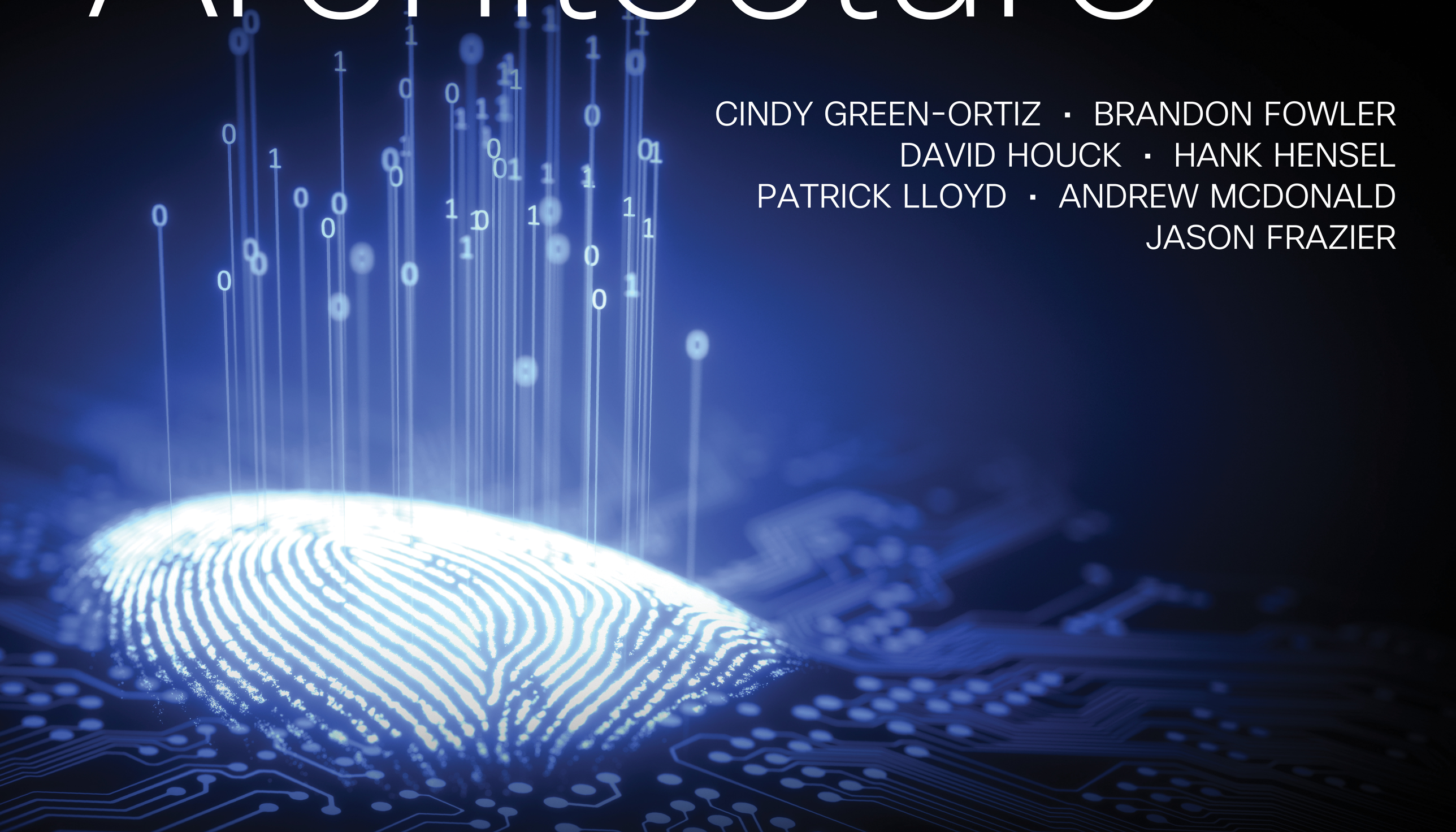
Zero Trust Architecture

CINDY GREEN-ORTIZ · BRANDON FOWLER
DAVID HOUCK · HANK HENSEL
PATRICK LLOYD · ANDREW MCDONALD
JASON FRAZIER



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

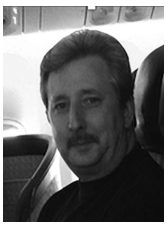
Brandon Fowler is a technical leader for Cisco Customer Experience Professional Services. He holds both CCNP Security and ITIL v4 foundation certifications. Brandon joined Cisco in 2018 with more than 12 years of experience across enterprise networking and security domains. For the past 8 years, his 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

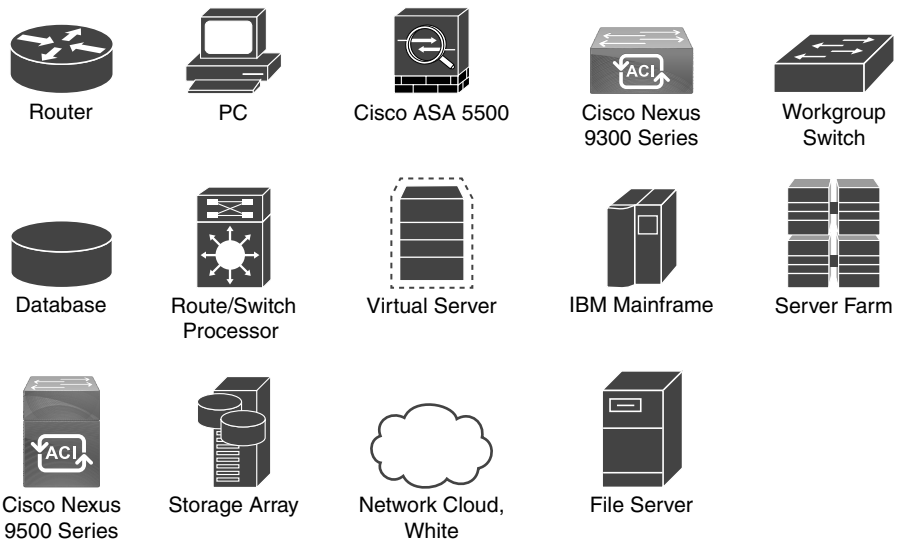
I must acknowledge three special people in my life. My grandfather, Darrell Smith, taught me how to be a man. My grandmother, Joyce Smith, taught me patience and love. I miss you both dearly, though you are still with me every day of my life. To my mother, Rhonda Frazier, you are a rock of wisdom, teaching 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 1

Overview of Zero Trust (ZT)

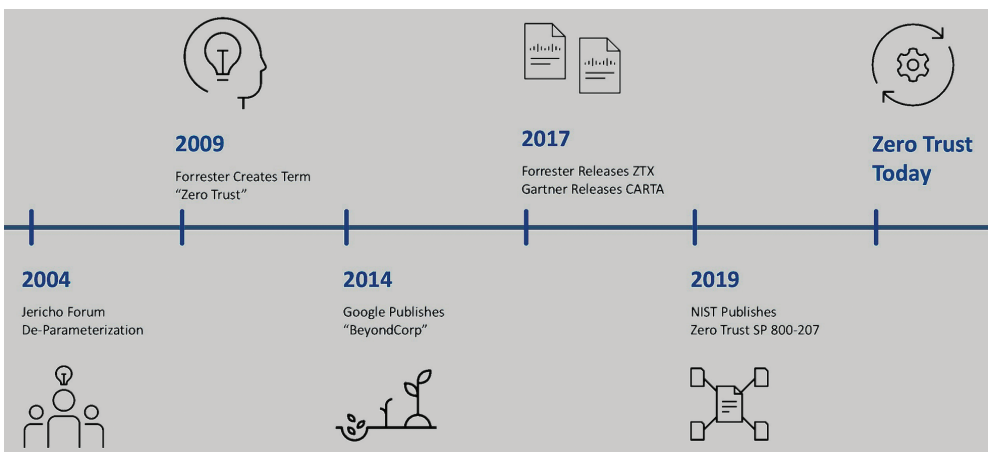


Figure 1-1 *Zero Trust Historical Timeline*

Planning

- Initial Meeting Planning
- Basic Artifact Requests and Questionnaire Review
- Delivery Logistics

Collect Data

- Hardware Resiliency
- Software Resiliency
- Network Topology
- Protocol and Configuration Analysis
  - Power and Environment
  - Network Device Services
  - Network Device Security

Analyze Data

- Hardware Resiliency
- Software Resiliency
- Network Topology
- Protocol and Configuration Analysis
  - Power and Environment
  - Network Device Services
  - Network Device Security

Presentation

- Executive Summary–Key Findings
- Detailed Technical Report Document
- Delete Out-Brief Presentation
- 90-Day Short-Term Network Improvement Plan
- 360-Day Long-Term Network Improvement Plan

