Microsoft

Zero Trust Business Strategy

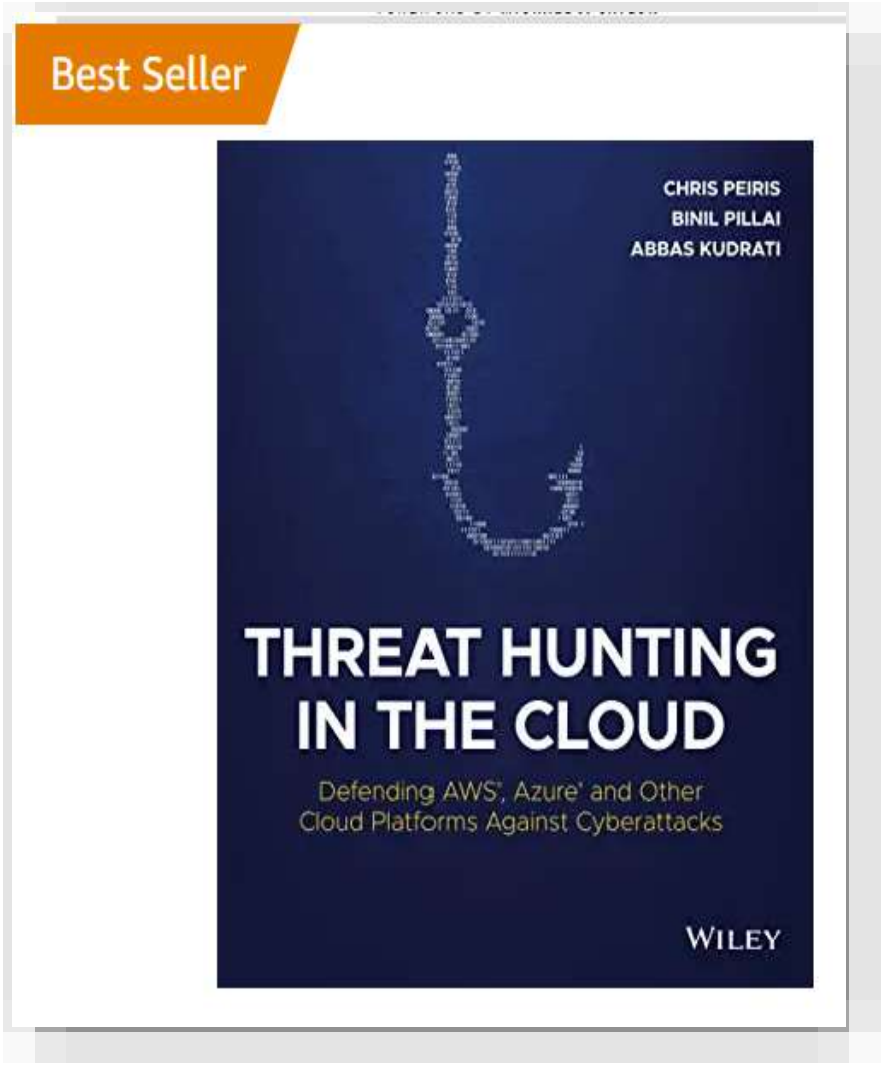
Abbas Kudrati
APAC Chief Cybersecurity Advisor
Microsoft
@askudrati

About me

"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

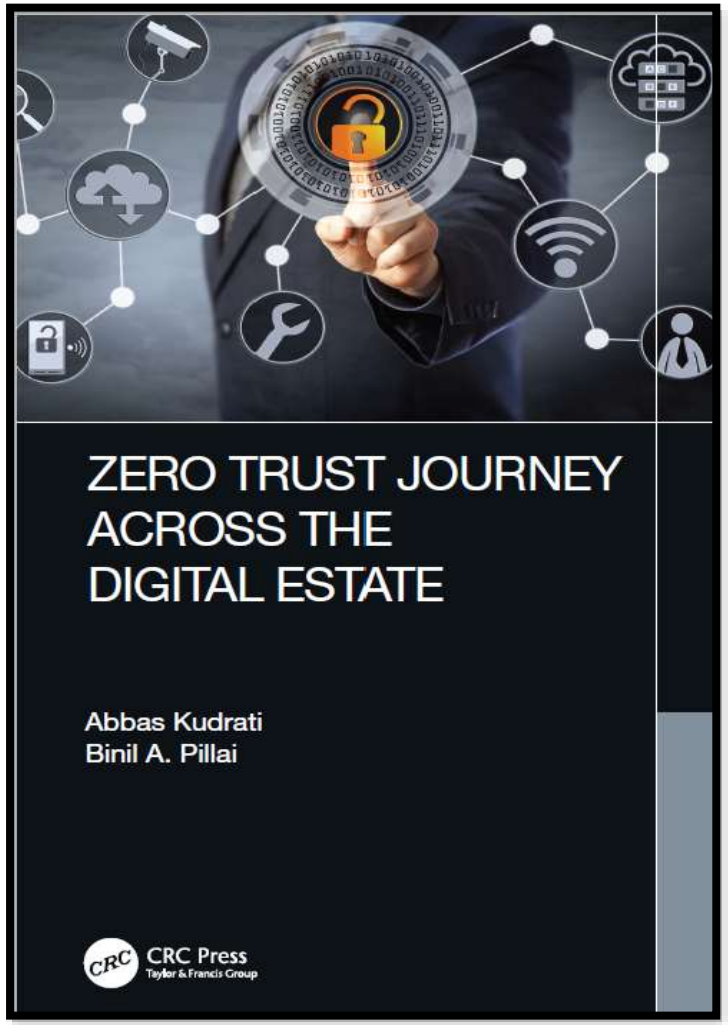
- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

