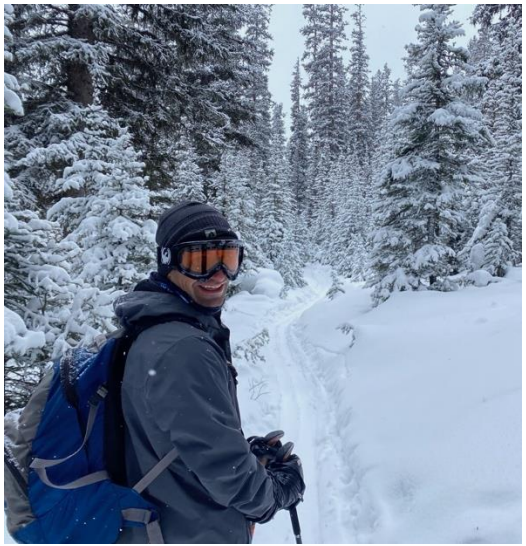
Simplifying Zero Trust Architecture

For the Warfighter

Brandon E. Lightle CCIE, CISSP, Customer Delivery Architect

Who is Brandon?



- Customer Delivery Architect at Cisco Systems
- CCIE & CISSP certified
- 15 years in the industry
- Assists DOD agencies with ZTA and C2C

Agenda

- Kick Off and Zero Trust Overview
- Marketing Ruins Everything
- Voice of the Customer-Use Case Challenges
- The ZT Journey
- An Action Plan
- Zero Trust Lifecycle Approach
- Conclusion

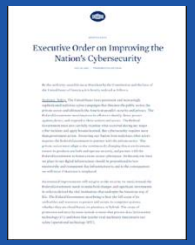
Fundamental Takeaways!

- Do not get caught up in marketing hype
- The Zero Trust Principles (aka Tenets & Pillars)
- Eat the elephant however you want
- Make the most use of what has already been purchased
- Develop a process
- Do something!

Public Sector Mandates

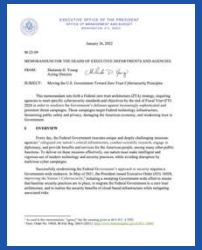
Civilian - 2024 Actions

Executive Order 14028
May 2021


Executive Order on Improving the Nation's Cybersecurity

- Achieve specific Zero Trust goals
- Submit a Zero Trust Implementation Plan
- Establish a Zero Trust Program Lead

Memorandum 22-09
January 2022


MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

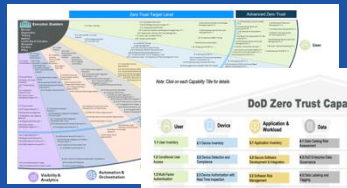
Specific Actions Completed by FY 2024

- Centralized Integrated IAM Platform
- Asset Inventory
- Application Inventory
- Automated Monitoring and Response of Categorized and Labeled Data
- Phishing Resist MFA
- Deploy Endpoint Detection and Response
- Application Authorization Monitoring and Analysis
- Implement Password Best Practices
- Encryption (DNS & HTTPS)
- Ongoing Security and Vulnerability Testing & Analysis
- Work towards ML/AI based continuous monitoring, detection and response
- Device & Identity Authentication Context
- Network, Application/Workload Segmentation
- Deploying Cloud Applications and Immutable Workloads in Cloud Environments (DevSecOps)

DoD – 2027 Targets

DOD ZT Strategy & Execution Roadmap

FY 2027 Target Level – 91 Activities



Comply to Connect (C2C)

Zero Trust Principles (aka Tenets & Pillars)

- Never Trust, Always Verify
- Least Privilege Access
- Assume Breach
- Micro-Segmentation
- Continuous Monitoring and Validation
- Identity and Device-Centric Security
- Dynamic Policy Enforcement

Zero Trust Easy Button

There is no switch to simply enable Zero Trust

- No single product covers all Zero Trust use-case
- Most vendors only touch a small piece of the spectrum

There is no benefit to wait until you believe you have a complete Zero Trust solution before starting!

- Zero Trust involves many facets of the business
- Zero Trust is an iterative and additive process
- Zero Trust (and Security) is continuous

Marketing Ruins Everything!