Figure 1-2 *Discovery Workshop Activities*

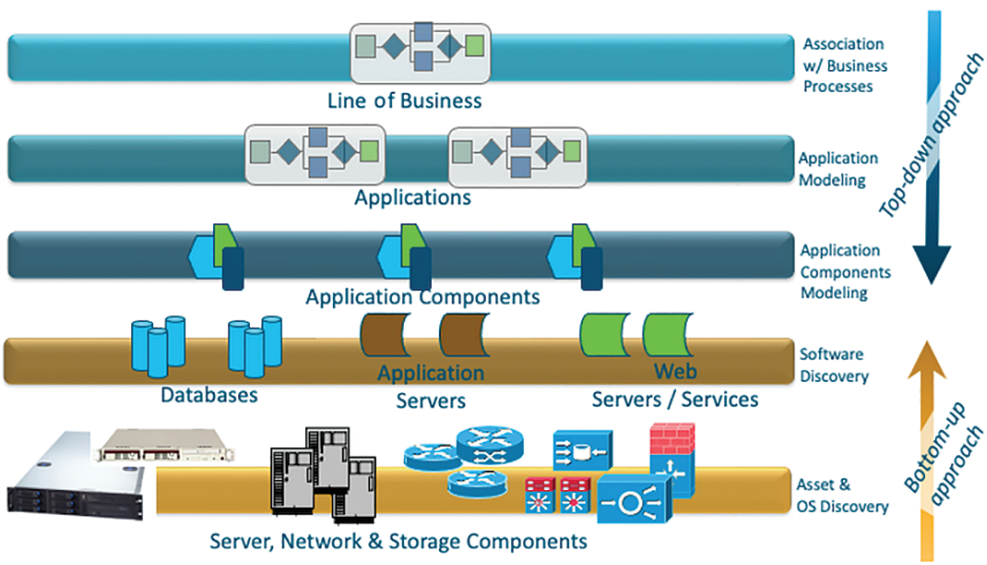


Figure 1-3 *Practical Top-Down Design Example*

Figure 1-4 *Cisco Zero Trust Capabilities*

Chapter 2

Zero Trust Capabilities

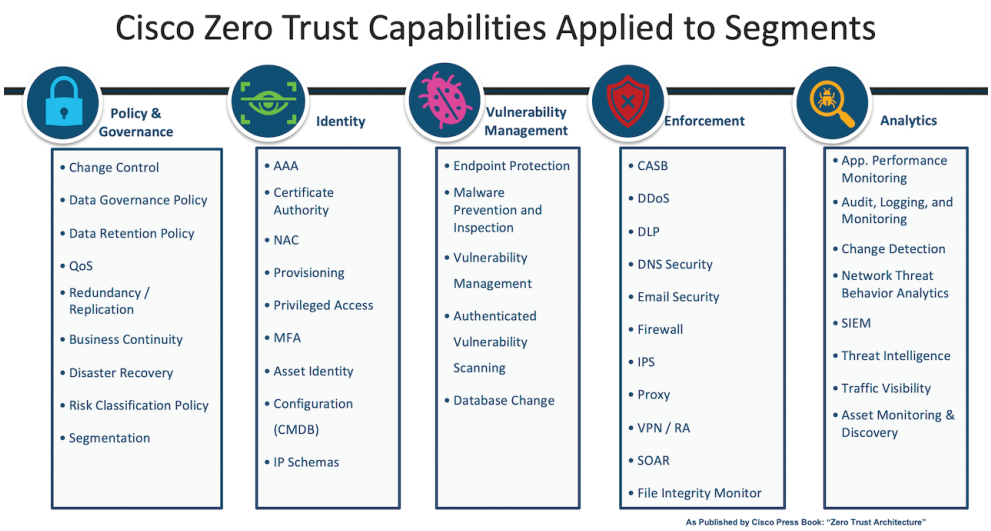


Figure 2-1 *Cisco Zero Trust Capabilities*

Chapter 3

Zero Trust Reference Architecture

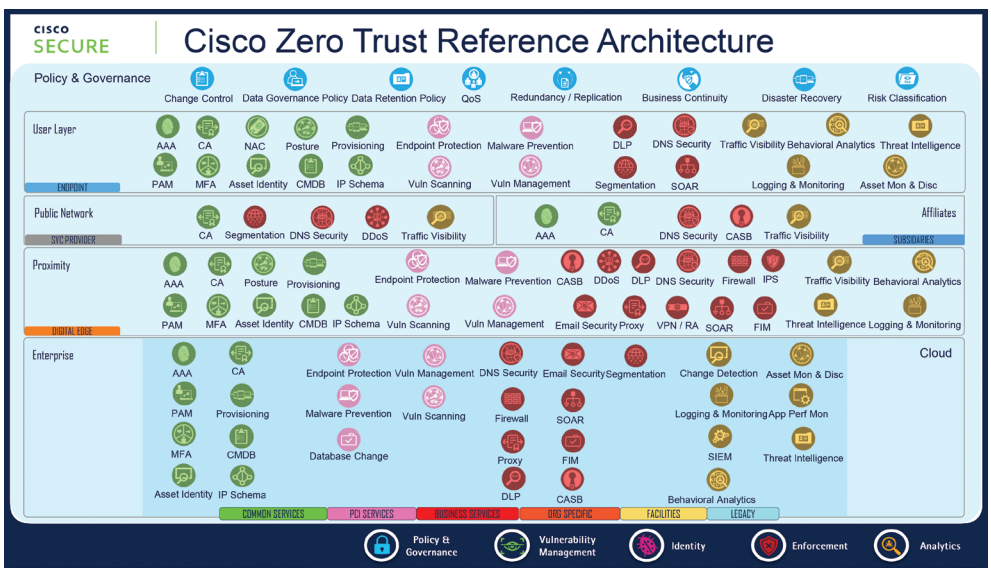


Figure 3-1 *Zero Trust Reference Architecture*

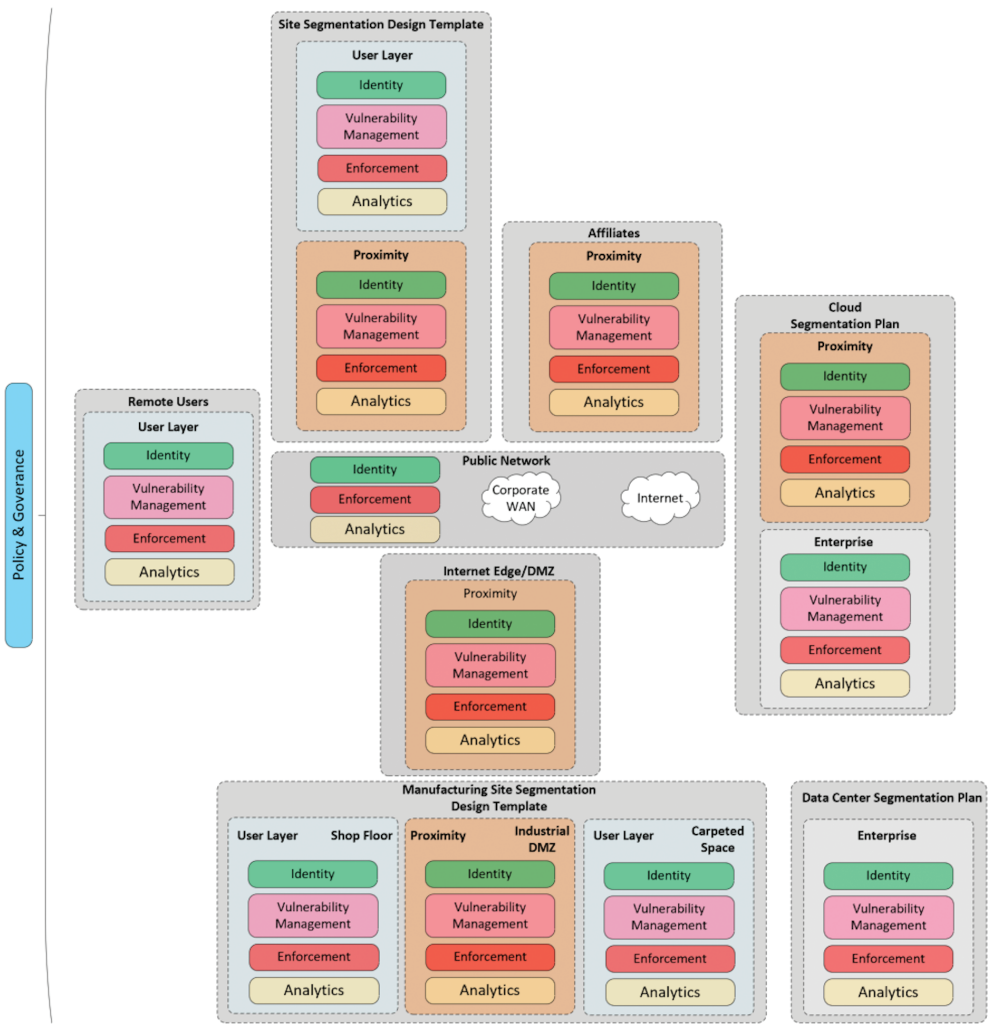


Figure 3-2 *Zero Trust Reference Architecture Overview*

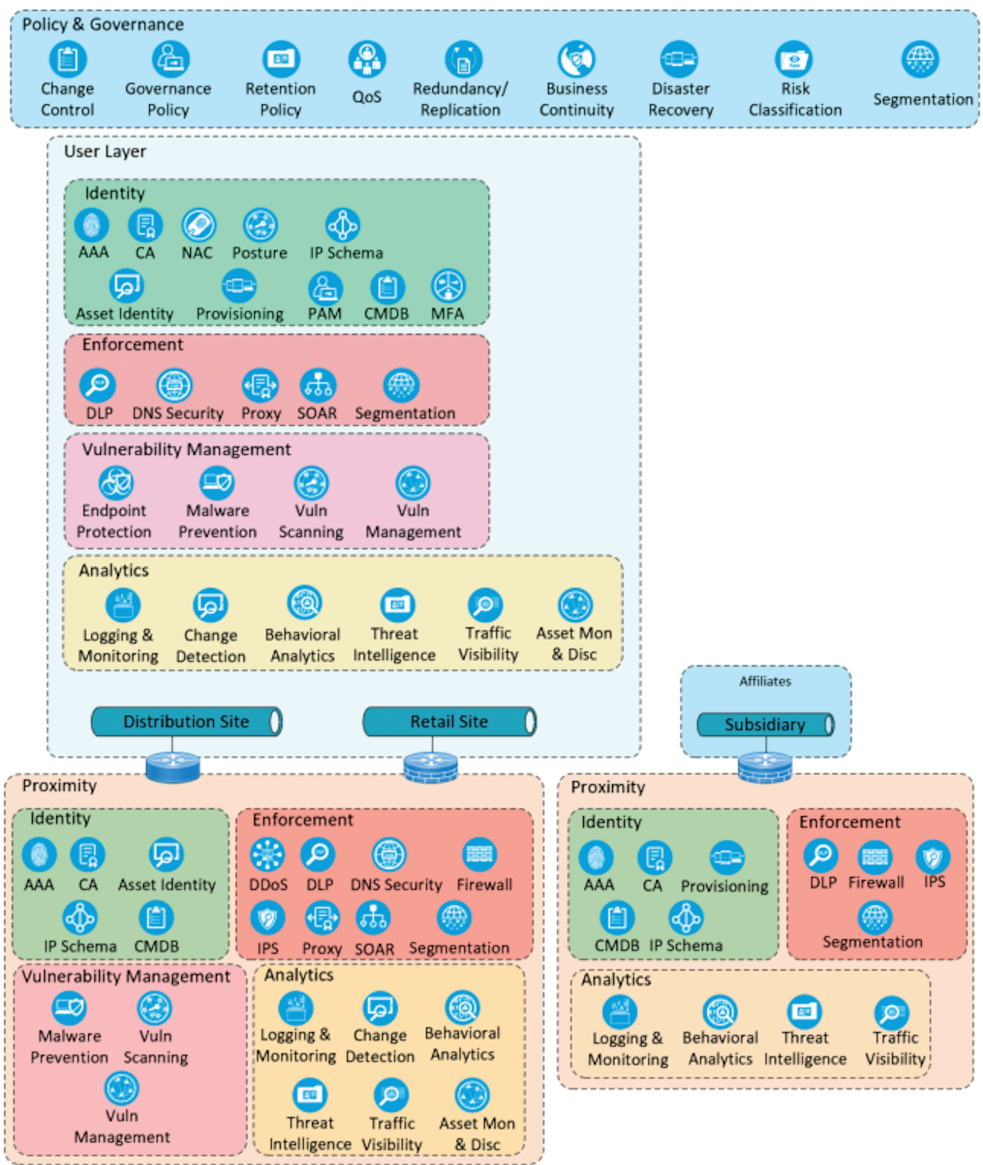


Figure 3-3 *Corporation's Branch Office Zero Trust Reference Architecture*

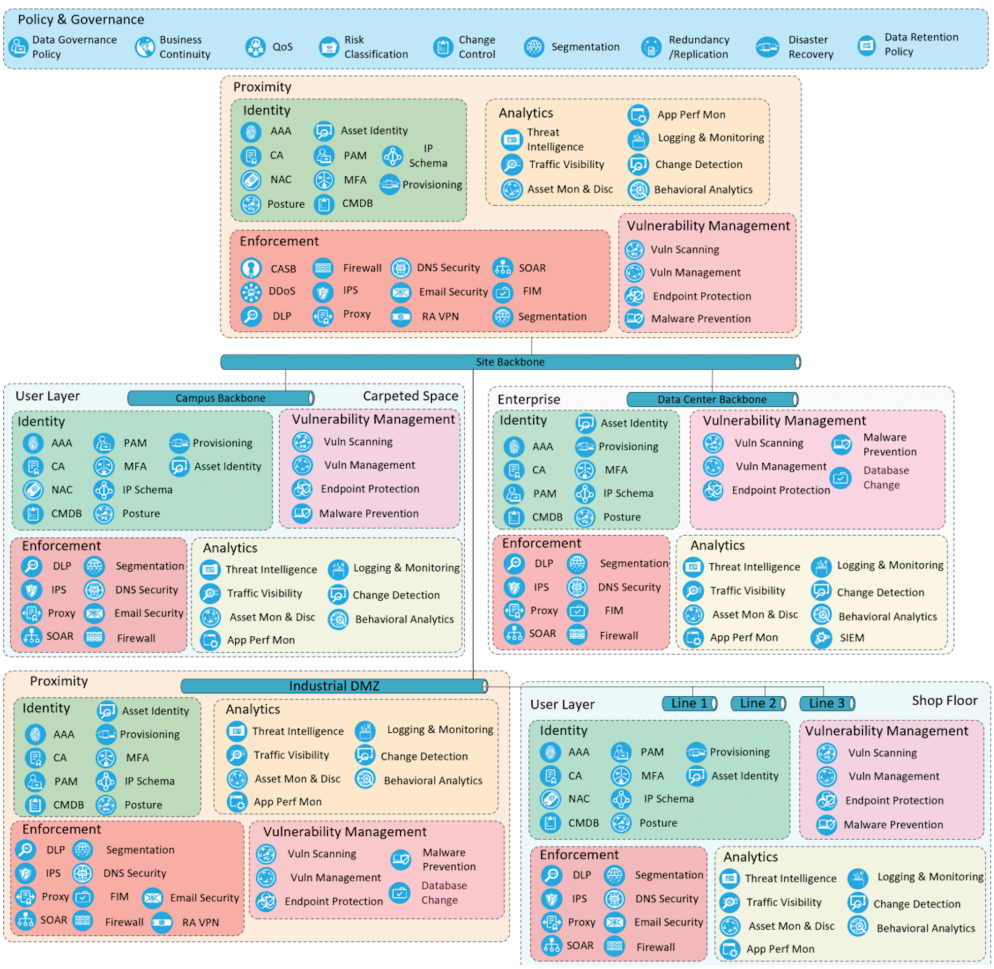


Figure 3-4 *Central Campus*

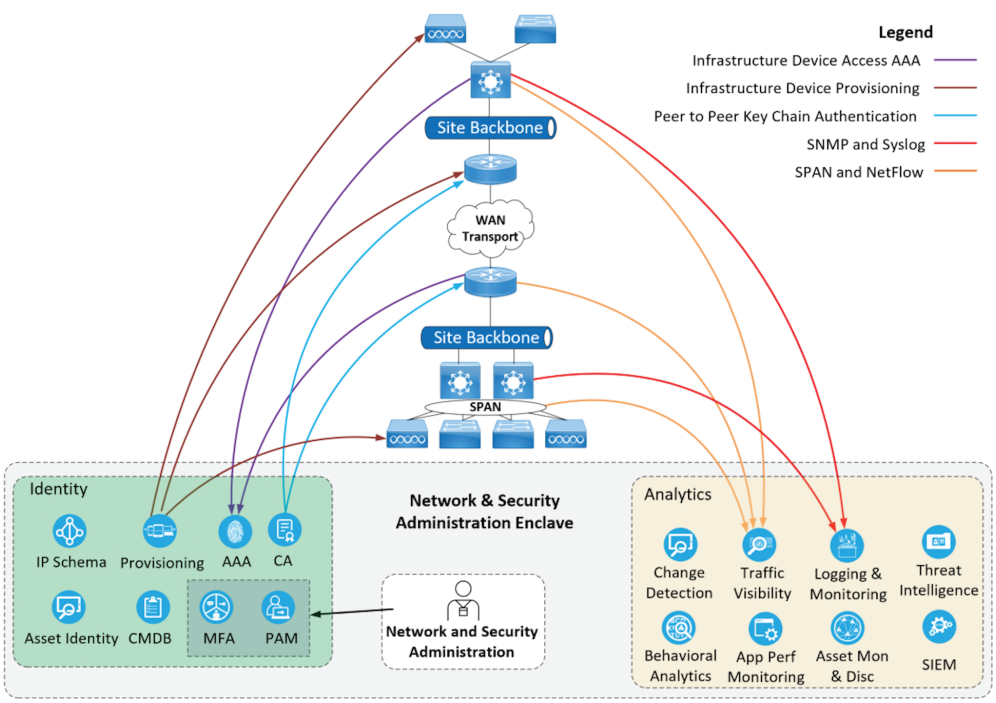


Figure 3-5 *Network Telemetry*

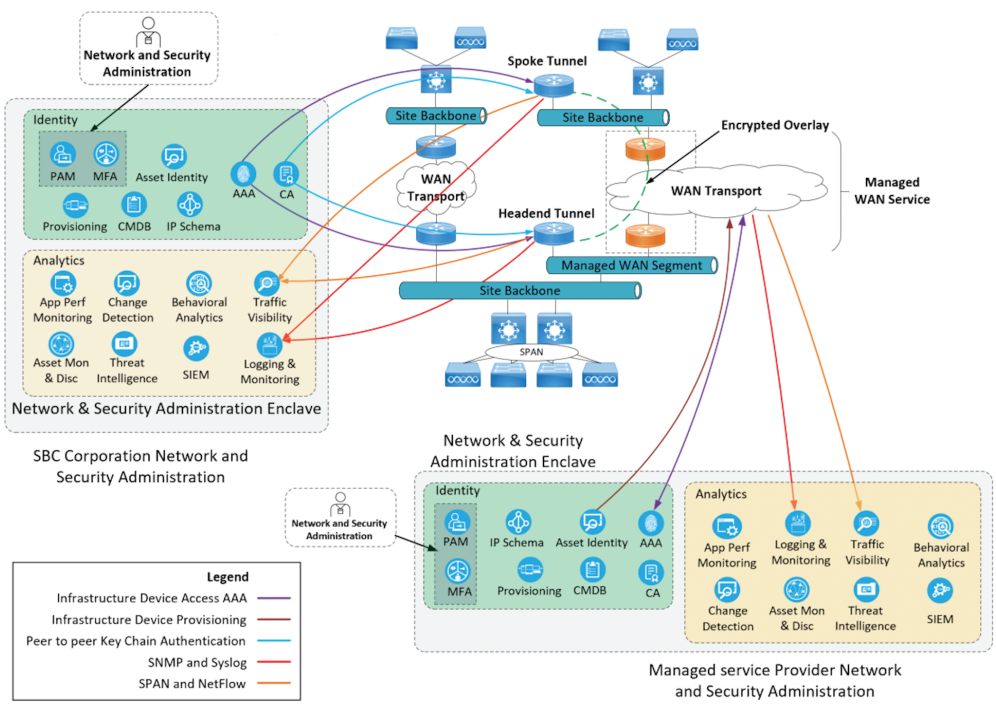