My Publications

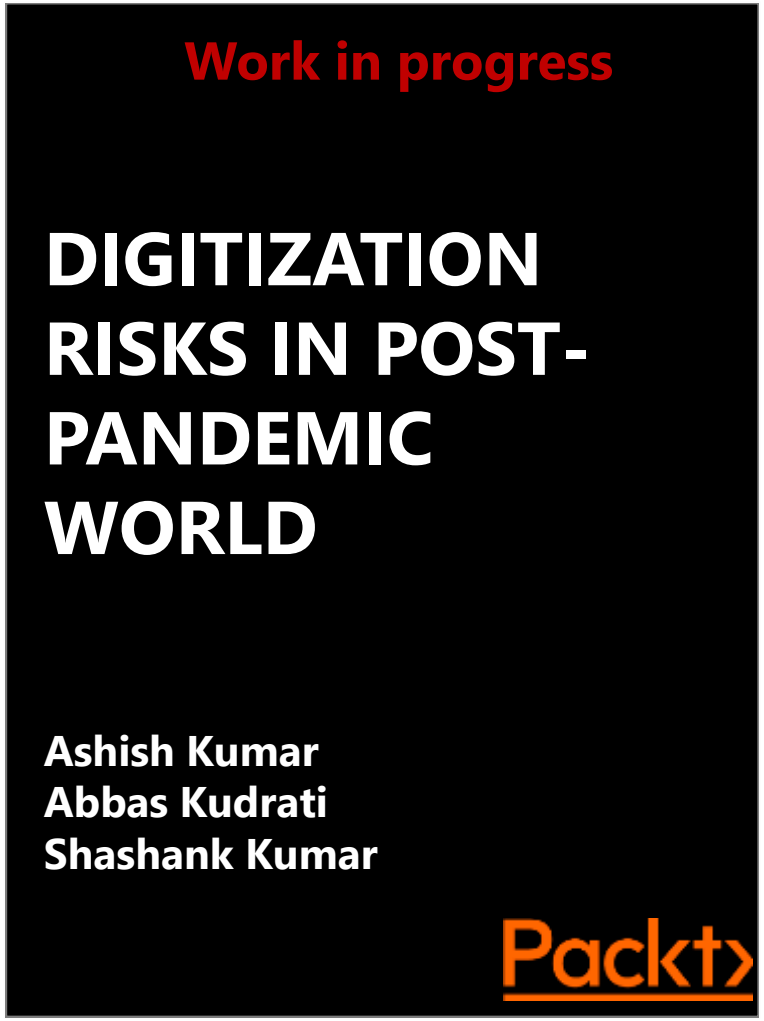


[Get it on Amazon](#)

Or send me a request for a free copy

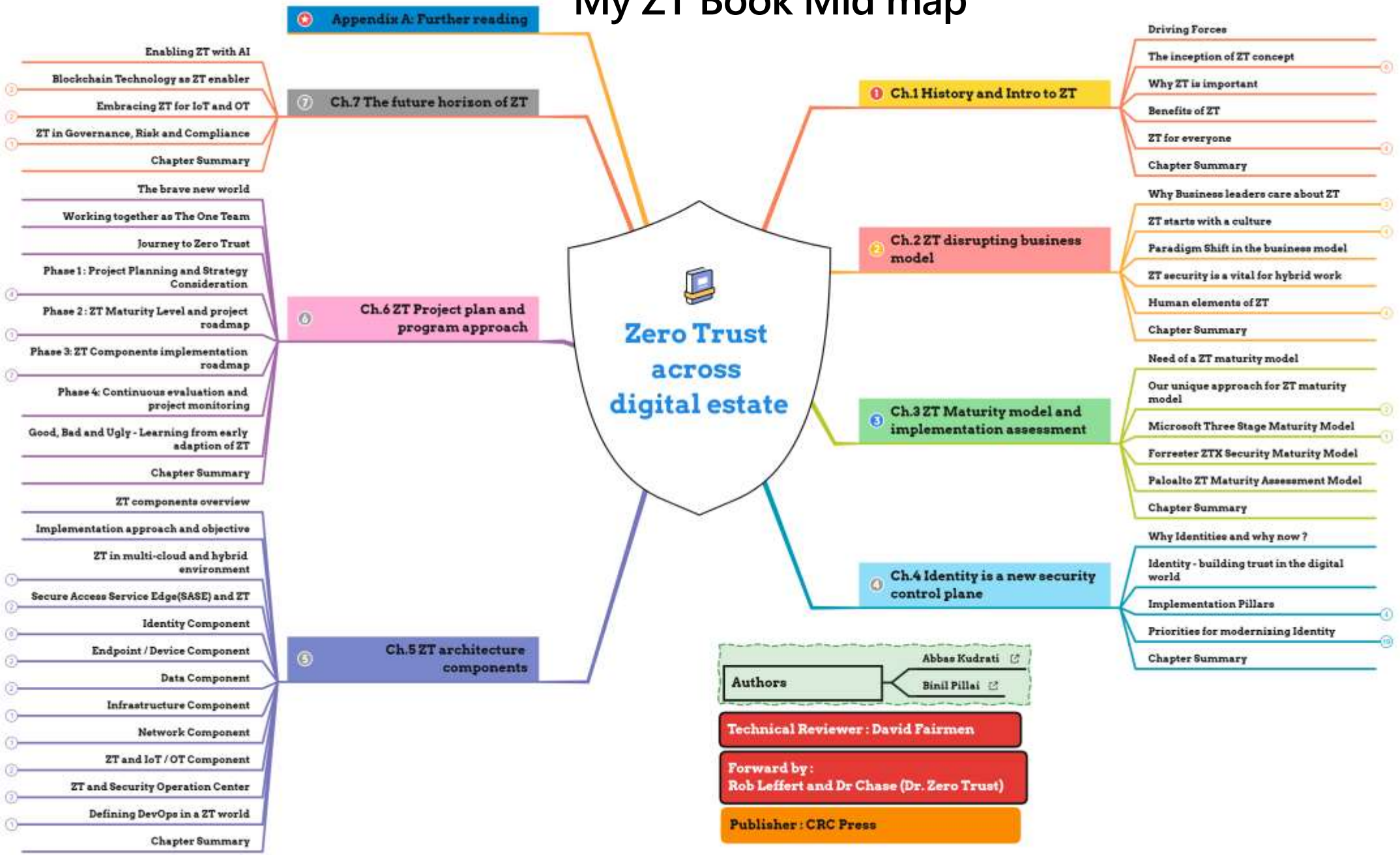


[Pre order on Amazon](#)