Every company that has a security product magically solves Zero Trust now

And There Are a Lot of Them

ZTA Market:
2024: $38B+
2027: $60B+

And They View It Differently

It’s segmentation

It’s ZTNA

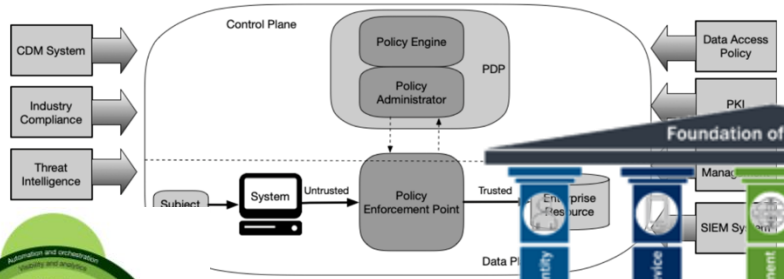
It’s endpoint security

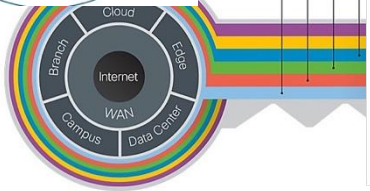
Zero Trust means different things to different people

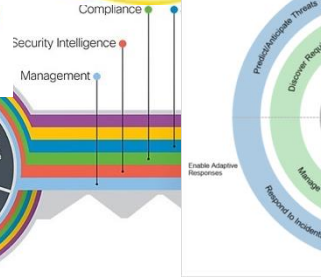
It’s firewall

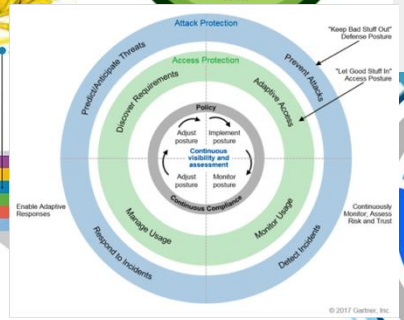
It’s identity

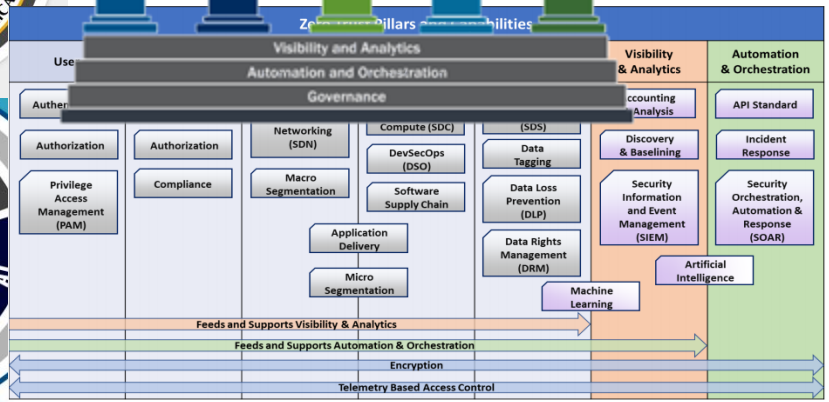
Standards / Models / Methods



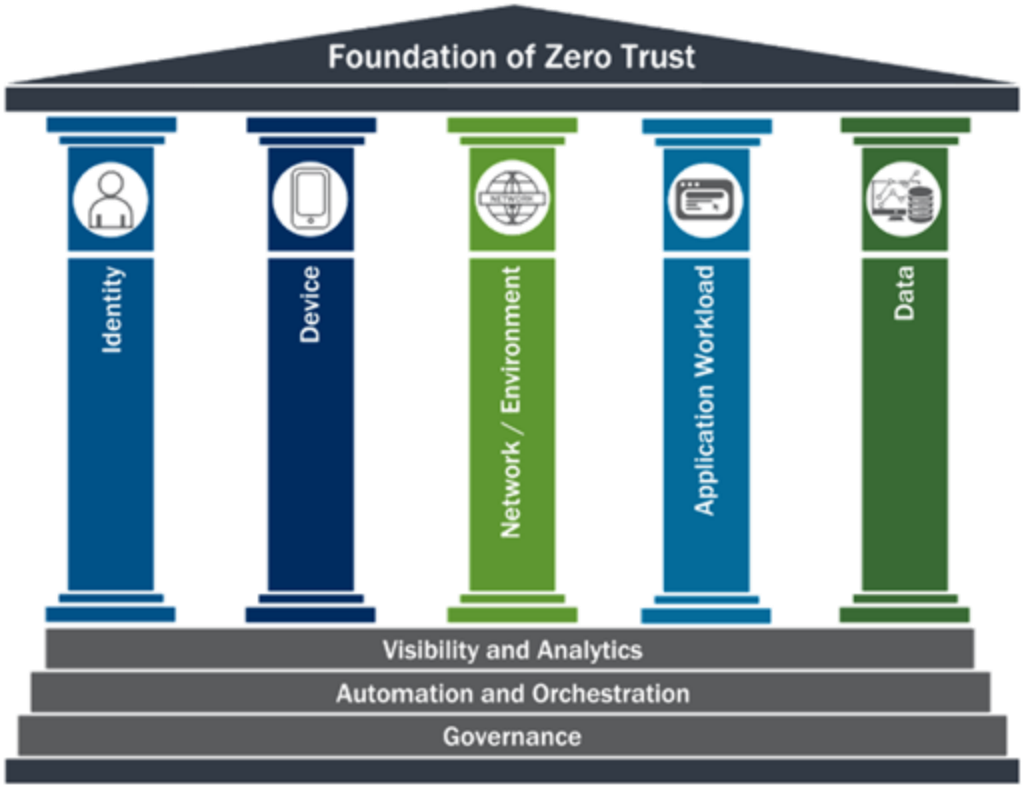








CISA's Zero Trust Model



ZTA (Some Assembly Required)