Figure 3-6 *WAN Control Points*

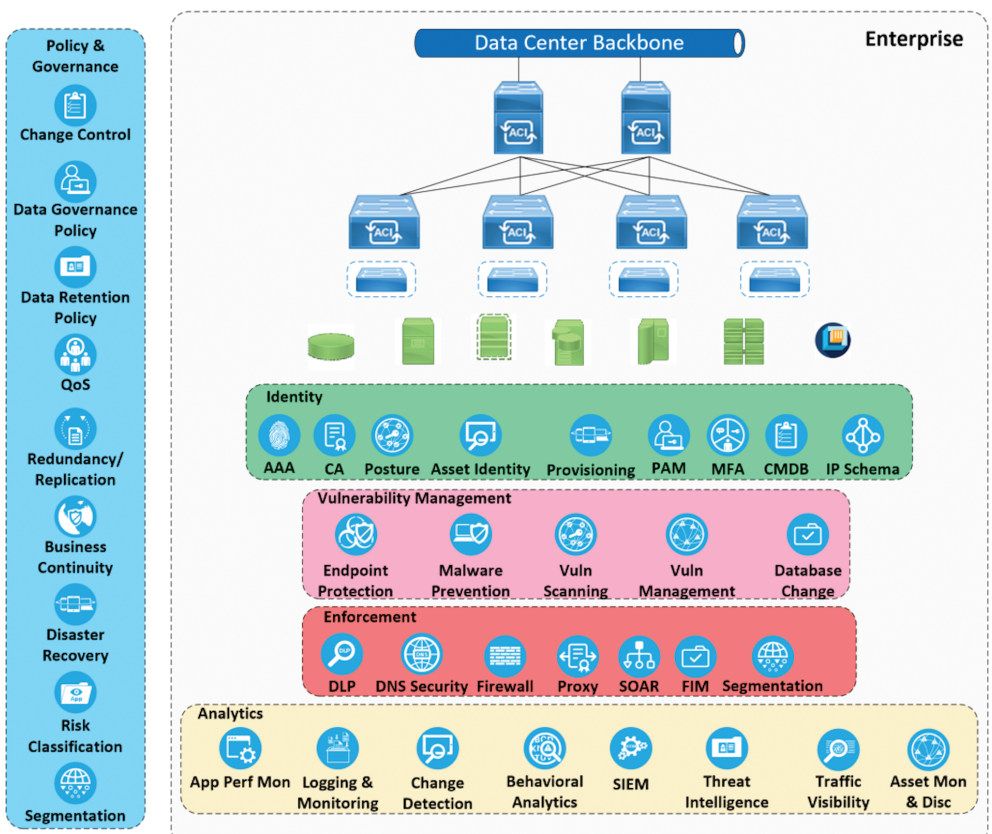


Figure 3-7 *Data Center Architecture*

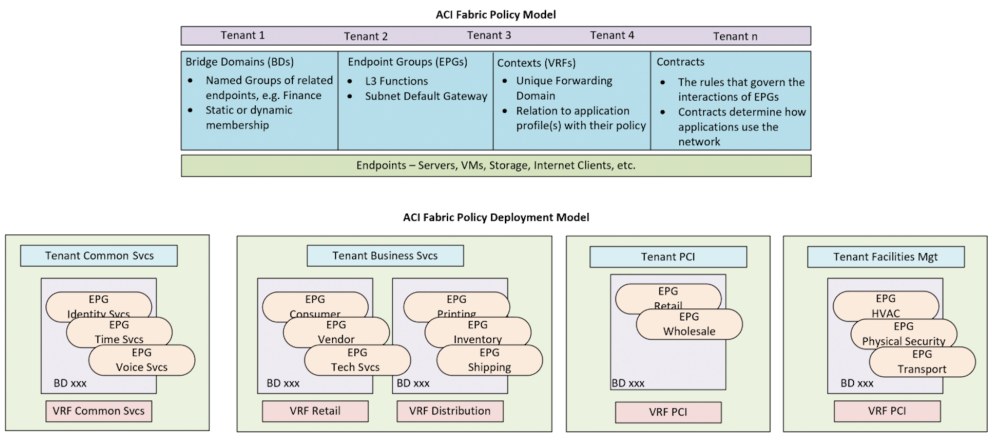


Figure 3-8 *Cisco ACI Fabric Policy Model*

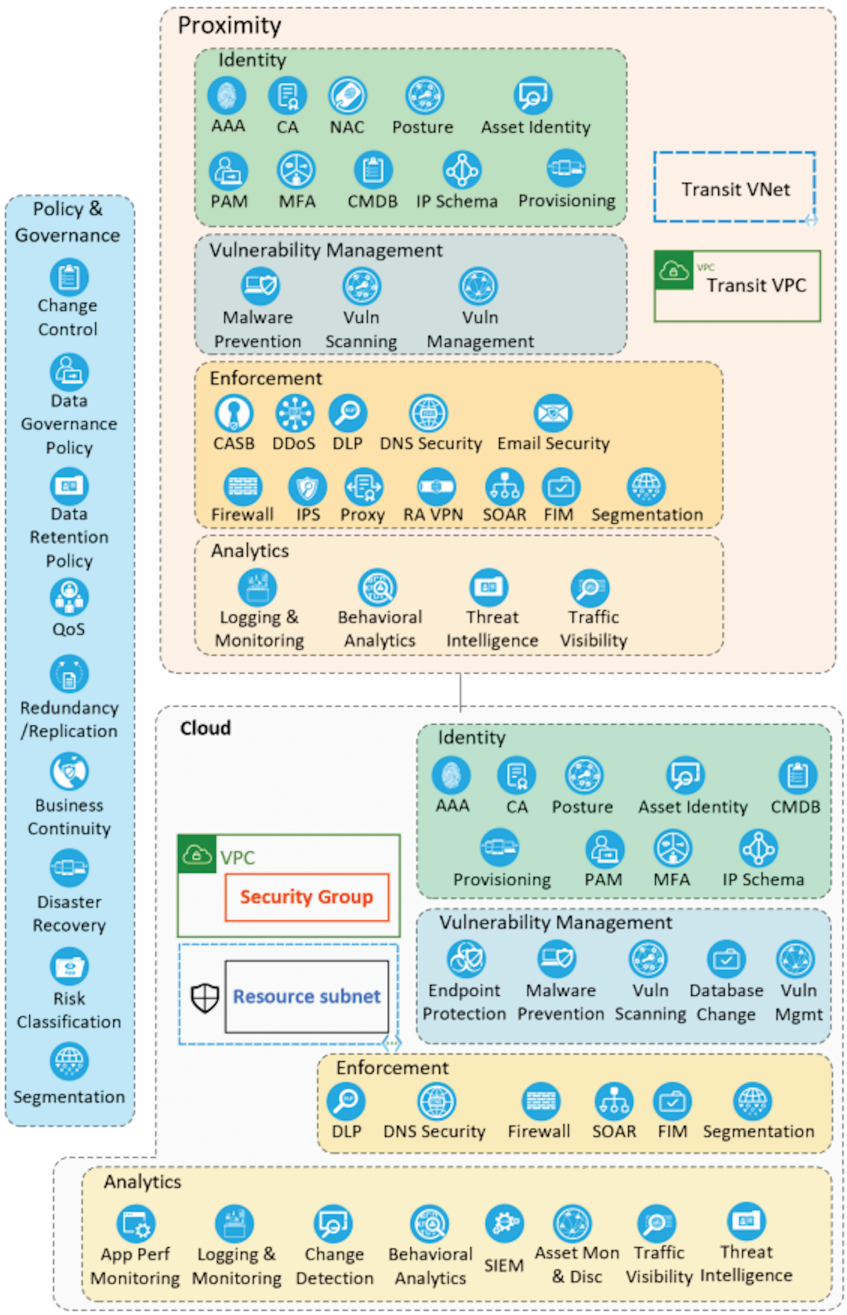


Figure 3-9 *Cloud Topology*

Chapter 4

Zero Trust Enclave Design

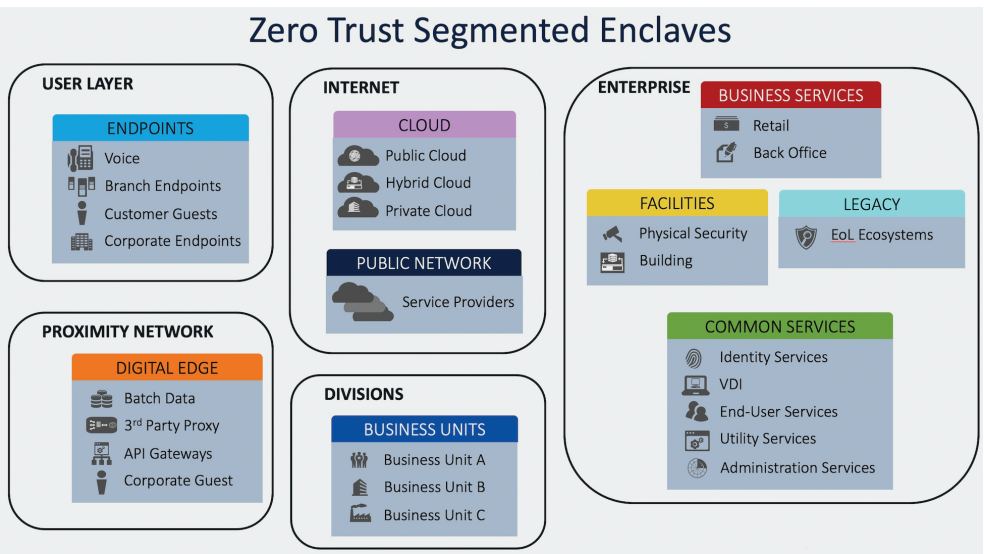


Figure 4-1 *Common Zero Trust Enclaves*

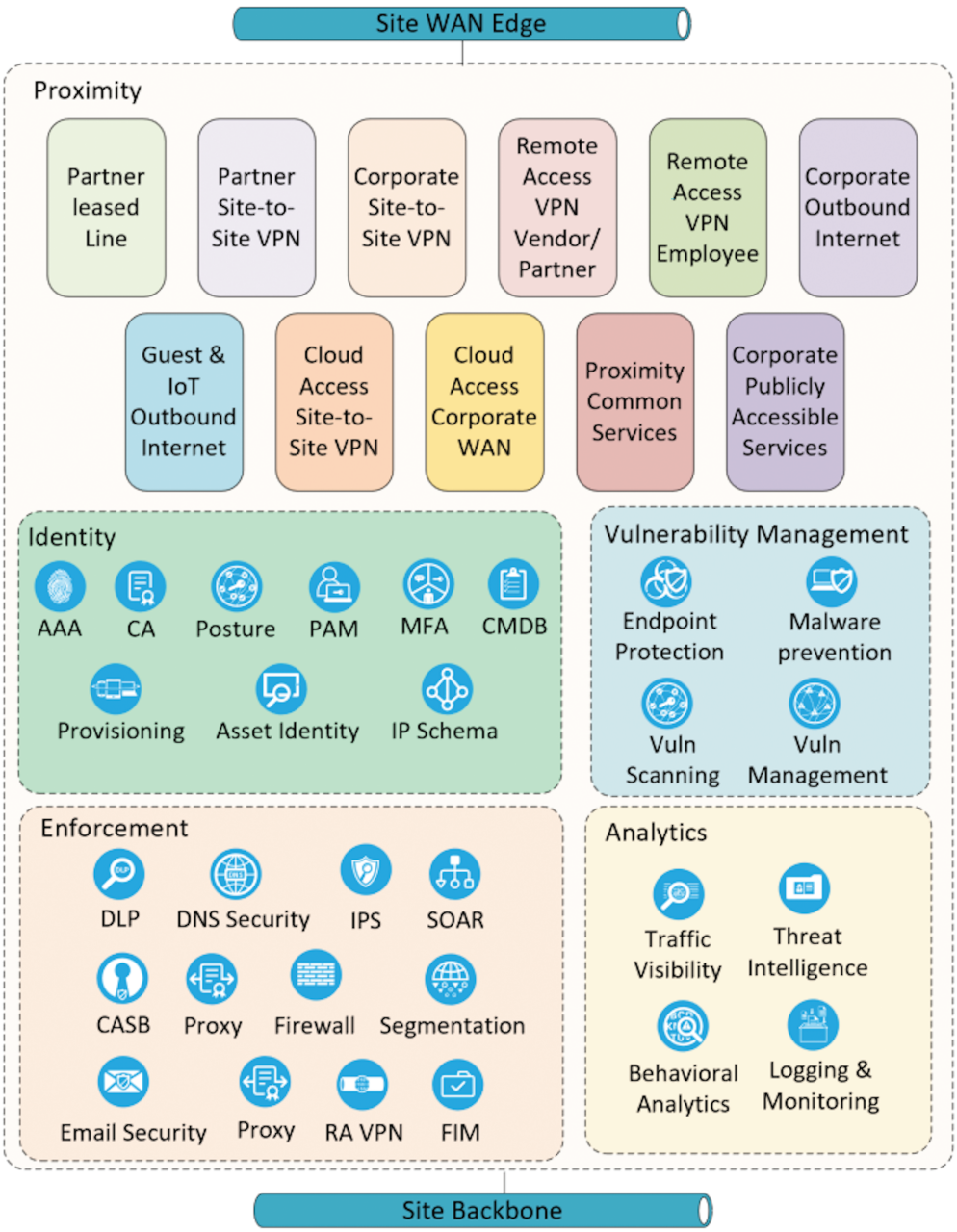


Figure 4-2 *Corporate Proximity Services*

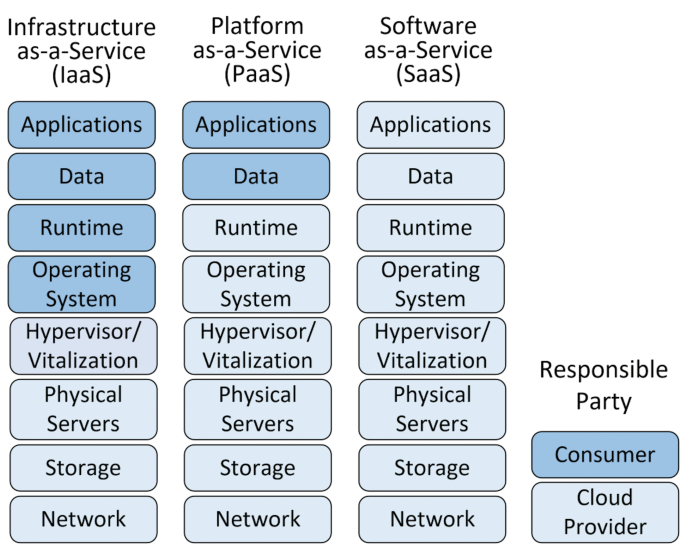


Figure 4-3 *Cloud Service Models*

Chapter 5

Zero Trust Enclave Design

Generation Type	Percentage	Billions of kWh
Fossil Fuel	60.8%	2504
Renewables	20.1%	826
Nuclear	18.9%	778

Source: US Energy Information Administration, "Frequently Asked Questions (FAQs)," www.eia.gov/tools/faqs/faq.php?id=427&t=3.

