Trust strategy and provides practical advice on how to "get it right." Finally, I was thrilled to see Jason and Jerry's inclusion of Chapter 16's discussion on Internet of Things devices and "Things." Too many cybersecurity personnel are fixated on information technology devices and ignore the risks associated with organizational operational technology, industrial control systems, and "Internet of Things" devices. Regardless of your organizational role, please pay attention to this chapter and recognize the importance of applying Zero Trust in protecting these important systems.

Wrapping up the book are three chapters crucial to every organization committed to properly implementing Zero Trust across their organizations. Chapter 17 provides an essential discussion on how to create and implement a meaningful Zero Trust policy model. Chapter 18 provides invaluable discussions on the most likely use cases your organization will address as you roll out your Zero Trust implementation. Chapter 19 is a welcome companion to the previous chapter, as it discusses how organizations should approach Zero Trust in order to have the strongest likelihood of success. Those who believe in the mantra "start small, think big, and scale fast" won't be disappointed by Jason and Jerry's practical advice. Finally, Chapter 20 provides a satisfying wrap-up of the book's journey through Zero Trust, with a reminder that security exists to enable organizations to achieve their missions.

Zero Trust isn't just a catchy aphorism, it is within our grasp and waiting to be implemented everywhere. This book will help you achieve your Zero Trust goals with velocity and precision. Nation-state actors and cyber criminals have proven that the perimeter-based security model is no longer valid. So have noteworthy insider villains like Edward Snowden. The time to move quickly and deliberately to the Zero Trust security model is now. Thankfully, due to the insightful work of Jason Garbis and Jerry Chapman, we now have a practical guide to how we can achieve our Zero Trust objectives.

Generals since Sun Tzu and Alexander the Great implemented the perimeter-based security model to defend their assets. They didn't have the Internet, mobile devices, cloud computing, and other modern technology. The Jericho Forum got it right; the perimeter is dead. Now is the time to embrace and implement Zero Trust everywhere. Our national security and national prosperity deserve nothing less.

—Gregory J. Touhill, CISSP, CISM,
Brigadier General, USAF (Ret.)

PART I

Overview

Zero Trust is a security philosophy and set of principles, which taken together represent a significant shift in how enterprise IT and security should be approached. The results can be enormously beneficial for security teams and for businesses, but Zero Trust is broad in scope and can be overwhelming. In Part I of this book, we'll be providing you with a historical and foundational introduction to Zero Trust, explaining what it is (and what it isn't), and depicting Zero Trust architectures in theory and in practice. This will help you make sense of Zero Trust, one piece at a time, and begin to think about how it can be applied to help improve your organization's security, resiliency, and efficiency.

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.

CHAPTER 2

What Is Zero Trust?

In this chapter, we're going to introduce Zero Trust as a concept, a philosophy, and a framework. In addition to a brief overview of the history and evolution of Zero Trust, we'll also be introducing some guiding principles. We believe there are *core* and *extended* principles common to every Zero Trust initiative, which are important to understand as you embark on your journey. Our goal for this chapter is to provide you with a working definition of Zero Trust based on these principles, and a set of foundational platform requirements.

History and Evolution

Traditionally, security boundaries were placed at the edge of the enterprise network in a classic "castle wall and moat" approach. However, as technology evolved, remote workers and remote workloads became more common. Security boundaries necessarily followed, and expanded from just the corporate perimeter to also encompass the devices and networks from which the remote user was connected, and the resources to which they were connecting. This forced security and network teams to accommodate these business requirements, and to adjust the models by which organizations applied security and access, with mixed degrees of success.[1]

In 2010, Forrester Analyst John Kindervag introduced the term "Zero Trust" in the influential "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security"[2] whitepaper. This paper captured ideas that had been discussed in the industry

[1]We're attempting to be diplomatic with this statement. It is an undeniable fact that enterprise network security and data security, as an industry, has failed to effectively protect our organizations from data loss and system breaches. Granted, we are facing sophisticated and motivated adversaries, but we believe that this widespread failure is largely due to the shortcomings of traditional infosec tools and approaches, and that Zero Trust will prove to be far more effective.

[2]Forrester, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security," September 2010

J. Garbis and J. W. Chapman, *Zero Trust Security*, https://doi.org/10.1007/978-1-4842-6702-8_2

for a few years, in particular promoted by the Jericho Forum. The Forrester document described the shift away from a hard perimeter, and toward an approach that required inspecting and understanding elements within a network before they could earn a level of trust and access. Over time, Forrester evolved this concept into what's now known as the *Zero Trust eXtended* (ZTX) Framework which includes Data, Workloads, and Identity as core components of Zero Trust.