Voice of Customer

Zero Trust Challenges & Insights

Regulatory & Mandates

- **Am I in Compliance & What to do next?**

Siloed Environments

- **Lack of Governance**

Limited Resources & Skills Expertise

Value out of Current Investments

Lack of Visibility

- Who's on Network & Who are talking to

Hybrid Integration

- Legacy, OnPrem, Private Cloud, Public Cloud

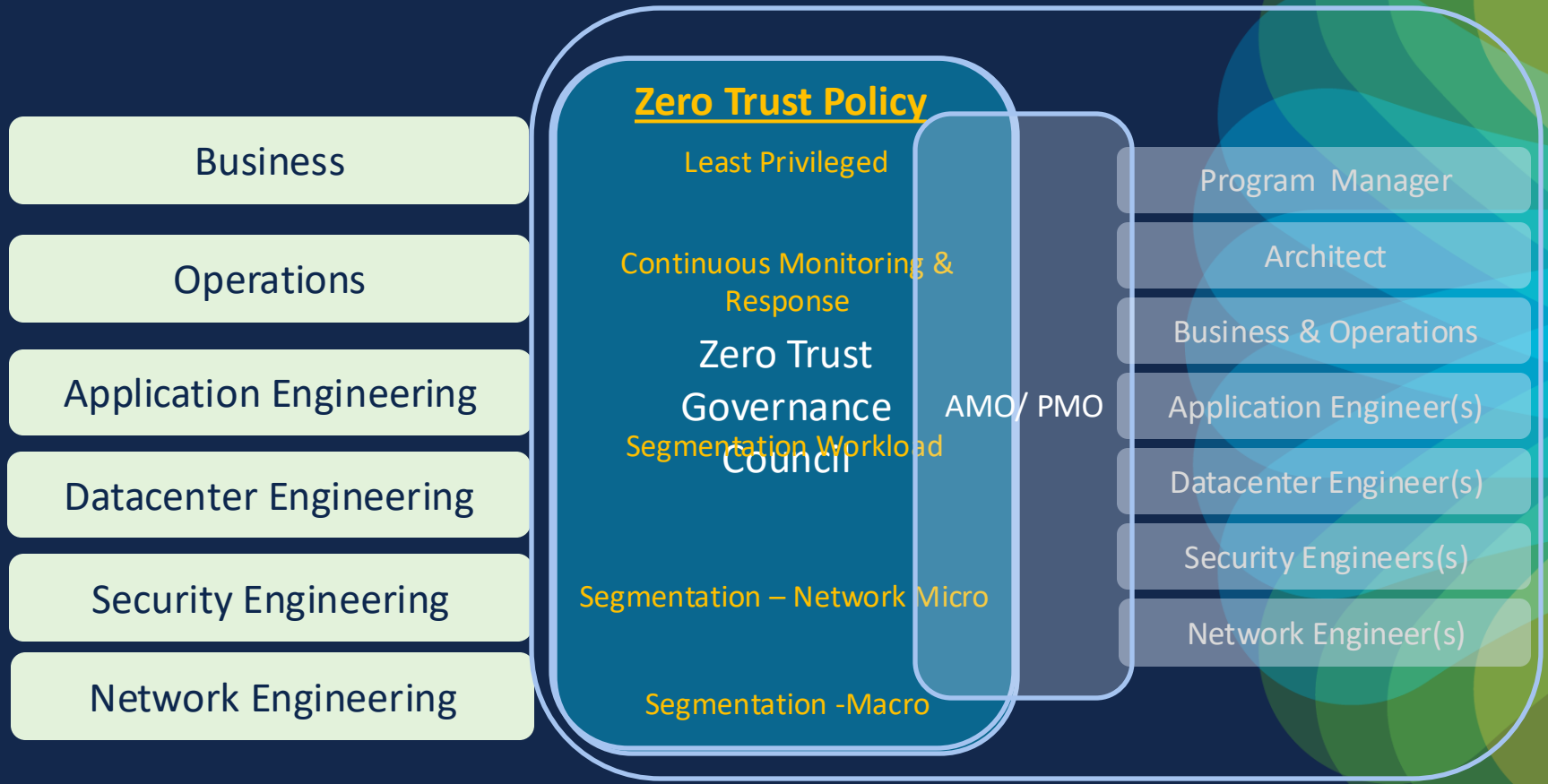
Measuring Success

- Business Outcome to Capability to KPI

Keeping up with Threats

- Evolving Landscape, Vast Amounts of Data

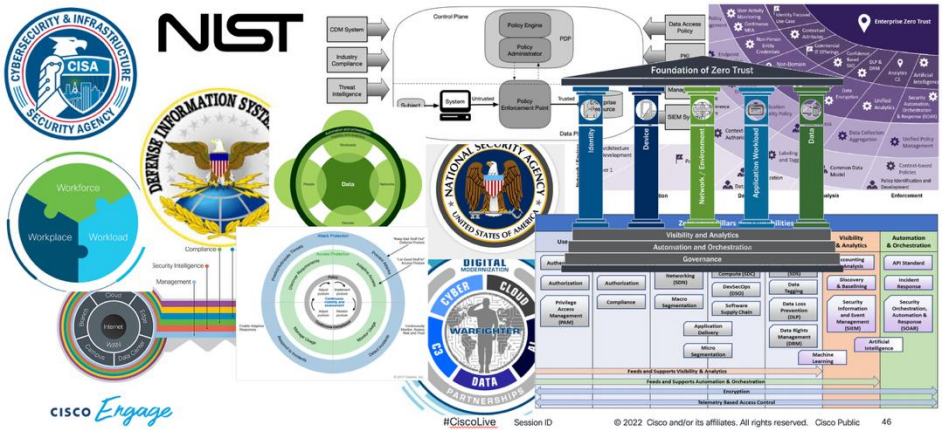
Challenges of Governance



The ZTA Journey

Zero Trust Architecture

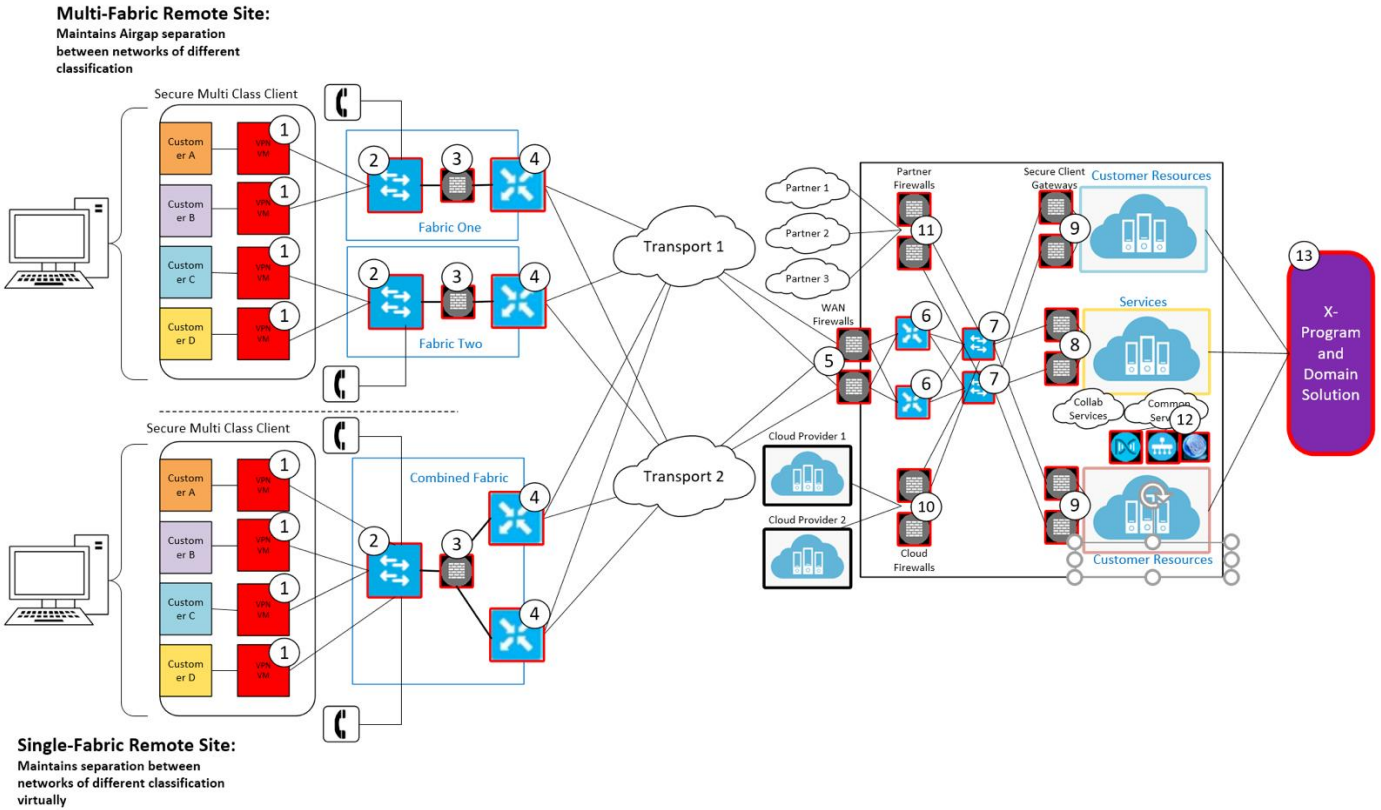
- A True end to end holistic architecture
  - We must treat it differently
- It is large, broad, and in-depth
  - Everyone has a framework



Zero Trust Architecture: Capabilities