Table 5-1 *2021 US Generation by Type*

Chapter 6

Segmentation

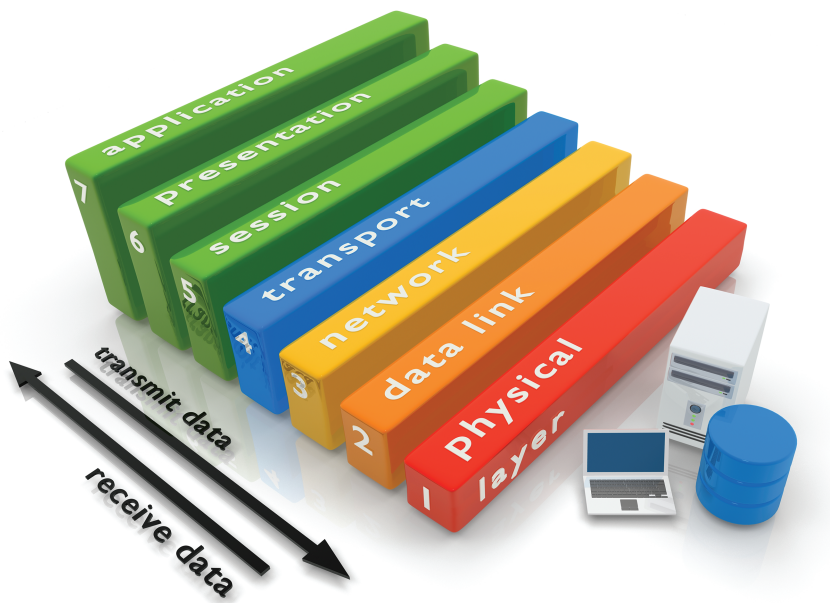


Figure 6-1 *The OSI Model*

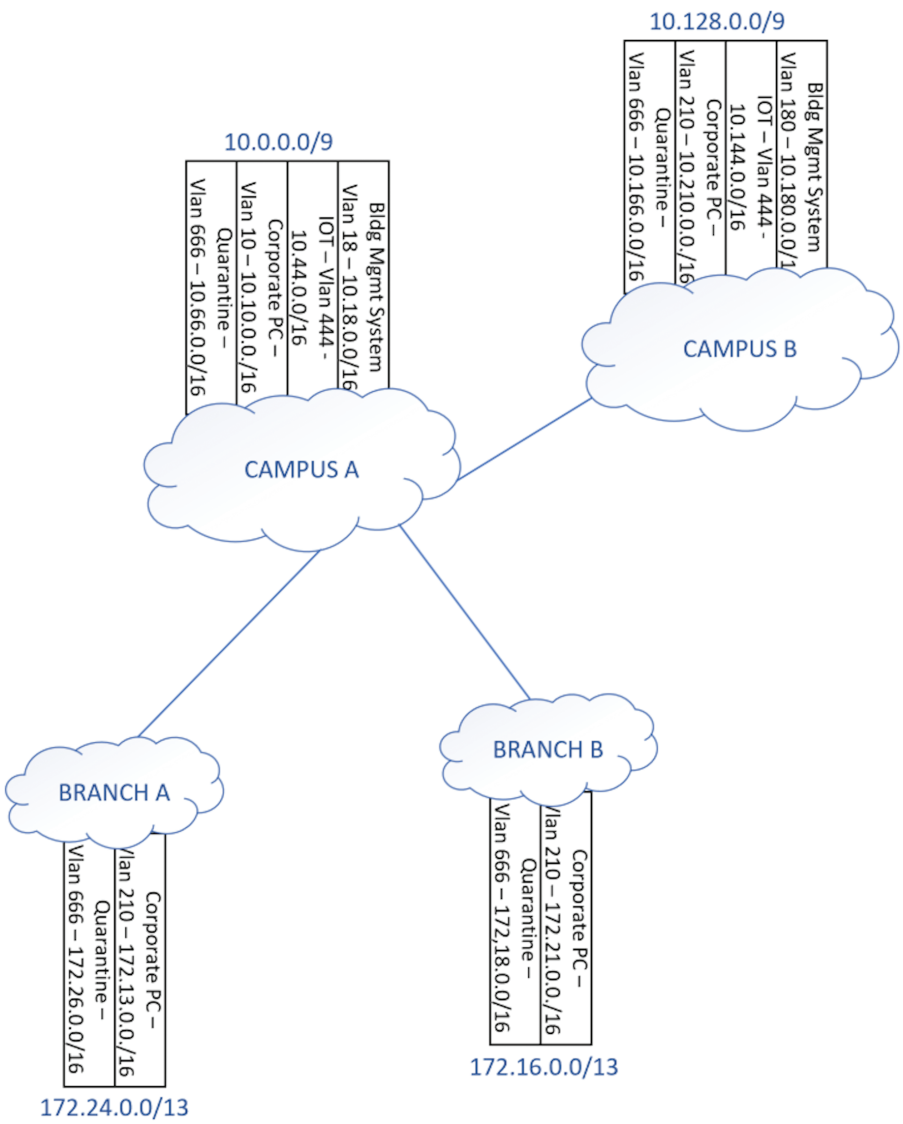


Figure 6-2 *VLAN-to-Subnet Mapping*

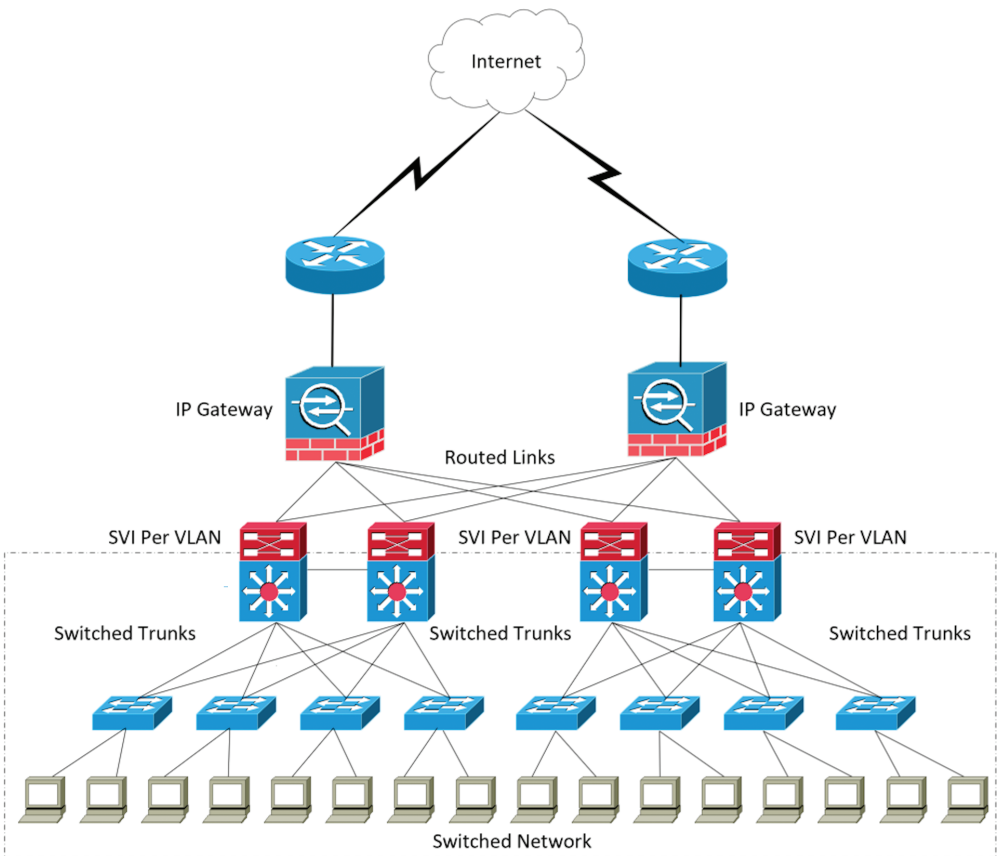


Figure 6-3 *Switched to Access Design*

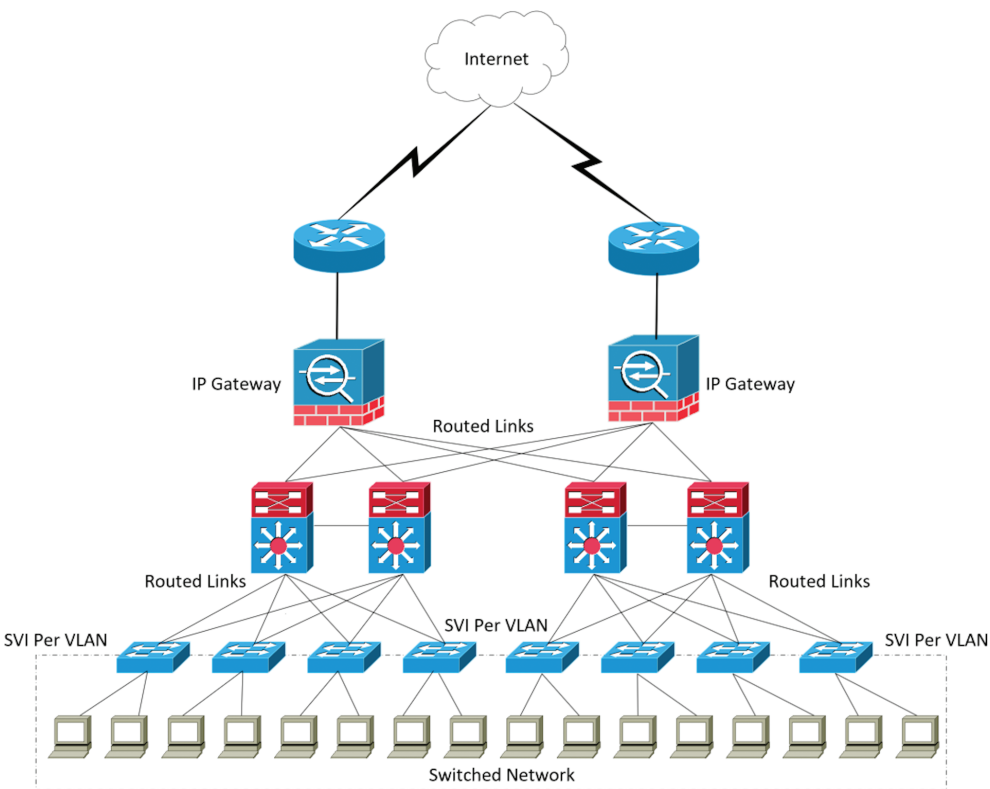


Figure 6-4 *Routed to Access*

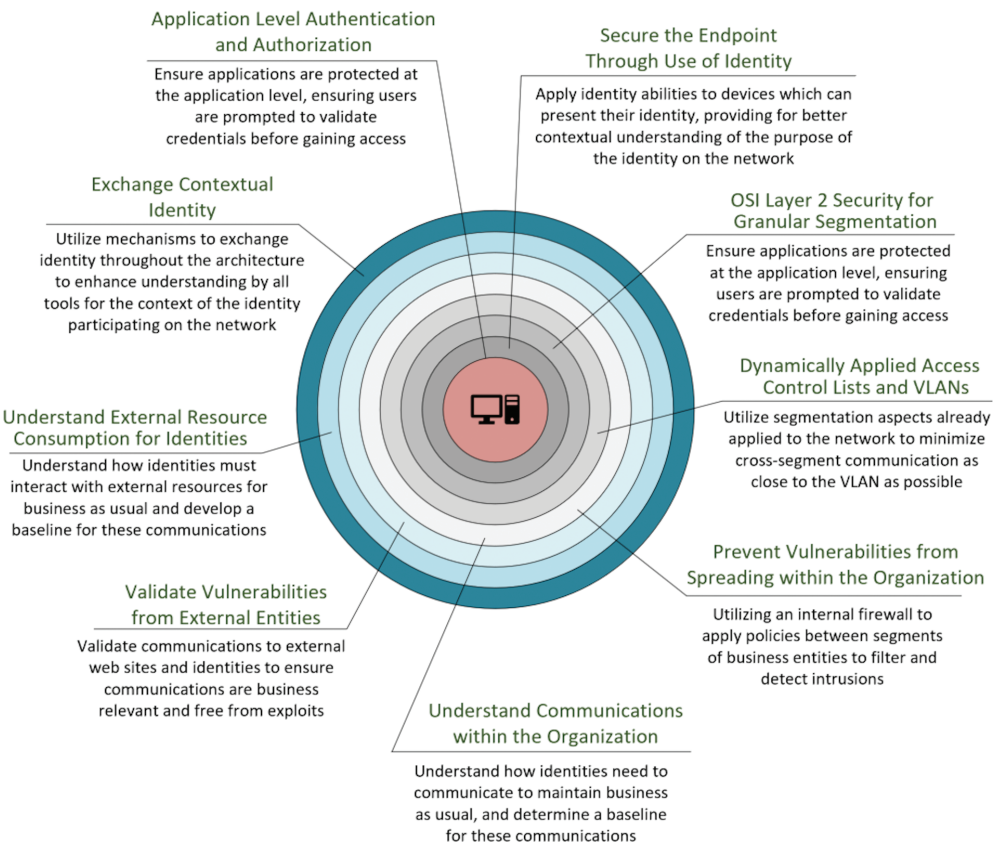


Figure 6-5 *Applied Methods and Considerations for Segmentation*

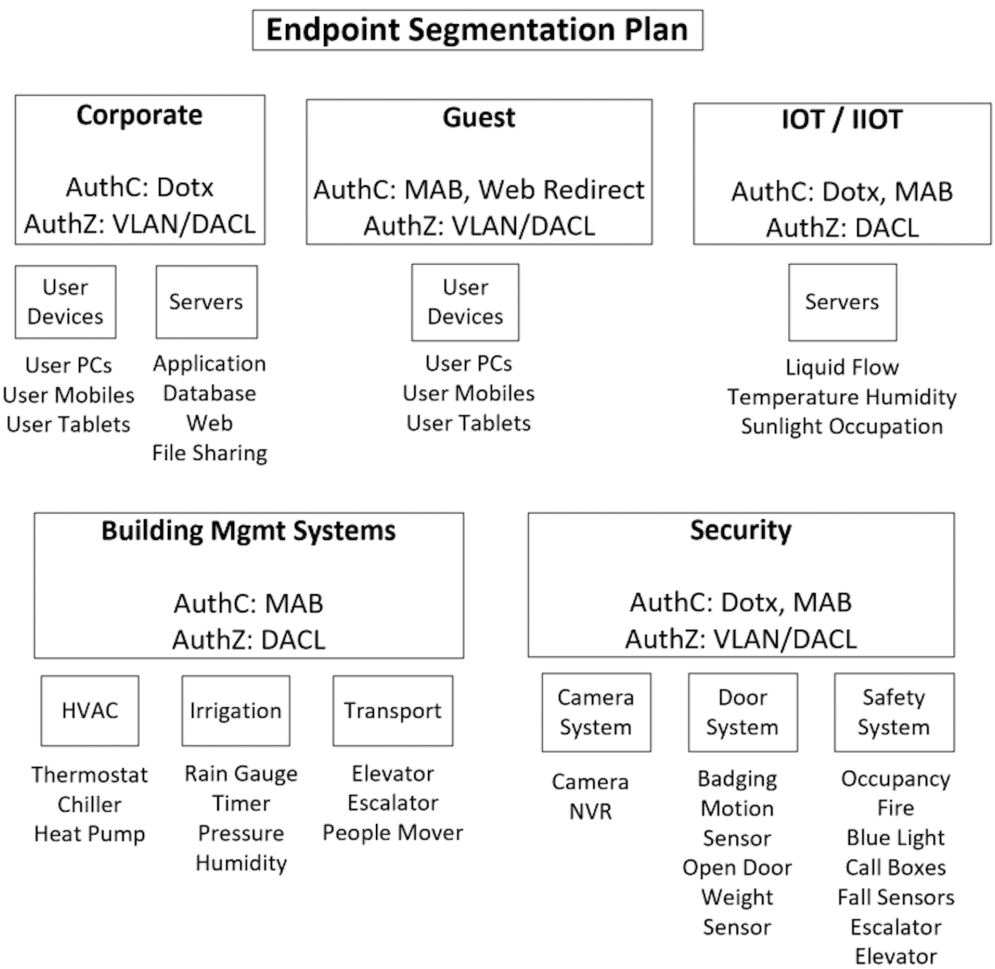


Figure 6-6 *Endpoint Segmentation Plan*

Example 6-1 *Various Access Control Lists*

```
! Standard Layer 3/4 Access Control List
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 10.10.64.1 eq 23

! Security Group Tag Layer 2/3/4 Access Control List
cts role-based access-list rbacl1
  permit udp src eq 1312
cts role-based access-list rbacl2
  deny ip log
cts role-based sgt 10 dgt 20 access-list rbacl1
cts role-based sgt 20 dgt 10
```

Chapter 7

Zero Trust Common Challenges

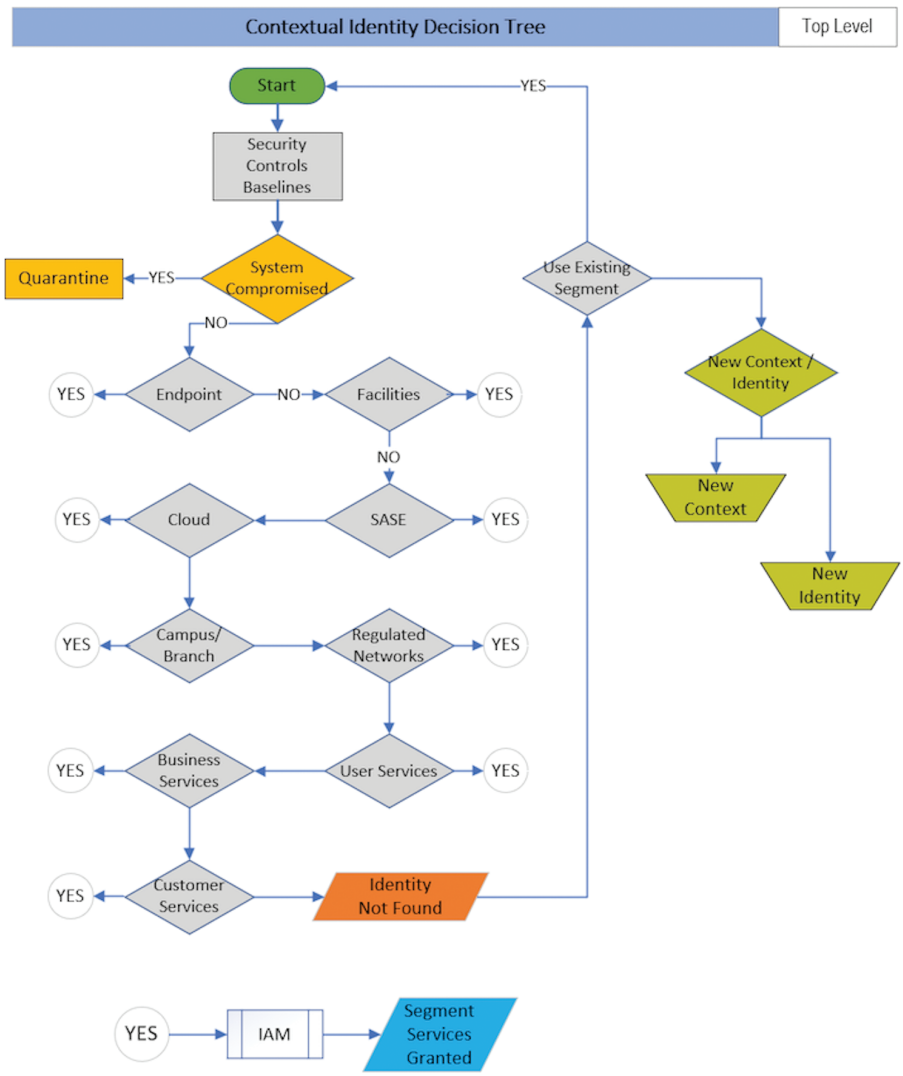


Figure 7-1 *Determining Contextual Identity*

Chapter 8

Developing a Successful Segmentation Plan

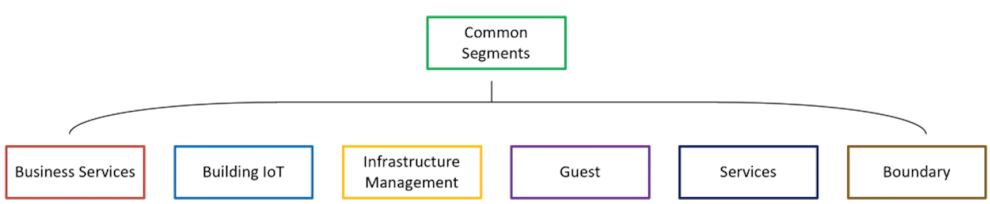


Figure 8-1 *Sample Healthcare Administration Building Segment Mapping*

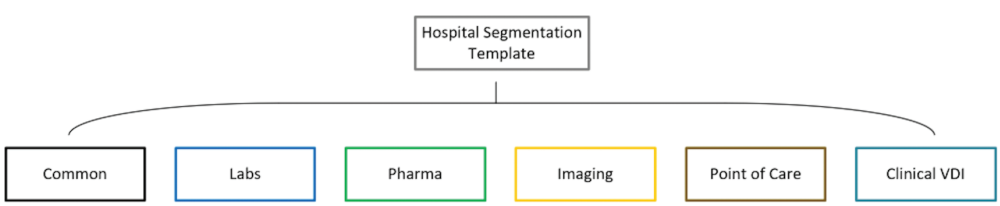


Figure 8-2 *Common Healthcare Endpoint Types*

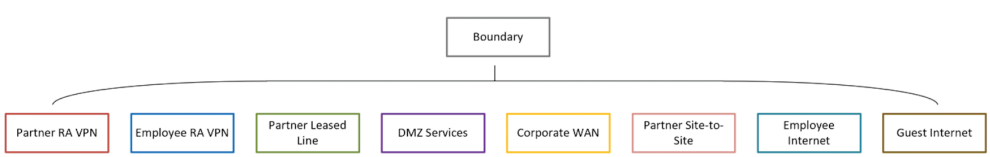


Figure 8-3 *Healthcare Boundary Service Segmentation Service Mapping*

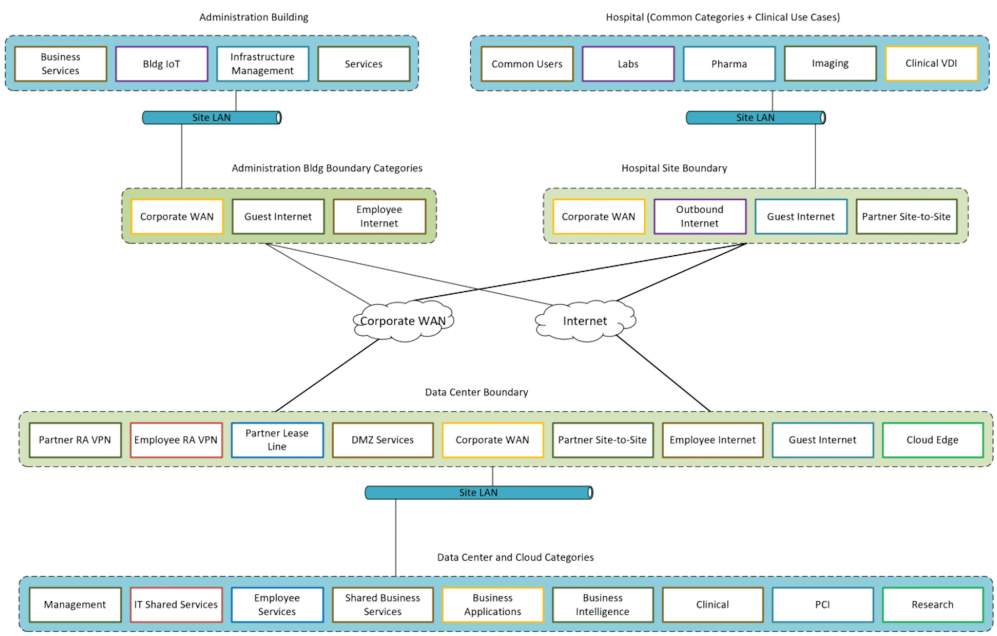


Figure 8-4 *Segmentation Model*

ENCLAVE TRUST MAPPING		TO	Enterprise		Facilities		Digital Edge		Cloud		Common Services			Business Services	
			Branch Endpoints	Corporate Endpoint	Physical Security	Building	Proxy to Third Parties	API Gateway	Private	Public	Identity Services	End-User Services	Administrative Services	Retail	Back-office Systems
FROM															
Enterprise	Branch Endpoints			Y	N	N	Y	N	Y	Y	Y	Y	N	Y	Y
	Corporate Endpoint		N		N	N	Y	N	Y	Y	Y	Y	Y	Y	Y
Facilities	Physical Security		N	N		Y	N	Y	N	Y	N	N	Y	N	N
	Building		N	N	Y		N	N	N	N	N	N	N	N	N
Digital Edge	Proxy to Third Parties		N	N	N	N		Y	N	N	Y	N	N	N	N
	API Gateway		N	N	Y	Y	N		Y	N	N	N	N	N	N
Cloud	Private		N	N	N	N	N	N		Y	N	N	N	Y	N
	Public		N	N	Y	Y	N	Y	N		N	N	N	Y	N
Common Services	Identity Services		Y	Y	N	N	Y	N	Y	N		Y	Y	N	N
	End-User Services		Y	N	N	N	N	N	Y	Y	N		N	N	N
	Administrative Services		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y
Business Services	Retail		N	N	N	N	Y	N	N	N	N	Y	N		N
	Back-office Systems		N	N	N	N	Y	N	N	N	N	Y	N	N	

Figure 8-5 *Policy Decision Matrix*

Chapter 9

Zero Trust Enforcement

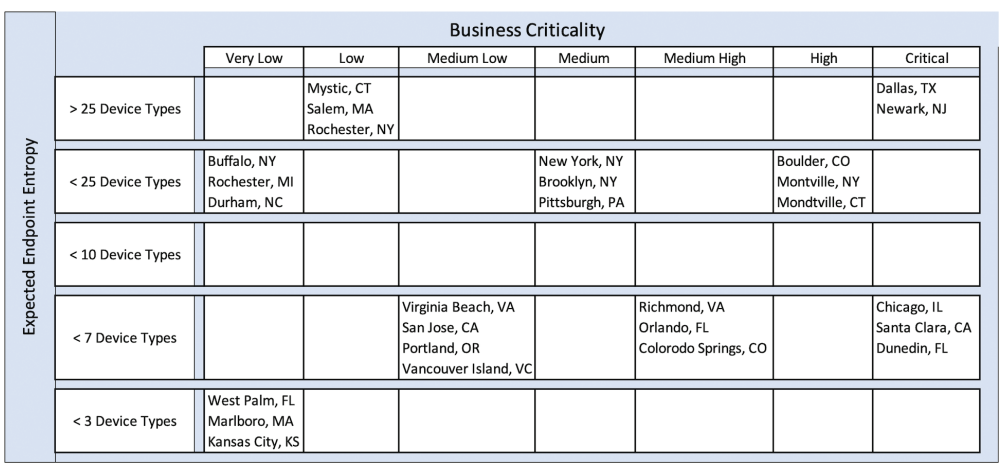


Figure 9-1 *Implementation Plan*

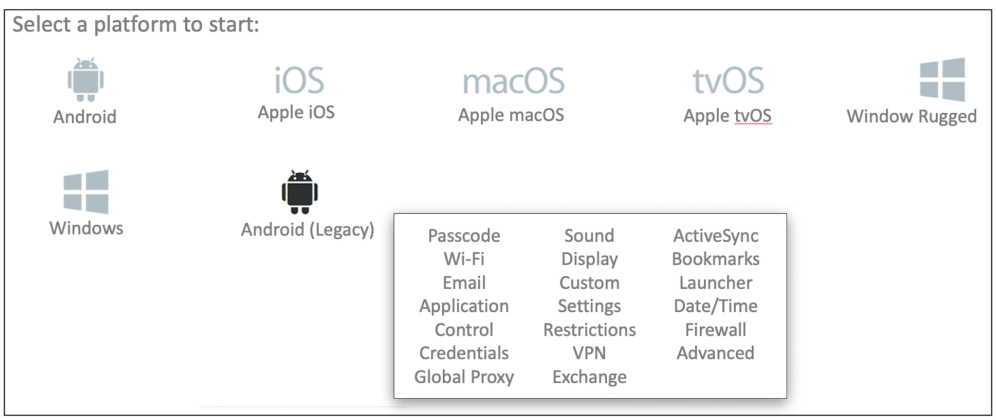


Figure 9-2 *Common Mobile Device Manager and Its Endpoint Device Abilities*

Corporate Endpoints	Contractor Devices	Data Center Devices
Medical Endpoints	Security Devices	Branch Devices
Manufacturing Endpoints	Media Devices	Quarantined Devices
Research Endpoints	Demo Devices	Remediation Devices
Lab/Nonproduction Endpoints	Network Devices	Shared Services Devices
Servers	Infrastructure Devices	Unified Communications Devices
IoT Devices/Sensor Devices	Headless Devices	
Guest Devices	Authenticated Devices	

Table 9-1 *Endpoint Mapping*

Chapter 10

Zero Trust Operations

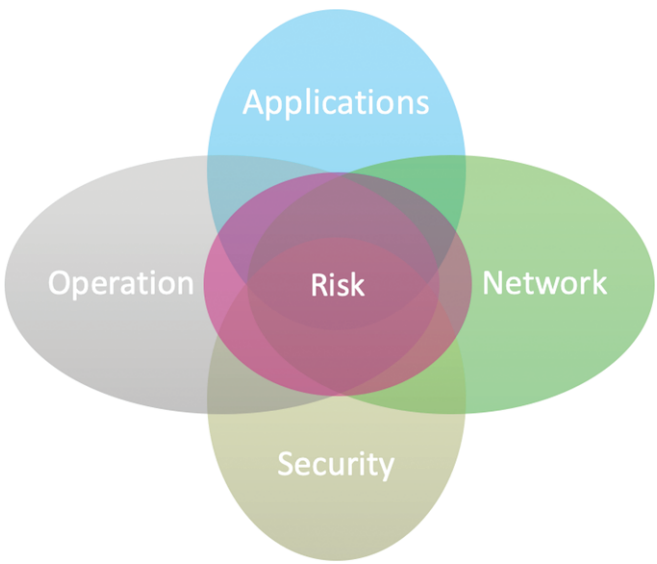


Figure 10-1 *Zero Trust Segmentation Cross-Team Alignment*

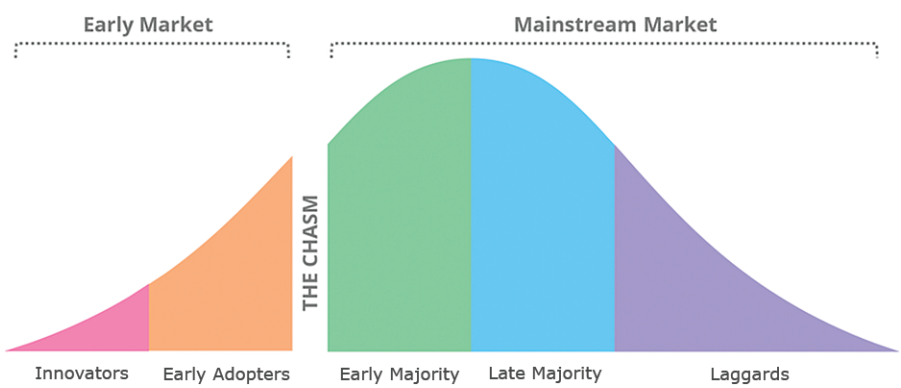


Figure 10-2 *Technology Adoption Life Cycle from* Crossing the Chasm *by Geoffrey A. Moore*

