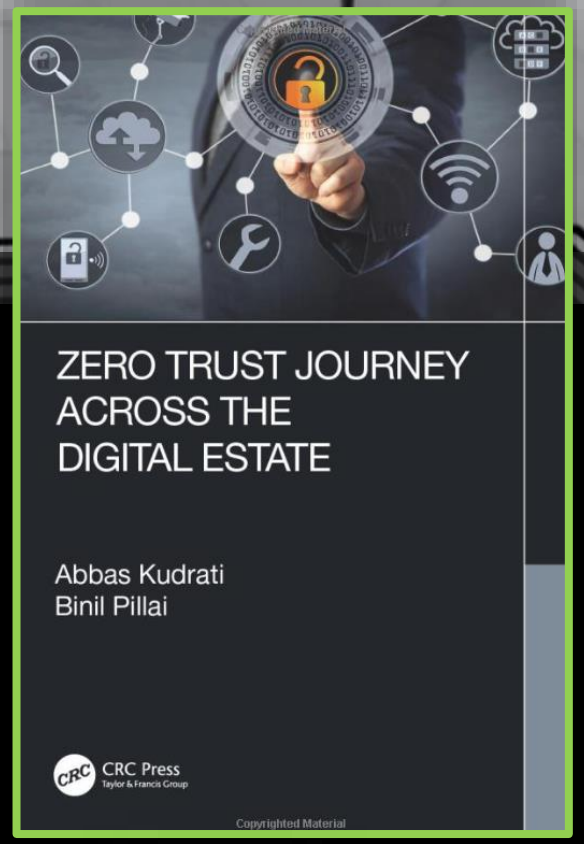
A Pragmatic Approach to Zero Trust Implementation

Abbas Kudrati

Microsoft's APAC Chief Cybersecurity Advisor
Author – Zero Trust Journey Across the Digital Estate

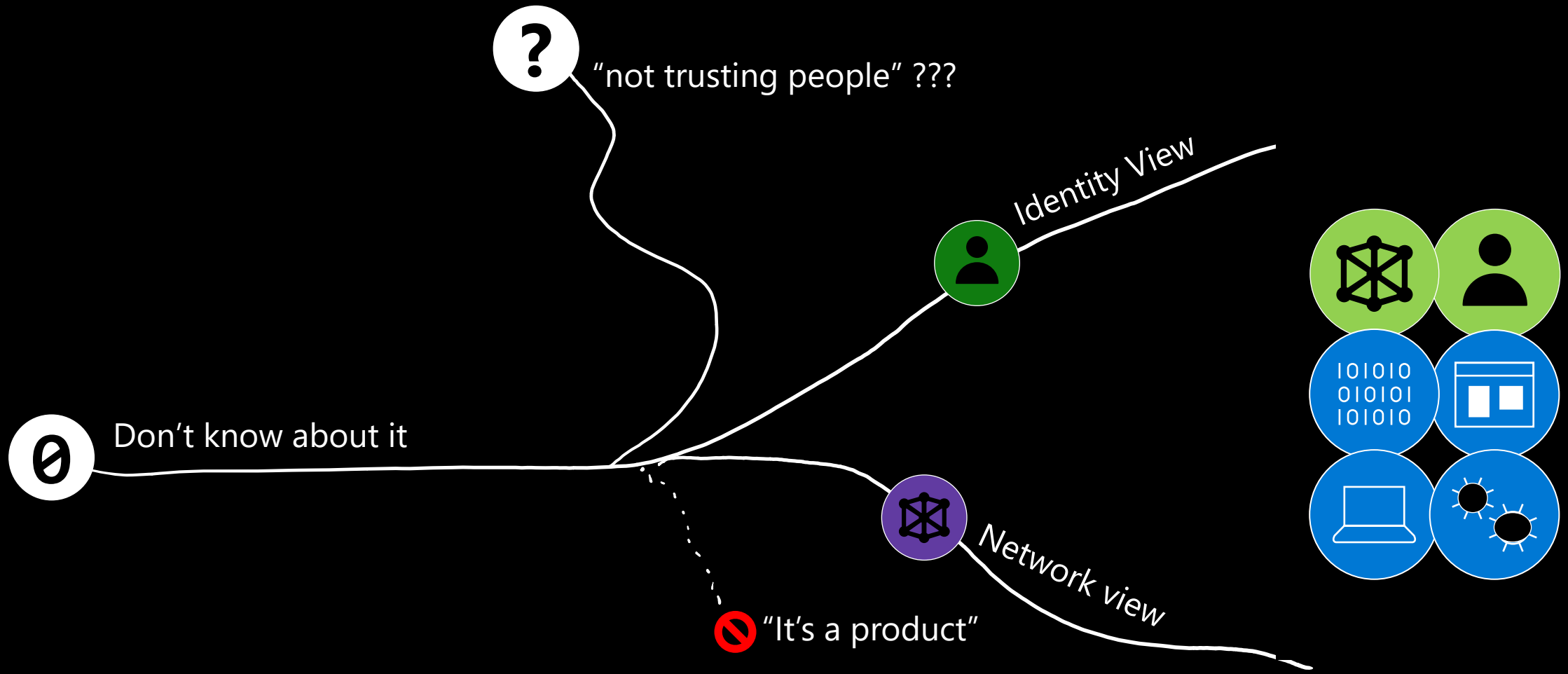


ZERO TRUST STRATEGIST CERTIFIED FORRESTER

ZERO TRUST certified ARCHITECT

ZERO TRUST TRAINING CONTRIBUTOR ZTT Contributor CLOUD SECURITY ALLIANCE

Zero Trust Perspective



Zero Trust is Misnamed

In order to get things accomplished, **trust must ultimately be extended**…..