1. User Inventory
2. Conditional User Access
3. Multi Factor Authentication (MFA)
4. Privileged Access Management (PAM)
5. Identity Federation & User Credentialing
6. Behavioral, Contextual ID, and Biometrics
7. Least Privileged Access
8. Continuous Authentication
9. Integrated ICAM Platform
10. Device Inventory
11. Device Detection and Compliance
12. Device Authorization w/ Real Time Inspection
13. Remote Access
14. Partially & Fully Automated Asset, Vulnerability and Patch Management
15. Unified Endpoint Management (UEM) & Mobile Device Management (MDM)
16. Endpoint & Extended Detection & Response (EDR & XDR)
17. Application Inventory
18. Secure Software Development & Integration
19. Software Risk Management
20. Resource Authorization & Integration
21. Continuous Monitoring and Ongoing Authorizations
22. Data Catalog Risk Alignment
23. Enterprise Data Governance
24. Data Labeling and Tagging
25. Data Monitoring and Sensing
26. Data Encryption & Rights Management
27. Data Loss Prevention (DLP)Data Access Control
28. Data Flow Mapping
29. Software Defined Networking (SDN)
30. Macro Segmentation
31. Micro Segmentation
32. Policy Decision Point (PDP) & Policy Orchestration
33. Critical Process Automation
34. Machine Learning
35. Artificial Intelligence
36. Security Orchestration, Automation & Response (SOAR)
37. API Standardization
38. Security Operations Center (SOC) & Incident Response (IR)
39. Log All Traffic (Network, Data, Apps, Users)
40. Security Information and Event Management (SIEM)
41. Common Security and Risk Analytics
42. User and Entity Behavior Analytics
43. Threat Intelligence Integration
44. Automated Dynamic Policies

Sample Reference Architecture (Security)