Releasing soon by July 2022

My ZT Book Mid map



Today’s reality | Distributed and hybrid

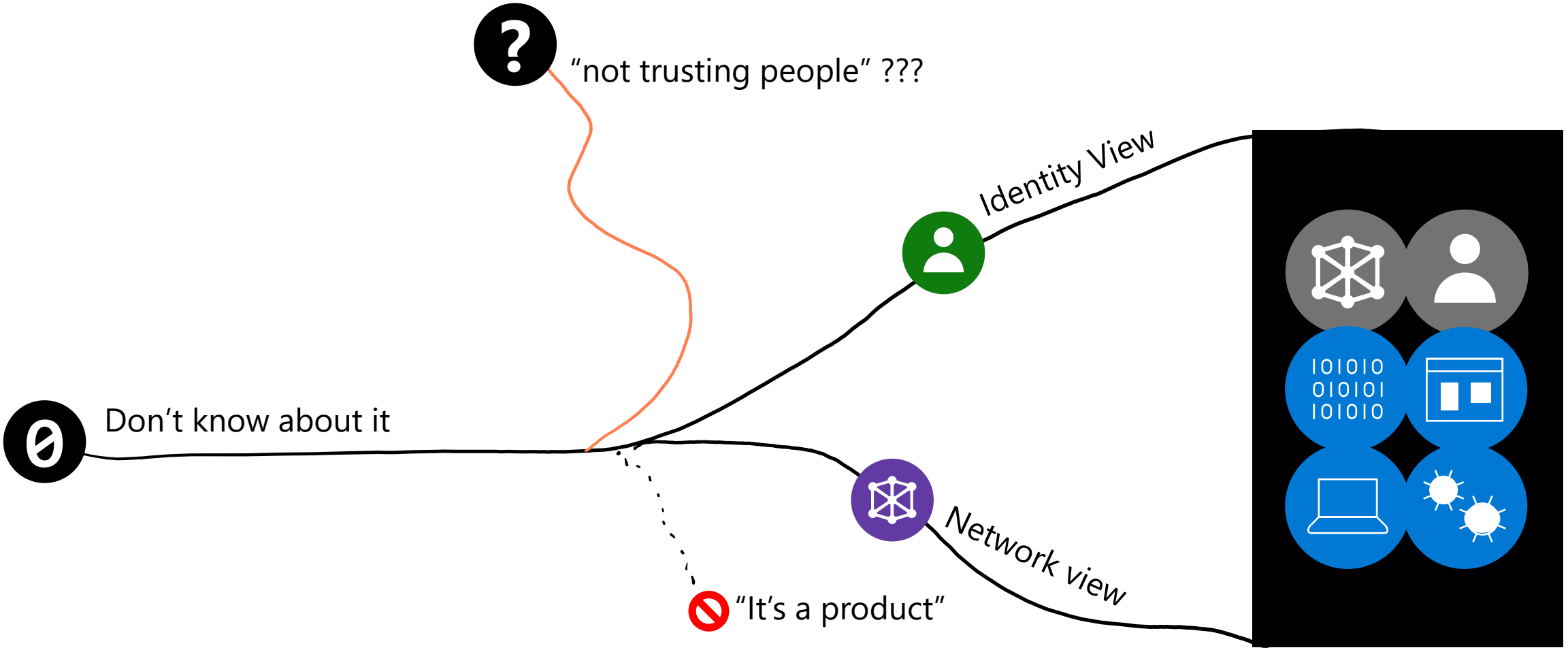
Where we work
has continued to rapidly evolve to a mix of locations.

The tools we use
are varied, from corporate to BYOD, cloud-based, or on-prem apps.

How we do our work
is an evolving mix of virtual, physical, collaborative, and data-driven styles.