……. and **continuously assessed** for acceptable levels of risk/trust…. and our security infrastructure should adapt accordingly.

Zero Trust is being abused as a marketing term

There are things you can absolutely do to move towards Zero Trust.

Zero trust is a **cybersecurity paradigm** focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.

Why Zero Trust is important

"We have used ownership and control of physical assets and location as an implicit **proxy** for **trust**"

This is a flawed security paradigm……

…..Existing security patterns leave too much implicit trust.

Zero Trust Perspective

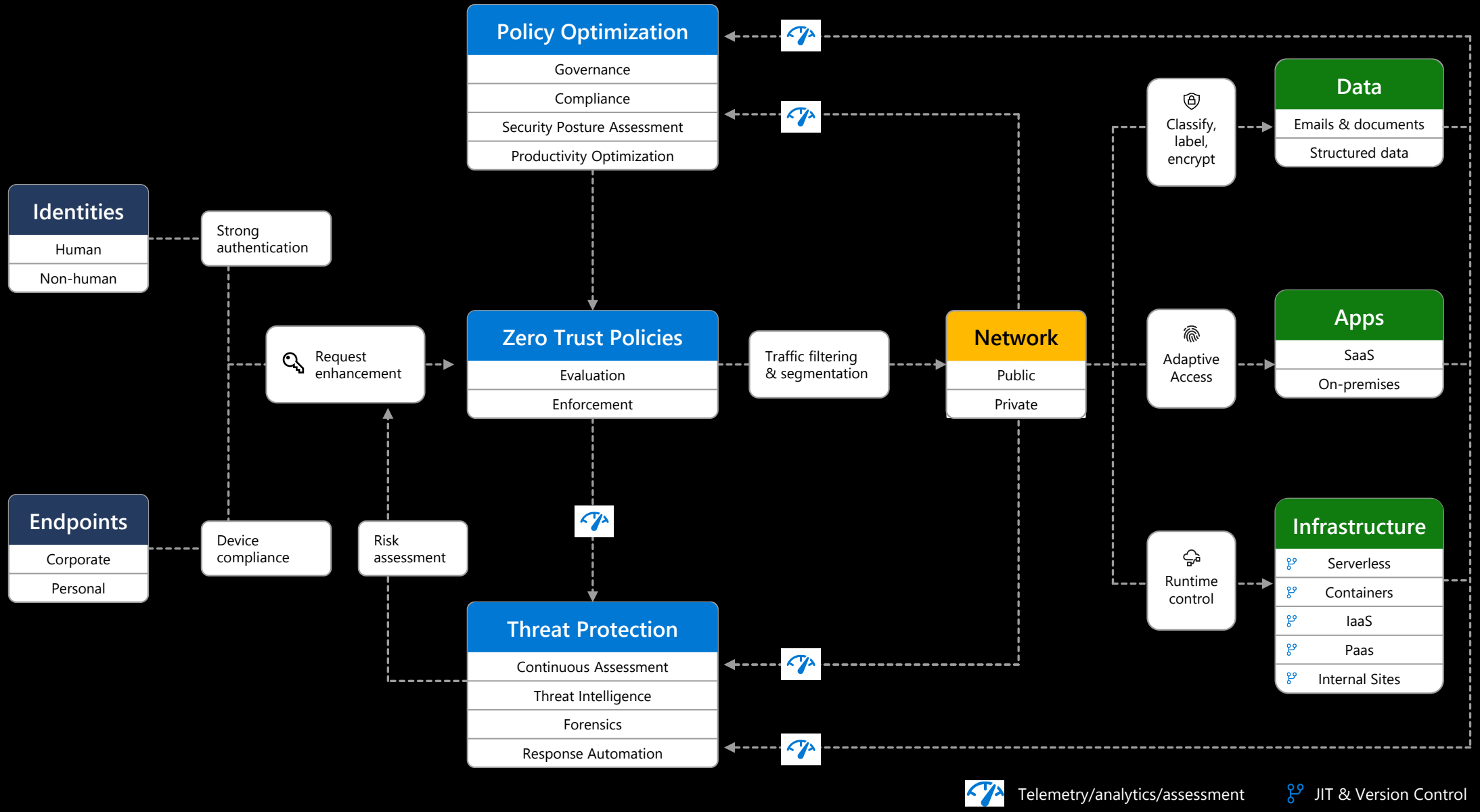
Zero Trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk/trust levels based on context – most notably Identity – that adapt to risk-optimize the organisation's security posture.

Zero Trust Principles

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes an open environment where trust must be validated.

