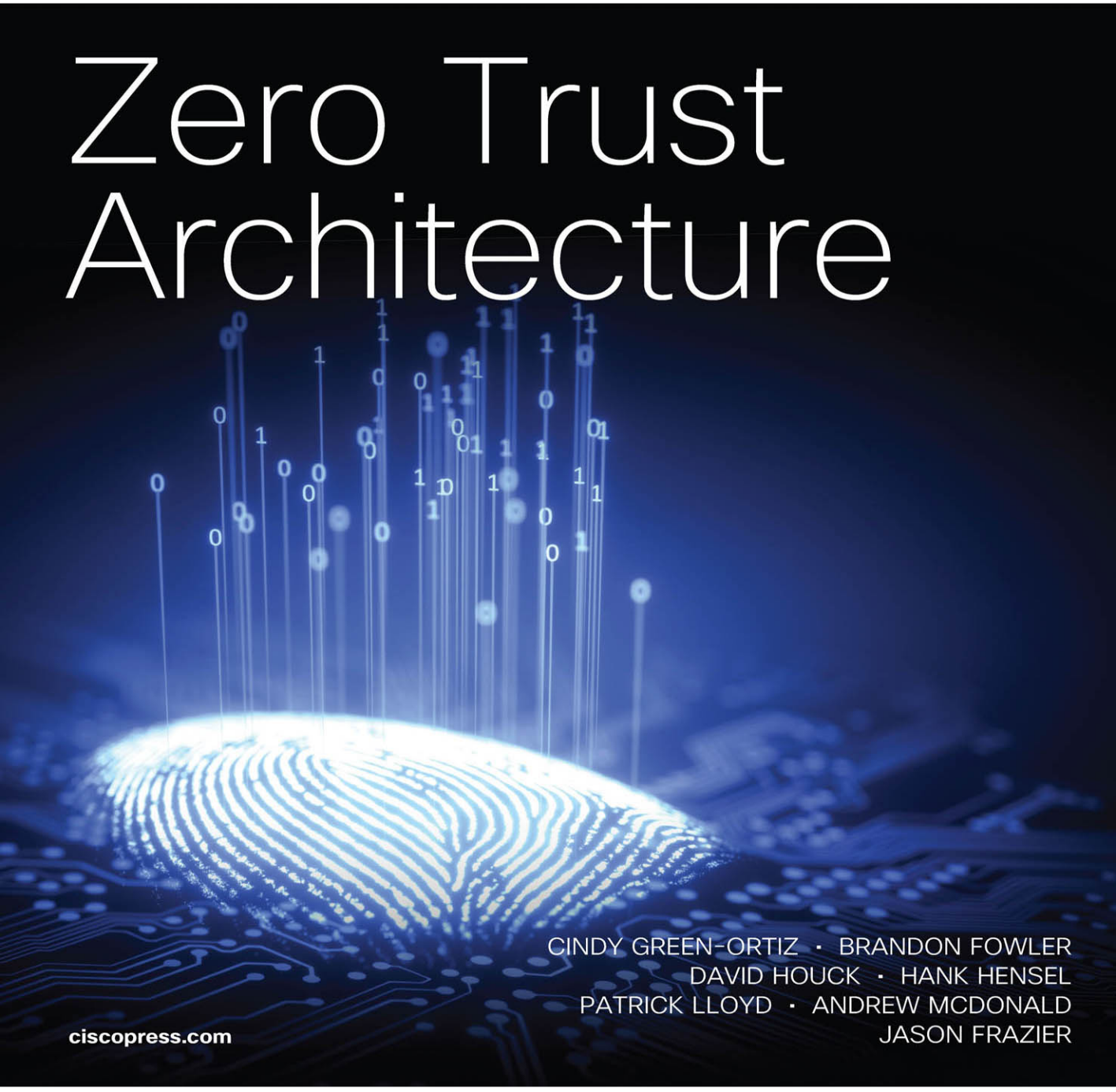


FREE SAMPLE CHAPTER

Zero Trust Architecture

Cindy Green-Ortiz, CISSP, CISM, CRISC, CSSLP, PMP, CSM
Brandon Fowler, CCNP Security
David Houck
Hank Hensel, CCIE No. 3577, CISSP
Patrick Lloyd, CCIE Enterprise No. 39750, CISSP
Andrew McDonald
Jason Frazier, CCSI

Cisco Press

Zero Trust Architecture

Cindy Green-Ortiz, CISSP, CISM, CRISC, CSSLP, PMP, CSM

Brandon Fowler, CCNP Security

David Houck

Hank Hensel, CCIE No. 3577, CISSP

Patrick Lloyd, CCIE Enterprise No. 39750, CISSP

Andrew McDonald

Jason Frazier, CCSI

Published by: Cisco Press

ScoutAutomatedPrintCode

Library of Congress Control Number: 2023906699

ISBN-13: 978-0-13-789973-9

ISBN-10: 0-13-789973-4

Warning and Disclaimer

This book is designed to provide information about Zero Trust Architecture. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity concerning any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Vice President, IT Professional: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Senior Project Editor: Mandie Frank

Copy Editor: Chuck Hutchinson

Technical Editors: Tom Diederich, Joseph Muniz, Brock Pearson

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Erika Millen

Proofreader: Donna E. Mulder

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Figure Credits

Cover: ktsdesign/Shutterstock

Figure 1.2a: Shutterstock

Figure 1.2b: Robert Kyllo/Shutterstock

Figure 1.2c: ktsdesign/Shutterstock

Figure 1.2d: dotshock/123RF

Figure 6.1: S.john/Shutterstock

Figure 10.2: HarperCollins Publishers LLC

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

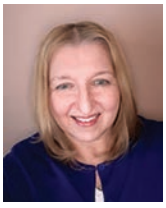
Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

About the Authors



Cindy Green-Ortiz

Cindy Green-Ortiz is a Cisco senior security architect, cybersecurity strategist, architect, and entrepreneur. She works in the Customer Experience, Global Enterprise Segment for Cisco. She holds the CISSP, CISM, CSSLP, CRISC, PMP, and CSM Certifications, along with two degrees—a BS-CIS Magna Cum Laude and AS-CIS with Honors.

She has been with Cisco for 6+ years. Cindy has been in the cybersecurity field for 40 years, where she has held D-CIO, D-CISO, and Corporate Security Architecture Leadership roles, founding two technology businesses as CEO. Cindy is a Cisco Chairman's Club winner (Club Cisco). She is an active blogger for Cisco and has published whitepapers for Cisco and the US Department of Homeland Security. She has spoken to many groups, including PMI International Information Systems & Technology Symposium-Cybersecurity Keynote; Cisco SecCon, and Cisco Live. Cindy is President Emeritus and serves now as the treasurer of Charlotte InfraGard and cofounder of the InfraGard CyberCamp. Cindy lives in Charlotte, North Carolina, with her amazing husband, Erick, and their two wonderful daughters. Cindy and her family love to travel and see the world.

Brandon Fowler

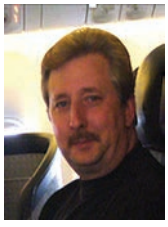
Brandon Fowler is a technical leader for Cisco Customer Experience Professional Services. He holds both CCNP Security and ITIL v4 foundation certifications. Brandon joined Cisco in 2018 with more than 12 years of experience across enterprise networking and security domains. For the past 8 years, his focus has been on identity, access management, and segmentation with expertise across multiple industry verticals, including retail and distribution, hospitality and entertainment, financial services, and healthcare. Additionally, he has helped to develop some of Cisco's current Zero Trust service offerings. Brandon also helps mentor and advise other employees within Cisco and enjoys being challenged and learning new technologies. In his personal time, he enjoys working on cars, photography, and video gaming.

David Houck

David Houck is a security architect, mentor, and advocate. He has been working with Cisco Customer Experience since 2011. David leads delivery teams in implementing solutions globally to financial, energy, retail, healthcare, and manufacturing organizations that focus on identifying and meeting technical and business outcomes. He has presented on the value and implementation of Cisco solutions globally to customers, partners, and internal audiences.

David has worked in networking and security since 2005, with experience in service provider voice, infrastructure, ISP operations, plus data center design and operation

before coming to Cisco to focus on security solutions and architecture. He enjoys mentoring to provide experiences and opportunities to see others flourish.



Hank Hensel

Hank Hensel is a senior security architect working for Cisco's CX Security Services providing security consultation, assessment, and design advisory services to Cisco's US and international customers.

Hank has worked more than 30 years (7 years at Cisco) in leadership positions in IT systems, cybersecurity, design, and integration. Hank's areas of expertise include security and infrastructure, project management, disaster recovery, business continuity, risk analysis and mitigation, data mapping, data classification, and cybersecurity infrastructure design. Hank has displayed his expertise and leadership in several different industries, including international banking and finance, healthcare, pharmaceutical, energy, renewable energy, oil and gas, passenger and transit rail, manufacturing, mining, wet infrastructure, chemical, nuclear enrichment, public sector defense, municipality and state infrastructure, and law enforcement. Hank's expertise and extensive training in networking, security, and strong focus with industrial control systems allow him to engage in nearly all areas of a customer's operations, policies, and practices. Hank holds CCIE (# 3577), CISSP, GICSP, and CMMC-RP, and other certifications.

Hank practices Cisco's core values in all customer engagements, which have directly contributed to his consistent project successes in every engagement he has been involved in. Hank's success can be attributed to these values and their consistent culmination by being recognized as a "Trusted Advisor" in nearly every engagement he has been a part of for Cisco.

Hank's role of trust and deep experience extend beyond customer relationships to new service offerings development and Cisco team support. Hank was the original developer of the current CX advisory segmentation service offering that has been in use for the last seven years and has contributed to the development of the new CX advisory Zero Trust service offering. Finally, Hank is currently contributing to building a consulting service offering for the renewables energy sector.

Patrick Lloyd

Patrick Lloyd is a senior solutions architect for Cisco's Customer Experience Security Services team. He focuses on identity and access management, including segmentation, network access control, identity exchange, and identity integration in the Northeast United States and Canada region.

Patrick has worked in technology delivery at Cisco for 13 years, ranging from stints in the technical assistance center (TAC), working as a routing and switching design engineer, security design engineer, and solutions architect. His focus is guiding customers through introducing visibility and identity exchange to minimize business risk and lateral attack vectors. Previously, Patrick worked in higher education and defense industries in system administration and operational roles.

Patrick has extensive experience in integrating identity into various industries, including healthcare, manufacturing, finance, and defense. Utilizing Cisco technologies and the methodologies covered in this book to build a layered security model, Patrick has architected segmentation architectures, including smart building architectures, for more than 100 customers.

Patrick's technology focuses span from TrustSec for segmentation, analyzing traffic flow with Cisco Secure Network Analytics/Stealthwatch for development of segmentation policies, implementing firewall and advanced malware protection, and securing critical building systems through policy and segmentation while maintaining availability.

Patrick resides in Durham, North Carolina, where he teaches self-defense and is a student pilot when not consumed with technology.

Andrew McDonald

Andrew McDonald is a Cisco network and security architect; he works in the Customer Experience, Security Advisory team for Cisco. He specializes in leading delivery teams creating network segmentation and Zero Trust designs and implementation plans.

He has been with Cisco for more than 22 years, working as an escalation engineer, network consulting engineer, systems integration architect, and security architect. Andrew has worked with global customers in all industry verticals and at every level, from front-line support engineers to C-suite executives across multiple technical disciplines. Andrew has worked in the networking and communications industry for more than 40 years. In 1981, he started as a telecommunications technician for Digital Equipment Corporation, where he developed an entry level into a lifelong career.

Jason Frazier

Jason Frazier is a principal engineer with the Network Services group in Cisco IT. In his current role, Jason focuses on Zero Trust technologies, Cisco DNA, operational excellence, automation, and security. Jason has deep knowledge of networking technologies, including programmability, enterprise network architecture, and identity.

Jason joined Cisco in 1999. He is known throughout the company for his work ethic, passion, loyalty, and drive. Jason currently holds nine patents. For Cisco Live, he is a veteran speaker, hackathon coordinator, blogger, booth orchestrator, or anything called for. Jason is also the author of Cisco Press books.

Jason has been happily married to his wife, Christy, for 22 years. Their oldest son, Davis (16), is Jason's best friend. Jason is also wrapped around the finger of their daughter, Sidney (14). Most nonwork time is spent doing something with or for his kids. He likes to spend time on a bike, when possible. Jason and family like to travel when they can. As a computer engineering graduate of NC State University, Jason and his family enjoy Wolfpack sporting events as well.

About the Technical Reviewers

Tom Diederich

Tom Diederich is a Cisco ONEx Community Storyteller. He joined Cisco's ONEx communities team in 2021. He has a bachelor's degree in journalism from The Ohio State University and maintains an active "Secret" level security clearance with the US Department of Defense.

Joseph Muniz

Joseph Muniz is the director of business development for security solutions at Microsoft and a security researcher. He is driven by making the world a safer place through education and adversary research. Joseph has extensive experience in designing security solutions and architectures as a trusted advisor for the top Fortune 500 corporations and US government.

Joseph is a researcher and industry thought leader. He speaks regularly at international conferences, writes for technical magazines, and is involved with developing training for various industry certifications. He invented the fictitious character of Emily Williams to create awareness around social engineering. Joseph runs thesecurityblogger.com website, a popular resource for security and product implementation. He is the author and contributor of several publications, including titles ranging from security best practices to exploitation tactics. Joseph's latest title, *The Modern Security Operations Center*, was released in 2021, and he has a title on virtual private networks.