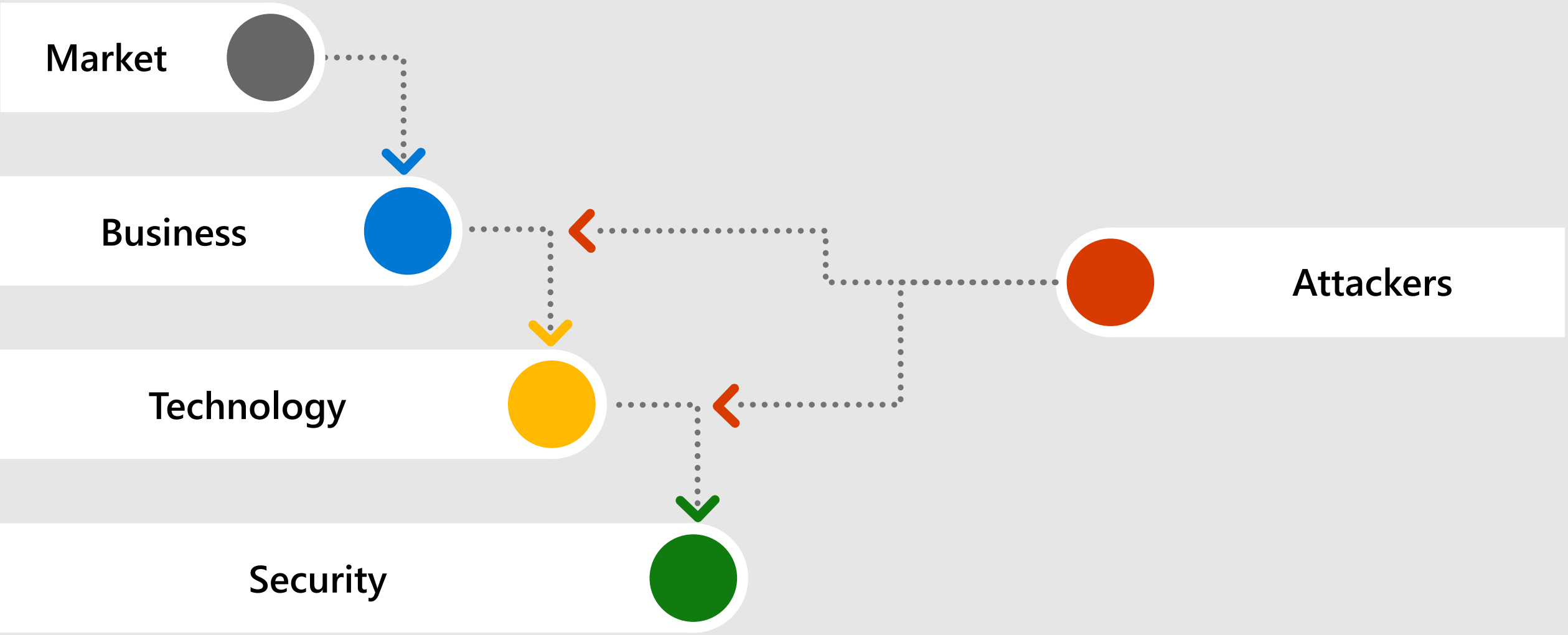
Evolving risks
Increasing volume and sophistication of threats, and a wider, more distributed attack surface.

Where are you on zero trust journey?

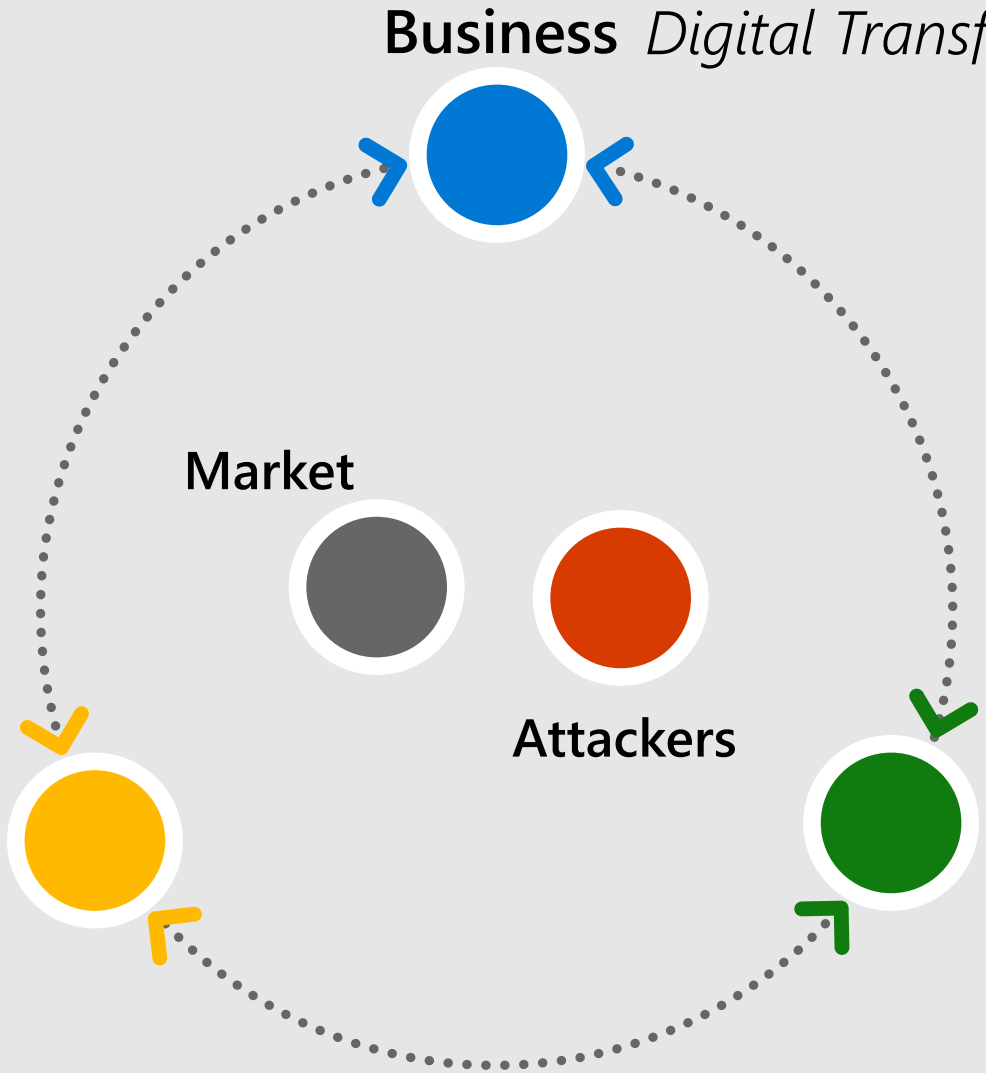


Introduction - Why Zero Trust is Important

The world is transforming rapidly



Working together



What is Zero Trust?