- **Assume breach** – Assume that attackers will succeed (partially or fully) and design accordingly
- **Verify explicitly** – Validate trust of users, devices, applications, and more using data/telemetry
- **Use least privileged access** – to limit the impact of any given compromise

Zero Trust Architecture



Ten Zero Trust initiatives you can start now

1. Conduct the maturity assessment
2. Implement conditional access for all (MFA, Passwordless)
3. Implement PAM (or minimum MFA) for all admins.
4. Encrypt all data at rest in public clouds with customer-controlled keys.
5. Remove admin rights from most Windows Users.
6. Segment end-users off the data center network.
7. Segment (ringfence) critical applications.
8. Implement lockdown/allow-listing on critical servers.
9. Engage with dev to scan containers for new apps
10. For Kubernates, link dev scanning to admission control.
11. **Make Zero Trust as an ongoing project / journey.**

Case Study: Microsoft

Major phases of Zero Trust Networking

Pre-Zero Trust

- ✓ Device management not required
- ✓ Single factor authentication to resources
- ✓ Capability to enforce strong identity exists

Verify Identity

- ✓ All user accounts set up for strong identity enforcement
- ✓ Strong identity enforced for O365
- ✓ Least privilege user rights
- ✓ Eliminate passwords – biometric based model

Verify Device

- ✓ Device health required for SharePoint, Exchange, Teams on iOS, Android, Mac, and Windows
- ✓ Usage data for Application & Services
- ✓ Device Management required to tiered network access

Verify Access

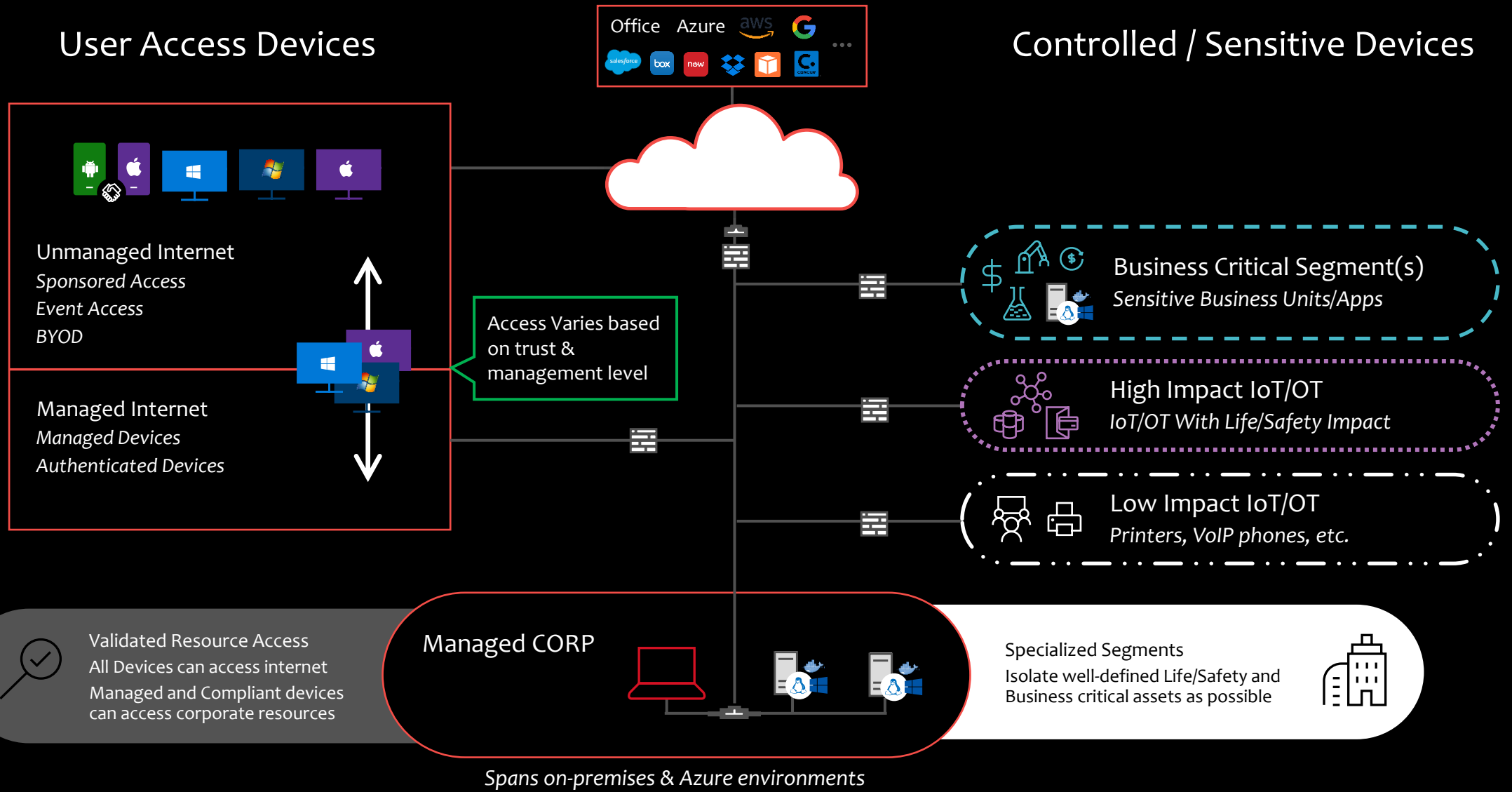
- ✓ Internet Only for users
- ✓ Establish solutions for unmanaged devices
- ✓ Least privilege access model
- ✓ Device health required for wired/wireless corporate network

Verify Services

- ✓ Grow coverage in Device health requirement
- ✓ Service health concept and POC **(Future)**

User and Access Telemetry

Zero Trust – Network Segment Transformation



Zero Trust Benefits

for both security and productivity

Increases security

1. Reduce risk of compromised users & endpoints
   - Remove user endpoints from enterprise network
   - Reduce VPN usage / attack surface
2. Improves security visibility
   - No blind spots for remote devices
   - Centralized view of risk, policy exceptions, and access requests
   - Deep insight into device risk and user session activity