Zero Trust Architecture Roadmap

Immediate (Now)	Short Term (6 – 12 Months)	Medium Term (1 – 2 Years)	Long Term (3 – 5 Years)
13. Remote Access	1. User Inventory	3. Multi Factor Authentication (MFA)	7. Least Privileged Access
10. Device Inventory	5. Software Defined Data Center (SDDC)	7. Software Defined Networking (SDN)	43. Threat Intelligence Integration
39. Log All Traffic (Network, Data, Apps, Users)	30. Macro Segmentation	31. Micro Segmentation	33. Critical Process Automation
	37. API Standardization	36. Security Orchestration, Automation & Response (SOAR)	

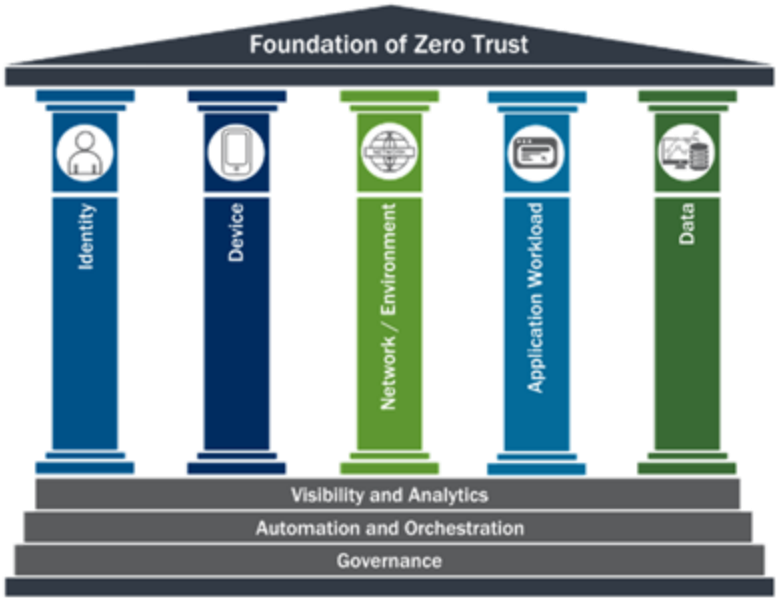
An Action Plan

An Action Plan

1. Identify a Framework
2. Understand Todays Capabilities
3. Identify Goals and Gaps
4. Create a Segmentation Plan
5. Create Reference Architecture
6. Create the Journey
7. Take Small Simple Steps

Step 1 - Identify a Framework

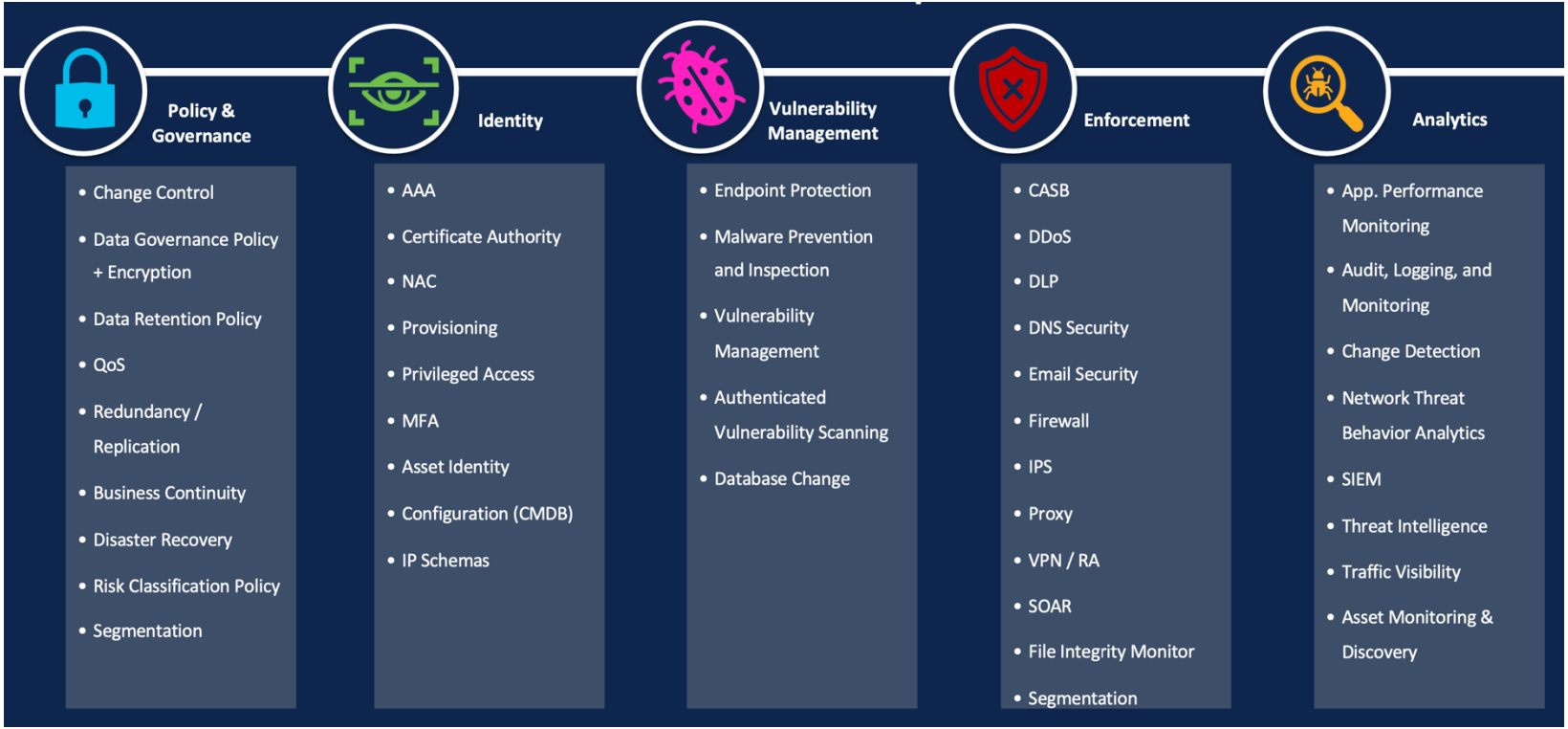
Identify a framework, model, or architecture