About the same time, Google began their internal BeyondCorp initiative, which implemented a version of Zero Trust and put in place foundational Zero Trust elements that effectively removed their enterprise network boundary. Google strongly influenced the industry with a series of articles documenting their groundbreaking internal implementation, starting in 2014. Also in 2014, the Cloud Security Alliance introduced the Software Defined Perimeter (SDP) architecture, which provided a concrete specification for a security system that supports Zero Trust principles.[3] We'll be examining both BeyondCorp and SDP through the lens of Zero Trust a bit later, in Chapter 4.

In 2017, industry analyst firm Gartner revised and refreshed their Continuous Adaptive Risk and Trust Assessment (CARTA) concept, which has many principles in common with Zero Trust. CARTA provides not only Identity and Data elements but includes risk and posture associated with identity and devices accessing the environment.

Further industry-wide emphasis on Zero Trust continued, as the US National Institute of Standards and Technology (NIST) released a Zero Trust Architecture publication[4] and an associated US National Cybersecurity Center of Excellence project in 2020.[5]

Zero Trust continues to evolve as vendors and standards organizations review and refine specifications and implementations of Zero Trust, recognizing it as a fundamental shift in the approach to information security. Ultimately, the industry has agreed that these changes and refinements are necessary, in order to prevent malicious actors from accessing private resources within organizational boundaries, exfiltrating data, and disrupting operations.

---

[3]See the CSA's Architecture Guide for SDP, https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/.

[4]NIST Special Publication 800.207—Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final, August 2020

[5]https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture.

We, the authors of this book, work in the information security industry, and both spend much of our time speaking to security professionals about Zero Trust. One common question we hear is "What's new about Zero Trust—how is it different from what's already been done?" It's definitely true that some elements of Zero Trust, such as *least privileged access* and *role-based access control*, are principles that are commonly implemented in current networking and security infrastructure (and must be utilized in Zero Trust environments), but alone they do not complete the picture.

Foundational security elements used prior to Zero Trust often achieved only coarse-grained separation of users, networks, and applications. For example, in most organizations, development environments are separated from production environments. However, Zero Trust amplifies this, effectively requiring that all identities and resources be segmented from one another. Zero Trust enables fine-grained, identity-and-context-sensitive access controls, driven by an automated platform. Although Zero Trust started as a narrowly focused approach of not trusting any network identities until authenticated and authorized, it has rightfully grown in scope to provide a much broader set of security capabilities across an organization's environment.

Let's briefly examine the Forrester and Gartner Zero Trust models, before we introduce what we believe are the key Zero Trust principles.

Forrester's Zero Trust eXtended (ZTX) Model

Forrester released their initial Zero Trust model in 2010, and in the following years, it has been revised and re-released as *Zero Trust eXtended* (ZTX). ZTX provides richer content and a well-rounded model that places data at the center, as shown in Figure 2-1. This reflects Forrester's belief that the data explosion in both on-prem and cloud environments is at the center of what has to be protected. The surrounding elements—Workloads, Networks, Devices, and People—are conduits to data and therefore need protection as well. Let's look at each of these elements in turn.