Assume breach | Explicitly Verify | Least privileged

Zero Trust Security Strategy - includes *multiple* modernization initiatives

Modern Access Control
Modern approach to access management

Secure Access Service Edge (SASE)

Modern Security Operations (SOC)

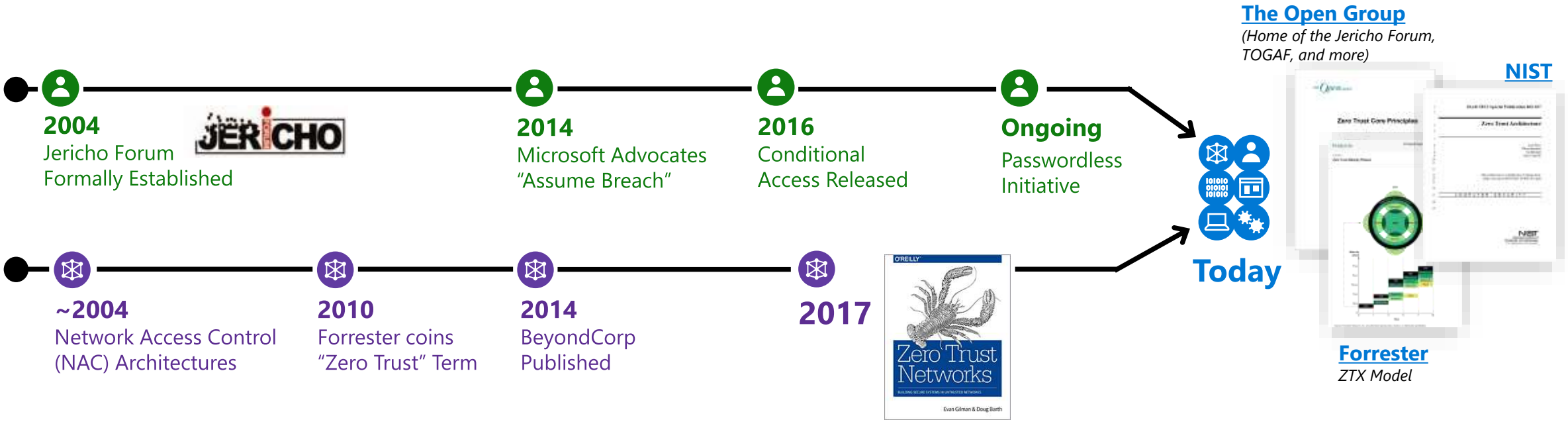
Infrastructure & Development Security

Data Security & Governance, Risk, Compliance (GRC)

IoT and OT Security

Modernization, Integration, and Automation across technical controls
Identity, Endpoint, Network, Application, Infrastructure, Data, and Infrastructure

“Zero Trust” has been around for a while



Historically slow mainstream adoption for both network & identity models:

Network – Expensive and challenging to implement
Google’s BeyondCorp success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

Increasing consensus and convergence (though still some variations)

Zero Trust Adaption report 2020 /21

EXHIBIT 3. HYBRID WORKPLACE INTENT

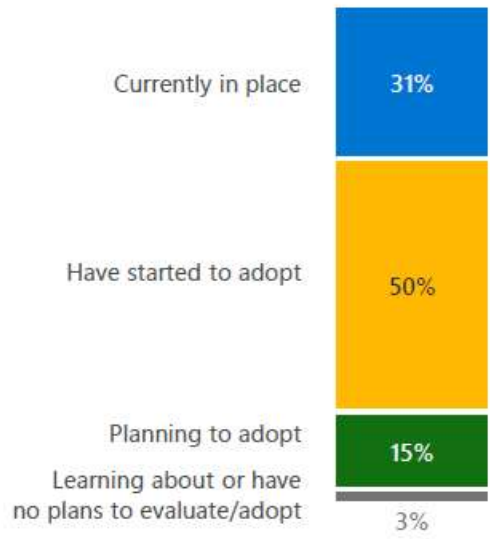


EXHIBIT 4. HYBRID WORKPLACE CONCERNS

Employees downloading unsafe apps	37%
An increase to IT workload	37%
Ransomware attacks	36%
Phishing attacks	35%
Improper use of personal devices	34%
Unauthorized access to data	31%
Inability to manage all devices	30%
Use of personal email accounts	30%
Non-compliance with data regulations	24%

EXHIBIT 1. ZERO TRUST IS CRITICAL

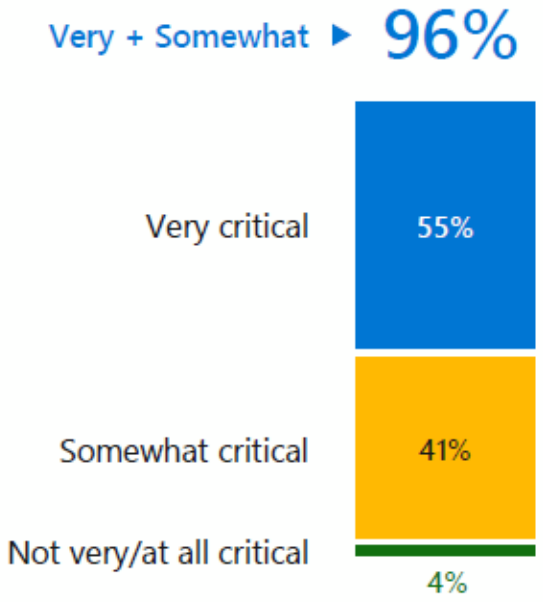


EXHIBIT 2. ZERO TRUST MOTIVATORS

Top Motivators	
Improve overall security posture	47%
Improve end user experience and productivity	44%
Transform the way security teams work together	38%
Simplify security stack	35%
Reduce security costs	35%