Map the ~45 capabilities to that framework

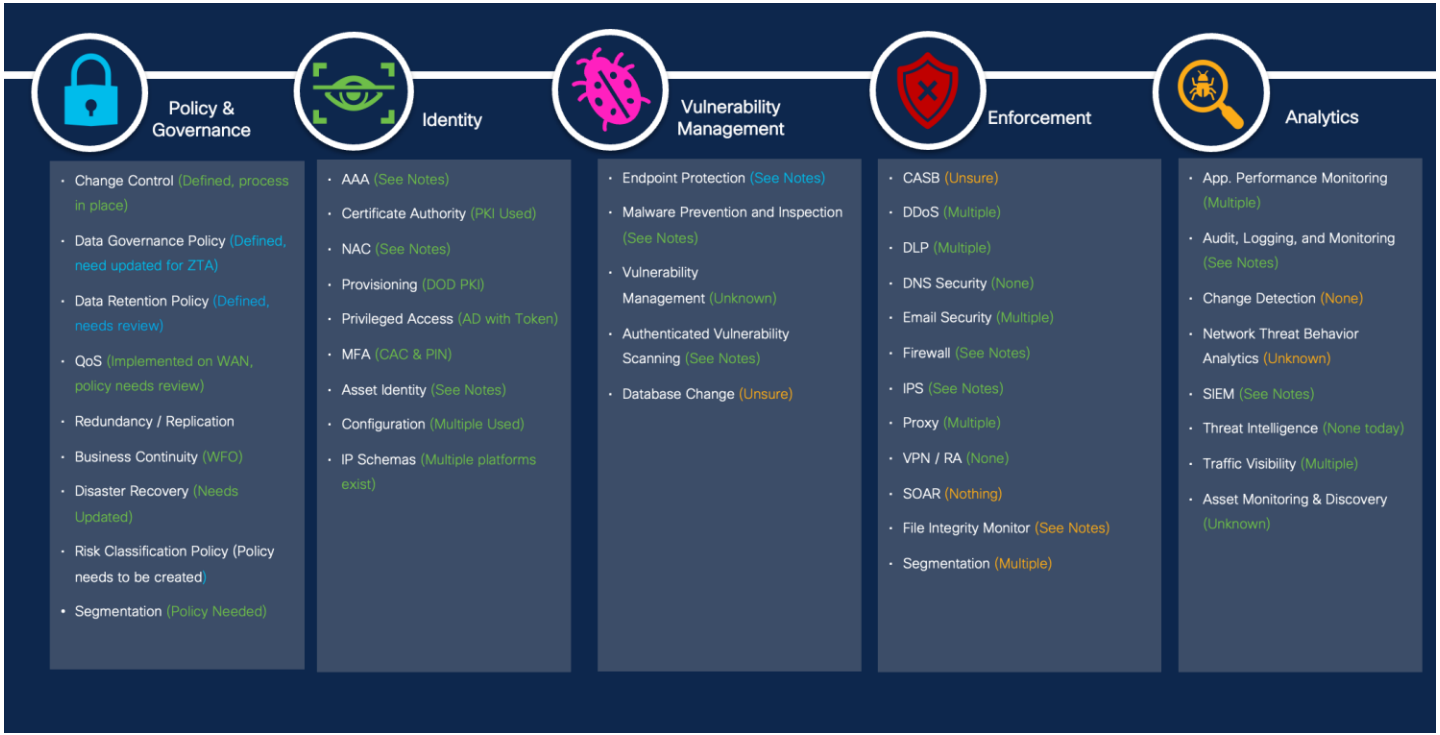
1. User Inventory
2. Conditional User Access
3. Multi Factor Authentication (MFA)
4. Privileged Access Management (PAM)
5. Identity Federation & User Credentialing
6. Behavioral, Contextual ID, and Biometrics
7. Least Privileged Access
8. Continuous Authentication
9. Integrated ICAM Platform
10. Device Inventory
11. Device Detection and Compliance
12. Device Authorization w/ Real Time Inspection
13. Remote Access
14. Partially & Fully Automated Asset, Vulnerability and Patch Management
15. Unified Endpoint Management (UEM) & Mobile Device Management (MDM)
16. Endpoint & Extended Detection & Response (EDR & XDR)
17. Application Inventory
18. Secure Software Development & Integration
19. Software Risk Management
20. Resource Authorization & Integration
21. Continuous Monitoring and Ongoing Authorizations
22. Data Catalog Risk Alignment
23. Enterprise Data Governance
24. Data Labeling and Tagging
25. Data Monitoring and Sensing
26. Data Encryption & Rights Management
27. Data Loss Prevention (DLP)Data Access Control
28. Data Flow Mapping
29. Software Defined Networking (SDN)
30. Macro Segmentation
31. Micro Segmentation
32. Policy Decision Point (PDP) & Policy Orchestration
33. Critical Process Automation
34. Machine Learning
35. Artificial Intelligence
36. Security Orchestration, Automation & Response (SOAR)
37. API Standardization
38. Security Operations Center (SOC) & Incident Response (IR)
39. Log All Traffic (Network, Data, Apps, Users)
40. Security Information and Event Management (SIEM)
41. Common Security and Risk Analytics
42. User and Entity Behavior Analytics
43. Threat Intelligence Integration
44. Automated Dynamic Policies