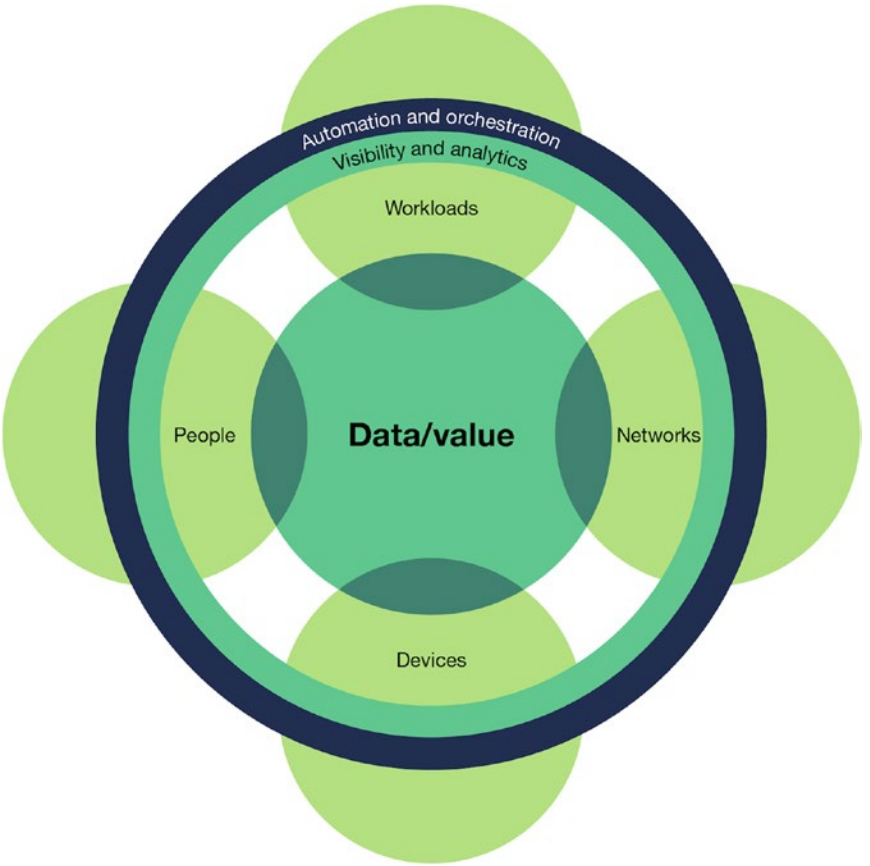

Figure 2-1. *Forrester Zero Trust eXtended Model (Source: The Zero Trust eXtended Ecosystem: Data, Forrester Research, Inc., August 11, 2020)*

> Data: *Data* (which Forrester also tags as "value" to highlight its importance[6]) is the center of the ZTX model, and it includes Data Classification and Protection at the core of the requirements to support the Zero Trust Model. Throughout the book, we view data as an element of the *Resources* that Zero Trust systems must protect. Additionally, Data Loss Prevention (DLP) should be a part of a Zero Trust architecture, and tied into the policy model with the ability to enforce contextual access policies where possible.

[6]In fact, Forrester states "in truth, what we considered solely as 'data' is now really 'value.' Whatever is of value to your business is the most critical asset to focus your defenses around, and you should defend that value at all costs," The Zero Trust eXtended Ecosystem: Data, Forrester Research, Inc., August 11,2020

Networks: The *Network* pillar of the ZTX model is primarily focused on network segmentation—both from a user and a server perspective—to provide better security based on identity-centric attributes. It's important to recognize that enterprises have many existing components that make up the traditional network security infrastructure, such as Next-Generation Firewalls (NGFWs), Web Application Firewalls (WAF), Network Access Control (NAC) solutions, and Intrusion Protection Systems (IPS). These components generally all have a role to play in a Zero Trust system. We'll introduce these components in a representative enterprise architecture in Chapter 3, and examine their relationship to Zero Trust at length in Part II of the book.

People: The *People* pillar of the ZTX model must include multiple elements of Identity and Access Management (IAM). Role- and Attribute-Based Access Control (RBAC and ABAC) are well-understood models within IAM, and Zero Trust enables the use of these more broadly, and more effectively, across the enterprise infrastructure. Multi-Factor Authentication (MFA) is another requirement and is essential to supporting Zero Trust. Finally, Single Sign On (SSO)—using modern, open standards such as OAuth and SAML—is another core element within the people pillar. As you'll see throughout this book, we're strong proponents of making Identity central to every Zero Trust environment.

Workloads: *Workloads*, as defined by Forrester, consist of the components that make up the logical functions that drive business within both customer facing and backend business systems—containers, applications, infrastructure, processes, etc. Zero Trust requires metadata-driven workload access controls, enforced consistently across hybrid environments. We'll be exploring this further in Chapter 17.

Devices: The security model for *Devices* should include the identity, inventory, isolation, security, and control of the device. In Chapter 3, we'll describe user agents which run on devices, and how they are core to the Zero Trust environment. We'll also see later, in Chapter 4, the ways in which devices were key to Google's BeyondCorp implementation.

Visibility and Analytics: *Visibility and Analytics* within ZTX is the consumption and presentation of data across the enterprise to support informed security decisions based on contextual information. We agree that this is critical, especially the consolidation of data across multiple disparate sources. There is not a single platform that exists today that spans the necessary breadth of functionality, but this is an evolving space. We'll discuss further in Chapter 11.

Automation and Orchestration: *Automation and Orchestration* within ZTX are required to automate manual processes, and to relate them to security policy and actions for response. We believe that this element is critical to the success of a Zero Trust platform—Zero Trust is inherently dynamic and adaptive, and the only way to achieve this is with automation and orchestration, across the enterprise environment. We'll discuss this further in the following, as Automation is one of our key Zero Trust principles.

Gartner's Approach to Zero Trust

Gartner has approached Zero Trust through a model they call CARTA—Continuous Adaptive Risk and Trust Assessment. The premise of CARTA is to provide continuous risk assessment as it pertains to users, devices, applications, data, and workloads, from a perspective of *Predict, Prevent, Detect, and Respond*.

CARTA uses the fundamental process of *Implement a security posture*, *Monitor the posture*, and *Adjust the security posture* through different planes of security. Gartner believes that these principles should be enforced across the entire enterprise and include security, policy, and compliance requirements throughout.