When Joseph is not using technology, you can find him on the futbal field. Follow Joseph @SecureBlogger.

Brock Pearson

Brock Pearson has been a thought leader in the cybersecurity industry as a consultant or educator for more than 22 years. He has worked for multiple firms, assisting Fortune 500 organizations, plus federal, state, and local government agencies in their quest to protect their data, systems, and computing environments. Within his consultative capacity, Brock has developed and executed cyber program strategies (people, processes, and technologies) and has assessed, enhanced, and transitioned those services to managed security services as necessary. Brock has primarily been engaged in the heavily regulated industry verticals including financial services, healthcare, and utilities. As an educator, Brock has developed and delivered enablement programs globally for two of the largest SIEM and UEBA products in the cybersecurity tooling space.

Dedications

To my beloved husband, Erick Ortiz-Alvarenga, every day is a blessing, and I am truly grateful for all your love and support. To our daughters, Angela and Anna, what a bright future you have. Know that are both loved and supported to reach your dreams. You both inspire me every day! To my Uncle Roger Green and my Aunt Joan Green, you bring me joy and always have a great story from back home. To my parents in heaven, Howard Green, and Nancy Salyers Green, I would not be where I am without your courage to strive for knowledge.

—Cindy Green-Ortiz

To my parents, Nick and Sherry, and my brother and sister-in-law, Derek and Melissa, who have always supported me and helped me become who I am today, I am forever grateful. To my mentors, teachers, and everyone else who has helped in small or large ways throughout the years, thank you for everything that you have done to impact my life and help me get to where I am today.

—Brandon Fowler

For all who teach, inspire, and mentor us. Those who provide the shared human experience of fueling the drive for learning and improvement. A world without these experiences and the people who dedicate themselves to share these experiences never progresses. Take the time to remember, recognize, and celebrate those who have contributed to who and where you are today. Be responsible and kind enough to share of yourself and share that experience with others.

—David Houck

To my wife (and dance partner), Catherine, and our daughter, Katrina, with love. In life, the accumulation of meaningful knowledge and experience does not happen by accident. It is sought and pursued over time throughout our lives. Thank you for your grace in encouragement, support, and especially patience with my long hours and travel over the years.

—Hank Hensel

To my parents, without whose support I never would have pursued dreams that seemed well beyond the reach of many. To the friends and family who supported me through some of the best, worst, and weirdest times we've been through together, your support and guidance are what made this book possible. This never could have been done without you.

—Patrick Lloyd

To my lovely wife, Sharon, for all her support through late-night troubleshooting, weekend cut-overs, long and frequent travel schedules, and listening to me talking about networking for the last 35 years. Also, to my two rotten kids, Charlie and Emily, who suffered through much the same, along with endless droning from "the troll hole" (my home office). No wonder neither of them went into IT. Finally, to my mother and father, who taught me the value of hard work and integrity.

—Andrew McDonald

To my wife, Christy Frazier, I love you so dearly. As the years go by, they just get better. Thank you for always supporting me. As I stand by your side, I am the luckiest man in the world. To my son, Davis Frazier, I am so excited to see you shaping into the man you are becoming. You are the best friend a dad could have. To my daughter, Sidney Frazier, there are no limits for your potential. I will forever be wrapped around your finger.

—Jason Frazier

Acknowledgments

With 40 years in this field, I have too many to thank for your help, guidance, and support. To name but a few, I would like to give special recognition to my friend-sister Patty Wolferd Armstrong, my lifelong mentor Denis McDuff, my Cisco mentors and colleagues: David Ankeney, Demetria Davis, Bill Ayers, Jr., Justin Taylor, Brian Conley, Jim Schwab, Michele Guel, Zig Zsiga, Cesar Carballes, Jason Penn, Chris Mula, Guilherme Leonhardt, Maurice DuPas, Aunudrei Oliver, and this authoring team, who have seen me at my best or at my worst and have helped me navigate life or work's ever-changing landscape. I am ever grateful to my high school science teacher, Mrs. Demchek, and my piano teacher, Edrie Ballard, who set me on my path.

—Cindy Green-Ortiz

I would like to recognize first my high school teacher, Wayne Whaley, who encouraged me to enter Cisco Networking Academy courses in high school and exposed me to the world of computer networking. Additionally, I want to recognize the managers and mentors that I have had along the way who gave me opportunities to prove myself and have helped guide and support me in my career through the years: Bo Osborne, Danielle Desalu, and Guilherme Leonhardt.

To the colleagues and mentors such as Ranjana Jwalanieh, David Houck, Cindy Green-Ortiz, Chris Roy, Dan Geiger, Daniel Schrock, Tim Corbett, Aaron Cole, and countless others who have over the years provided support, friendship, and a place to vent during the more frustrating moments this career can bring, a big thanks to all of you.

—Brandon Fowler

Many people play roles in our lives that impact us on our journeys. I would like to recognize some of those who have had the greatest impact on my journey:

Teachers: Ben Poston, who taught me rigor; Preston Wannamaker, who helped me embrace failures

Leaders: Danielle Desalu, who gave me opportunity and visibility; Guilherme Leonhardt, who tempers my rough edges

Mentors: Maurice Spencer, who selflessly pushes me forward; my late grandfather, Mel Houck, who challenged me to always ask how and why

Friends: Jim Kent, who supports me in the best and worst of times; Chris Brady, who inspires me to take new paths and find fulfillment

—David Houck

I must give special recognition to my father, Ron Hensel, who taught me to see the world like an engineer. To not only understand how things work but also systematically seek to understand why things work. Based on your lessons, in my career, I have been able to solve most any problem by using both analytical and creative thinking.

—Hank Hensel

In a technology career spanning multiple decades, one does not reach apexes in technical knowledge without exposure and guidance from some of the best managers, mentors, and sounding boards in the industry. It has been my privilege to work with some of the most fantastic people who guided me through a long career in the industry, and sometimes pushed me beyond my limits to grow:

My friend and colleague, Chris Mula

My mentor and first manager at Cisco, Kenneth Huss

My sounding board and hardest working person I've ever met, Courtney Carson

The multitudes of mentees and engineers who have questioned my ideas, forced me to rethink solutions, and offered the spark that turned into the designs contributing to this text.

—Patrick Lloyd

I was incredibly lucky to stumble into this industry in its formative years. In the days when we used the telephone network to carry data, I was given a wonderful opportunity to learn, grow, and evolve with the industry. Along the way there were a few people who stood out and gave me the chances I needed to succeed. First, I would like to thank Chip Duval for handing me a multiplexor, a spool of cable, and a book and said, "Make this work." Second, I would like to thank one of my first managers, Frank Ignachuck, who said, "If you need to be managed, I will manage you." I never needed to be managed after that. Lastly, I'd like to thank one of my customers, Jeff Toye, who gave me a chance to prove myself where others would not have. These lessons in self-learning and reliance helped me build a career where after 40 years, I still learn something new every day. Thank you for the opportunity.

—Andrew McDonald

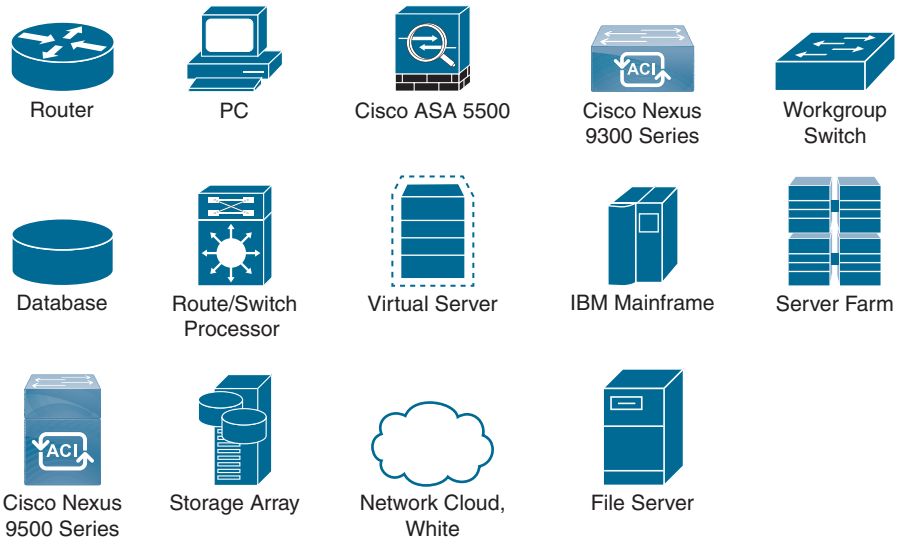
I must acknowledge three special people in my life. My grandfather, Darrell Smith, taught me how to be a man. My grandmother, Joyce Smith, taught me patience and love. I miss you both dearly, though you are still with me every day of my life. To my mother, Rhonda Frazier, you are a rock of wisdom, teaching me relentless passion and drive.

—Jason Frazier

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Preface

Where does the idea start to write a book?

For me, there were many signposts along the way. Years ago, when I was young, I knew that books were my way to see the world and to think in a different way. Without them, I would have never ventured from deep in the mountains far from the world outside. I was always a natural scientist, experimenting on anything and everything. Taking apart most things and putting them back together—well, almost. Writing a book was always a thought in my young mind.

Fast-forward many years, I have worked with this group since joining Cisco six+ years ago. With them, we have been solving problems, helping people, and making a difference every day around the world. To say that this is what drives me is an understatement.

The needs of my customers and my teammates drove me to want to start this effort. Understanding the concept of Zero Trust was something I was presenting, speaking, designing, and advising about—over and over. Everyone having a varied understanding.

The only way I could think to solve the issue of getting everyone on the same page was to set out the concepts in writing. It started as a small idea, and then it kept growing. My mentors all said, "You should write a book!" The idea became a reality.

After I approached everyone on this writing team one by one, we formed a tightly bound group, strengthened by the need for the information to be put on paper and standardized in way that was easier to understand and, most importantly, repeatable.

Thank you to each of my coauthors for making this dream come together. It would have never happened without you!

I hope this book helps you, the reader, and makes a difference on your journey.

—Cindy Green-Ortiz

Prologue: Jason Penn, Cisco Director, Customer Experience

"Zero Trust is going to be super easy," said no one ever. While this quote is clearly said in jest, the reality is that Zero Trust is a complex topic, dealing with complex technologies being implemented in complex environments. However, as I tell my children, just because something is difficult does not mean that it's not worth doing and, most importantly, doing well.

I once had a security executive tell me that the security industry might be the only industry where you can buy more and more products but never really feel as though you're achieving better and better results. Even 10+ years later, there is a lot of truth in that statement. To me, this is the crux of what Zero Trust really is—namely, weaving together a grouping of security technologies to increase your security posture, increase

your visibility, decrease your response times, and generally feel as though you're using security tools to get better at protecting your critical corporate assets. Wouldn't it be nice if the tools worked for you, instead of the other way around?

In the modern day of "work anywhere," cloud-native/hybrid cloud/multicloud, and so on, there is a seismic shift in the way we access and consume applications, data, and infrastructure. At the same time, the normal adversaries (nation-state, hacktivists, hobbyists) are still out there, but getting better and more aggressive. Which is why I believe the Zero Trust framework is critically important and should be looked at seriously.

Okay, so you're clearly interested in Zero Trust as a concept (you've made it this far into the book anyway). What led you here is probably a common set of questions, such as

- What really is Zero Trust?
- How and where do we start this journey?
- What does success look like?
- When are we done?
- What do we have in our portfolio already?
- What are we missing?
- What do we have that is possibly duplicative?

These questions are valid and common, and they warrant real thought and inspection. And as is typical with these types of initiatives, the answers will vary from company to company based on business objectives, risk tolerances, compliance considerations, and a myriad of other variables that are unique to your company, your industry, and your situation. Which essentially means that you are going to want to create a workable plan that addresses your specific needs. *Workable* being the operative word. A plan that "boils the ocean" is no plan at all.

I have spent many years as a security practitioner, specifically helping organizations with their current and future states, gaps, and strategic direction. In that time, I have learned the value of having a realistic plan that is directionally accurate but also flexible. Not flexible to the point where you rewrite it every year, but flexible enough to nudge the direction or timelines based on the current situation, whatever that may be.

Additionally, I find great value in a plan that allows more frequent, small victories. A plan where it is possible to report forward progress and keep people interested. Hence, the earlier comment about not "boiling the ocean"; biting off too much in a single sitting will inevitably result in frustration, failure, and eventually a loss of funding.

This book is intended to be a guide on how to navigate the entirety of the Zero Trust journey, from concept and planning to a phased approach to execution, across multiple different industry sectors. It is written to face the realities head-on and provide practical examples that are based in experience and that can be used to enlighten your journey.

I hope that you enjoy the topic, the guidance, and the love and experience that went into creating this book. The authors are truly passionate about Zero Trust, so much so that they used their spare time to write a book about it. Talk about dedication!

Foreword: John Strong, FBI Special Agent in Charge, Retired

"Change is the only constant in life." We have all heard this maxim that is credited to the Greek philosopher Heraclitus. In my 30-plus year career as an FBI Special Agent, I saw many examples that supported this. I learned that if you are slow or unwilling to evolve with the changing threat environment, you are eventually going to lose. The threats we face are always evolving. In the cyber world, they are doing so at breakneck speed. If your organization isn't recognizing and effectively reacting to these changes, your security stance is becoming less effective every single moment—and your risk is growing.