Increases productivity

1. Can work anywhere you want
   - Apps & Data available anywhere
   - Empowers everyone including security
2. Can choose your own device
3. Single Sign On (SSO) across enterprise apps and services
4. Improved “Access Denied” experience:
   - Prompt to increase trust (e.g. MFA)
   - Limited access to apps/data

Better security *and* user experience from “Password-Less" authentication

Summary

- An organization must integrate ZT across the digital estate to gain the Zero Trust security model to gain the maximum advantage Zero Trust security model. You will be required to adopt a phased approach that targets a specific tenant of Zero Trust, available resources and priorities.
- It will be essential to consider each investment carefully and align them with current business needs.
- The first step of your journey does not have to be a significant lift and shift to cloud-based security tools.
- Many organizations will benefit significantly from utilizing the hybrid infrastructure that helps you use your existing investments and begin to realize the value of Zero Trust initiatives more quickly.
- Fortunately, each step forward will make a difference in reducing risk and returning trust in the entirety of your digital estate.

Reference

- Zero Trust page: https://aka.ms/zerotrust
- Zero Trust maturity model: https://aka.ms/ztmodel
- Zero Trust assessment: https://aka.ms/zttool
- Zero Trust deployment guidance: https://aka.ms/ztblogs
- Implementing a Zero Trust security model at Microsoft LINK
- Microsoft's approach to Zero Trust Networking and supporting Azure technologies LINK
- Microsoft helps employees work securely from home using a Zero Trust strategy LINK

Thank You !

Scan this QR Code to connect with me on LinkedIn

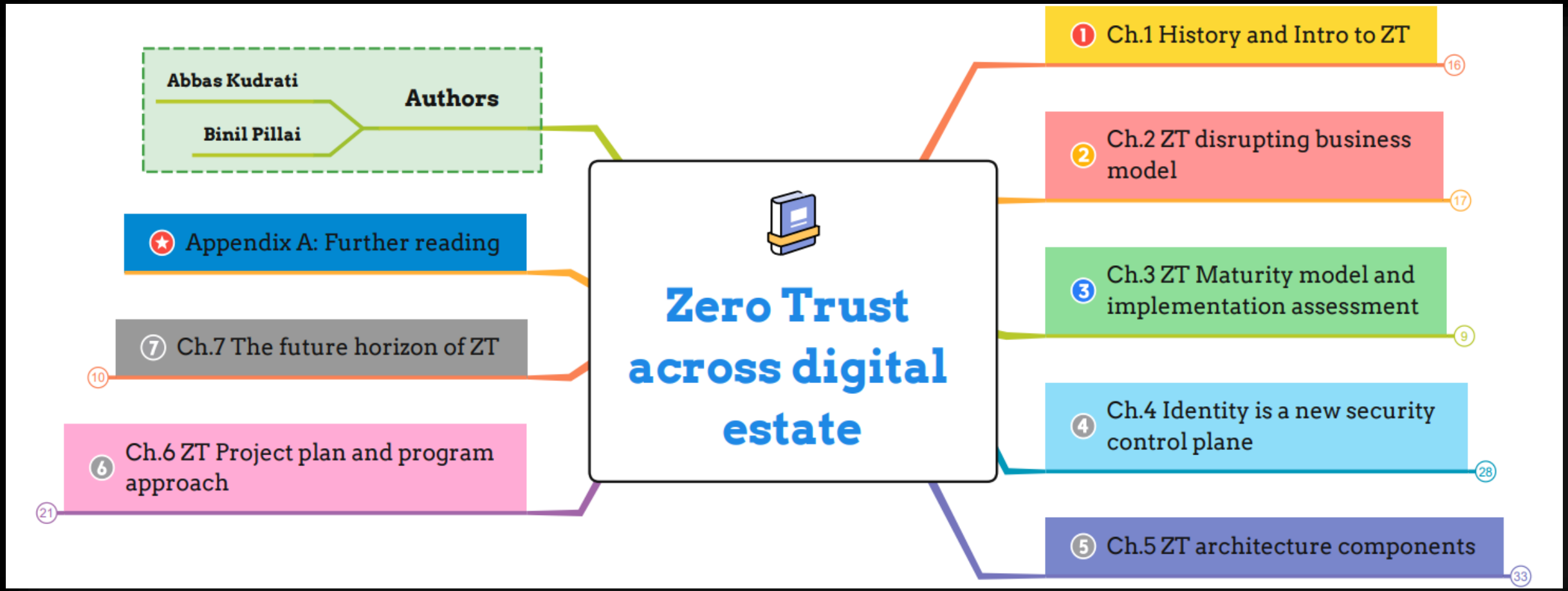
Slides copy on

https://aka.ms/abbas

“Conference” folder

Appendix
About the book

Book Chapters Mind Map



Authors:
Abbas Kudrati(right)
Binil Pillai(left)