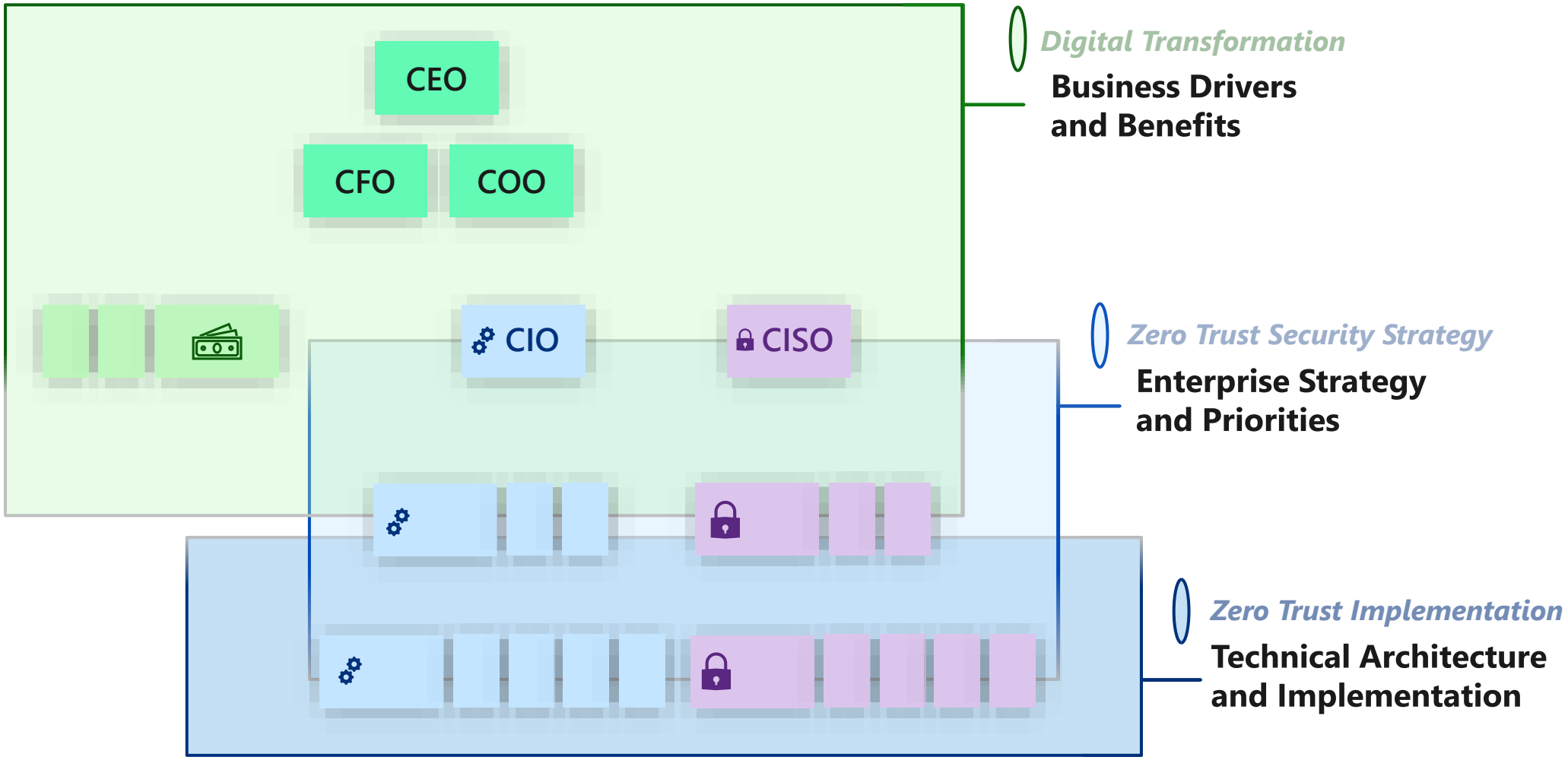
	US (2020)	US	DE	JP	AUS/NZ
Zero Trust implementation	70%	79%	75%	76%	71%
• Fully implemented	27%	44%	19%	32%	28%
• In progress	43%	35%	56%	44%	43%

35% Fully implemented

42% Implementation in progress

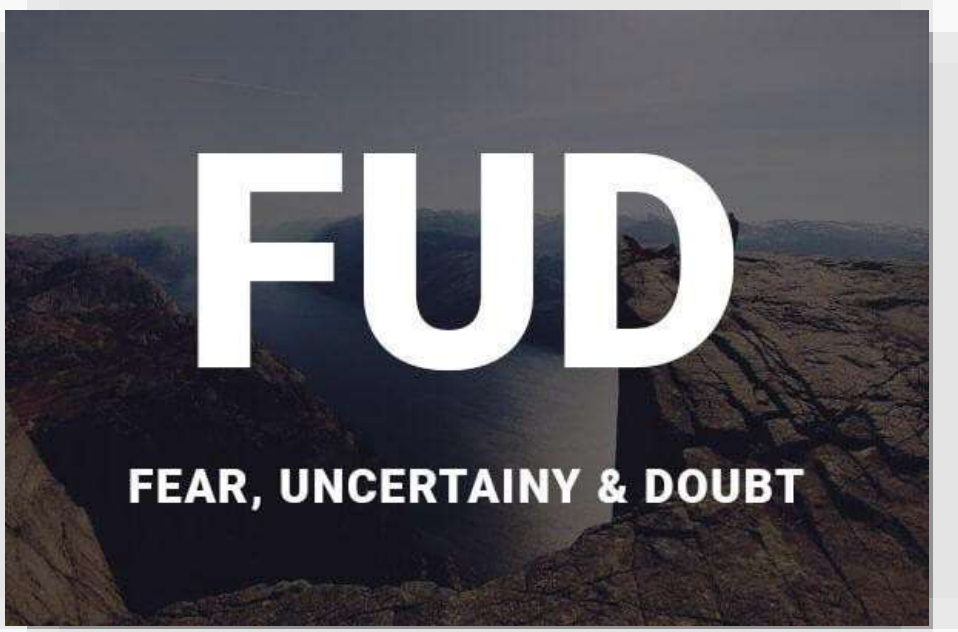
Perspectives on Zero Trust Security Strategy