From its start in 1908, the FBI developed over the years into the world's premier law enforcement agency. When I joined in 1990, the Bureau had well-honed training and tactics to solve many sophisticated federal offenses. We were good. Some, including me, said we were the best. But we were inflexible. Slow to adapt to the growing threat of terrorism. Reactive.

Events like the Oklahoma City bombing and 9/11 were game changers for the organization. It was no longer acceptable for the FBI to arrive after the crime was committed and solve it. The only stance acceptable to the American people was a Bureau that was proactive and could stop these events before they happened. Since those terrible events that occurred over 20 years ago, the FBI has morphed into a much more intelligence-driven and proactive organization that is prepared for the dangers we face today. It wasn't a pain-free or linear transformation, but we got there. To keep pace with the cyber, terrorism, and traditional criminal threats of today and tomorrow, the FBI has to continuously evolve and adapt to meet the challenge.

Likewise, your business security posture has to evolve with the threats you face before you have your game-changing event. We have gone from the days of locks, fences, and cameras protecting the crown jewels of our organizations to securing them in the cloud. The workplace is no longer static. The public health threat posed by COVID-19 put us on the express lane to a work from anywhere world where fewer and fewer work from "the inside." The insider threat no longer comes predominately from within. Even hackers have changed with the times. We have moved from the destructive teenaged hackers in the basement to sophisticated cyber-criminal cabals using commoditized tools and ransomware as well as state-sponsored hacking organizations. Even that difference has become blurry, as some hackers working for governments will use those same skills and tools in their own criminal endeavors while off duty.

Once someone with authorized access to your systems decides to steal or sabotage, how far can they get? A criminal who has compromised an employee's credentials, can they run amok? A hacker who has slipped in through the cracks, are they lurking in the shadows of your systems? Do you know? Are you sure?

Trusting a device merely because it is within the "corporate fence line" or connected through a VPN no longer creates a solid security posture. If you are not implementing Zero Trust as part of your security plan, you are leaving doors open, which could lead to the loss of your most precious data. Are you ready to secure those doors? If you are, it's *probably* not too late.

During the last quarter of my career, I proudly served as the Special Agent in Charge of all FBI investigations in North Carolina. The Tarheel state is home to many large corporations, including some high-tech powerhouses. We knew that we couldn't effectively protect the citizens and corporations across the state without the assistance of our private sector. We drew upon this wealth of resources and teamed with corporate security professionals from across the state in a public-private partnership known as InfraGard. That's where I had the honor of meeting and partnering with dedicated security experts like Cindy Green-Ortiz.

Cindy served as the president of the Charlotte InfraGard chapter, where she led the effort to share threat intelligence and industry best practices to close security gaps. Being elected to that position by her peers showed the high esteem in which those professionals held Cindy and her leadership. I found their confidence in Cindy to be well-founded.

Cindy not only addressed the concerns of the day. She also had a focus on the future. By dedicating her time, talent, and vision, Cindy was instrumental in inspiring and motivating young minds during the annual, weeklong summer cyber camp for STEM-focused high school students cosponsored by InfraGard and the Charlotte FBI field office. Those talented young people are part of the next generation to take on the cybersecurity challenge. I couldn't have asked for a better partner than Cindy.

Zero Trust fits today's work environment and aligns with the principle of least privilege. It's the latest evolution of security for IT infrastructure and data in today's cloud-based, location-agnostic workplace.

How focused is your organization on the management and monitoring of credential usage? Four out of five network attacks involve the use or misuse of credentials. Are you comfortable that those people and devices that are fully vetted have access to all the data they need, yet only the data they need, to perform their jobs effectively? Have you done all you can to limit the "blast radius" of malevolent access to your systems?

I commend you for starting your journey toward Zero Trust with this book. Zero Trust is flexible in its design and can be tailored to meet unique and specific needs in your security strategy and give you robust ROI.

Your attention now will make it much less likely that you will be calling my former colleagues at the FBI about being hit by a ransomware attack or some other compromise of your organization's crown jewels. Keep up the good fight!

—John Strong, Special Agent in Charge, FBI (Retired)

Introduction

The goal of this text is to provide the reader with tried-and-true methods to implement Zero Trust Architecture throughout an organization based on the combined 85 years of security and architectural experience across all authors. These architects and engineers work together daily across tens of organizations, hundreds across their respective careers, to migrate organizations toward a consistent and replicable Zero Trust Architecture for sites throughout the world. Throughout this experience and the design of a Zero Trust Architectural process, observations of where organizations are most successful have been factored into this text. In addition, discussions entailing where common mistakes are made, or assumptions made that have been proven, generally, false are found throughout.

While there is significant debate throughout the security world regarding the effectiveness of Zero Trust and how aspects of Zero Trust may differ between organizations and their own idiosyncrasies, this text is meant to provide a broad recommendation and guidance to assist organizations, architects, and engineers on their journey toward Zero Trust. Considerations made when evaluating these assumptions and mistakes typically include an organization's business behavior, industry, and capabilities. Additional considerations also include the best ways to mitigate organizationally unique risks, and analysis that can only be done within the organization. This analysis must consider unique facts and insights to best align the proper recommendations within the Zero Trust methodology for an organization's specific needs.

Goals and Methods

This text is meant to be our attempt to articulate what we, the authors, have seen work in the hundreds of customers that we've worked with over the years who are pursuing similar Zero Trust goals. With the continuous changes occurring in the industry related to Zero Trust, and the components that are seen as making up the Zero Trust concept, this reference serves as a point-in-time baseline for what we believe is the most practical approach for most customers.

In a manuscript written to guide customers, the 80/20 rule always must apply. The goal pursued here is that methodologies within this book will assist 80 percent of customers' work toward their Zero Trust goals with minimal variation on the methods stated here. For the 20 percent of customers who have already gotten to a point in their pursuit of Zero Trust that renders much of what is in this text as ancillary to their goals, the hope is that this text might serve as a reference model for operations and engineering—specifically, for how to continue to improve or operate the Zero Trust Architecture.

Throughout the text, we use a fictional customer made up of use cases from across industries, with the names and concepts changed to better illustrate problem statements with Zero Trust solutions. Not only do we hope that this method will aid in your

learning, but we hope that it will provide a relatable technology and business concept definition, while protecting the innocent customers who have made very relatable decisions or mistakes.

Many will notice that broader concepts are used throughout the text with some avoidance to state the singular be-all-and-end-all technologies that must be present to accomplish a goal or milestone. This approach is purposeful. As Zero Trust evolves, and it continues to do so every day, products will change, but their functionality and business-aligned goals will remain the same. This is the pattern we've observed throughout tens of years in the industry, and with the hope that many of us will have tens of years more.

Who Should Read This Book?

Zero Trust Architecture (Networking Technology: Security) is for network cybersecurity engineers and architects. The primary audience is for network cybersecurity engineers and architects who are responsible for creating a framework based on a set of principles assuring monitored and managed least-privilege access security controls to remediate and mitigate advanced cybersecurity threats. The secondary audience is other networking staff members who have interests in mature least-privilege cybersecurity access strategies in relation to their specific corporate business environments.

This book should be read and used by intermediate to advanced readers. Because of the methods explored in the content, industry experts could reference this book.

Strategies for Implementation of Zero Trust

The key to pulling the organization's teams together will be an executive sponsor who has broad oversight across business units and any areas of the organization that may be affected by the application of the Zero Trust journey. The executive sponsor should be positioned to influence the participation of the disparate teams required for the project and have direct ownership of outcomes. This may entail an executive at the C-suite with mandates from the board of directors, may be a team of executive managers, or may be a singular senior manager with broad influence and authority. Regardless of the person or team, due to the changes in ongoing operations, configurations, and differentiated access, the executive sponsor must have the authority to accept changes to policy and prevent access to individuals while shielding operations staff. At the same time, this executive sponsor must have the influence and connections within the business to socialize and gain buy-in from across the organization. Preparing for and driving toward the implementation of Zero Trust requires broad support and involvement from a wide range of teams within the organization. In addition, programs should account for key performance indicators of the business, providing a metric for evaluating how the program is working and what improvements will be needed to get the program off the ground. Both aspects are critical to the success of the program.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with.

The book is organized into 11 chapters and one appendix and covers the following topics:

- **Chapter 1, "Overview for Zero Trust (ZT)"**—This chapter starts by providing an historical overview of Zero Trust. Next, we provide an introduction into Cisco's five Zero Trust capabilities to present the scope of a Zero Trust security infrastructure. Finally, this chapter begins a fictional organization's use case that will be used as you read to give practical examples of each chapter's discussion topics.
- **Chapter 2, "Zero Trust Capabilities"**—This chapter further defines and explores the previous chapter's introduction of Cisco's Zero Trust Capabilities: Policy & Governance, Identity, Vulnerability Management, Enforcement, and Analytics.
- **Chapter 3, "Zero Trust Reference Architecture"**—This chapter presents the Zero Trust Reference Architecture and then breaks down the overall architecture into distinct practical service area locations. Typical service areas explored in further detail includes campus, branch, core network, WAN, and cloud.
- **Chapter 4, "Zero Trust Enclave Design"**—This chapter deals with how the application of a Zero Trust model to an architecture will vary in its construct between different layers of the network, including branch, campus, WAN, data center, and cloud.
- **Chapter 5, "Enclave Exploration and Consideration"**—In this chapter, we discuss and analyze some of the so-called gotchas, or unique attributes, for organizations and industry verticals, and call out considerations.
- **Chapter 6, "Segmentation"**—This chapter examines the aspects of communications before attempting to restrict objects, which is key to a successful Zero Trust segmentation-based deployment.
- **Chapter 7, "Zero Trust Common Challenges"**—This chapter covers many common challenges encountered while implementing Zero Trust.
- **Chapter 8, "Developing a Successful Segmentation Plan"**—As an organization strives to develop a plan of how to classify and segment endpoints while maintaining business as usual, this chapter helps organizations plan for the future of Zero Trust.
- **Chapter 9, "Zero Trust Enforcement"**—This chapter examines a practical plan for how an organization might align with a stepwise approach and ensure that when an enforcement mode for a security-based mindset is reached, an organization can have confidence that as much due diligence as possible has been done to be successful.

- **Chapter 10, "Zero Trust Operations"**—This chapter covers the fundamentals of what should happen when a Zero Trust environment enters a steady operational state, the network and assets are still monitored, and traffic is logged and audited.
- **Chapter 11, "Conclusion"**—Utilizing the five core principles of Zero Trust presented here is a great starting point. However, continuous improvement and reuse of each principle throughout an organization's journey will be key to the ongoing success of Zero Trust.
- **Appendix A, "Applied Use Case for Zero Trust Principles"**—This appendix provides use case examples of an organization's journey that will be key to the ongoing success of Zero Trust.

Chapter 2

Zero Trust Capabilities

Chapter Key Points:

- This chapter provides an overview of the five pillars of Zero Trust, including how to overlay policy, being identity-led, providing vulnerability management, enforcing access control, and providing visibility into control and data plane functions.
- We provide ways to identify what Cisco defines as Zero Trust Capabilities and where to start looking in the organization for these capabilities.
- We also provide an extensive reference, or "dictionary of capabilities," that can be used for many efforts within an organization.
- Capabilities outlined in this chapter may be broken down further, but for the purposes of achieving Zero Trust, the book focuses on the critical capabilities needed.
- We establish a foundation to build Zero Trust into an organization.

The cornerstone to creating a Zero Trust strategy is to identify the capabilities of an organization using a focused process to identify how well a capability is addressed by reviewing technical administration capabilities, functional cross-organizational process capabilities, and overall adoption of the capabilities.

By reading and referring to this chapter of the book, you will be able to identify what Cisco defines as Zero Trust Capabilities as well as where to start looking within an organization for these capabilities. The organization will need to review its requirements related to policy creation and fulfillment, along with what is deemed critical infrastructure, to define the overall risk tolerance for issues or gaps.

After a risk tolerance level is established for the organization, an assessment of the available capabilities should be performed. Risk assessments are often performed by an outside organization to remove critical biases and to enable all parts of the organization to consume the findings of the assessment. Priorities and gaps that are identified should establish a strategy for going forward and a roadmap for a Zero Trust–driven organization.

Following chapters in this book outline use cases, methods, and best practices to implement Zero Trust, as outlined in this critical foundational chapter.

Cisco Zero Trust Capabilities

The pillars of the Cisco Zero Trust Capabilities, as outlined in Figure 2-1, represent various capabilities that are necessary for a successful Zero Trust strategy. These capabilities are not all inclusive but function as the minimum required set of capabilities necessary. Some organizations may need more specific capabilities relevant to their unique use cases.