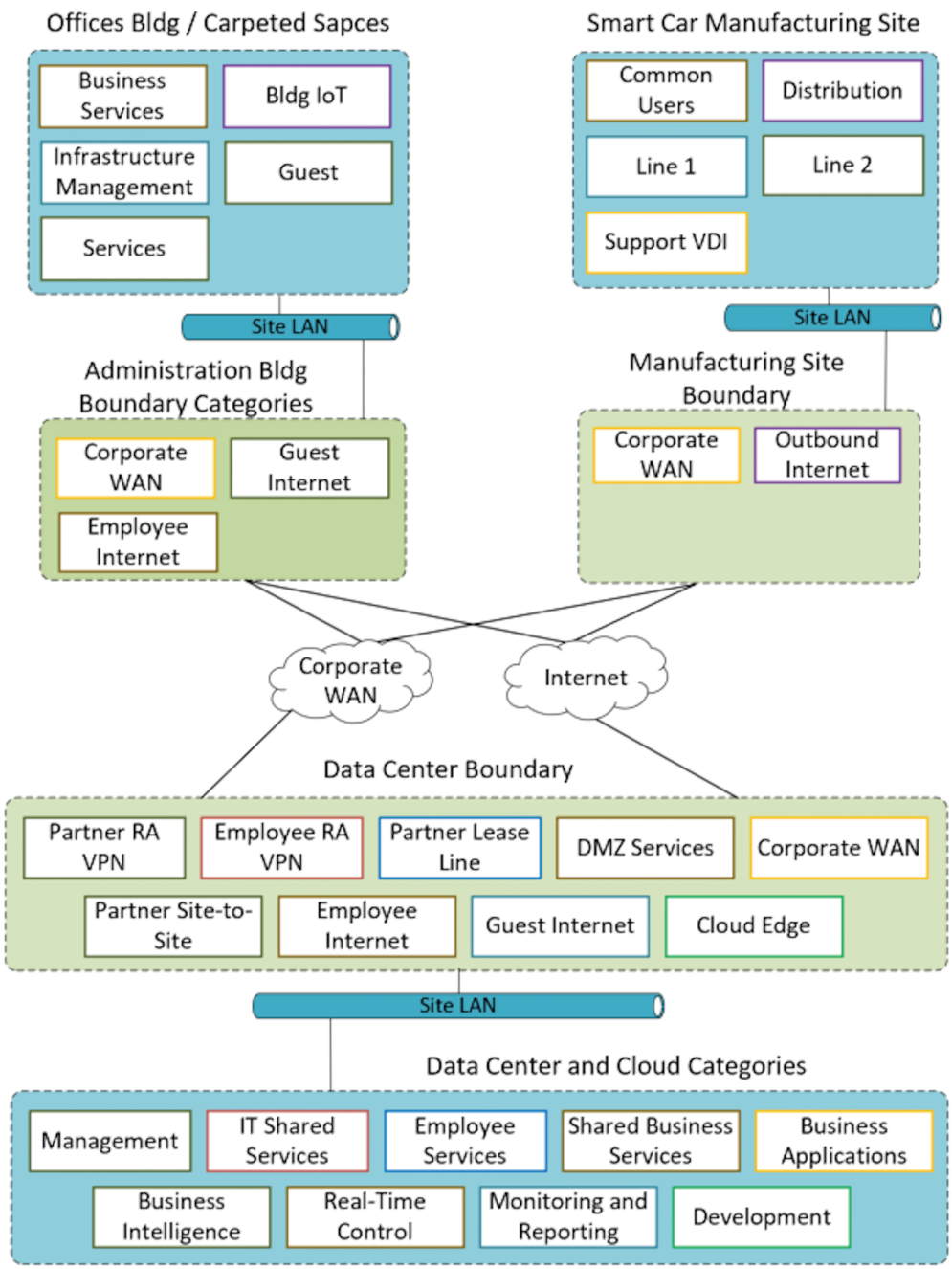


Figure 10-3 *Manufacturing Segmentation Plan*

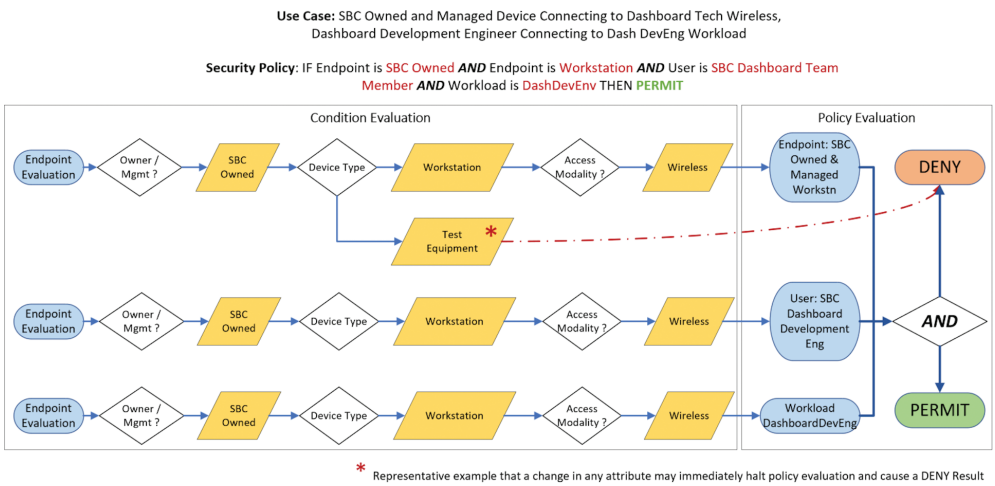


Figure 10-4 *Zero Trust Attribution Decision Flow*

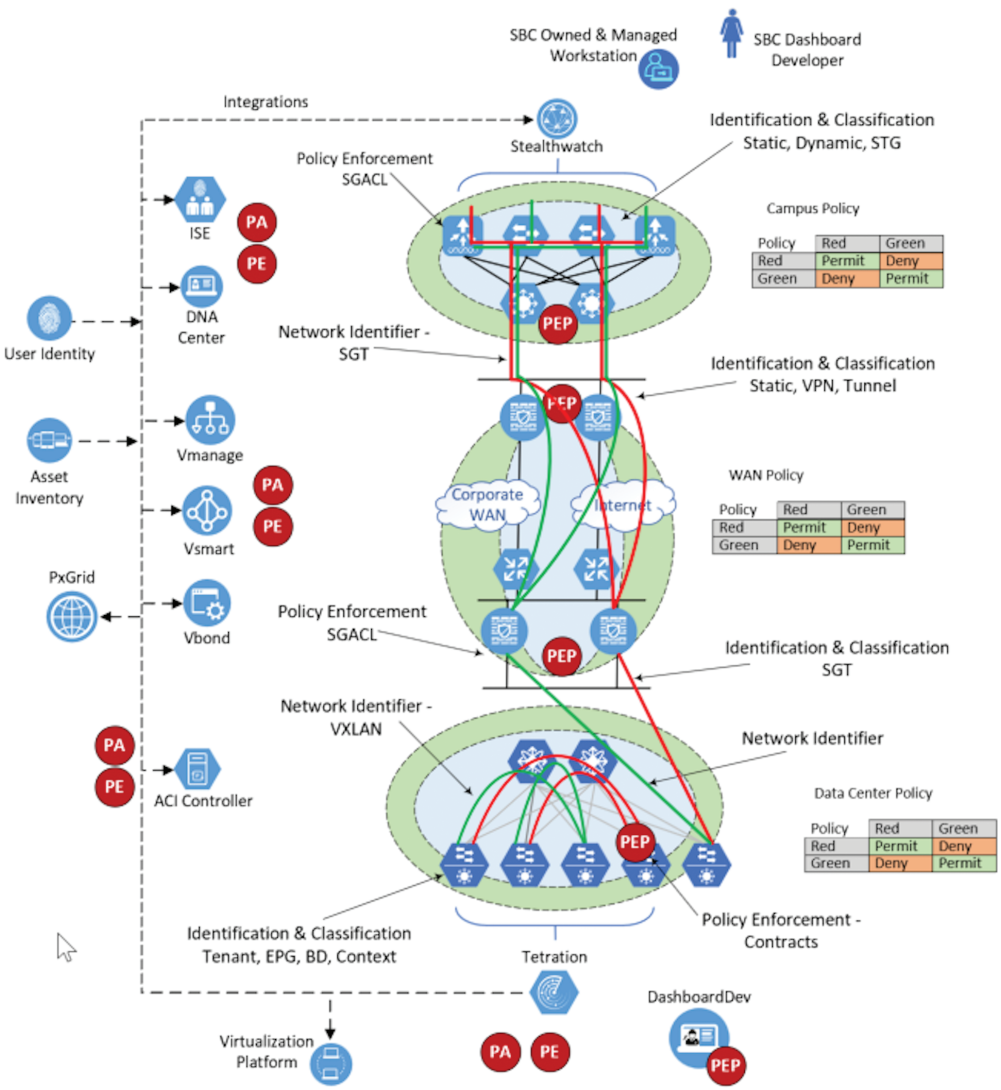


Figure 10-5 *Policy Maintenance: Where to Look*

Chapter 11

Conclusion

Figure 11-1 *Zero Trust Operations: Continuous Improvements*

Appendix A

Applied Use Case for Zero Trust Principles

Business Problem

Smart Building Central Inc. (SBC) was embarking on a state-of-the-art building, slated to be its new headquarters and be "A place that people would want to work." The new headquarters, deemed Smart Building Central, was slated to be a smart building with the goal of making working from the office as close to working from home as possible. Every system in the building, with few exceptions, would be connected to the network, with the backbone of the building being based on Cisco switching and wireless technology. With those endeavors, SBC Inc. also wanted to avoid being the next cybersecurity incident headline by ensuring that devices would only communicate in a manner that was sanctioned by the system's owners. This meant developing a secure communication bus between interacting systems, ensuring that the communications were mapped, controlled, and secured for daily operation within Smart Building Central.

The risk was significant. Smart Building Central's interconnected campus consisted of Internet of Things–based devices, mobile applications to interact with IOT devices, and a wealth of applications and middleware to control systems across the building. With this goal of creating the ultimate work-from-home experience, and the assistance of Cisco Security Services, Smart Building Central began its journey toward "the art of the possible." The knowledge that the approach would need to be as structured in its application as it was in its goal served as the guiding light toward success.

Goals and Drivers

The goal of Smart Building Central was to make the headquarters building a place where employees would want to work but also to show off the technologies to SBC's end customer in a sort of "art of the possible" partnership between Cisco and SBC Inc. SBC's line of building enablement technologies—including elevators, escalators, cameras, HVAC

systems, lighting systems, irrigation systems, and security systems—would all be the central showcase of Smart Building Central, along with custom-developed integration software and brokering systems.

With breaches of recent years top of mind, SBC knew that there would be a need to understand how a centralized mobile app could integrate to change environmental factors around the individual worker. It would need to be able to locate users within the building on the scale of feet, and help them navigate to building services, both in normal times and during emergencies. Combined with the expected functionalities of any office building, including scheduling conference rooms, payment system integration, and even ordering from the resident Coffee Shop, smart technologies were meant to link users to services in a seamless manner. However, unauthorized communications had to be prohibited from high-risk systems, such as HVAC systems communicating with point of sale. The largest challenge to be overcome was going to be the flat nature of the network, designed for no more than a couple thousand users. SBC Inc. defined new goals:

- Priority Goal #1: Understand all devices within an environment or building, their users, and network access devices.
- Priority Goal #2: Evaluate the ability for all devices to be authenticated and dynamically authorized to the network through testing of sample devices, identified within the discovery process.
- Priority Goal #3: Determine communications required externally for each device as identified.
- Priority Goal #4: Determine the internal communications required for each device identified.
- Priority Goal #5: Ensure that all devices are onboarded into the asset management database, providing a single source of truth for devices unable to actively authenticate.
- Priority Goal #6: Force authentication for all devices capable of authenticating.
- Priority Goal #7: Exchange authentication data with peer systems within the environment.
- Priority Goal #8: Apply differentiated policy for actively authenticated devices.
- Priority Goal #9: Apply differentiated policy for devices unable to actively authenticate.
- Priority Goal #10: Provide metrics to prevent authentications that were not legitimate in nature.

Application of the Principles of Zero Trust

Like many deployments, Smart Building Central was designed by its technical architects in alignment with classic networking aspects, aligning with a common "hard perimeter with soft, gooey interior." Their classic design focus had as its key tenet that any device could get onto the network and have its communication limited only at the perimeter firewall.

All other connectivity internal to the network was allowed with few enforcement mechanisms utilized within the "network trust boundary." This was described by Cisco's architects as a "connectivity over security" model. Due to the nature of its business, SBC Inc. found itself in a position where it would need to align with multiple regulatory requirements, including a need for authorized access, understanding of contextual identity, prevention of interactions between devices with no business interacting internally, and understanding of interactions with external entities. SBC not only had to account for devices interacting on behalf of business as usual but also had to plan for periodic review, auditing, and attempted exploitation of the devices and network as part of their future considerations.

The first step toward implementation of Zero Trust at Smart Building Central was a workshop, as described in Chapters 1–3. In its first attempt to hold a workshop, SBC started by inviting director-level talent from its networking and network security teams. As seen in Figure A-1, within the greater reporting structure of SBC Inc., networks fell under the chief technology officer, while network security fell under the chief information officer.

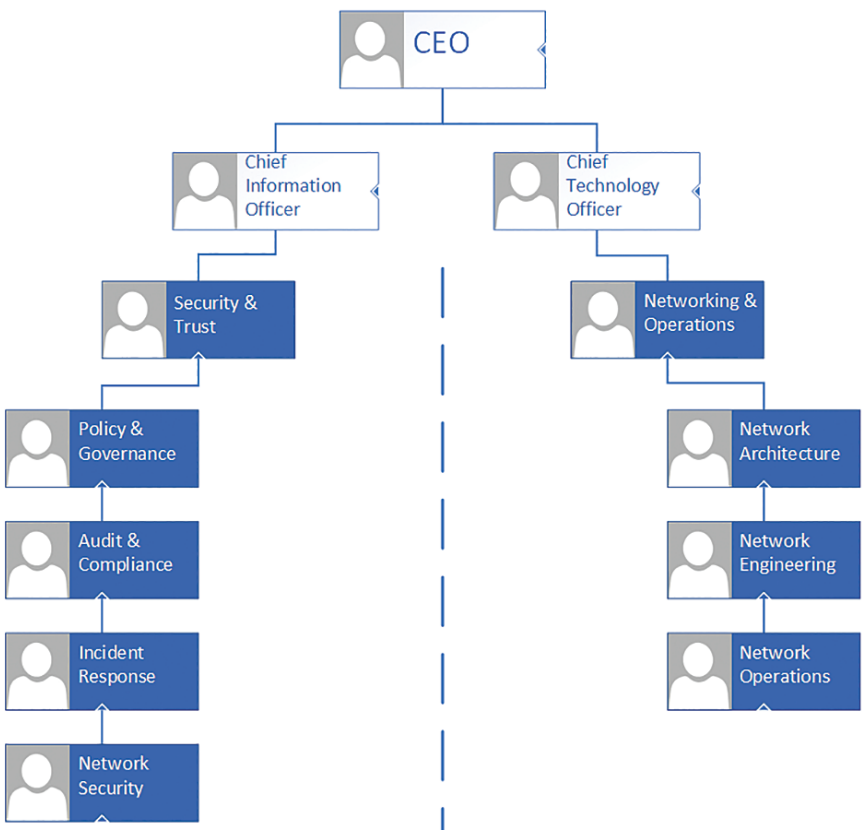


Figure A-1 *Organization Chart of SBC Inc.*

Within the SBC Inc. culture, this hierarchy made for challenging interactions for a multitude of reasons. To begin, the two teams had different motivations and definitions of success with relation to those motivations. The networking team, which was within the same reporting structure as the network operations team, was focused on getting devices onto the network. Their primary goal was ensuring endpoints were able to conduct their business functions. The burden of doing so was already challenging. The typical process for an endpoint that was added to the network was distributed across multiple functions with no definitive process defined for the exact requirements the endpoint, user, or department must follow to gain network access. Unfortunately, this presented itself to a fair number of additional challenges, short timelines, and removal of any roadblocks that prevented a device from getting onto the network for a legitimate business purpose.

The network security team was admittedly often at odds with the networking team. Being responsible for audits, penetration tests, incident response, and misconfigurations, the network security team was quite a bit more conservative in their approach to allowing connectivity on the network than the networking team. Throughout the policy and governance phase of the Zero Trust engagement, it quickly became clear that a singular mission statement and some level of personnel to facilitate that mission statement had to be defined. So long as both teams conflicted in their view of the definition of "success," no practical progress could be made. SBC needed to avoid the inevitable use of timelines alone to dictate the approach to the problem statement of "excessive access and connectivity." SBC Inc. wanted to avoid making the same mistakes by implementing the same methods as used in all other architectures. Due to the need to align with regulatory requirements that would be unique to Smart Building Central, the same approach would fail in its ability to align with these regulatory requirements, causing loss of government contracts, manufacturing grants, and in-house payment systems.

The first task agreed upon between the attendees within the initial workshop was a need to define the outcomes required for the successful deployment of Smart Building Central. This definition of the successful outcome needed to be solely defined as the success criteria, not considering the current processes or governance that existed within SBC Inc. at the time. Five goals were determined to define success for Smart Building Central, all to be shared across organizations within SBC Inc. These goals included

- The ability to definitively identify a device as it was connected to the network, resulting in the device being provided only the access it required to fulfill its business purpose.
- Prevention of unauthorized devices introduced from within Smart Building Central to access any key resources within the building or within SBC Inc. data centers.
- Minimization of impact of any one device being compromised within Smart Building Central or the greater SBC Inc. preventing business as usual within Smart Building Central.