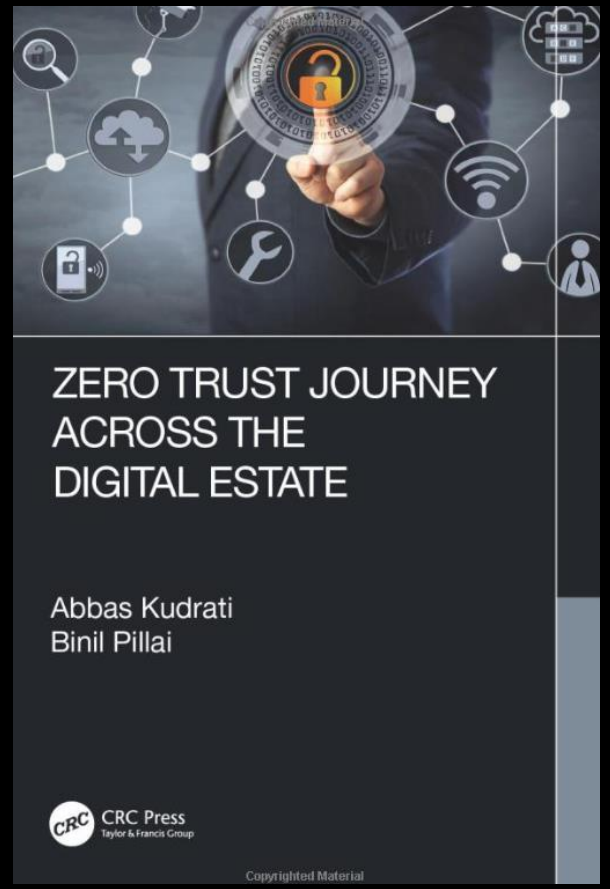
Backward by:
Dr. Chase Cunnigham (Dr. Zero Trust)

Book Description

- "Zero Trust is the strategy that organizations need to implement to stay ahead of cyber threats, period. The industry has 30 plus years of categorical failure that shows us that our past approaches, while earnest in their efforts, have not stopped attackers.
- Zero Trust strategically focuses on and systematically removes the power and initiatives hackers and adversaries need to win as they circumvent security controls.
- This book will help you and your organization have a better understanding of what Zero Trust really is, recognize its history, and gain prescriptive knowledge that will help you and your enterprise finally begin beating the adversaries in the chess match that is cyber security strategy."

What's unique about this book ?

- Authored by Thought leaders and Practitioners
- Written in simple and easy to understand language
- You will learn the history of Zero Trust concept and definition of this concepts from Forrester, Microsoft, Netflix, Google, NIST, Open Group and many more
- Target audience across all levels including nontechnical executives to technical architects
- Real life case studies on Zero Trust implementation by real customers across the world
- Vendor natural Zero Trust Assessment Toolkit created with the partnership with Deakin University, Australia, toolkit can be downloaded from the link provided in the book's Chapter 3
- Technical examples contributed by SMEs from Microsoft, Netskope, Silverfort and Zscaler
- Dedicated chapters on Identity security and Zero Trust project plan
- **Get your copy from Amazon or Routledge (CRC Press)**



From Australia

Vivek

★★★★★ **Comprehensive guide for Zero Trust journey**

Reviewed in Australia on 15 December 2022

I was looking for a book which goes beyond the concepts of Zero Trust Architecture and actual guidelines on implementation. I'm happy to say that this book has delivered on what I was expecting. There are several examples of real companies who have implemented ZTA. I liked that the book covered all aspects of ZTA implementation such as strategy, business alignment, culture etc., and not just technical components. I highly recommend this book for anyone who wants to understand ZTA and needs practical guidance on implementation.

One person found this helpful

Srisatya

★★★★★ **Great book for Data Security professionals**

Reviewed in Germany DE on December 20, 2022

Verified Purchase

Great book for Data Security professionals

Report abuse

From the United States

PurpleDuck

★★★★★ **Great Book !**

Reviewed in the United States US on November 10, 2022

Verified Purchase

Ok, I teach Zero Trust and am the head of security for the company I work for. I am always looking for a good Zero Trust book since Zero Trust is still evolving. I have read so many books and white papers (Jericho, BeyondCorp, etc.). And I teach a 3-day boot camp on Zero Trust. Since Zero Trust is still evolving, I love to read new takes or angles on Zero Trust and Zero Trust Architecture. So after reading and learning so much, it is rare to find a book that excites me. This is one of those books not only does it offer some new insight (thank you), and also offers some tools to utilize and some great ideas. This bok is worth every penny, and I plan to incorporate some of the ideas in the 3-Day book camp. A very good read, even if you know ZT and ZTA.

Thus I would highly recommend this book.