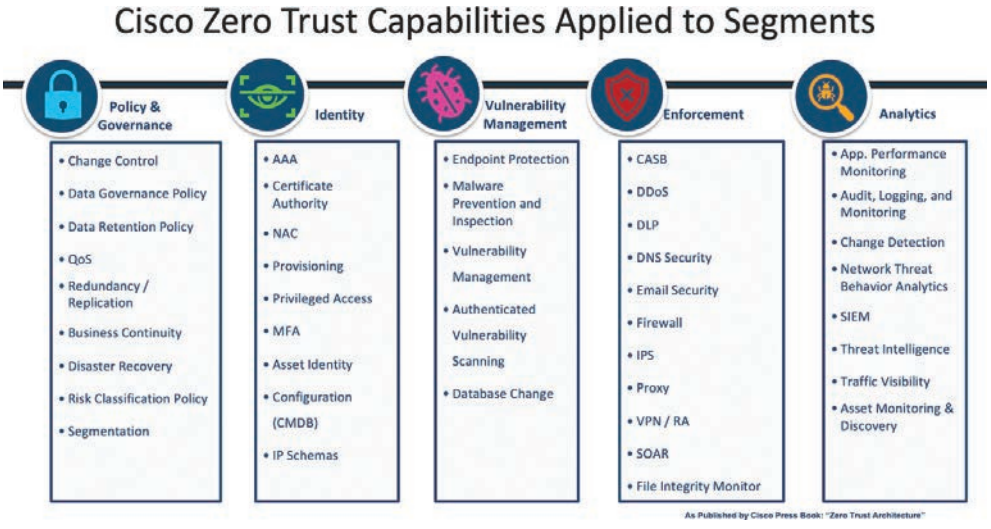


Figure 2-1 *Cisco Zero Trust Capabilities*

This chapter develops your understanding of each capability and what that capability can be used for within an organization to move toward developing a stronger security posture against would-be attackers. We begin with the Policy & Governance pillar because it establishes what can or cannot be done within the organization. We then move to the Identity pillar, which establishes the identity of not only users but also devices, transport, and many other object types. It cannot be understated how important Identity is to establish a stronger security posture.

The Vulnerability Management pillar enables organizations to identify, track, and mitigate known vulnerabilities to reduce organizational risk. The Enforcement pillar capabilities are what traditionally are thought to be security operations center (SOC) or network operations center (NOC) tools; however, as the team reviews these capabilities regarding Zero Trust, you will see that these capabilities extend beyond these groups and are used or managed by multiple teams throughout the organization. In the Analytics pillar, we review how an organization can see what is happening to objects and what is acting upon them inside and outside of the environment.

Having well-established governance, identity stores, vulnerability management, enforcement, and visibility capabilities enables a Zero Trust strategy.

Policy & Governance Pillar

Finding the right balance of security and business enablement is a crucial requirement for any Zero Trust strategy. The primary category to help achieve this balance is the Policy & Governance pillar of Cisco's Zero Trust Model. With the Policy & Governance pillar, an organization may establish how tightly the entire organization is governed, how long information is retained, how the organization will recover in an emergency, and how important sets of data are managed from group to group. Organizations also need to focus on their industry, their regulations, the organization and its business goals, and their customers' risk tolerance levels. The Policy & Governance pillar focuses on key factors that must be established to enable the Zero Trust journey.

Change Control

It is necessary for many organizations to have change management services. Many use the Information Technology Infrastructure Library (ITIL) change management process. ITIL is an accepted approach to managing Information Technology services to support and enable organizations. ITIL enables organizations to deliver services. Frameworks such as ITIL help establish architectures, processes, tools, metrics, documentation, technology services, and configuration management practices.

Changes must be coordinated, managed, and details disseminated to relevant parties. A unique characteristic of Zero Trust means that changes will occur end to end within the environment, so special care must be paid to ensure smooth forward progress. As a critical part of the change process, testing provides the ability to ensure that production deployments in support of Zero Trust can be accomplished in a timely and effective fashion.

Data Governance

It's critical to classify data and to understand where it is stored and how it is monitored for compliance to organizational policies. Some examples of data classifications are personally identifiable information (PII), Electronic Protected Health Information (ePHI), Payment Card Information (PCI), Restricted Intellectual Property, and Classified Information. Data governance also includes a well-defined and maintained configuration management database that contains where all data stores are located, who owns them within the organization, along with data classification, labeling and storage, and access requirements.

Data Retention

Data retention is dictated based on organizational and regulatory requirements. After an incident, the ability to determine the cause of an outage or breach is critical information that must be retained both for restoration of service as well as audit purposes. Data retention must consider data at rest, how long the data must be stored, and when the data should be purged to limit organizational liability. The legal and compliance teams of the organization manage policy requirements on what data an organization must retain and for how long.

Quality of Service (QoS)

Quality of service, including the marking and prioritization of key traffic in times of micro or long-term congestion, is a key component of availability to ensure that control plane traffic continues to flow to ensure Zero Trust capabilities function as intended. QoS provides for preferential treatment of traffic to meet defined policy requirements to ensure that critical functions necessary for security and business functions continue without undue impairment. Without this safeguard in place, organizations run the risk of congestion on the network having unpredictable impacts to traffic and the solutions that rely on that traffic.

Redundancy

Redundancy is necessary to maintain availability and is part of a Zero Trust strategy. Critical components of the ecosystem are required to be duplicated by many frameworks, standards, regulations, and laws. Redundancy can have multiple aspects: control plane redundancy is necessary for the functioning of capabilities, whereas data plane redundancy is necessary to ensure that business functions continue unimpeded.

Replication

Replication involves the duplication and the encryption of key data stores to backup storage arrays and offline storage backups, which provide a restoration path in the event of partial or complete loss of an environment due to ransomware. Software automation is necessary to ensure that the proper environments are replicated to proper locations. Without replication automation, errors are inevitable, and critical data stores may be overwritten, creating a large-scale outage requiring full restoration of one or many databases.

Auditors, regulators, or governing bodies routinely validate these controls. The key point to note is the regulations, standards, or laws are the minimum of replication that should be in place for the organization. Protecting an organization's data is its top concern. Without protective controls—that is, encryption and locations around these replicated data stores—there can be no data integrity, confidentiality, and in the end availability; therefore, a gap in Zero Trust is created.

Business Continuity

Confidentiality, integrity, and availability are the foundation of all security programs and are necessary in a Zero Trust strategy. Business continuity relies on a well-executed Zero Trust strategy. The development of business continuity teams and business continuity documentation that can be accessed by the critical teams in the event of a crisis is a cornerstone to business continuity. Please note that a business continuity plan (BCP) should always be protective of human life first, in all cases. Ensure teams are safe at the outset of plan activation and throughout the event. A well-developed communication plan will assist in locating and checking in on those associated with the organization. The plan should also be protective of what is shared publicly to provide a level of protection to recovery efforts.

The second most important step is maintaining the integrity of data in the middle of responding to a business continuity event. Maintaining data integrity may seem trivial to some of those responding to a critical event, but that is exactly when an attacker will attack. Ensure "temporary" controls or measures do not expose the organization to issues with data integrity along with availability. Some ransomware attacks may activate the business continuity plan and be the cause of an organization-level outage. Restricted or intellectual property may be at risk.

Work out these scenarios in advance and partner with your nearest fusion center and other government entities to respond to these critical types of events. Tabletop exercises may expose gaps, but putting teams through BCP drills reveals how prepared teams are to respond and may uncover shortcuts that could expose the organization's critical data stores.

Disaster Recovery (DR)

Typically, a disaster recovery event is activated as soon as a problem has been detected, but many times the business continuity plan (BCP) should be activated. After the BCP team assesses the situation, recovery efforts are officially started. The DR plan may include many of the same contacts from a leadership perspective as the BCP does, but the DR plan focuses on recovering a solution, a set of solutions, or the critical infrastructure of the organization.

The scope of any DR event may be assessed and categorized as minor, or it could go more broadly. At first, the event may impact only one aspect of the business or even one solution, but this is where teams should not have tunnel vision and should consider other systems and environments that could be also impacted. Activating the proper process and notifying the right level of leadership is a function of the business continuity plan based on impact and risk. It is important that proper criteria have been established for DR planning, primarily the criticality of the system to the organization and impact upon daily functioning and therefore the acceptable limits of data loss and recovery time. This is normally classified into two categories, recovery point objective (RPO) and recovery time objective (RTO). RPO defines the amount of time acceptable for transactional data loss. Stated another way, RPO is the amount of data or work that will be unrecoverable

after a system failure. RTO, on the other hand, is the amount of time it takes to restore the system and data back to normal. These are minimum variables that should be defined for each system where it is determined that DR capability is required.

DR plans go hand in hand with the business continuity plan. With proper controls as defined in the "Policy & Governance" section of the book, disaster recovery should be achievable and complete. Development and testing of a DR plan are part of the standup procedures for new environments. Each environment must define a method of recovery prior to "production go-live" events so the definition of what constitutes a successful recovery can be worked through and can be checked off as complete during an actual DR event or during a DR test. If the plan is not created after the application has been purchased, many installation requirements are forgotten, neglected, or known by only a handful of individual team members. Testing of the DR plan is required for both new and old ecosystems. The adage still holds true: "If there is no testing, there is no DR plan." Adding to that, without a business continuity plan and a disaster recovery plan, there cannot be a valid and implemented Zero Trust strategy.

Risk Classification

Risk classification helps inform multiple other capabilities such as data governance, business continuity, and redundancy. This includes classifying the risk for data as well as capabilities. For data, risk must be assessed to understand the criticality of the data to the organization. For capabilities, risk must be classified to understand what impact to the organization may occur if that capability ceases to operate as expected.

Risk classification structures should be developed with compliance and legal teams to ensure that the business is protected and to ensure business continuity. Having a Zero Trust mindset as these classifications are developed or updated will go a long way to provide greater protections and controls put in place, while at the same time enabling the business.

Identity Pillar

Identity is a concept to represent entities that exist on a network and is analogous to what an entity *has* or *is*. Sometimes, entities may offer a configured or known credential, while other times they do not. Identity alone is not enough to gain access to data. Determining identity is a fundamental process of authentication. Organizations using an identity alone as a basis to grant access to an object from a central authority are not

aligning to a full Zero Trust strategy, because full context of the identity has not been established. As an example, possessing a driver's license as identification does not allow anyone on an airplane. Someone or something must verify the identification matches the entity attempting to use the license against valid confirmation information.

Authentication, Authorization, and Accounting (AAA)

What is meant by the phrase "Triple A"? In simple terms, *authentication* is a validation of the "who" or "what" of an entity, *authorization* is the set of resources or data to which the authenticated entity can access, and *accounting* is the record of interactions that occur throughout the operation.

The first step for any entity accessing the network is to authenticate. This step requires that the entity requesting authentication—be it a person, computer, or any number of other networked devices—must provide details about itself in at least one form. These details may be provided directly by the entity, for example, using a username and password, a certificate, or a MAC address provided by the entity.

Authentication can be accomplished using multiple criteria, which is referred to as multifactor authentication. The process of authenticating does not imply the permissions to which the entity may interact. Take, for example, an ATM: anyone can walk up to one with a valid debit card and insert it into the machine. With the proper PIN code, the user will authenticate, but the possession of the card and PIN code does not explicitly provide details to which accounts that person should have access, which leads to the second "A," authorization.

Authorization involves taking the identity of the authenticated entity and, in combination with other conditions, determining through a defined policy what level of resource or data access should be provided. Depending on the policy engine in use, these conditions can become quite granular. Some examples of additional conditions for authorizing network access might include device health or posture, a directory service group membership, time and day variables, device identity, or device ownership. Going back to the ATM example, after authentication, the customer is provided access to their accounts after a policy engine makes the necessary determinations, such as permission to view and interactions allowed with each account.

Finally, accounting is a way to record the actions an entity on the network takes for audit purposes. This includes documenting when the entity attempts to authenticate, the result of that authentication, and what interactions are made with the authorized resources and ends after the entity disconnects or logs off from the network. This accounting data is crucial for both troubleshooting and forensic purposes. In troubleshooting, it provides valuable data to help identify where in the process of AAA the entity is encountering a problem, such as why they are not getting authorized to expected data or resources. For forensic purposes, it provides the ability to understand when an entity accessed the network, what actions were taken, and when it disconnected or if it is still connected to the network.

AAA Special Conditions

It is also important to mention the challenges for AAA brought about by the rapid increase in Internet of Things (IoT) devices. In most cases, these devices operate in a more rudimentary fashion when it comes to network connectivity and may not be capable of providing a username and password for authentication, much less a certificate. In some cases, while these capabilities may be available from the device, a lack of suitable management may make use of these features not technically feasible. In either case, it is important to ensure that alternatives are available to authenticate and authorize these devices effectively and safely. Commonly, this will mean using the MAC address to authenticate the device against a database, and authorization will follow a similar set of conditions as for other entities. There are numerous efforts underway to improve the interaction of IoT devices, especially regarding enterprise networks, such as the Machine Usage Description (MUD) attribute, which provides the purpose of the device to the policy engine. Ultimately, though, these devices can be more easily spoofed when authenticated through MUD or MAC address-based paths, so caution must be taken. This lower level of confidence in positive identification and authenticating the entity in detail means special thought and care must be taken when assigning authorization to resources or data.

Certificate Authority

An alternative but slightly higher overhead for identifying devices uniquely within a network is the ability to present a certificate. A certificate, simply put, is a unique identity issued to a user or endpoint, which relies on a chain of trust. This chain of trust consists of a centralized authority being the root of the trust, and branches in a tree-like structure providing for distributed trust the world over. Issuance of a certificate to endpoints or to users provides for an "I trust this authority, and therefore I trust this entity" ability.

Certificates are typically considered a stronger method of authentication because of the ability to both prevent exportation of the identity and providing for the ability to validate the identity presented within the certificate against a centralized identity store—for example, Active Directory, which is the Microsoft Directory Store; Lightweight Directory Access Protocol (LDAP), which is an Open-Source Directory Store; or Azure Active Directory Domain Services (Azure AD DS), which is cloud-based.

By blocking the private aspects of the certificate from being exported, the certificate cannot be shared with another user or even another device, making it a secure identification mechanism. In addition, like directory service attributes, alternative names and attributes can be added into a certificate that can be used to uniquely identify an endpoint and what access the device should be provided on the network.