- The ability to enable next-generation smart capabilities with devices allowing for both comfort as well as health and safety alerting for both administrative and individual authorized users within the building.
- Metric-based re-evaluation of priorities of Smart Building Central's implementation of these technologies to define whether additional adjustments to tactical approaches to solving these challenges needed to be implemented, or whether the charter was infeasible for SBC Inc. as a company.
- The collective agreement across SBC's management that these goals were their guiding principles ensured no one entity could dictate the approach or metrics upon which the outcome could be measured.

Policy and Governance

The first determination made by attendees to the Smart Building Central Zero Trust deployment meeting was that a change in culture had to occur for the implementation of any additional restrictions to be introduced. Knowing that conflicts in the past had prevented similar projects from getting off the ground within SBC Inc., leaders within both the network and network security teams agreed that changes to the organization well "above their paygrade" would need to occur. An understanding of the business impact of not doing so would need to be well articulated to leadership within the disparate organizations to drive this change. The largest challenge to be overcome was separate measurements of success for network and security teams, specifically being uptime for business-related applications versus resources spent on responding to threats on the network, respectively. With the requirement to identify, understand, and enforce access for identities throughout the Smart Building Central campus being a key success factor for the implementation of Smart Building Central, priorities and metrics had to change. This change seemed drastic: an evaluation respective to whether security would inhibit the goals of the business versus SBC Inc. having the business at all. Without success in the form protecting the network from threats, SBC Inc. would lose its contracts to do business—the lifeblood of the company.

Throughout introduction to this use case, the term *initial* has been used in a purposeful manner. With the realization and agreement between network and network security teams that decisions to be made had to be made at a higher authority level, the ability to succeed without having this charter in place was prevented. Internal meetings, alliances at the highest levels, and mutual understanding of success across the business units within SBC Inc. had to be accomplished to enable this success. Over the course of three months post-workshop, SBC Inc. determined changes that needed to be implemented to ensure success of the Smart Building Central project. The first was a move of the network security team into the same organization as the network team, falling under a separate leader reporting through the chief technology officer. It was determined, based on business culture, that having teams report to separate executives with differing metrics of success

would continue to inhibit success. This success applied to not only the Smart Building Central project but also future projects that would be influenced by the technologies required to make Smart Building Central a success. With Network Administration, Network Security, and Network Operations all reporting through the same executive management, a singular authority could provide edicts for successful implementation of technologies that would fuel Smart Building Central.

It is important to note that teams concerned with audits, penetration testing, incident response, and policies governing each of these aspects continued to report through the chief information officer. This alignment provided for an independent body that could help influence the technologies and controls required when applying them to the Smart Building Central project. In addition, this alignment gave the network and network security teams the ability to define their largest pain points that must be overcome to accomplish the goals set out before them. Those pain points included

- The inability for either team to track, determine, or influence new purchases of devices that would require network connectivity.
- The lack of any communication to either team on the requirements for a device on the network before new devices were connected to the network.
- An inability to validate that devices were properly configured or onboarded with proper settings to connect to the network.
- A culture of consistent exceptions that allowed for the loudest or most influential users to connect devices to the network without question as to the merits of the connectivity or business purposes.
- A lack of visibility into what was currently on the network and, more importantly, whether those devices belonged on the network.

A large aspect of Smart Building Central's success would be overcoming the pain points as defined by the network and network security teams. To do so, the collaborative team could now present a need for definitive policy to require which devices were provided what access and how. This information would be communicated to the newly formed corporate security team. Then, the corporate security team, made up of policy writers, auditors, penetration testers, and incident response engineers, could now act in an advisory role to the network team. The team would maintain a separated responsibility of ensuring the compliance of users to corporate standards, while the network security team merely had to build in the controls to validate that compliance.

The corporate security team, now with this newly defined responsibility, created policies aligned with Zero Trust core principles:

- All users who wish to partake in network communications with any device, application, or username must agree to adhere to policies for the protection and control of data flow within the SBC Inc. network.

- All devices must be clearly identified through network discovery means before being allowed to participate on the network in any manner. Identification of the device must include
  - Who owns, manages, troubleshoots, and maintains the device, including its respective life cycle and vulnerability management techniques.
  - The type of device, its purpose on the network, and assurance that it adheres to the identification policies defined for participation.
  - The expected location or locations for the user or device when interacting with the network.
  - The expected life cycle of the user, device, or application as it interacts with the network, including whether it is constantly connected, or intermittently connected.
  - The medium that the user, device, or application expects to be connected over.
  - The expected interactions, ports, protocols, and communication patterns that a user, device, or application had regarding other identities within the network.
  - The exception to this policy is guest users who do not belong to SBC Inc., its partners, affiliates, or authorized network users.
- All devices that interact with the network must have validation by the owner, manager, or operational technician that the device has been properly onboarded in accordance with onboarding standards for SBC Inc.
- Any unauthorized device added to the network will be removed from the network with haste, and the responsible owner, manager, or technician prevented from reintroducing the device until all previous steps were validated by the network audit team to ensure compliance.

These simple but clear policies ensured that respective teams were made responsible for devices on the network, as opposed to overloading two teams with responsibilities that should be distributed across the company. As a result, these policies also increased the collaboration between network teams who would be responsible for ensuring a device could get on the network, and network security teams who ensured that control mechanisms were put in place to allow only required connectivity. This collaboration allowed for the respective teams to focus on properly onboarding and identifying devices, as opposed to auditing and ensuring that repeat offenders or application owners who disagreed with the policies were all held to account. In Smart Building Central, following policies would be the only way to add devices to the network.

Understanding the Business

Post-reorganization, Smart Building Central still had one major gap: When it came to the devices, users, and even applications that used the network, SBC was reactive in removing

unauthorized devices. With regulatory requirements being a net-new addition to the building, its infrastructure and endpoint management, changes in processes would also need to be considered to better identify and act in a proactive manner to remove threats as soon as they were identified. The first step in this process was to better understand the business of SBC Inc., and specifically how the business was broken down. The understanding for which business units, their purpose within the company, and their reliant endpoints, users, and applications would ensure each business unit could fulfill its purpose. In the second workshop held to plan for the implementation of Smart Building Central, senior leaders were invited to participate to work through what their business was responsible for, key systems the business relied on, and known interactions for those systems.

Considering the needs of Smart Building Central to be a headquarters building with enabling technologies, it was agreed that the leaders from current Corporate Operations would be invited to an identity-focused workshop, including business units with allocated space with Smart Building Central. These Corporate Operations departments, including Finance, Human Resources, IT, Marketing, and Partner Sales, were assigned into the corporate endpoints category, which would later become one of the enclaves used to organize and enforce policy. Each department within the corporate endpoints category was asked a series of questions:

- How do your users typically access resources to do their jobs?
- What types of endpoints do you, your employees, and your partners or contractors use when they connect to the network?
- Through which medium do your users connect when they connect to critical resources?
- What are the critical resources that you rely on to do your job?
- Is your department active only during standard business hours, or do you regularly have long shifts? Do these shifts differ per time of year?
- Do your employees utilize their mobile devices at work for either personal or professional reasons?
- What systems within your standard working environment could be improved to make your use of the office more effective?

As would be expected, these questions, even when provided ahead of time to department heads and senior leadership, resulted in a variety of answers. The most common answers were small handfuls of application names or IP addresses being provided, especially by nontechnical resources. The answer to what could be improved, however, was broad and varied. Users needed the ability to present in an ad hoc manner devices that were most effective to their working patterns, an ability to easily find available collaboration spaces, and an ability to move to collaboration spaces most suited to brainstorming for the project at hand.

It was found that SBC Inc. had standardized on Lenovo laptops for all employees and had a stringent exception process to prevent the use of any other brand of laptop accessing corporate resources due to exploitation the company had suffered years prior. At the same time, other laptops could connect to the wireless guest network while on site for Internet access, and data could easily be transferred to them via physical means. Employees commonly utilized this tactic to work on laptops with larger screens, less stringent requirements on installed applications, or on machines where they were less likely to have their activity tracked. This behavior was typical of IT and Marketing users, both departments containing technical users who understood workarounds to policies that existed preceding the policy rework.

It was also found that most users split their time accessing resources on their corporate devices between wired and wireless networks, mainly because those employees who were in the office would dock their laptops when at their desk. This activity would cause the laptop to prefer the wired connection but switch to wireless when attending meetings, sales briefings, or events away from the employee's desk. The wireless network, being solely preshared key authentication, provided a medium over which third-party devices could be joined with little control over the owner or purpose on the network. There was also significant disregard for hiding the password needed to join the SSID. So little caution was given to the preshared password that plastic placards could be found throughout IT cubicles with a "frequently asked questions" list, including the key for anyone to observe and use.

Both aspects of security policy limitation were directly contributed to by the lack of identification techniques for any resource on the network. Most identification of endpoints was both reactive and done via tribal knowledge or manual lookup efforts. For many of the applications that employees utilized to do their regular jobs, there was little understanding of how these applications interacted between themselves, with application owners having left the company sometimes over a decade ago. With these application owners gone, the management of the application was left to no one in particular. If an application broke, technicians would log in to it with either default credentials that had never been changed, or with credentials that were static and part of a knowledge base that anyone on the network could gain access to. The significant risk of these practices being common across departments created a renewed sense of urgency with senior management of SBC Inc. to secure business processes and to identify devices and applications. Truth be told, senior resources within SBC Inc. did not realize how large of a risk the network and its connected devices had become.

The next aspect of the identity workshop for each of the respective corporate departments was an ask about roadblocks to doing their daily work or encouraging employees to come into the office. With Smart Building Central being slated to be an innovation forum for new ideas and enablement technologies, SBC Inc. wanted to hear from its business units what would encourage employees to want to come into the office, as opposed to being remote or working from home. The most desired aspect of working from the

office was to network, socialize, and build their relationships with coworkers to feel more aligned with the business and the team that they worked on. Many of the participants alluded to "conversations around the water cooler" being an aspect that they valued most about being in the office but complained that the office was commonly far too noisy and distracting. One of the largest asks was to have collaboration areas where employees could work together on projects without the need to shout over cubicle walls. However, a major aspect of this collaboration was being able to seamlessly share ideas digitally without the need to find or schedule a conference room, which was already a very difficult task. It also was not guaranteed that the collaboration was best suited for laptops with standard mouse and keyboard layouts. Many employees noted they would rather be able to effortlessly share their tablet or phone screens with each other than to whiteboard with smart pens, enabling them to better share, edit, and save ideas for future development and expansion. This meant providing areas that could be easily accessed, connected to, and collaborated within, without distracting others or needing to clear multiple technological hurdles to do so.

With these asks, understandings, and recommendations from those occupying the building, the company's innovation engineers were invited to the workshop to illustrate their vision for Smart Building Central's future technology enablement. The innovation team, focused on employee experience as well as marketing of SBC's products, painted a futuristic picture of a headquarters that the market leader in smart buildings should provide:

- Ensure that there was as little downtime in the workday as possible; this effort was mainly a function of ensuring that employees could get to meetings and destinations as quickly and efficiently as possible. This innovation was enabled through a vast array of technological solutions:
    - For employees to get to another floor and meeting as quickly as possible, the longest amount of time spent was waiting for an elevator to climb multiple stories. To mitigate this wait, the SBC Inc. innovation engineers had created an application that would inform a centralized controller of an employee's need to take the elevator to another floor. This controller worked the same way that rideshare services did: an employee could use a web page or mobile application to inform the controller that they needed an elevator to another floor. After the employee enrolled in this need, location tracking was enabled for their mobile device and tracked in relation to distance from the elevator. This location tracking both provided a GPS-like navigation path within the application for the user to get to the closest elevator and their ultimate destination, as well as scheduled one of the six elevators in Smart Building Central to arrive with a destination of the employee's floor already programmed in. This location tracking was able to factor in calculations of where the user was at a given time, their walk speed, and distance from their destination for the application to schedule their elevator ride.

- Resembling common coffee shop mobile applications, Smart Building Central incorporated a mobile ordering system to the building's coffee café and cafeteria. With full menus provided within the app, employees could order their most common orders on the way to a meeting without having to worry about whether fresh coffee was available or food was provided at the destination conference room floor.

- Ensure that meetings were most successful and collaborative through seamless interaction. Technology was used to ensure that conference rooms were both available and easy to use regardless of the technology an employee possessed:
  - From within the same application as navigation and food ordering, conference rooms could be scheduled on demand with a click of a mobile phone button. Virtual meetings, provided by Cisco WebEx, were automatically joined as soon as the user entered the physical room, as detected with motion-sensing abilities. If the user elected to invite others to the virtual meeting, they would be automatically notified of the virtual address for the room.
  - Conference rooms were outfitted with sharing technology that was compatible with all Apple- and Android-based phones, providing the ability to share or mirror screens from any device on the building's Wi-Fi network and display content to the series of TVs found within the meeting room they were invited to participate in.
  - The mobile application, recognizing the owner of a conference room, would allow change in temperature, adjustment of shades, change in overhead lighting, and volume of the virtual participants on the screen in the room.
  - For Smart Building Central's centralized conference space, able to accommodate thousands of visitors for the exploration of innovative ideas that SBC Inc. sold, audio/visual systems could be used to broadcast to internal television networks within Smart Building Central as well as companywide.
- Ensure the comfort of all who would visit Smart Building Central:
  - In conference spaces, thermal imaging cameras were used to calculate the number of attendees, determine the ambient temperature, and adjust the conference room temperature to maintain consistent audience comfort.
  - With Smart Building Central being in a sunny geographical area of the country, one of the greatest complaints was the temperature and light in other building offices. While having a corner office was a privilege, the glare and heat generated by windows surrounding the office made it unbearable in the hot summers. The same went for conference rooms full of participants in physical meetings. Like the temperature-sensing technologies in conference rooms, temperatures could be adjusted on a per room basis. This was combined with lumen-sensitive

windows that could detect direct sunlight and change the tint of the window through electro-chromic glass inserts, saving both energy and time of pausing due to glare or heat concerns.

- All conference rooms, private offices, and the employee gym were outfitted with online music streaming built into the building mobile app.

The ideas presented within the workshop were futuristic, innovative, and concentrated on creating an employee focus for Smart Building Central. However, in the spirit of Zero Trust, SBC Inc. knew to align with the newly created policies for endpoint participation on the network, large changes would need to be made ensuring the security of not only critical resources within the SBC Inc. network, but also to maintain the comfort and safety of employees. The first step would have to be introducing a definitive identification mechanism into the building's infrastructure.

Identifying and Vulnerability Management

To break the massive undertaking of identifying devices on the network into practical amounts, Smart Building Central first was broken into five Virtual Routing and Forwarding (VRF) instances: Corporate, Building Management Systems, Labs, Guests, and IOT. For each Virtual Routing and Forwarding instance, 100 VLANs were allocated in a fashion that could provide predictability to a device's initial category on the network. For all corporate PCs, tablets, and managed mobile phones, for example, devices were allocated to the Corporate VRF. However, how could SBC Inc. be sure that just because a device was connected to a switchport that belonged to the Corporate VRF, that it was a corporate-provided device?

Smart Building Central deployed Cisco's Identity Services Engine to identify devices throughout the network, while also aligning with new policies that would require that the device be definitively identified. For IOT devices specifically, Identity Services Engine was complemented by Cisco CyberVision, specializing in operational technology identification. The greatest advantage that SBC Inc. had working in its favor is a culture of consistent corporate endpoints, all of which were centrally managed. PCs managed through group policies were already the standard workstation of choice after the removal of third parties that were unmanageable. This allowed SBC Inc. to push new group policies to managed endpoints that would enable the device to present its username and device credentials to the network. These credentials were subsequently verified by Identity Services Engine and referred to Active Directory for validation. Once validated, endpoints would be actively probed for software installation related to endpoint management agents being enabled, anti-malware agents being up to date, and the presence of the Thousand Eyes clients was utilized for measuring network response times. The use of vulnerability techniques such as "posture checking" verified that the largest portion of devices on the network in Smart Building Central, the PCs that users were issued, were validated in both

their management status as well as ownership. All PCs that could not be identified or verified being up to date were prevented from accessing the network, with a resulting need to visit IT staff to remediate any management issues.

For applications and servers that had to exist on Smart Building Central's network and be local to the building itself, the initial step in identifying them was via their physical location on the network. Smart Building Central had a centralized main distribution facility (MDF) within the building where all servers were required to be located. In addition to being physically secured from other areas of the network, the MDF contained switches only allocated to servers that were required to be mounted in server racks allocated to the department. Policy enforcement could therefore consider this physical location as one attribute of the contextual identity used to enforce policies associated with these servers and applications.

For applications or servers connected to these devices, switches were unable to identify themselves using a native supplicant on the devices. As a result, the owner of a device had two options. The first option was an acknowledgment from the application owner that the device must be added into an asset management database, including properties for the device such as its owner, manager, troubleshooting contact, purpose, life cycle, interactions, protocols, and ports utilized to fulfill its function. All of these attributes were utilized to track the asset and to write strict policies for its interactions on the network. The risk incurred by the application or endpoint owner was that while the application may be business critical in nature, its inability to be identified and enforced would incur potential impact to SBC's contracts, and therefore, it would be prevented from executing functionality not explicitly documented.

The alternative second option to populating the asset management database manually was to provide SBC's IT department the ability to collect this information automatically using an agent installed on the server. This agent, which was part of Cisco's Secure Workload solution, collected behavior from the device's communications and provided for the ability to enforce policies or alert on deviation from those policies while not enforcing for critical applications. Upon the device's deployment, initial information would need to be populated, including the owner, manager, troubleshooting contact, purpose, and life cycle for tracking the device and ensuring it was understood who the responsible party would be should the device change its behavior. However, the behavior tracking ability of the Secure Workload agent lessened the burden of understanding all protocols and ports and ensured that a mechanism to enforce these policies existed as close to the server as possible.

Comfort-sensing devices were classified into the IOT Virtual Routing and Forwarding instance. Comparable to devices that would enable other aspects of the business, these devices would need to be classified in an equivalent manner to servers, ensuring that the identity of the device could be determined in a programmatic way. Ownership of the device was documented, and expected behavior of the device was understood. However, it was immediately accepted by the owners of the devices, the network engineering

department, and the Smart Building Central innovation team that most of these devices would not be able to have an agent installed on them. Especially for small sensor devices with minimal memory onboard, limited network stacks present, and often a proprietary interface required to configure and change settings on the device, there was no way that a standard method of deploying an agent or evaluating that the device's behavior could be done local to the device. After accepting this limitation, SBC Inc. created a "tiger team" deemed "The Key Masters" inside of SBC Inc. network engineering to overcome the challenge.

The Key Masters' charter was to be an onboarding, analysis, and troubleshooting team specifically for IOT devices within the Smart Building Central environment. With the newly created asset management database as their source of truth, all devices must be onboarded and evaluated by the Key Masters before being allowed on the network. This process was tedious but required collaboration with the owner, manager, and troubleshooting contact for each device, typically being identical. The device was first connected within a secured, hardened environment and would need to be connected alongside its systematic dependencies. For example, for smart thermostats that were connected to the network, the entire system that could influence or communicate to or from the smart thermostat would need to be built out within the hardened lab. Much of this knowledge came from product owners, who either had already implemented this system in other areas of SBC Inc. or were subject matter experts on the product itself and its ability to perform functions on the network. Knowing that devices within a system must interact for successful functionality, each device was entered into the asset management database and categorized into a unique system name, specific to its function, with each device also having a role within the system.