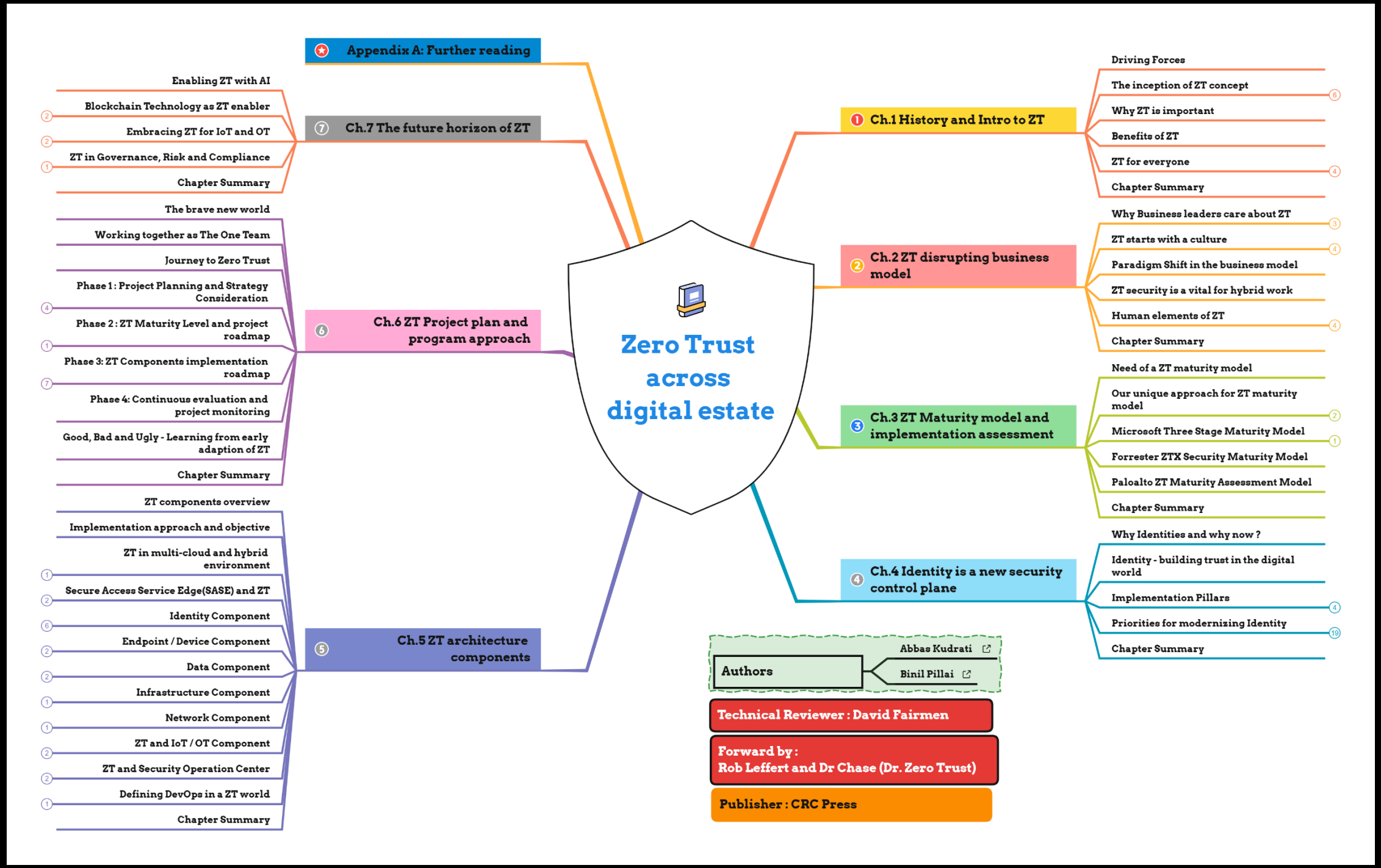
jonathan hering

★★★★★ **The Most comprehensive and in depth Content on Zero Trust**

Reviewed in the United States US on March 20, 2023

The reason I love reading this book is that I am not a Security Expert Abbas Kudarti makes it accessible for people that would like to study Zero Trust Paradigm from scratch the book gave me a wide perspective on Information security alongside practical tools on how to Implement Zero Trust Architecture for every modern enterprises across industries

Thank you for your feedback. | Report abuse


Zero Trust across digital estate
Appendix A: Further reading
Ch.7 The future horizon of ZT
Enabling ZT with AI
Blockchain Technology as ZT enabler
Embracing ZT for IoT and OT
ZT in Governance, Risk and Compliance
Chapter Summary
Ch.6 ZT Project plan and program approach
The brave new world
Working together as The One Team
Journey to Zero Trust
Phase 1 : Project Planning and Strategy Consideration
Phase 2 : ZT Maturity Level and project roadmap
Phase 3: ZT Components implementation roadmap
Phase 4: Continuous evaluation and project monitoring
Good, Bad and Ugly - Learning from early adaption of ZT
Chapter Summary
Ch.5 ZT architecture components
ZT components overview
Implementation approach and objective
ZT in multi-cloud and hybrid environment
Secure Access Service Edge(SASE) and ZT
Identity Component
Endpoint / Device Component
Data Component
Infrastructure Component
Network Component
ZT and IoT / OT Component
ZT and Security Operation Center
Defining DevOps in a ZT world
Chapter Summary
Ch.1 History and Intro to ZT
Driving Forces
The inception of ZT concept
Why ZT is important
Benefits of ZT
ZT for everyone
Chapter Summary
Ch.2 ZT disrupting business model
Why Business leaders care about ZT
ZT starts with a culture
Paradigm Shift in the business model
ZT security is a vital for hybrid work
Human elements of ZT
Chapter Summary
Ch.3 ZT Maturity model and implementation assessment
Need of a ZT maturity model
Our unique approach for ZT maturity model
Microsoft Three Stage Maturity Model
Forrester ZTX Security Maturity Model
Paloalto ZT Maturity Assessment Model
Chapter Summary
Ch.4 Identity is a new security control plane
Why Identities and why now ?
Identity - building trust in the digital world
Implementation Pillars
Priorities for modernizing Identity
Chapter Summary
Authors
Abbas Kudrati
Binil Pillai
Technical Reviewer : David Fairmen
Forward by :
Rob Leffert and Dr Chase (Dr. Zero Trust)
Publisher : CRC Press

Zero Trust Maturity Assessment Toolkit

Zero Trust Cybersecurity Maturity Assessment

This is an assessment toolkit to measure your organization's zero trust cybersecurity maturity level across 8 main domains.