A Journey that affects everyone a little differently



What Zero Trust is not about…

- Literal
- An Adjective
- For Sale
- Instant
- A Destination
- One Size Fits All
- A Revolution



ZT Business Strategy

- **Create clarity**
  - Synthesize the complex
  - Ensure shared understanding
  - Value understood

- **Generate energy**
  - Inspire optimism, creativity, and growth
  - Create an environment where everyone does their best work
  - Build organizations/teams that are stronger tomorrow than today

- **Deliver success**
  - Drive innovation that people love
  - Be boundary-less in seeking solutions for the Zero Trust program
  - Tenaciously pursue the right outcomes

Do’s and Don’t

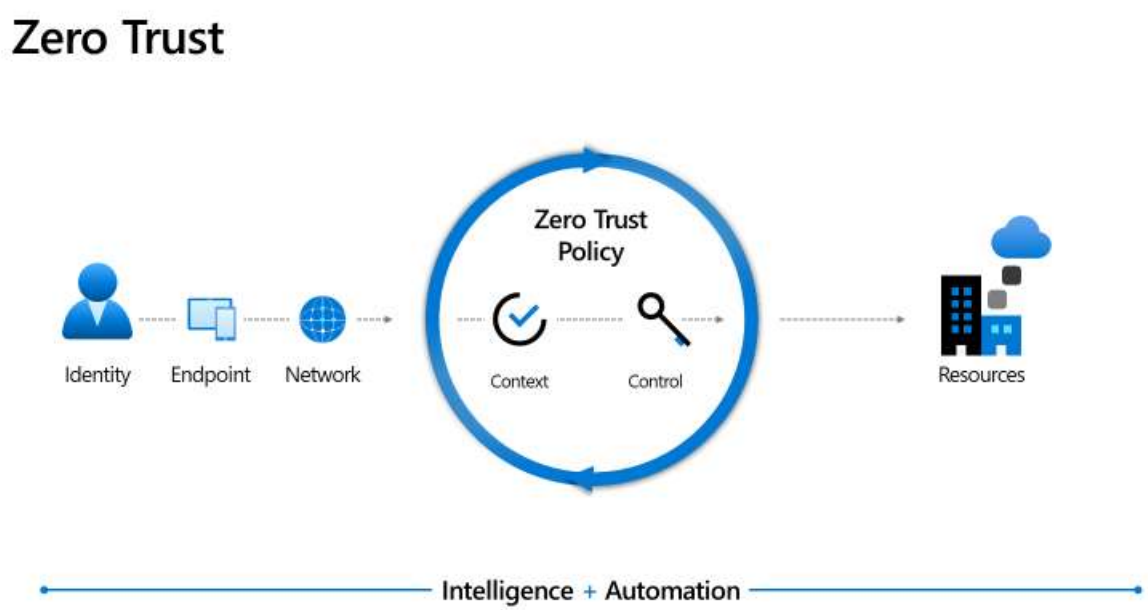
- Is ZT right for you ?
- Gain support from and buy in from key executives
- Identifying key inter dependencies across the organization
- Understanding your information assets.
- Understanding your user population
- Identifying your application exposure / risk exposure
- Understanding and grouping of key business user population and core application combination
- Start with few basic fine-grained controls

Next Steps

- Prepare, engage and unify key stakeholders across your organization on your vision for Zero Trust.
- Start the discovery of your current state and objectives for the Zero Trust program.
- Identify personas for your Zero Trust program.
- Work together with Microsoft to Identify capabilities and technical security gaps in your existing environment.
- Document and prioritize in a solution backlog prior to Program/Sprint planning.

Appendix: Resources and Learning links

Zero Trust networking maturity model



Traditional	Advanced	Optimal
Few network security perimeters and flat open network	cloud micro-perimeters with some micro-segmentation	ingress/egress cloud micro-perimeters and deeper micro-segmentation
Minimal threat protection and static traffic filtering	Cloud native filtering and protection for known threats	ML-based threat protection and filtering with context-based signals
Internal traffic is not encrypted	User to app internal traffic is encrypted	All traffic is encrypted
Many ingress/egress	Fully distributed	

Microsoft has rich set of cloud native services designed to help you move to zero trust model

Learn more about zero trust networking at https://www.microsoft.com/security/blog/2020/06/15/zero-trust-part-1-networking/
https://www.microsoft.com/en-us/security/zero-trust

Zero Trust Rapid Modernization Plan (RaMP)

Prioritize rapid progress on highest positive impact

Roll out to IT Admins first
- Targeted by Attackers
- High potential impact
- Provide technical feedback

Top Priorities – *critical security modernization steps*

User Access and Productivity

1. **Explicitly validate trust for all access requests (via Azure AD Conditional Access)**
   a. **User Accounts -** Require Passwordless or MFA for all users + measure risk with threat intelligence & behavior analytics
   b. **Devices** - Require device integrity for access (configuration compliance first, then XDR signals)
2. **Increase security for accessing key resources**
   a. **Apps –** Enable Azure AD for all SaaS, for VPN authentication, and publish legacy on-premises/IaaS via App Proxy
   b. **Data -** Discover and protect sensitive data (via Cloud App Security, CA App Control, Microsoft Info Protection)
3. **Governance** to continuously monitor security posture and reduce risk (via Secure Score)

Modernize Security Operations

4. **Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Azure Defender)
5. **Unify Visibility** with modern Security Information and Event Management (SIEM via Azure Sentinel)
6. **Reduce manual effort -** using automated investigation/remediation, enforcing alert quality, & proactive threat hunting

As Needed – *typically driven by cloud adoption or OT/IoT usage*

Operational Technology (OT) and Industrial IoT

Discover – Find & classify assets with business critical, life safety, and operational/physical impact (via Azure Defender for IoT)

Protect – isolate assets from unneeded internet/production access with static and dynamic controls