Certificates are typically exchanged with the policy engine via Extensible Authentication Protocol–Transport Layer Security (EAP-TLS). These certificates can be assigned to either the endpoint or the user itself. The combination of user and machine certificates creates a unique contextual identity. This contextual identity provides differentiated access based on the attributes associated to the type of identity, whether that be user, application, or machine.

Network Access Control (NAC)

A network access control system provides a mechanism to control access to the network. There are many solutions available to provide this Zero Trust Capability to maintain control of who or what accesses the network for any organization. The NAC system needs to have the ability to integrate with the other Zero Trust Capabilities, described within this chapter. The NAC system will directly participate in the Policy & Governance, Identity, Vulnerability Management, Enforcement, and Analytics pillars. Policy & Governance must influence the configuration of the NAC system.

After a device is purchased, onboarded, and identified, there needs to exist a database and policy engine to validate the identity using AAA (see the previous section). This policy engine should contain

- Integrated authentication into a directory service
- Endpoint posture for vulnerabilities
- Ability to control endpoint access via policy

For example, with identity, there is a reliance upon Directory Services, or a certificate authority, which requires that the NAC system integrate with the identity store to determine and enforce AAA. NAC should utilize this identity to link vulnerability into the contextual identity, then apply and enforce controls, and then log these actions locally or to an integrated system, such as a Security Information and Event Management (SIEM) system. Logging events being generated in the NAC system requires collection of what was done and why to be able to better analyze devices on the network and their potential security implications to the network.

Provisioning

Provisioning is a process to acquire, deploy, and configure new or existing infrastructure throughout an organization based on Policy & Governance. Provisioning heavily impacts the decision-making process when implementing a Zero Trust strategy. Provisioning happens in multiple phases across multiple groups in the environment. All stakeholders must understand the importance of a unified policy and process.

Organizations define their own needs to meet specific requirements. A comprehensive Zero Trust strategy requires a wholistic approach that addresses the flexibility needed in the process and while maintaining tight controls that enforce the policies of the organization and regulating bodies. Proper provisioning practices dictate that a common form of tracking and visibility of access needs should be documented during all stages of the infrastructure life cycle. The following sections detail some Provisioning policy enforcement categories to consider.

Device

Some common device types range from printers, computers, IoT, OT, specialty equipment, and managed, and not managed. Groups responsible for creating, maintaining, and

executing these functions exist in almost every facet of an organization. Devices need to respect the presence of Zero Trust controls in any physical, logical, or network environment.

User

Users can exist in many parts of the organization but, unlike devices, should all be controlled within a defined role within the organization. User identities created for third parties must map to a role with the organization. Access for devices, people, and processes relies on these role-based user accounts. These accounts may represent multiple roles for differing functions. Zero Trust relies upon user identity, which is an important attribute in aligning policy to an action. "User" is a component of the Zero Trust Identity Capability for user attribution, assignment, and provisioning and builds a foundation for establishing trust.

People

A Zero Trust strategy should inform and guide all onboarding and offboarding processes within an organization of each entity. People have the potential of becoming soft targets and therefore vulnerabilities to the organization. Security threat awareness, training, and testing help build resilience within the people who work for the organization. The scope of provisioning as it relates to people applies not only to those with access to systems. Provisioning of users, devices, access, services, assets, and many other important aspects of provisioning are affected through these processes. Zero Trust controls attempt to apply attribution to any interaction with people throughout the organization, third parties, or partners. These concepts can branch out to encompass interactions with any asset by a person to any connection.

Infrastructure

The Identity of infrastructure objects defines what an object is, what an object needs to function, and relates the object to what are valid activities of the object to support the organization.

Infrastructure provisioning processes create the pathways through which access to objects occurs. Administrators need to define what protections are needed to enable the use of the infrastructure to support the user community and the functions of their role. Administrators tasked with supporting the infrastructure mediate how and when provisioning steps interact with services and flows.

Services

Services enable an application or a suite of applications to support and allow users to fulfill their defined user role within the organization. Without services, there is no point in giving a user access to an application. The services attribute for Identity capabilities is used to define access attributes for users to be able to execute critical functions assigned to their roles.

Service Identity provisioning processes interrelate devices, users, people, and infrastructure to further build contextual identity capabilities. Documenting the access requirements and restrictions associated to devices, users, people, and infrastructure creates policy that can be directly enforced by Zero Trust. Services rely on consistent and accurate identity information derived from provisioning to define these policies in an effective manner. Access denial and access acceptance are attained through the documentation of these identifiers and classifying what is allowed to utilize the service and under what conditions the service is being requested.

Privileged Access

Privileged access is elevated user access required to perform functions to support and manage systems. Privileged Access can be found within any portion of the infrastructure, including network appliances, databases, applications, operating systems, cloud provider platforms, communications connectivity systems, and software development. Privileged access should follow the concept of "least privileged access" and should be limited to a very small population of users. Types of users leveraging privileged access include but are not limited to database administrators, backup administrators, third-party application administrators, treasury administrators, service accounts, and systems administrators, along with network and security teams.

Privileged access introduces higher risk to data, availability, or controls. Privileged access may be leveraged by attackers to cause the most damage to an environment, ecosystem, or proprietary information, making this type of Identity what an organization should highly guard, monitor, and control.

To monitor and control privileged access, solutions are available to control this higher level of access, with timers to allow access, and stronger controls, including the logging of changes made while leveraging privileged access levels of Identity. It is recommended that organizations audit the use of privileged access on a routine basis with management oversight and signoff. Many regulations and laws require privileged access controls be put in place within an organization, with demonstrable compliance to external auditors on a routine basis. Teams should review the requirements for their organization based on regulations and legal team guidance.

Multifactor Authentication (MFA)

Multifactor authentication is the practice of leveraging factors of what a user knows (i.e., password), what a user has (i.e., managed device or device certificate), who a user is (i.e., biometrics), and what a user can solve (i.e., Captcha with problems); it is a foundational principle of Zero Trust. These aspects allow for many interpretations, and therefore, the Policy & Governance pillar needs to address the requirements of MFA within a given organization that are pushed out to all users of the environment.

Classical usernames are identifiable through email addresses, and passwords may not be well configured by users or are reused on many systems, making them easily vulnerable to brute-force attacks. By leveraging additional factors of MFA, organizations increase

their resistance to attack; however, strong onboarding/offboarding of employees, interns, and contractor processes with monitoring and auditing is required to maintain control of identity stores and MFA factors and to limit unauthorized access.

In some cases, organizations may want to move to a true "passwordless" access control methodology using only device certificates to increase convenience to the user population. It is recommended that organizations review this method with legal teams and regulating bodies prior to moving to a true "passwordless" approach. For example, for most operating systems, after the user logs in to the machine, a supplicant is presented a certificate as an authentication mechanism to a policy engine. Are a user login and a device certificate enough for the organization and the regulations with which they are required to comply? These challenges to defining MFA may occur, so organizations should be specific on whether MFA is two or more of the same factors or a unique combination of factors. These details need to be specified by the organization via Policy & Governance.

Asset Identity

Asset identity is a method, process, application, or service that enables an organization to identify physical devices that interact with the organization with certainty of the actual real device type, location, and key attributes.

Organizations need to be able to identify all unique assets operating within their ecosystems. Based on the identity of the asset, the metadata adds context that will drive Policy & Governance requirements for the asset type involved or the specific asset that is necessary for a Zero Trust strategy implementation. Examples of assets that are critical for identification are not limited to servers, workstations, network gear, telephony devices, printers, security devices, and low-powered devices.

More difficult to identify are assets that include devices that do not respond to requests for unique identity like low-powered devices. These devices may not have a supplicant, or even conform with standardized RFCs dictating the format, frequency, and protocol for responses. In these cases, unique asset attributes need to be used to identify the endpoint. Passive abilities are available to identify an endpoint and have been built into standards used to manufacture devices. The unique MAC address embedded into a device's network interface card (NIC), for example, has the first 24 of 48 bits reserved to uniquely identify the manufacturer of that endpoint against a known database of registered and reserved organizationally unique identifiers (OUI). The MAC address is a data element in standard configuration management databases.

Configuration Management Database (CMDB)

A configuration management database is an important repository of critical organization information that contains all types of devices, solutions, network equipment, data center equipment, applications, asset owners, application owners, emergency contacts, and the relationships between them all.

Whether the attribute used is the MAC address of an endpoint, a serial number unique to an aspect of the endpoint, or a unique attribute assigned to the endpoint or combination of its properties, a CMDB or an asset management database (AMDB) should exist to ensure that devices, services, applications, and data are tracked and provide critical information to respond to important events or incidents.

The information contained within the CMDB ensures that solutions may reference the data in the CMDB to control access to only authorized objects. Discreet onboarding processes are required to support a Zero Trust strategy. A description of exactly what needs to be known when an endpoint is put onto a network, with roles, responsibilities, and with updating requirements, is part of a mature organization's Zero Trust profile.

The use of a consistent onboarding process will ensure an optimized and efficient onboarding process can be practiced. This consistent onboarding process ensures that similar provisioning practices are followed across unique vendors, and configurations are applied in a consistent way to identify entities within the network. While variations may occur in devices, even from the same vendor, consistency in identifying the device in alignment with an onboarding process will lead to a notable change in security posture. Critical elements to review when differentiating devices or device types include

- Firmware versions
- Base software versions
- Individual hardware component revisions
- Organizational unique identifier (OUI) variation for NICs

Internet Protocol (IP) Schemas

The Internet Protocol schema provides identification of services or objects via unique IP addresses. Necessary to any Zero Trust Segmentation program is having an IP address schema or plan to enable communications from workload to workload, within and outside of an ecosystem. Organizations should not focus specifically on the IP address to create a Zero Trust Segmentation strategy, but rather use an IP schema as another tool in an administrator's toolbox to assist in identification of workloads and/or objects.

Another consideration is whether an organization should use provider-independent (PI) or provider-aggregated (PA) IP space to improve the security profile, while potentially adding an additional benefit of the organization easily moving from one provider to another.

Most organizations prefer to go with a provider-independent IP space. As stated in the technical paper "Stream: Internet Engineering Task Force (IETF)":

> a common question is whether companies should use Provider-Independent (PI) or Provider-Aggregated (PA) space [RFC7381], but, from a security perspective, there is minor difference. However, one aspect to keep in mind is who has administrative ownership of the address space and who is technically responsible if/when there is

a need to enforce restrictions on routability of the space. This typically comes in the form of a need based on malicious criminal activity originating from it. Relying on PA address space may also increase the perceived need for address translation techniques, such as NPTv6; thereby, the complexity of the operations, including the security operations, is augmented.

Best practices to create a stable IP space environment include implementing an addressing plan and an IP address management (IPAM) solution. The following sections detail the three standards of IP addressing spaces that can be used to create or combine to create an IP Schema.

IPV4

Internet Protocol version 4 addresses, better known as IPv4 addresses, enable workloads to communicate over public mediums utilizing a standardized 256-bit addressing standard. It is well known that the world is running out of IPv4 addresses, and this has become a driver for organizations to move to IPv6.

IPV6

IPv6, with its standardized 128-bit address, is expected to be almost inexhaustive with the ability to assign an address to every square inch of the earth's surface. This direction to implement IPv6 is difficult and should not be entered into without a well-vetted plan. This is further complicated by a need to map out significantly more address space within IPV6, typically a 56- or 64-bit allocation to a given organization, and the flows between endpoints within the address space.

To begin, a directional plan to move to IPv6 has become a legal matter and requirement for some organizations in recent years. Workload communication over IPv6 is becoming necessary, especially when working with public sector agencies. Working on a Zero Trust migration and an IPv6 migration in the same program is a daunting task. A recommendation would be to develop a roadmap to making incremental improvements over time. As part of these incremental improvements, and especially as organizations start to roll out IPv6 greenfield, a mapping of communication for how endpoints interact with each other across their respective communication domains is highly recommended. While most engineers and administrators inherited the design or design standards for IPv4 networks, organizations have a unique opportunity related to IPv6 and its ability to be part of a security strategy.

Each workload that gets an IPv6 address and can communicate over IPv6 also has a unique identity that can be associated back to IPv6. With such as a massive address space available within IPv6, identity can be tied back to the addressing, or at least associated as another tool in the network engineering toolbox.

Dual Stack

In many cases organizations need to use IPv6 address space in a "dual stack" implementation that includes IPv4 addresses, as well as IPv6 addresses to enable a transition.

In the case that a transition must be managed as a dual stack, this process requires double the work for administration teams. Implementing dual stack requires that each workload gets an IPv4 and an IPv6 address and can communicate over IPv4 or IPv6. This dual stack process can create a high degree of administrative overhead, including mapping out addresses, designing recognizable subnets or network architectures, and managing network devices by applying the same identity and policies to two separate addresses. Being in this dual phase of implementation tends to go on for several years or is a permanent method to manage the organization's IP address issues.

Vulnerability Management Pillar

The Vulnerability Management pillar refers to the Zero Trust capability to identify, manage, and mitigate risk within an organization. Effective implementation of vulnerability management requires well-defined Policy & Governance practices that are integrated into the solutions used to manage vulnerabilities. A Vulnerability Management organization needs to be established within the organization using best practices, such as the ones found in the Information Technology Infrastructure Library (ITIL) or those provided as part of the NIST Cybersecurity Framework. Many regulations, laws, and organizational policies rely on effective Vulnerability Management processes to classify known risks, to prioritize these risks for mitigation, to enable leadership to own these known risks, and for response to regulating bodies.