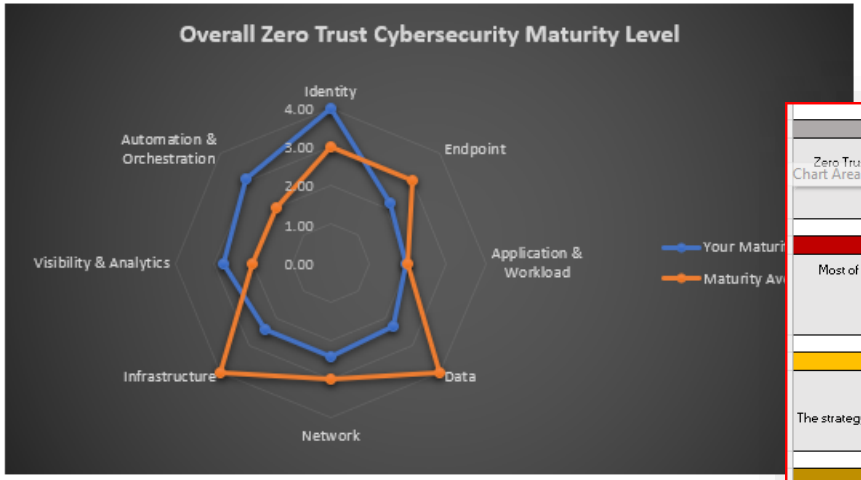
The Zero Trust Cybsecurity Model below describes how security teams should achieve to improve Zero Trust Cybersecurity. There are 55 questions in terms of 8 domains: Identities, endpoint, application workload, infrastructure, data, networks, people, visibility & analytics, and automation & orchestration. It usually takes no more than 30 minutes to answer all questions.

Zero Trust Domain		To what extent has your organization deployed the following Critical Success Factor (CSF) statements?		NIST CSF	ISO/IEC 27001	ACSC Essential Eight	Your Answer (1 = Not on roadmap 2 = On roadmap 3 = Deployment scoped 4 = Partially deployed 5 = Completely deployed)	Maturity Weight	Maturity Average	Maturity Gap	Impact (1 = Minor 2 = Limited 3 = Moderate 4 = Severe 5 = Catastrophic)	Likelihood (1 = Rare 2 = Unlikely 3 = Possible 4 = Likely 5 = Almost Certain)	Total Risk
							Update your answers				Update your answers	Update your answers	
Identity *An identity refers to the common dominator across networks, endpoints, and applications, such as people, services, or IoT devices.*	ID1	Internal users (employees) perform "multi-factor authentication (MFA)" to access all critical business systems.	MFA is a efficient way to enhance the security of internal user accounts by reducing the attacks associated with compromised passwords, such as brute force, credential stuffing.	PR.AC-7	A.9.2.4	Multi-factor authentication	5	1	4	1	2	2	4
	ID2	External users (third parties) perform "multi-factor authentication" to access critical business systems.	MFA is a efficient way to enhance the security of external user accounts by reducing the attacks associated with compromised passwords, such as brute force, credential stuffing.	PR.AC-7	A.9.2.4	Multi-factor authentication	5	1	3	2	5	5	25
	ID3	Single sign-on (SSO) (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate internal users to all critical business systems.	SSO can elevate user experience, improve productivity of internal users by logging in at regular intervals (often once a day) and revamp security by decreasing the number of attack surfaces.				5	0.8	3	2	4	3	12
	ID4	Single sign-on (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate external users to all critical business systems.	SSO can elevate user experience, save time of external users by logging in at regular intervals (often once a day) and revamp security by decreasing the number of attack surfaces.				5	0.8	2	3	4	3	12
	ID5	Identity management system is deployed in the cloud.	Cloud-based IDM systems can improve efficiency and security in an era of remote work.		A.9.4.4		5	0.6	3	2	3	3	9
	ID6	Enterprise resources (servers, databases, software as a service(SaaS) applications, intranet business systems, etc.) have a specific security policy engine for access control (e.g., cloud access security broker (CASB), firewall, mobile device management (MDM)).	The policy engine is an important component to determine whether to grant access to a resource by monitoring and enforcing specific rules.	PR.AC-6	A.9.4.5		5	1	4	1	3	4	12
	ID7	Identity and access management (IAM) system integrates with privileged access management (PAM).	The integration of IAM and PAM can save time and simplify the process of protecting the identity of all users.				5	0.6	4	1	3	3	9
	ID8	There is a process to regularly (at least every six months) check whether the privilege users' administrative rights are as per approved.	Regular review and validation of privileged users' administrative permissions is a necessary step for privileged access management.	PR.AC-4	A.9.2.5	Restrict administrative privileges	5	0.6	4	1	4	3	12
	ID9	Have a policy for role-based access, rather than simply based on network boundaries.	Role-based access control policy (RBAC) makes sure that users have varying levels of access rights depending on their role.	PR.AC-4	A.9.2.2		5	0.8	3	2	4	4	16
	ID10	Real-time user risk and sign-in risk detections are enforced when evaluating access requests.	Risk can be detected in a timely manner and organizations can quickly respond to suspicious behavior.	PR.AC-7			5	0.8	3	2	4	4	16
Endpoint / Devices *A device refers to any hardware asset that can connect to a network, including internet of things (IoT) devices, mobile phones, laptops, servers, BYOD and others.*	EN1	All corporate-owned devices (workstations and smart devices) are enrolled by a device enrollment manager.	This can refine management and identification of devices.	ID.AM-1			1	0.6	4	-3	4	4	16
	EN2	Internal users' smart devices are enrolled in a mobile device management system.	This can manage, control, monitor and secure the internal users' smart devices.	ID.AM-1	A.11.2.1		3	0.8	3	0	4	4	16
	EN3	Access to corporate resources from external users' smart devices is provided by mobile application management.	This helps to manage external users' smart devices to secure the access to data.	PR.AC-3	A.9.4.4		3	0.8	3	0	3	3	9
	EN4	Both corporate and BYO devices need to be continuously verified before being granted access to corporate resources.	With the elimination of perimeter, access control is based on device risk.	PR.AC-1			1	1	2	-1	5	5	25
	EN5	Managed devices are required to be compliant with IT configuration policies before granting access.	This helps to make sure that the configuration of managed devices is known and trusted.		A.10.1.1		4	0.6	3	1	4	4	16
	EN6	Endpoint detection and response (EDR) tools are used to enable real-time device risk evaluation.	This allows continuous monitoring and understanding of device risk in real time.	PR.IP-8			5	0.8	4	1	4	3	12
			This can prevent the attacks caused by browsing malicious URLs, such as spamming and										