Monitor – unify threat detection and response processes for OT, IT, and IoT assets (via Azure Defender for IoT)

Datacenter & DevOps Security

Security Hygiene – Rigorously monitor + remediate security configurations, security updates, MFA, and more

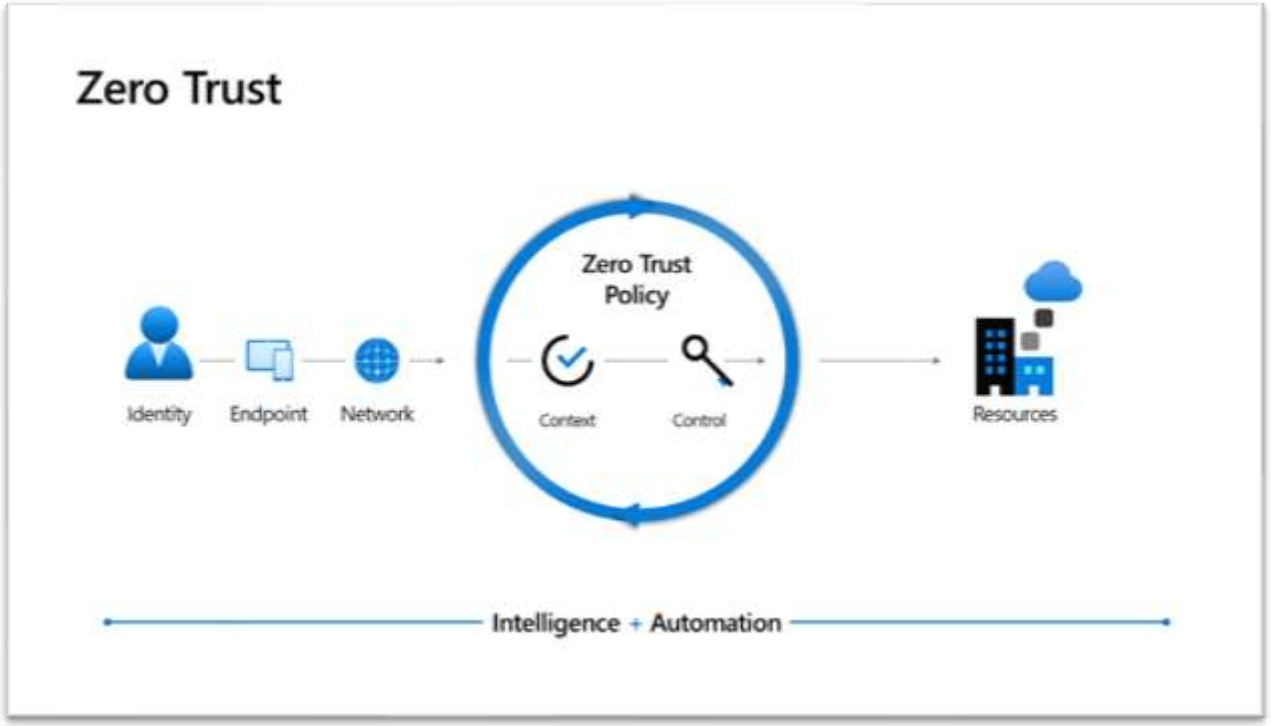
Reduce Legacy Risk – Retire or isolate legacy technology (Unsupported OS/Applications, legacy protocols)

DevOps Integration – Integrate infrastructure + development security practices into DevOps with minimal friction

Microsegmentation – Additional *identity and network* restrictions (dynamic trust-based and/or static rules)

ZT builds on classic security
Align to cloud migration schedule

Zero Trust Resources



- Zero Trust page: https://aka.ms/zerotrust
- Business Plan: aka.ms/ZTbizplan
- 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

- Zero Trust: Security Through a Clearer Lens session (Recording | Slides)
- CISO Workshop Slides/Videos
- Microsoft's IT Learnings from (ongoing) Zero Trust journey

Zero Trust Program Approach (Example)

Sprint 0

3-4 weeks | **2 weeks**

Discovery | Sprint planning

Day 1	6 to 9 days	2 Weeks	2 Weeks
Zero Trust Program Initiation (This workshop)	• Governance (½ - 1 day) • Identities (1 – 1½ day) • Devices (½ - 1 day) • Apps (½ - 1 day) • Infrastructure (1 day) • Network (1 day) • Data (½ - 1 day) • Security Management (1 – 1½ day)	Zero Trust Maturity Assessment Program Roadmap	Delivery Sprints planning
Key Outcomes	Briefings, Maturity Scoring	Roadmap	Milestone Plan, Backlog
Kick-Off	**Workshops & Deep Dives**	**Program Tracks**	**Sprint Planning**
• Customer Objectives Workshop • Microsoft and Zero Trust Brief • Review Pre-Engagement Questionnaire • Introduction to Agile Delivery Approach	• Topic-focused strategic and technical discovery/briefings aligned to Zero Trust/Microsoft Secure Pillars • Capabilities and Personas Selection • Technology and capability deep dives • Define and structure Objectives and Key Results (OKR's) • Clear set of outcomes defined in Azure DevOps (ADO)	• Program Roadmap by track • Report out to key stakeholders • Recommendations and priority delivery • Create a Risk Register to capture any blockers during the Zero Trust Journey	• Sprint Plan define & prioritize epics • Sprint Solution Backlog • Establish Tooling • Define Sprint Burndown

Sprint Program

***n* weeks**

Epics

4 Weeks	4 Weeks
Delivery Sprints	
Sprint Reporting	Sprint Reporting
Sprint 1	**Sprint *n***
• Daily Standups • Demonstration • Retrospective • Sprint 1+ planning • Increment 1	• Daily Standups • Demonstration • Retrospective • Sprint 1+ planning • Increment N

Microsoft

Thank you!

https://aka.ms/abbas