The identifying aspect of IOT devices was found to typically be solely in the devices' unique MAC address. The MAC address was therefore used to authenticate the devices in a passive manner, given their inability to actively identify themselves. This MAC address was documented in the asset management database and then exchanged into Identity Services Engine. Utilizing the organizationally unique identifier (OUI) of the MAC address, the address was classified into its product and manufacturer category for use as part of the applied authorization policy. The device was then passively identified regarding its expected posture, or how the device should look to the network. Aspects of the device's interaction with the network—for example, headers contained within its HTTP requests, contents of its DHCP address requests, the hostname either provided or configured for the device on the corporate DNS server, and whether the device responded to queries via SNMP—were all considered to create a scoring system for whether a device was what it represented itself as.

With a profile of what the device looked like within a controlled and verified environment, the next challenging task was to fully understand not only the interactions docu-

mented within the system schematic for the devices but also how these interactions occurred between each product in the system. The innovation team for Smart Building Central did as much due diligence as they could in determining the systems to be implemented into Smart Building Central, including tracking the system deployment notes and documentation from the manufacturer. These schematics were provided to the Key Masters for their consideration in their documentation on the expected behaviors. Many of the guides offered as documentation additionally included a list of ports and their expected usage when a system was deployed on a network. What the Key Masters quickly found, though, is that developers for the software or firmware utilized by most devices rarely had a networking background or skillset. This issue became evident through the collection of interaction traffic utilizing Cisco Secure Network Analytics and tracking the conversations found within NetFlow. What the Key Masters determined was that obvious interactions that may be prevented by a firewall (such as access of cloud services, shared services such as DNS and DHCP, and even identity services such as Kerberos) were documented, as seen in Figure A-2.

However, most manufacturers of devices that would be found within the IOT VRF didn't plan for their interacting systems to be prevented from communicating openly with the IOT devices. Smart Building Central's desired application of validated traffic flows and enforcement of any communication outside of those flows was not a consideration. Therefore, manufacturers rarely documented the interactions within the system. This required that the Key Masters collect and document what equated to 10 times the number of connections provided by manufacturers, and create records for each of the interactions, protocols, and ports within the asset management database for later consumption.

The documentation of these interactions served two purposes for Smart Building Central. The first was to ensure that policies could be written in a distributed manner, across multiple enforcement points to prevent communication to or from the device as required. The use of TrustSec as a Layer 2 enforcement mechanism between devices that were expected to be deployed within the same VLAN resulted in a policy that would be configured within Identity Services Engine. This policy allowed only those communications in a protocol and port manner. Devices that would be required to be part of separate VLANs could have their VLANs dynamically assigned to them through a RADIUS "push" containing the VLAN. Further restrictions were applied in the form of downloadable ACLs, also configured within ISE. For devices that needed to interact across VRFs—a thermostat to the chiller or heat pump that would cool or heat a room, for example—policies would be deployed to a firewall. Any devices that would need to interact with cloud-based resources could have their policy applied directly to the cloud server they were interacting with via the IP tables mechanism modified with Cisco Secure Workload.

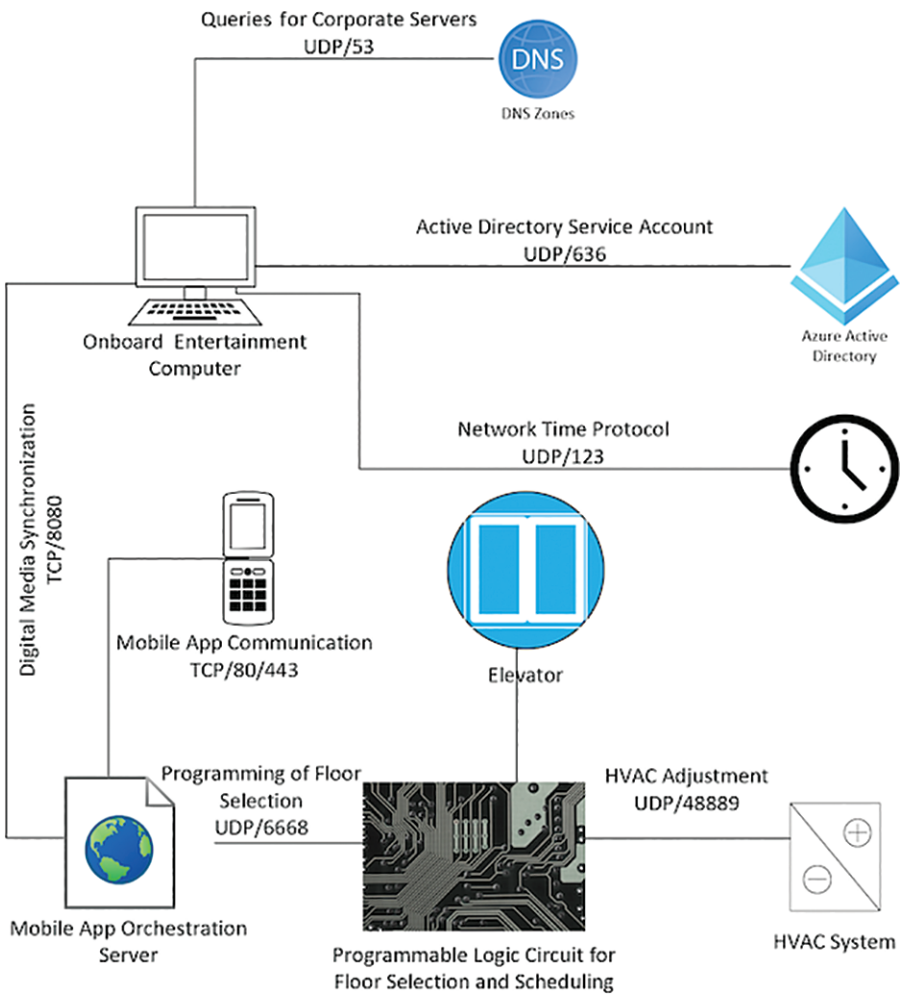


Figure A-2 *Elevator System Interaction Diagram*

The second purpose of documenting the behavior of each of the devices within each system was to develop a baseline communication to understand whether the device was behaving differently in the field than what was observed in the lab. This change in behavior was thought to potentially indicate some level of compromise. As the Key Masters found out very quickly in the testing process, utilizing vulnerability management and evaluation tools on IOT devices with limited network stacks can easily, and without warning, cause the devices to stop responding to any network communications. The programmable logic circuits that control chillers and tell them to turn on for only as long as the thermostat

indicates that temperature is incorrect in the room, for example, will stop responding when an NMAP or vulnerability scan is run against them. To resume normal operations, the device required a reboot, typically predicated by complaints by those in the room that was facilitated by the chiller were far too warm or too cold. This was a direct dichotomy with the goals Smart Building Central had for the smart systems. Therefore, the traffic mapping and interactions associated with each system were tracked with custom-built scripts that would fire alerts based on the NetFlow telemetry ingested by Cisco Secure Network Analytics. These alerts would indicate to administrators that the baseline communication was not conforming with known patterns, or had completely stopped, which would indicate a problem. The alerts and information provided could be macro (system-to-system ongoing communication) or micro (header content change) in nature.

Application of Enforcement

Even with identification of devices done and mapping of communication baselines being complete, the criticality of systems within Smart Building Central caused anxiety across all aspects of the business. With demonstrable impact that could be incurred by inadvertently shutting down a chiller merely by attempting to evaluate it for vulnerabilities, senior management was even more concerned about the balance of business as usual, with the ability to adhere to regulations allowing the business to function. Throughout the identity phase of the Zero Trust testing, the Key Masters applied varying levels of enforcement techniques to each system and evaluated what impacts each would have on the system. Knowing that some devices within the building management system were never meant to be networked when originally developed, there was a known risk to applying authentication at all. This phase yielded an additional discovery into which enforcement technique would work best for each system.

For many of the devices that ran building management systems—programmable logic circuits specifically—the original system was built as a series of components that could be easily swapped in and out of their case using PCI ports, some also having USB 1.0 ports. The assemblers of the devices, having assembled some of the components in the mid-1990s after the initial introduction of PCI and USB to the market, would never have expected that wired or wireless LAN cards would be attached via the connection bus. Therefore, logic used when sending signals to and from the connection bus was simplistic in nature, some devices being found to interpret any level of enforcement or prevention of access at the access layer switch port as a disconnection. This result made for a need to work around these devices and apply lesser security to the type of device at the initial connection, in favor of moving the enforcement technique to a higher layer in the network topology, such as the firewall. Key to this understanding and determination was the use of the Identity and Vulnerability Management phases, as the device did not present any sort of error to the network based on the application of this enforcement. It simply shut itself down and stopped responding until it disconnected and reconnected.

With this need for distributed enforcement in mind, the network security team for Smart Building Central designed a plan for application of security across each VRF and throughout the network, as shown in Figure A-3. The major components of the enforcement application included a series of technologies, including TrustSec for intra-VLAN communications, downloadable ACLs for inter-VLAN communications, firewalls for inter-VRF communications, firewalls for external communications, and DNS policies for external resolution.

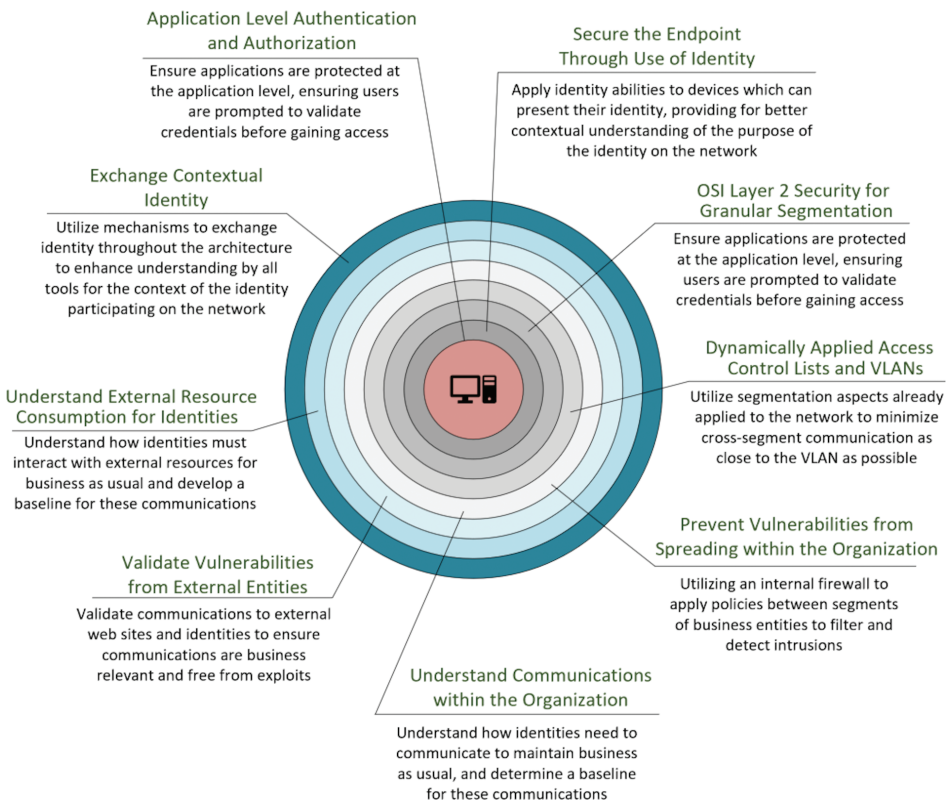


Figure A-3 *Distribution of Enforcement Mechanisms*

Firewalls

The firewall continued to be Smart Building Central's perimeter security device of choice. However, the standard for deploying firewalls for remote sites, regardless of their function, was what some would consider far too complex. SBC Inc., being a manufacturing company and having several innovation centers throughout the world, had many contractors who partnered with the company to administer and update various types of devices. Elevator computers, thermostat logic, and sensor monitoring by emergency

services companies were major focuses and would be required within Smart Building Central. Therefore, agreements were created with vendors to allow set IP addresses and sites to access these systems inbound through the firewall. In addition to the inbound rules required, some contractors had a physical presence within the SBC Inc. offices, but it was unpredictable where these contractors would work from at any given time. Their technician responsibilities often brought them to various offices with a working agreement with the contractors to allow them to work from any SBC Inc. building, giving them a temporary "home base of operations."

With this agreement in place, the SBC Inc. standard for deploying firewall rules was to replicate the inbound and outbound exceptions for these contractors to every firewall in the company's firewall fleet, in addition to local rules for site-specific business purposes. When the initial template was provided for the Smart Building Central application of firewall rules, it was found that the sheer number of rules would overload most vendor firewalls for the scoped size of throughput and endpoints found within the building. The company's network security team provided 350,000 rules that would need to be populated onto the firewall for these purposes. Given the burden these rules would have on firewalls to be implemented, another approach had to be taken.

The first step in reducing firewall rules was to revisit the Identity phase of the Zero Trust principles to identify what rules applied to which contractors and whether some of the rules could be removed. Comparable to the realized risk of not having a definitive asset management database, each corporate firewall of the SBC Inc. fleet had thousands of rules without any identifying characteristics, remarks, or understanding of their purpose or life cycle. To reduce the firewall rules and, in extension, distribute the enforcement techniques, SBC Inc. had to evaluate which rules were required. Many of these rules should have been removed long before and could be applied to endpoints via a different mechanism. Therefore, an effort was undertaken to understand firewall rules through a series of evaluations:

- Each firewall rule was first evaluated against the DHCP scopes internal to SBC Inc. to determine whether a suspected owner could be identified. The overall architecture of SBC Inc. being distributed branches that must connect back through campus or data center sites did provide some identification abilities. DHCP scopes could be linked to smaller offices with only a handful of business units. For these sites, and the business units identified, team also attempted to identify destinations through tribal knowledge, or knowledge that existed within teams already, as opposed to relying solely on DNS records.
- For connections that could not be readily identified using DHCP scopes specific to a site, DNS lookups were performed into the last known endpoint that occupied the address that was being allowed access through the firewall. One significant advantage that SBC Inc. had in this regard was a centralized SIEM system that logged 13 months' worth of data per corporate requirement, giving them a lookback on the activities of any given endpoint or user for the last year.

- For rules that were unable to be identified using DHCP tracing, tribal knowledge, DNS lookup, and log analysis, the rule was incrementally disabled on each of the company's four campus firewalls, while remaining active on data center firewalls. An expectation that users would complain when they were unable to access destinations via one data center but allowed to access it through another was accounted for. The effect of disabling the firewall rules only on campus firewalls incrementally ensured limited impact to the business while waiting for these complaints. In addition, which firewall was disabled could be planned around business priorities, such as the number of contractors flowing through each firewall on a regular basis.

The result of the analysis completed for 350,000 firewall rules was that only approximately 125,000 were used actively within the organization. This included removing nearly 50,000 that were overlapping rules, having little or no effect. As these rules were cleaned up as part of the process, the number of rules shrank significantly. Of the 125,000 rules implemented and used, it was determined that many were duplicate rules that existed for all 175 campuses and branches that SBC Inc. allowed contractors to visit. Most of these rules could therefore be simplified and applied on a device category basis with downloadable ACLs—a more simplistic and distributed approach.

Identity Services Engine (ISE)

For the firewall rules that pertained directly to overlapping subnets traversing to a small number of destinations, Identity Services Engine policies were written to accommodate this access. With the age of the firewall estate, it was safely assumed that SBC Inc. did not use the next-generation features of its firewalls. Features such as TCP randomization, TCP normalization, or even intrusion prevention policies were not applied to individual connections. While SBC Inc. had IPS systems deployed separately from its firewalls, it was determined this would be combined into the next-generation firewall offering of Firepower Threat Defense. This also enabled identity to be directly exchanged with the firewall for further policy enforcement.

With this determination made, access control lists were built, allowing access from endpoints outside of the Smart Building Central network into one of 24 jump hosts used to permit this access based on contextual identity. The results of this access were rules consisting of a combination of who, what, where, when, and how, and more specifically rules could be written that allowed for authenticated contractors' differentiated access. The policy applied looked comparable to the following:

> *A contractor found within a contractor's active directory group (who), authenticated via a VPN client into Smart Building Central (how), accessing the VPN from outside of Smart Building Central (where), via a laptop running Windows or Ubuntu (what), within business hours only (when), could traverse to one of 24 sites used as jump hosts for customer devices for administration.*

This comparatively simple rule, based on contextual identity, further reduced the rules to be applied to contractors by almost 10,000 rules, with at least one wired and wireless subnet in each of 174 external sites being allowed access to these jump hosts.

With firewall rules minimized and well within the quantity of rules that any firewall vendor could accommodate, focus shifted to corporate endpoints, collaboration endpoints, and guests. Within Smart Building Central, the innovation teams had a dream of a paperless building. All signage was easily updated and presented on screens strategically positioned within the building to allow information sharing as well as an automated emergency function that would change all signs to point to their nearest emergency exit in times of emergency. Similarly, when entering the building, all guests were registered on iPads, and all badges were reusable and linked to the identity registered on the iPad and were used to identify and track users throughout the building. There was an interest in ensuring all presentations were digital, files hosted centrally for consumption on mobile devices, and presentations done wirelessly to also minimize the number of cords required within the building. Both goals played into a clean, conservation-focused, and sustainability goal.

As mentioned earlier in the appendix, Smart Building Central utilized Android- and Apple-based presentation products to allow any devices to connect to them and share the entirety of a user's screen or a singular application. The challenge came when this goal was applied to both corporate endpoints, as well as guests. It was well established that all collaboration endpoints would be part of the Corporate VRF of the network, especially given the nature of full-mesh traffic connectivity needs between softphones. A similar communication pattern applied to video collaboration devices within the building. But the use of Android and Apple presentation devices provided a distinct advantage to the collaboration and security solution, because it allowed these devices to be treated as a separate input to the collaboration devices altogether. This input was switched to when a shared screen triggered the device. These devices therefore existed in a "shared services" VRF of the network, with enforcement applied to allow communication to these devices via a firewall and identity-based policy for both corporate endpoints as well as guests.

This identity-based enforcement mechanism was a combination function between Cisco Identity Services Engine and the inter-VRF firewall of choice, Cisco's Firepower Threat Defense platform. As each corporate user connected to the network, regardless of medium, the endpoint was required to authenticate to the network, and an authorization policy applied. Within this authorization policy, a TrustSec tag was applied, identifying the user as a corporate user on a corporate endpoint. The same procedure occurred for SBC-managed mobile devices, with a similar Corporate Mobile TrustSec tag applied to the endpoint's session. Guests were provided with login credentials when they entered the network as part of their registration via iPads at the physical security desk. This credential was then associated with their badge and the device used to log in to the guest network.