Zero Trust Cybersecurity Maturity Level Report

We define six levels of Zero Trust cybersecurity maturity: non-existent, initial, informal, defined, managed and measurable and optimised. Based on your responses, your organisation is at the Level 2.

Dimension	Score	Maturity Leve	Maturity Avera	Maturity Gap
Identity	4.00	4	3	1
Endpoint	2.18	2	3	-1
Application & Workload	1.95	1	2	-1
Data	2.29	2	4	-2
Network	2.43	2	3	-1
Infrastructure	2.40	2	4	-2
Visibility & Analytics	2.75	2	2	0
Automation & Orchestration	3.08	3	2	1
Overall	**2.63**	**2**	**3**	**-1**



Level 0

Zero Trust has not been considered for placement into the roadmap or is only on the roadmap for most organizations in this phase.

During this preparation phase, organizations are deploying initial discovery and assessment activities.

Level 1

Most of the organisation will be at this stage during the start of their Zero Trust journey. At this basic level, fundamental integrated capabilities are implemented.

The strategy here is to start small and focus on strategic wins.

Level 2

At the advanced level, the capabilities are further integrated and refined.

The strategy for this level is to advance the zero-trust journey with more robust identity management, data security, and advanced threat detection and response capabilities.

Level 3

At this matured level, organisations have deployed advanced protections and controls with robust analytics and orchestration.

The strategy for this level is complete and extend Zero Trust across advance threat intelligence, threat hunting, advance automated at the SOC and seamless access for the end-users.

Level 4

At this level, performance is monitored and measured through-life and reported back to appropriate Domain Authorities within a clear Governance Framework.

Level 5

At this level, there is an enterprise-wide, integrated, highly automated approach to monitoring and reporting and the Governance Framework enables systemic understanding and communication of risks and opportunities.

Zero Trust Domain

Companies must build eight capabilities to effectively manage the maturity of zero trust. These 8 domains are: Identities, Endpoint/Devices, Application & Workload, Infrastructure, Data, Networks, Visibility & Analytics and Automation & Orchestration.

Identity

An identity refers to the common dominator across networks, endpoints, and applications, such as people, services, or IoT devices.

Supporters

Zero trust allows organizations to embrace the flexibility that their teams demand, while increasing the security of their systems. The question for security professionals isn't whether to embrace zero trust, the question is where are we along the journey?

Omkhar Arasaratnam, Engineering Director, Google

Security can longer scale in the way we have done things for 20+ years. We need a new way of doing things to get leverage in our model. Zero Trust is foundational for the future of every security program. However, Zero Trust is a journey and will not happen overnight.

Jason Clark, Chief Strategy Officer, Netskope

Zero Trust is just as much a business enabler as it is a security paradigm.

Zero Trust enables business agility – without Zero Trust, secure cloud consumption is but a pipedream.

Brett James, Director, Transformation Strategy for Zscaler

Supporters

Zero Trust should be the key security strategy for all companies, and implementing it requires unified analysis and enforcement across all users, devices, resources, and environments that eliminate siloes and blind spots to accurately assess the context of each authentication and enforce adaptive access policies everywhere.

Hed Kovez, CEO and Co-Founder, Silverfort

Gone are the days of deprecated VPN hair pinning and lateral movement issues. Zero Trust (Cloud) architectures have now evolved from a touted "nice to have add-on" to an imperative for BOTH CIOs and CISOs looking to improve both operational resilience and security controls.

Nick McKenzie, CIO & CISO, Bugcrowd

Trust is a human emotion and is the single greatest vulnerability when we think about cyber security. Given the interconnected and complex world we live in, if we stop assuming a level of trust and start challenging everyone inside and outside of our ecosystem, we can improve security.

Nicola Nicol, industry expert

When it comes to implementing Zero Trust architecture, focus on Progression over Perfection.

Bret Arsenault, CISO, Microsoft

My other publications(Author, Contributor & Tech Editor)

https://www.amazon.com/author/abbask