Endpoint Protection

An endpoint protection system not only provides the capability to detect threats such as malware but also provides the ability to determine file reputation, identify and flag known vulnerabilities, prevent the execution of exploits, and integrate behavioral analysis to understand both standard user and machine behavior to flag anomalies. It may also provide some level of machine learning, which can attempt to prevent zero-day malware or other endpoint attacks by monitoring for attributes that are common for malware, relying less on published intelligence data.

Endpoint protection should be able to monitor the system to detect malware and track the origination and propagation of threats throughout the network. Each individual endpoint protection agent has a small view of the environment in which it is connected. However, when data is aggregated between devices and combined with network-level monitoring, it is possible to provide a more complete picture of how a piece of malware enters, propagates, and impacts a network.

Endpoint protection should be able to provide a clear picture as a piece of malware enters and begins to spread through the network. Systems that can run endpoint protection will begin to detect and restrict the actions of the threat, while at the same time beginning to generate alarms. Systems will begin taking retrospective actions to understand where a malicious file originated. This in turn provides the ability to aggregate this data across all the protected endpoints and network monitoring systems, making it possible to illustrate the entry point and impacted systems until its detection.

In other considerations around the endpoint, the protection must extend beyond the endpoint itself. An example of this would be that it is rare to find any enterprise network that does not have Internet of Things (IoT) or operational technology (OT) endpoints. These endpoints may be part of a building management system, such as thermostats or lighting control features, or programmable logic controllers running conveyer systems in a warehouse. The commonality between IoT and OT is that both will be unable to utilize endpoint protection applications, and therefore administrators must rely more heavily on all the other controls available to provide protection. It may be difficult at first to understand how an endpoint protection application on a desktop could help protect a thermostat, but this capability comes down to the forensics being available in these systems.

Malware Prevention and Inspection

Malware is one of the most prevalent threats facing organizations. Due to this widespread usage of malware and its targeting of businesses for monetary gain, organizations cannot solely rely on malware prevention to occur at the endpoint. This is especially true when considering the number of IoT and OT endpoints that cannot run endpoint protection systems. Therefore, it is imperative that malware prevention be layered throughout the ecosystem, deployed on dedicated appliances, or in combination with other security tools. As discussed with endpoint protection, these network-level malware prevention and inspection capabilities must be able to integrate and work in concert with other systems to provide the greatest possible benefit. If the ecosystem can detect malware, it can then communicate this with connected endpoints to alert them of both the presence and type of malware to allow each endpoint to act against the threat. In addition, inspection systems can alert administrators to the threat and begin response efforts if the systems are unable to address the threats automatically.

An additional strength provided by malware prevention and inspection systems is the ability to have a central control point for scanning and blocking of malware. By placing a malware prevention and inspection system prior to a manufacturing network with OT endpoints, for instance, it allows for greater risk mitigation for those business-critical endpoints that are incapable of running their own malware prevention tool sets. As data moves in and out of these segments, malware can be quickly identified, and other connected systems and administrators can begin to take action to remove the threat to keep the organization running. Defense-in-depth means that malware prevention and inspection must occur as often as possible and be well integrated to the overall security ecosystem of an organization to achieve Zero Trust.

Vulnerability Management

Vulnerability management systems fulfill the role of identifying when exploits are possible on a system due to misconfigurations, software bugs, or hardware vulnerabilities. As technology advances in capability, software must become more complex to provide the features that can take advantage of these additional capabilities. At the same time, this software is being developed too quickly to maintain quality, leading to mistakes or oversights, known as bugs or vulnerabilities. From a security viewpoint, there are many instances where these bugs do not pose a problem, but as complexity and the pace of development increase, the quantity of bugs will increase as well, and it is inevitable that some of these bugs will be exploitable. Proactive discovery of these exploits and the ability to remediate before they can be leveraged by an attacker is of paramount importance to protecting an organization. The larger the organization, the greater the importance of a vulnerability management system to allow administrators to quickly ascertain the health of software deployed and identify these exploits as soon as they are made known.

The number of applications that are installed in an organization may not be always known. It is common for the count of applications to be well into the thousands, requiring operations staff to try to identify when each of these applications may be vulnerable to an exploit. Visibility, automation, and AI are required to support and scale vulnerability management teams due to the sheer number of objects within an organization. Vulnerability management systems provide the ability to scan the network and endpoints consistently and reliably against a database of known threats that is continually updated. These systems provide the automation and scale necessary to look across thousands of endpoints and their applications to understand what software is present, the vulnerabilities within that software, and to monitor the remediation efforts as patches or other upgrades are undertaken.

A vulnerability management system should also provide the ability for administrators to quickly understand and prioritize the vulnerabilities present. It is not enough to just rate the threat from a vulnerability based on its impact but should also factor in how often attackers are leveraging the exploit, the level of complexity to exploit, and the number and criticality of the systems that are vulnerable. Zero Trust strategies rely on context for decision-making, and vulnerability management is no different. If the particulars of an organization cannot be factored into the exploit analysis, administrators run the risk of spending precious time remediating exploits that would realistically have minimal to no risk to the organization and delay actions against those threats for which they are truly vulnerable. Some of these lower-risk items may be already appropriately mitigated and should be tracked, along with other mitigated risks, as part of a residual risk database. Residual risk is a method to track any remaining risk after evaluation of security controls and mitigations are completed because it is not possible to completely remove all risk in most scenarios.

Authenticated Vulnerability Scanning

Authenticated vulnerability scanning, where a vulnerability scanner is provided valid credentials to authenticate its access to the target system, is a major component of a

well-rounded vulnerability analysis program supporting a Zero Trust strategy. On its face, vulnerability scanning seems logical: scan the network and look for known vulnerabilities that could be exploited so that the organization has visibility into what should be fixed. Authenticated vulnerability scans, though, are a bit less obvious to some, with frequently posed questions like Why should I bypass security I already have in place? Or does it really matter if there is a vulnerability where I have security mitigations like multifactor authentication in front of my application? It's important though to separate the concept of authenticated vulnerability scanning from penetration testing. For the latter, allowing access through authentication controls would defeat the purpose, but the goal of authenticated vulnerability scanning is to gain better visibility into an organization's current level of risk. Authenticated vulnerability scanning is just another layer of a defense-in-depth strategy that allows a closer look at the vulnerabilities in an application that may otherwise be protected only by a username and password. Most security professionals would agree that relying only upon a username and password would be unwise, which highlights why authenticated vulnerability scanning must be a part of any Zero Trust strategy.

These authenticated scans remove the blind spot and provide insight into the true level of risk of an application or system. Once an attacker has made it onto a system, even if the account compromised has minimal privileges, other exploits may easily allow for additional actions to be taken utilizing the initial target as a jump point. Common exploits include privilege escalation or the ability to gain further visibility to other assets for pivot opportunities to spread deeper into the network, or to more critical systems. By implementing authenticated scans, these vulnerabilities can be more easily identified, and fixes or mitigations can be assessed to ensure that the risk to the organization is both understood and minimized or eliminated, if possible.

Systems such as multifactor authentication or passwordless authentications that rely upon hardware security keys can make the implementation of authenticated scans more difficult. It is important to thoroughly evaluate the scanning tools to be used to ensure that they are successfully navigating these hurdles and performing full authenticated scans against the potential targets. Some scanners may report a successful scan, dependent on configuration, even if part of the authentication fails or the entire scanning session does not maintain authentication. It is therefore imperative that the scanning platform is accurately assessed and that threat feeds are updated and regularly reviewed to ensure that configurations meet the vendor best practices and are providing the visibility expected by the organization. In certain cases, it may be appropriate to leverage multiple scanning platforms or related tool sets, such as endpoint protection systems, dependent on network and application architecture.

Unauthenticated vulnerability scanning essentially provides a "public" view of potential vulnerabilities that may exist on the scanned system. This view represents what a malicious attacker would have access to without user credentials. These scans typically discover fewer vulnerabilities because they don't have access to user-level services.

Database Change

Acting as critical repositories of data regularly accessed by both employees and customers, databases are some of the most important knowledge repositories of an organization and may be commonly referred to as the "crown jewels" of the organization. The content of these databases can vary greatly, such as internal employee data for HR teams, product designs, customer data generated from an ERP system, company financials collected for accounting and executive teams, and system audit logs utilized by IT teams.

The scope and breadth of these databases means that many tend to be both very large in size and numerous in count for most organizations. Both their criticality to the smooth functioning of an organization, as well as their size and scope, can make them enticing targets for an attacker and are critical for organizations to ensure the integrity and confidentiality of the data stored. Data integrity and confidentiality are critical for ensuring that business decisions are made from sound data sources. By controlling risk and unauthorized access surrounding databases, the organization is protected from fines being applied by regulating bodies. Database change monitoring is therefore a critical component of Zero Trust to ensure that data is reliable and available when needed.

A Zero Trust strategy must incorporate robust monitoring of database systems to monitor for unexpected changes to any database, whether it be malicious or inadvertent to identify threats both due to a targeted attack as well as misconfigurations or other user errors that might introduce problems into the database or its operation. These monitoring systems must be able to quickly detect the changes in behavior and help to take action to ensure that any impact to the organization is minimized as much as possible. Monitoring database changes can also help to act as a check and balance for other security controls, such as monitoring for the source IP address of an administrator accessing the database and alert if that connection attempt does not take place from a jump box authorized for such a connection.

The selected database change monitoring tool must be able to correlate across multiple databases regardless of their type or location, providing alerts based on the actual usage patterns of the organization to their data rather than the individual database itself. It must also provide an appropriate reporting mechanism that can direct alerts into the organization's chosen ticketing system when human intervention is necessary to further analyze or respond to a detected event. Some systems may also provide other features such as data insights regarding volume and context of data within each database, which can assist with audit scoping. Other features may also include the ability to classify the data stored based on regulatory labels, policies, and vulnerability notifications for the database software itself. Database change solutions may integrate with privileged identity systems to control access end to end with controls applied to specific database fields.

Enforcement

Enforcement is the ability of an organization to implement Policy & Governance rules using solutions, methods, and attributes to restrict and control access to objects within the organization. The ability to enforce policy is a key result of Zero Trust. Building on the Security Capabilities of Zero Trust covered in this chapter, the Enforcement pillar builds controls over the concepts described in Policy & Governance, Vulnerability Management, Identity, and Analytics.

Cloud Access Security Broker (CASB)

A Cloud Access Security Broker typically sits between a specific network and a public cloud provider and promotes the use of an access gateway. These gateways provide information about how the cloud service might be used, and also govern access as an enforcement point. CASBs attempt to provide access control through familiar or traditional enterprise security approaches.

Further, CASBs are typically offered in an X-as-a-Service model at the front door to a cloud presence. This capability allows movements of workloads into a cloud-hosted model while helping to track and manage entity behavior. CASBs can also help to monitor what data flows in through the network-to-network interconnection (NNI). One example of this enforcement control is to allow only encrypted traffic into specific zones.

A CASB can also be useful in dealing with "shadow IT." Due to the ease of setting up a tenant or subscription on a cloud provider, many business units may decide to bypass normal IT processes to obtain cloud-based services on their own, leaving IT with a massive blind spot. CASBs can help by monitoring traffic between an organization's network and cloud service providers to bring these out-of-standard groups into focus and allowing for IT to remediate. This same visibility also allows for some reporting capabilities on the usage patterns of cloud systems by the organization.

Distributed Denial of Service (DDOS)

A denial of service (DoS) or distributed denial of service (DDoS) is a cyber attack that is used to attack an organization by denying access to critical resources. This kind of attack may negatively impact customers, employees, businesses, or third parties given the scope. DoS attacks can originate from anywhere. These attack vectors represent the inability for a targeted system to be used the way in which it was intended.

For networks, intended use relies on a working control plane and a working data plane. The interruption of either could impede the system from working as expected or designed. Most systems that attempt to offer any sort of protection in this area are based on the ability to realize an attack via a signature, which defines the patterns observed in another organization. If the organization is the first to observe the attack "in the wild," then the organization needs solutions to help redirect the traffic to minimize impact via a "sandbox" or other attack response process.

When multiple systems are networked together toward a target, this is known as distributed denial of service (DDoS). The primary difference between a DoS and DDoS is that the organization being targeted may be attacked from many locations at one time. Typically, DDoS attacks are more difficult to mitigate or remediate when compared to single-source DoS attacks.

Data Loss Prevention (DLP)

Data loss prevention is an enforcement point that controls and prevents the loss, misuse, or ability to access data or the intellectual property of an organization. Data is the "crown jewels" of the organization and must be protected using many capabilities and controls.

DLP programs control information creation, movement, storage, backup, and destruction. When the organization maintains inventories of data at rest, having visibility of where this data goes and where the data is allowed to go must be monitored. This data movement implies visibility over networks, static devices, mobile devices, and removable media. Also, DLP programs control what and how data will be retained or destroyed. Strategies for DLP should be developed and approved before technology solutions are employed to control the data.

Domain Name System Security (DNSSEC)

Domain Name Systems (DNS) represent how humans or machines interact with one another. DNS translates domain names to IP addresses so Internet resources can be used. DNSSEC is a protocol extension to DNS that authenticates and/or inspects DNS traffic to maintain policy or protect systems from accessing resources they should not be allowed to access. A DNSSEC system can also be used to protect attackers from manipulating or poisoning responses to DNS requests.