Corporate users with personally managed cell phones were treated similarly, just with a use of their Active Directory credentials to log in to the guest central web auth portal, as opposed to credentials provided at registration. This methodology provided a required level of accounting and attribution of behavior for each guest, with the ability to revoke access to the guest network should the user leave campus with their badge or take other nefarious actions while on campus. Both identities, in the form of tags, were exchanged from Identity Services Engine to the Firepower Threat Defense platform. This exchange allowed for creation of a rule allowing for corporate endpoints and corporate mobile devices, found in the Corporate VRF, as well as guest devices, found in the Guest VRF, to communicate through the firewall to the Shared Services VRF based on their contextual identities. In addition, this methodology allowed for limitation of any guest or corporate device from communicating with others within its peer group, preventing the potential spread of malware. This rule similarly prevented communication between corporate endpoints and guest devices to prevent sharing of information between trusted and untrusted sources. This rule ensured that while functionality had to be allowed from the three groups to perform the same action, the three were prevented from communicating in undesired ways.

A similar approach was used for the administration of IOT devices, which were determined to have a management GUI. IOT devices existed within the IOT VRF of the building and typically included thermostats, sensors, IP cameras for both security and temperature sensing, and the programmable logic circuits for elevators, escalators, and smart glass. Each set of separate systems had to interact with some sort of management controller, including the mobile application processing unit, and their respective controllers for system functionality. These controllers were all consistently placed in the Building Management Systems VRF, which was separated from the sensors themselves by the Firepower Threat Defense firewalls.

Like the identification and authorization methods used for collaboration units, endpoints that needed to communicate with their management systems were configured with credentials where supported and profiled to determine the functionality of the device. For devices that were known to not have the ability to actively authenticate to the network with credentials, their MAC addresses were onboarded into an asset management database as part of the new responsibilities of the Key Masters post-completion of the system interaction testing. If the endpoint's MAC address was found in the asset management database and should have a device profile, or "look" like it should when participating on the network, it was provided its respective IOT tag. These tags were controlled in their interactions with building management systems via the Firepower Threat Defense firewall, and only known and validated protocols and ports allowed to traverse.

TrustSec Tags

One aspect of the initial goals that Smart Building Central had for endpoints within its network was the minimization of impact for any exploitation that was observed within

the network. This meant ensuring that should a device be compromised within a system, a series of measures was used throughout the enforcement mechanisms to ensure that the potential impact on the rest of the network was minimized. These measures resulted in the use of TrustSec tags within the network, assigned to each unique device as it joined to the network, and associated with a unique session ID created when the device joined the network. However, one common mistake that many organizations will make, as noted in Chapter 7, is focusing on all endpoints as unique groups, increasing operational efforts through the number of policies written for endpoint interactions. While TrustSec tags were used within Smart Building Central, the Key Masters were very careful not to overwhelm the network operations team with hundreds of potential tags and settled on a maximum number of 10 tags that would be deployed throughout the network. Within each of these 10 tags, additional "sub-tags" were planned for, and they were typically associated with the separate endpoint groups but were planned to be implemented only when absolutely required, and well after Smart Building Central's go-live date. One aspect that had to be considered for the 10 tags to work was the required interactions between devices within each VLAN and which communications were considered critical.

Key to ensuring Smart Building Central did not expand beyond its capabilities for TrustSec was carving out the exact use cases that would require TrustSec. This plan included those which could potentially have endpoints that could be exploited within the same VLAN. The ability to control the communication in some other way, such as downloadable ACLs, separate VLANs, or a VRF termination on a firewall, was paramount. It was determined that the TrustSec tags to be created for Smart Building Central would be of the following types:

- Corporate endpoints (PCs and managed mobile devices)
- Collaboration endpoints
- IP security cameras
- Printers
- Print servers
- IOT
- Guests
- Building management systems
- IT

During the identification and traffic mapping phase, the most challenging endpoint that the Key Masters had to map out was that of IP cameras. IP cameras were found to serve two purposes within Smart Building Central—both physical security, as well as thermal imaging and measurement of ambient temperature. While cameras differed in firmware,

their behavior was identical when connected to the network: when the device was newly connected to the network, it would first reach out to its peer group within the VLAN via a multicast message, followed by a broadcast message, asking which network video recording system it should connect to for sending its video feeds. Whenever the device's firmware was corrupted due to rapid power on/power off events, or in the event of a power surge, the device would reset all information previously configured on it relating to a statically configured network video recorder and perform the same action. For security purposes, it was determined by the SBC Inc. corporate security team that in lieu of losing access to physical security cameras and visibility into any area of the network, they would much prefer the dynamic ability for cameras to discover their network video recorder dynamically and be statically configured after the loss of connectivity than have a loss of connectivity until a technician could visit the physical device. A risk analysis of this behavior had to be undertaken to determine the best course of action.

On one hand, leaving all IP security cameras open to peer-to-peer communication could lead to a loss of physical connectivity within the building if exploited by a device on the same VLAN. At the same time, preventing this communication had a similar effect, where devices were lost during an event that was determined to potentially happen significantly more frequently in nature. It was determined that IP security cameras, needing to communicate on port 6668, would be restricted to this port local to their peer group to exchange configuration information, as well as multicast and communication toward the firewall to communicate to their controller. However, because of the critical role these cameras played within the network, and their respective behavior, they were "carved out" to be a separate TrustSec tag and have a unique policy applied to them.

Other devices, such as thermostats and sensors, were classified as IOT sensors in a more generalized enclave mainly because the loss of configuration for each of these devices would result in a need to visit the device, but there was less risk of impacting daily operations of the building until that visit could be completed. These devices also having a limited number of unique ports used to communicate within their peer groups resulted in a shared set of ports that would be allowed to communicate on. This result was applied, keeping in mind that some devices would be able to communicate on erroneous ports to their operation, regardless of whether devices within the group listened on all the allowed ports or not.

Most other peer-to-peer traffic flow within Smart Building Central was prevented with TrustSec tags, because the need for devices to communicate in this pattern was limited. One of the major goals Smart Building Central had, for example, was to change the culture as it related to communication to printers. To ensure that data loss prevention mechanisms, centralized printer authorization, and ease of use were all implemented for print jobs within Smart Building Central, IT operations teams wanted to ensure that any given PC could communicate only to a centralized print server. This print server would then relay printed documents to the required printer of the user's choice, which could also be

recommended based on location within the building to which the print job was sent from. Knowing that PCs, printers, and the print server would all exist in the same VLAN in many cases, TrustSec tags were once again the optimum application of enforcement to be applied. A policy was implemented with corporate machines able to communicate only to print servers and explicitly blocked from communicating with printers directly. Printers would then be allowed to communicate to print servers, forcing the print servers to function as a centralized middleman to printers and PCs for control purposes.

With the need of Smart Building Central to move away from classic networking techniques, such as allocation of blocks of IP addresses to certain types of endpoints or departments, the general layout of PCs, mobile devices, printers, print servers, and corporate devices was to distribute them all within a single VLAN. This further caused a need for TrustSec tags as an enforcement mechanism. However, for digital signage devices that would utilize static IP addresses for easier management, there was a need to allocate a set of IP addresses that would be reachable by IT systems, not reachable by the standard corporate system, and unable to infect other digital signage should the device become compromised. This need was approached by laying security enforcement mechanisms on the endpoint's session.

The first layer of security was to dynamically assign these devices to their respective VLAN so that if they were moved between network ports, especially in the case of a conference where large densities of signage would be required in the conference area, there was little to no overhead by operations teams. To do so, digital signage devices would authenticate to the network with a unique credential to the device, be profiled based on its unique endpoint attributes, and be applied a VLAN specific to digital signage in a dynamic manner. The switch the endpoint was connected to, having the VLAN existing but not assigned, was configured via RADIUS to assign the VLAN to the session. On top of the dynamically assigned VLAN, the IOT tag was applied to the digital signage, preventing peer-to-peer communication between IOT devices; and finally a downloadable access control list was applied, allowing the device to access its two digital signage controllers, residing in the building management system's VRF at two singular IP addresses.

DNS

The final challenge for enforcement that Smart Building Central ran into was the vast use across all platforms of cloud services, both internal and external to the company's public cloud. Throughout the Key Masters' discovery phase and traffic analysis done to determine communications, they found that 93 percent of all endpoints within Smart Building Central utilized the cloud for hosted dynamic content of some form. Not only did popular smart assistant devices rely on the cloud almost exclusively for content that was served to them, but on-site gym devices with streaming services, PCs accessing websites within the cloud, IOT thermostats that received updates to their firmware from the cloud, and sensors that sent readings to a cloud server owned by SBC Inc. all presented a

significant risk to the success of Smart Building Central. The largest concern that Smart Building Central had with regards to its systems was that of the potential for a device to reach out to a cloud server that was eventually deprecated or no longer available. The potential for attackers to re-create this resource to serve nefarious means, including malware or ransomware, was significant in its potential. While security mechanisms were used internally to prevent the spread of this malware, there was still a necessary risk that needed to be mitigated around the potential for exploitation from within the cloud.

Smart Building Central, to mitigate this risk, stood up its own DNS servers for the smart building, as opposed to relying on the exclusive use of corporate DNS services. These DNS servers acted as a subsidiary of corporate DNS services but then forwarded all external resolution requests to Cisco Umbrella for resolution. Cisco Umbrella, seeing more than 170 million DNS requests per day, provided a level of intelligence to DNS resolution for Smart Building Central that the corporate DNS services of SBC Inc. did not have. For each DNS request being sent to Umbrella, the request was evaluated for a set of criteria around the trustworthiness of the website that was being requested. These criteria included

- The age of the DNS record as registered
- The owner of the DNS record according to its registration
- Whether the website presented a secured certificate upon request
- The content observed by Umbrella DNS that the website served up
- The business relevance of the content being served

The advantage of Umbrella DNS seeing so many requests daily is that it contains information on commonly accessed malware and ransomware cloud resources so that they can be classified and actively blocked before any traffic even traverses to the site in question. For Smart Building Central, this meant the ability to prevent sites that may have been spoofed, as well as an enforcement ability within Umbrella DNS to filter out content irrelevant to the business while presenting a warning page to the user, such as traffic with strictly adult themes, violence, sites used strictly for data sharing, or those that were considered overtly political in nature. This filter was applied strictly to corporate PCs, IOT devices, and other corporate devices and was not applied to the guest or personal mobile phones areas of the network.

Analytics

As can be imagined, the distributed authorization and enforcement mechanisms throughout Smart Building Central made for a massive analytics data set to be consumed and utilized, both to influence policy as well as troubleshoot traffic traversal issues where dynamically applied controls were present within the network. Smart Building Central had a SIEM for consumption of security events, including passed and failed auth, firewall

allowed and denied flows, and syslog events for attempts to log in to systems throughout the network, but one major gap still existed within the architecture. The management of SBC Inc. was very interested in evaluating how well their security was working in relation to the number of threats that were potentially dangerous to Smart Building Central that we blocked. While one aspect of this was the number of devices that were prevented from communicating based on being blocked from accessing the network altogether, another was the number of flows that were blocked in transit due to the application of TrustSec. TrustSec, not being a stateful firewall, will drop communications between endpoints within the same VLAN; however, on some network access devices it lacks the ability to indicate that this drop occurred. This inability makes for a challenge in both evaluating where these drops occurred and troubleshooting when flows that were expected to occur were unsuccessful.

To mitigate this troubleshooting and analytical need, Smart Building Central employed the use of three products. The first was Secure Network Analytics (SNA). Secure Network Analytics, with its ability to collect NetFlow traffic from across the network, can indicate where the traversal of traffic, containing a source and destination for the traversal, does not make it to its destination. This is based on observing the expected path and whether the packet makes it to the final device within that flow. Should a PC, for example, attempt to communicate to a digital signage device directly, the flow record would indicate that the communication between the two devices was dropped at the switch to which the digital signage device was connected due to an unauthorized flow occurring according to the TrustSec matrix. This failure could then be logged to the SIEM and analyzed to determine whether the attempt to access the device was in error, as indicated by a one-time access, or whether it was a pattern of access attempts, such as a scan of the network or an attempt to write nefarious information to devices as found in the packet contents.

In addition, both the Key Masters and the IT operations group used Secure Network Analytics on an ongoing basis. Try as they may to ensure that the culture of Smart Building Central was changed, allowing only pre-authorized and approved purchase devices onto the network, plenty of resources within Smart Building Central were still attempting to purchase or bring devices into the building without getting authorization first. In the spirit of adherence with policies written, the device would still be authenticated with the user's credentials, documentation provided when the device was found to be unauthorized, and information provided to IT operations. A device owner would still need to provide the type of device and its business relevance to the network, as well as justification relating to why the device was never properly onboarded through the proper processes. Most of these requests cited "timelines to success" and indicated a slow process of changing company culture.

For the first few months of Smart Building Central's existence, the IT operations teams, while attempting to educate staff into the proper processes, would utilize Secure Network Analytics to dynamically determine what resources endpoints needed to

communicate to while allowing them to remain connected to the switchport that they would be allocated. This effort came in the form of statically quarantining devices that were unauthorized, providing them minimal access to the network, and then analyzing them on the fly to create proper authorization policies for them. This practice was discontinued after the first quarter of Smart Building Central's business-as-usual period due to interference with other priorities IT operations held. The result was that users were forced to go through proper onboarding processes after the policy was well established.

The second major tool used within Smart Building Central to analyze traffic traversal was Cisco Secure Workload. Secure Workload was a requirement within the Smart Building Central premises for all physical and virtual servers deployed. The goal of Secure Workload was to analyze communications of the servers with endpoints in such a fashion that alerts could be generated for interactions that occurred that were outside of the expected behavior of consumption of resources from the server. For example, to prevent cross-site scripting or command injection into server communications, Secure Workload could fire an alert specific to the virtual server in question when such a behavior was observed. Due to the limitations of data center switches within the local main distribution facility of Smart Building Central, Secure Workload was also used to apply policy directly to the server, without relying on the switch to which it was connected. Secure Workload makes use of IP tables present on the server to modify its communications to those communications that are strictly required as applied from a policy server, the Secure Workload Management Center. This made for easy application of policies down to the port and protocol level for physical servers within the premises.

The reliance of mobile phones on cloud services for navigation and ordering of elevators within the Smart Building Central premises was also a major use of Cisco Secure Workload. Much of the resources required to be done in building navigation, as well as the server-side application processing for interaction with elevators, smart lighting, and similar building services, was hosted in a major public cloud provider. While groupings based on allowed ports and protocols could be allowed and associated with the cloud servers, understanding which devices were interacting with these servers and enforcing policy related to these interactions was a major concern of Smart Building Central. Deployment of Cisco Secure Workload provided this visibility, enforcement, and analytical capability, comparable to physical servers, through the modification of IP tables.

The final analytics engine used within the Smart Building Central deployment was Cisco Thousand Eyes. With the building reliant on critical IOT systems that could have an impact on the health and safety of occupants of the building, Smart Building Central had a major goal of preventing the network administrators' favorite complaint of "my endpoint's connection is too slow!" Cisco Thousand Eyes was implemented to constantly measure the connectivity indicators within the building as well as to the cloud for indications of high latency and downtime of the application or server. It was also used to measure the response time to more easily determine whether the endpoint was prevented from accessing the application, whether there was impact on response time, or whether

the endpoint should be consulted to determine why it wasn't reaching out or processing information received from the application server in a reasonable amount of time.

Conclusion

With the success of Smart Building Central and the changes made to the organization to address limitations exposed in the planning phases of Smart Building Central, SBC Inc. decided that the Zero Trust model would be applied to all net-new building deployments, renovated buildings, and maintained real estate in that priority. Not all of the company's real estate was smart device integrated. There are, however, significant numbers of devices within every building that would not have been known to be connected until the identification phase occurred for that building.

By breaking up these steps utilized for Smart Building Central's success within its Zero Trust journey, SBC Inc. was able to create a roadmap and evaluation standard for progress and milestones applied to each of its other buildings. As opposed to the question "When will the building be secured?" the more value-aligned question "Which phase is the building at, and how far along?" could be used to determine progress.

Because of the journey that is Zero Trust, no single destination awaits the organization that pursues it; removing trust from a network is an ongoing and never-ending process. The mountain of Zero Trust, seen in Figure A-4, is most definitely a journey. However, for organizations that choose to pursue Zero Trust, a mindset of the value realized throughout the process justifies the investment and helps validate where the organization is within the journey, like a map.

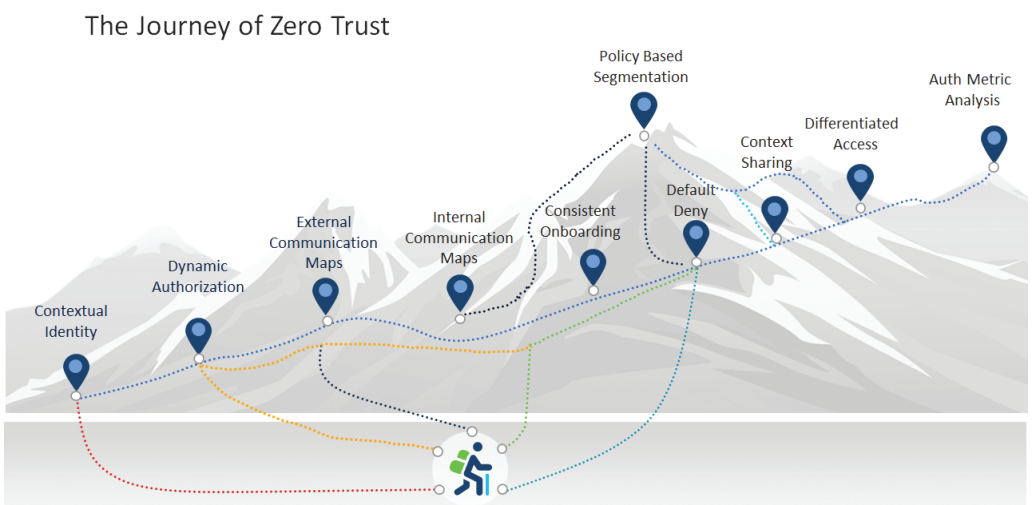


Figure A-4 *The Mountain of Zero Trust*

For Smart Building Central, that journey continues with new device onboarding, life-cycle management of devices that are at the end of support by their vendor, and a need to onboard replacement devices, while still providing them the access they require. Luckily, the principles of Zero Trust provided SBC with a roadmap of how to do exactly this, develop its own priorities for value realized, and maintain operation of one of the smartest and people-oriented buildings in the world.

Though the name of the organization has been changed, we hope that this real-life use case will assist organizations to understand, rationalize their own use cases, and then realize their goals to begin and achieve a successful Zero Trust journey.