Email Security

Email security represents the ability of an organization to protect users from receiving malicious emails or preventing attackers from gaining access to critical data stores or conducting attacks (for example, ransomware attacks.) Email security typically complements any ability to prevent data loss by monitoring outbound email.

Email is a common threat vector that enables attackers to communicate to end users who may not have security threat awareness practices at the top of their minds. It is important to remove malicious emails using security solutions prior to an end user interacting with the email to reduce risk to the organization.

Firewall

A firewall is a network security device that monitors incoming and outgoing boundary network data traffic and decides whether to allow or block specific traffic based on a predefined set of security rules. The general purpose of a firewall is to establish a barrier between computer networks with distinct levels of trust. The most common use of a firewall is to protect a company's internal trusted networks from the untrusted Internet. Firewalls can be implemented in a hardware-, virtual-, or software-based form factor. The four types of firewalls are as follows:

- **Packet Filtering:** Packet filtering firewalls are the most common type of firewalls. They will inspect a data packet's source and destination IP addresses to see if they match predefined permitted security rules to determine if the packet should be able to enter the targeted network. Packet filtering firewalls can be further subdivided into two classes: stateless and stateful. Stateless firewalls inspect data packets without regard to what packets came before it; therefore, they do not evaluate packets based on context. Stateful firewalls remember information of previous packets and can then make operations more reliable and secure, with faster permit or deny decisions.
- **Next Generation:** Next-generation firewalls (NGFWs) can combine traditional packet filtering with other advanced cybersecurity functions including encrypted packet inspection, antivirus signature identification, and intrusion prevention. These additional security functions are accomplished primarily through what is referred to as deep packet inspection (DPI). DPI allows a firewall to look deeper into a packet beyond source and designation information. The firewall can inspect the actual payload data within the packets, and packets can be further categorized and stopped if malicious data is identified.
- **Network Address Translation:** Network Address Translation (NAT) firewalls map a packet's IP address to another IP address by changing the packet header while in transit via the firewall. Firewalls can then allow multiple devices with distinct IP addresses to connect to the Internet utilizing a single IP address. The advantage of using NAT is that it allows a company's internal IP addresses to be obscured to the outside world. While a firewall can be dedicated to the purpose of NAT, this function is typically included in most other types of firewalls.

- **Stateful Multilayer Inspection:** Stateful multilayer inspection (SMLI) firewalls utilize deep packet inspection (DPI) to then examine all seven layers of the Open Systems Interconnection (OSI) model. This functionality allows an SMLI firewall to compare a given packet to known states of trusted packets and their trusted sources.

Intrusion Prevention System (IPS)

An intrusion prevention system is a hardware- or software-based security system that can continuously monitor a network for malicious or unauthorized activity. If such an activity is identified, the system can take automated actions, which can include reporting to administrators, dropping the associated packets, blocking traffic from the source, or resetting the transmission connection. An IPS is considered more advanced than an intrusion detection system (IDS), which can also monitor but can only alert administrators.

An IPS is utilized by placing the system in-line for the purpose of enabling inspection of data packets in real time as they traverse between sources and destinations across a network. An IPS can inspect traffic based on one of three methods:

- **Signature-based:** The signature-based inspection method focuses on matching data traffic activity to well-known threats (signatures). This method works well against known threats but is not able to identify new threats.
- **Anomaly-based:** Anomaly-based inspection searches for abnormal traffic behavior by comparing network activity against approved baseline behavior. This method typically works well against advanced threats (sometimes referred to as zero-day threats).
- **Policy-based:** Policy-based inspection monitors traffic against predefined security policies. Violations of these policies result in blocked connections. This method requires detailed administrator setup to define and configure the required security policies.

These IPS inspection methods are then utilized in single or layered combination methods on one of the system's platforms:

- **Network Intrusion Prevention System (NIPS):** A NIPS is used in the previously mentioned in-line real-time method and is installed strategically to monitor traffic for threats.
- **Host Intrusion Prevention Systems (HIPS):** A HIPS is installed on an object, which can typically include endpoints and workloads. Inspection of inbound and outbound traffic is limited to this single object.
- **Network Behavior Analysis (NBA):** An NBA system is also installed strategically on a network and inspects data traffic to identify anomalous traffic (such as DDoS attacks).
- **Wireless Intrusion Prevention System (WIPS):** A WIPS primarily functions the same as a NIPS except that it is specialized to work on Wi-Fi networks. The WIPS can also identify malicious activities directed exclusively on Wi-Fi networks.

IPS security technology is an important part of a Zero Trust Architecture. It is through IPS capabilities and by automating quick threat response tactics that most serious security attacks are prevented. While an IPS can be a dedicated network security system, these IPS functions can also be incorporated in firewalls such as the NGFW and SMLI systems.

Proxy

A proxy acts as an obfuscation and control intermediary between end users and objects to protect organizational data from misuse, attack, or loss.

Proxies are deployed in several circumstances, but for most organizations, there are two primary use cases. One is a proxy to the Internet, where the proxy is placed in-line between the corporate user community and the Internet. These proxy services are often combined with other control capabilities to provide secure web gateway, email security, DLP and other outbound traffic, to the Internet traffic controls. This set of controls can be located on-premises or could be cloud-based. Policy enforcement controls can then be employed on all outbound Internet traffic. Policy enforcement through a proxy can then impact which sites and services can be accessed, whether files can be transferred, what user identity attribution can be gleaned, or which network path is taken, to name a few.

The second common use case is a reverse proxy, where control is placed in front of offered services (that is, intranet and/or Internet) where the proxy acts as an intermediary between application front-end services and the user community. Reverse proxy services often supply load balancing, encryption off-loading from application front ends, performance-related caching, and AAA of sessions and users.

With the current evolution of general network architectures, where users and services can be located anywhere, the function and location of a proxy have an important role in a Zero Trust Architecture. Corporate users cross a boundary to communicate with Internet-based cloud and SaaS services on a routine basis. Internet-based users cross a boundary to access private cloud and corporate data center services. These boundaries are not only key policy enforcement points, but they are also opportunities to derive attribution from endpoints, users, and workloads. This attribution can be used to determine the current posture of the objects involved in the connection request.

Virtual Private Network (VPN)

A virtual private network is a method to create an encrypted connection between trusted objects across the Internet or untrusted networks and is an important method to be leveraged in Zero Trust Architecture designs. VPNs take many forms, from carrier-provided Multiprotocol Label Switching (MPLS) services to individual user-focused remote access (RA) VPNs.

If we look at this solution from a security controls perspective, VPNs can provide general traffic isolation and routing controls, which reduce the attack surface through broad control over where network packets can be forwarded. Remote access VPNs may also help

organizations categorize use cases and policy definitions that may exist to identify users, endpoints, and functional groups.

If an organization were to make a full accounting of its various VPN deployments, it would document organizational constructs such as how MPLS VPN and Virtual Routing and Forwarding (VRF) may be deployed to isolate traffic across business units, divisions, or subsidiaries. It also would account for vendor, partner, and customer access mechanisms along with service and application access requirements.

Security Orchestration, Automation, and Response (SOAR)

Security orchestration, automation, and response or SOAR is set of solutions that enables an organization to visualize, monitor, and respond to security events. A SOAR is not a single tool, product, or function. The intention of a SOAR is to automate routine, repeatable, and time-consuming security-related tasks. The SOAR ties disparate systems together to provide a more complete picture of security events across multiple security platforms. A SOAR is used to improve an organization's ability to identify and react to security events.

From a Zero Trust perspective, these capabilities can also be used to enable, update, and monitor Zero Trust policies across the entire security ecosystem. For example, orchestration capabilities utilized to tie vulnerability management systems with network access controls could allow for policy adjustments to be made based on discovered endpoint vulnerabilities where connecting devices with known vulnerabilities are no longer allowed to connect to the network until remediation occurs. Also, automation could be used to provide unattended remediation services to devices that have been flagged as untrustworthy.

File Integrity Monitor (FIM)

As an enforcement control applied to a Zero Trust architecture, a file integrity monitor provides the ability to detect potentially nefarious changes made to the files or file systems supporting services and applications. FIM capabilities are typically applied to server platforms but can be deployed across any platform with an accessible file system. File change detection and alerting could be used in a Zero Trust Architecture to affect the trust status of a system that has experienced recent changes. Zero Trust policy may direct sessions to be limited and/or restricted completely to or from systems where unexpected file changes have occurred.

To realize Zero Trust capabilities from this control, organizations must expend effort in setting baselines for known and expected behaviors. Administrators will then need to define which categorizations of file changes will trigger actions to isolate systems where change has been detected. Change detection policy and change detection alerting must then be translated into response plans and actions. This activity could be arduous and time-consuming but will result in less effort expended chasing false positives. Tying the FIM capabilities into a SOAR architecture can then result in automated isolation and remediation for impacted workloads.

Segmentation

Segmentation is the art of identifying and classifying sets of services, applications, endpoints, users, or functional classifications and isolating them from other sets of systems. This isolation is typically accomplished through various techniques that focus on network traffic controls. These sets of controls will vary depending on where they are applied and the classification of the assets being segmented. For example, isolating a corporate intranet from the Internet will require significantly more capabilities due to the scope and scale of business services that need to traverse this boundary. In contrast, isolating building management systems attached to the corporate network from general-purpose corporate workstations would be a "deny any" rule, assuming one can clearly identify building management systems and corporate workstations. The foundational process for identification and classification of corporate assets is essential to creating a Zero Trust Architecture, where defining segments or enclaves is used to establish trusts to other enclaves and sets of controls employed to protect sets of assets within an enclave.

Analytics Pillar

The Analytics group of Zero Trust Capabilities is an extremely important aspect of the Zero Trust deployment process. The need for analytics, like the ongoing need to continue to look for and gain more insight into anything identity based, is constant and ever evolving, with a need to sort through a massive amount of data sometimes likened to "noise" to find the data that indicates what is happening within the ecosystem.

Analytics comes in many forms and can be anything from the analytics associated with changes made to the network that may attempt to overcome the Zero Trust implementation, including tracking users and their actions on the network throughout their time both on and remotely connected to the network. Analytics about what threats are found within the network that provide more insight into how to detect these threats, and, of course how these threats were blocked will all come into play and will help overcome any reluctance that management, business units, operational staff, or administration staff have when it comes to the implementation.

Application Performance Monitoring (APM)

Application performance monitoring is the process of establishing data points on the performance of an application by observing the behavior from user interactions as well as via synthetic testing. These data points can be used to establish a baseline that can then be used to understand when the application is deviating from that baseline and requires investigation.

The data points collected can include CPU usage, error rates, response times or latency, how many instances of an application are running, request rates, user experience, and more. This data can also be utilized to ensure that an application is meeting a specified level of performance or availability as part of a service-level agreement (SLA). A well-rounded APM should be able to monitor not only down to the application code level but also across the infrastructure supporting the application to ensure a complete picture of the health and performance of an application. This means the APM solution setup process will need to include stakeholder decision-making on how to implement monitoring and tuning of the solution for optimal effect in each unique environment.

APM is a necessity for Zero Trust Architectures because users may access an application from various locations using disparate devices that may or may not be managed by the organization. When a user experiences a problem with an application, it is imperative that the operations and engineering teams can quickly understand whether the issue is related to the application itself or if there are factors beyond the organization's control. This data is important to ensure that an unhealthy application is restored to a healthy state or, if outside factors are causing the issue, that the users are informed so they can adjust as necessary to improve their experience. As mentioned, APM can also provide a way to track application performance against a service-level agreement, so Software-as-a-Service offerings can be monitored to ensure that the organization is receiving the level of service they have agreed to with the vendor.

Finally, APM provides the ability to utilize synthetic tests, which are tests that the APM runs to simulate normal user behavior but in a repeatable fashion. These tests can be useful in periods of low user utilization or after a change to an application or its supporting systems to function as a check and balance. The output of these tests may help an organization quickly ascertain whether the changes made have had a meaningful negative impact to an application and allow for quicker resolution. Due to their repeatability by isolating as many variables as possible, synthetic tests run at regular intervals may also be able to highlight minor deviations that, if left unchecked, can turn into user-impacting issues. This enables the organization to proactively address the issue and keep the application in a healthy state to improve user satisfaction and improve organization efficiency.

Auditing, Logging, and Monitoring

Audit, logging, and monitoring are an ongoing process that takes in the identity and vulnerability assessment of an endpoint and attempts to link or align this assessment with what the user or device is doing on the network throughout its life cycle on the network. The challenge of logging and monitoring is the sheer number of devices and users who access the network on a regular basis, and the need to crunch vast amounts of data to validate and archive what users and devices are doing. In addition to the need for users to administer network devices through command issuance, upgrade, periodic reboot, and similar actions, the organization also must track the behaviors of users and devices as they then connect through the network access devices and the potential responses that are sent back to the actions taken by these devices.

The phrase "signal within the noise" has been used throughout this book without much detail on what that signal is that should be looked for and sorted through. After the identity of a user or device has been determined, the identity's expected behavior is mapped out, actions are taken to determine the potential vulnerabilities that exist within that identity, and enforcement is applied to attempt to prevent that identity from communicating with resources that it is not meant to do so. What could arguably be considered the most ongoing labor-intensive aspect of the equation is now required. This aspect is the need to monitor the behavior of that user or device while validating that this behavior is expected and aligns with security policy.

Change Detection

Change detection is when change occurs within the ecosystem, and that change is detected. Many times, this is not the case because there may be gaps in change detection tools within the organization. Working to close those gaps, even across Shadow IT environments, enables an organization to improve Zero Trust capabilities.

Change detection is just as it sounds. Changes happen. Organizations need to know what was changed, how it was changed, who authorized and/or did the change, where the change was made, and when it was changed. The organization needs to know all changes that occur, for research, response, or regulatory requirements.

For change detection in Zero Trust, if a change is made that violates policies, we want to be able to identify whether automatic alerts will be generated and sent to SOC, NOC, or appropriate personnel, including all of the what, how, who, and when information. Change detection can be very challenging; changes typically occur constantly in IT environments. Changes can include software updates or patches that are frequently applied. Configurations are frequently updated or newly created to support changes. The following types of solutions identify changes or detect unauthorized changes:

- File Integrity Monitoring Solutions
- Syslog
- Messaging
- Privilege access solutions
- SIEM

Network Threat Behavior Analytics

Behavior analytics enables the method of Zero Trust that is to be able to define what traffic is expected in the environment or what traffic is out of norms in the environment. As a part of monitoring, organizations need to focus on not just what they are able to pull into a file that contains activity; organizations also need to analyze that information to make it actionable. When we say "make it actionable," it is important to understand that organizations need to be able to see what traffic is doing in the organization's environment

whether in the data center or in the cloud. This is where network threat behavior analytics comes into a Zero Trust strategy.

Informing network behavior analytics with threat information and intelligence is critical to create greater understanding of the traffic in the environment, with current threats that are changing every day, every hour, and every minute. Network threat behavior analytics solutions are only as good as how they have been tuned for the organization.

Most organizations have enormous amounts of data transferring to and from data centers and externally to third parties. It is important for organizations to monitor this activity and define whether it is normal or if the activity is out of the norm. By implementing automation to sort through the alert information, organizations can use their teams to look at what is shown in the anomalies and what are the exceptions. By sorting out the "noise" and by extracting pertinent information, teams are able to respond with solutions to the most important events as they occur, instead of SOC or NOC personnel getting lost in the avalanche of information being collected when trying to track down relevant information.

One of the key takeaways is that organizations must be able to look at their information flow and define what has been compromised or is in a nominal state. This must be done in a structured way due to the level of traffic involved in the environment. Monitoring of network threat behavior analytics is a regular function that must be maintained and updated. It is not a "set it and forget it" set of solutions. For organizations, it is a very important part of any security operations center or any network operations center. The data must be analyzed in many ways. Next, we look at a few key concepts to analyze the data flow.

A common term in network threat behavior analytics is *lateral movement,* or *east-west movement*. When we talk about lateral movement, we must think about what normal traffic is between applications, databases, and endpoints and what is abnormal behavior.

- Does this traffic go to an unknown repository inside the environment or ecosystem?
- Are there communications between servers that should not talk to one another?
- Is database traffic being transferred into a file for exfiltration?
- Is there some kind of nefarious activity going from or to various objects on an intermittent basis or at a high frequency?
- Do communications originate from a compromised endpoint?

Rules should be established in these tool sets to alert key resources to unexpected behavior in the environment. Another form of network threat behavior analytics modeling is looking at *north-south movement*, or *vertical movement*, which is traffic coming into or going out of the organization. Organizations need to ask questions like these:

- Is data moving using standard methods, or are there command and control communications between malware and known threat actors in the world?
- Are there geographic tendencies of the data going to places where the organization is not doing business?

- Are there organizations that should not be receiving information from them?
- Why is data moving out of the organization in large volumes?
- What destinations are receiving traffic from the organizations? Valid or invalid?

These are valid questions to review and monitor, to establish rule sets that conform to the organization's best practices. Organizations should define what actions should be taken when they see abnormal traffic performing outside of the baseline. When looking at this traffic, many times we see a combination of east-west traffic with periodic north-south traffic, to a command and control (C2) host outside of the organization.

In addition to network behavior, the same analytical process can be used by other tools for applications or cloud data. These tools will ingest data available to them using sources such as logs, API data, and other telemetry feeds to define a baseline for user or entity behaviors. As with network behavior analytics, other behavior analytic platforms will likely require a degree of tuning to help adapt the system to each particular organization. An example might be accounting systems that experience increased utilization for reporting during quarter or year-end financial events, where the number and frequency of user visits will increase as data is compiled to support financial reporting requirements. The output from application or cloud behavior analysis tools is similar to those supporting the network, in that they enable security personnel to more rapidly identify variances in access frequency or duration that may require further investigation. An attacker in the network may not be actively exfiltrating data or operating in a way to trigger the network behavior analysis tools but, if actively focusing on high-value systems, could still be discovered by other behavioral analysis platforms. Thus, ensuring that behavioral analysis beyond the network is also addressed helps to alleviate blind spots and prevents a false sense of security.

Security Information and Event Management (SIEM)

A Security Information and Event Management solution enables an organization to ingest enormous amounts of log and audit data from multiple systems and process this information into actionable data on security threats for response.

To have manual review of this data would be both ineffective, and potentially, even counterproductive. Therefore, a well-tuned and maintained SIEM is key to ensuring that the right information is presented in such a manner to be actionable in a Zero Trust Architecture.

A robust SIEM should be able to capture all desired events that are sent from the syslog or other sources and typically requires that the SIEM be designed and implemented in a distributed manner to ensure no blind spots or data gaps exist. It should be able to classify the source of the logs that it receives to add intelligence into the analysis process, with different analysis algorithms being applied to servers as opposed to network devices. A SIEM should have the ability to tag sources of events with some sort of metadata labeling system, giving the ability to add ownership by department, user, use case, or organizational data to the event source. It should be able to sort sources of events into a classification system. It should also support secure transport so that messages sent between systems of interest and the SIEM prevent eavesdropping.

The same need for behavioral monitoring goes for the ability to analyze denials from enforcement actions, such as access control lists or authentication failures. While it may be expected that a device is prevented from accessing the network or a specific device on the network, once enforced, that attempt to access that device should be limited or halted by the source device altogether. When the attempts to access the network or device continue, a threshold should be set indicating abnormal behavior thresholds have been met, which will trigger an alert on the SOC console, which will in turn lead to investigation of the identified issue. This approach can also take into consideration the identity of the device or user attempting to access the network or a certain resource. An alert to a specialized team, such as one that supports the C-suite executive team, would then be sent and prioritized for remediation.

The SIEM should directly integrate to organizational data brokers, such as a CMDB, ticketing system, or other security event monitoring solutions. This integration can provide additional valuable information that enhances the quality of data in the SIEM. Integration may also trigger external activities to occur via ticketing systems or other monitoring systems like in a network operations center.

For example, in many identity-based network access control products, the addition of data into tables, such as local users, or the addition of invalid data into tables to attempt to undertake a SQL injection attack may not trigger a syslog. However, inquiries via the API of the user database table can detect changes and utilize intelligence built into the SIEM to monitor and alert on this invalid data injection attempt.

There is commonly confusion for some on the differences between a SIEM and other seemingly similar tools, such as extended detection and response (XDR) and security orchestration, automation, and response (SOAR) platforms. While the intent for these tools is similar in their goal to aggregate and analyze data from multiple sources, they differ in that SOAR is focused on supporting multiple security tools to coordinate their activity based on one or more inputs. An XDR, on the other hand, concentrates on utilizing collected data from endpoints, which provides a large-scale view of changes to the environment because many security events will either ingress or occur at the endpoint, making it a valuable data stream.

Threat Intelligence

Threat intelligence is information that is collected by incident responders, governments, application vendors, equipment vendors, and many other sources. This intelligence gains more usefulness when it is ingested directly and in real time into the network, security, and application solutions within the organization. The information consists of things such as indications of compromise (IOCs), Common Vulnerability and Exposures (CVEs), IPS rulesets, and other types of information surrounding new or ongoing security events.

The global threat landscape is constantly evolving and shifting. The concept of collecting threat intelligence brings a clear focus into the strategy of Zero Trust. Understanding the environment in which an organization operates—with an eye on what is trusted and what is not—is what creates and tunes threat intelligence for an organization. Relationships between different types of active threats and the associated Internet activity to malicious

domains provide deeper insights into patterns of malicious actors' behavior. Keeping an eye on what is happening in the world, the country, the regulating bodies, and the news surrounding the organization can help inform the overall security standing and posture of an organization.

Partnering with key organizations that help connect an organization to its critical infrastructure community is critical. Working with fusion centers, government agencies, and public–private intelligence-sharing organizations helps you to partner with like or disparate organizations that will be important in a crisis. Setting up these relationships when times are good helps to support organizations when times are bad. In the US, organizations like InfraGard (Infragard.org) connect the community and are free to join.

Understanding the organization's risk tolerance and key goals provides "tuning" to the intelligence that needs to be collected. Key questions include

- Have there been changes to security reporting laws that impact the organization?
- Are there new requirements that the organization is required to respond to?
- Has there been a breach of a supply chain organization?
- Does the organization have a robust third-party risk program?
- Do third and fourth parties have a duty to report issues or breaches they have experienced in the contracts the organization has in place?
- In public source news, does the organization observe threats that are impacting the organization, suppliers, governments, or treaty groups?

Taking this observed information and turning it into action requires solutions and tools that keep a constant vigilance over the threat landscape. An organization must have several methods to obtain threat intelligence and digest that intelligence directly into the organization's solutions as well as to the teams and leaders of the organization. Being able to react and respond to critical situations and make correct business decisions based on the threat landscape enables companies to outperform their competition. Public sector organizations or agencies are better able to respond correctly to nation-state actors.

Most sources should be readily and automatically ingested by the processes, solutions, and services with a primary focus on the diversity of threat feeds and methods of intake in the overall solution set for the organization. Firewalls, automated segmentation solutions, anomaly detection solutions, monitoring solutions, endpoint protection solutions, and host protection solutions are examples, all of which need to have active thread feeds and the ability to alert when changes occur that affect the organization.

Traffic Visibility

Traffic visibility is the ability to view the full data activity of an organization at the time of occurrence and the ability to aggregate the traffic to be usable in the future. Many critical infrastructure organizations are required to retain traffic visibility information for extended amounts of time due to laws or regulations. This information should be

aggregated into specific systems that support profiling of endpoints, security events, network events, or data analysis information.

Another requirement of traffic visibility is to ensure that there are no blind spots in the organization's span of control. If there are blind spots, there will be issues with compliance to regulation based on industry (for example, PCI, FCC, FFIEC, and many others). When there are blind spots within an organization, they will weaken the organizational posture related to Zero Trust and may even degrade the function of critical capabilities.

Traffic visibility tools are also critical components of determining and creating segmentation enforcement policy.

Asset Monitoring & Discovery

The asset management database is a set of tools that are consistently and reliably updated as assets have been purchased, retired, or, in the case of building the asset management database, currently exist in the network. For those devices that currently exist in the network, a specified amount of information should be set as a standard to be populated, to give those monitoring the analytics for potential threats or security breaches within the network a fair advantage in investigating the endpoint. Policy & Governance should define the attributes that should be collected for each asset type.

Asset management is another key area to ensure that organizations have a standardized life cycle for all assets to provide the most effective and efficient usage of those assets for their intended purpose. The intent of an asset management program is to simplify operations and reduce risk by ensuring that the entire life cycle of the assets is mapped out and approved processes are followed from prior to acquisition up to the point of decommissioning or disposal. This includes standardizing as much as possible, such as configurations that make it easier to track for unapproved changes or modifications to these assets, while also ensuring that new deployments are fit for use. A lack of proper asset management can easily lead to lost productivity as users are unable to access key resources, such as applications, resources, or data repositories. With proper asset management, an organization gains the ability to harden configurations, ensure physical and virtual maintenance is regularly performed, and validate designs, while ensuring that assets are fit for use. While for the purposes of Zero Trust, the operation and configuration of an asset are likely to be the first line of thought, asset management must extend beyond this to include the entire life cycle of an asset, including the evaluation and acquisition, design, operation, maintenance, and replacement or decommission of the asset. The final point of replacement or decommission must also be properly managed to ensure that the asset is appropriately purged of any proprietary or sensitive data to limit risk to the organization.

Summary

In this chapter, we covered the pillars of Cisco's Zero Trust Capabilities, which are Policy & Governance, Identity, Vulnerability Management, Enforcement, and Analytics.

Policy & Governance is the organization's policy and sets the groundwork for how endpoints and data are governed on the network. While this pillar should be strict enough to act as the "badge and shield" allowing for enforcement actions to be taken, it needs to strike the right balance between allowing devices to perform their business purpose on the network while maintaining least privileged access.

Identity is key to applying the policy because it determines the context in which an object and its respective business purpose on the network. Identity provides the necessary context required for solutions to provide effective security controls on the network.

Vulnerability Management evaluates this risk of compromise through the evaluation of device communications, baseline behavior, known vulnerabilities, open ports and responses, and susceptibility to malware infection.

Enforcement considers each of the pillars to prevent access to critical resources within an organization based on a policy. Enforcement employs proactive and reactive control mechanisms.

The Analytics pillar considers information found throughout the other pillars and determines whether threats are actively prevented, whether identities changed throughout their life cycle on the network, and where enforcement actions prevented access to resources that were required for the entity's business purpose. This analysis influences all other pillars to keep up with the changing landscape of Zero Trust and security threats.

References in This Chapter

- É. Vyncke, K. Chittimaneni, M. Kaeo, and E. Rey, RFC 9099, "Operational Security Considerations for IPv6 Networks," August 2021.
- Maya G. "ITIL Change Management Process," ITIL Docs, June 30, 2021, www.itil-docs.com/blogs/news/itil-change-management-process.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z