Step 1a – Map Capabilities to Framework



Step 2 – Understand Todays Capabilities

Capture and Identify Current Capabilities



Step 3 – Identify Goals and Gaps

Create a “Score Card” to gather details

Policy & Governance											
Tracking #	Individual controls	Questions	Observations	Recommendations	POC For Further Information	Budget	Resolution Priority	People %	Process %	Tech %	Overall Condition
100	Change Control	Do you have defined configuration standards, what is the process for defining these, are they updated and how is adherence validated									
101	Change Control	Do you run a change management processes, who are the key stakeholders, talk me through the process and how security is invested in it, is it documented, what is the approvals process, how are unplanned changes identified, what are the repercussions for unplanned changes									
102	Change Control	How do you identify that patches are required, does this span all technologies in your business, how do you rate the risk of missing patches									
103	Change Control	how does this risk management drive the remediation process, what is the visibility into the current situation and how does this compare to the plan,									
104	Change Control	what are the optics of this and to whom are they circulated, what is the roll out plan and supporting infrastructure									
	Change Control										

Step 3a – Populate a Score Card

Generate a “Score Card” based on data gathered

Zero Trust Capabilities- Current State										
Policy & Governance		Identity		Vulnerability Management		Enforcement		Analytics		
Change Control	2.5	AAA	2.7	Endpoint Protection	2.4	CASB	2.1	App. Performance Monitoring	2.1	
Data Governance Policy	2.9	Certificate Authority	2.4	Malware Prevention and Inspection	2.3	DDoS	2.0	Audit, Logging, and Monitoring	2.1	
Data Retention Policy	2.4	NAC	3.1	Vulnerability Management	2.3	DLP	2.0	Change Detection	1.0	
QoS	2.0	Provisioning	2.3	Authenticated Vulnerability Scanning	2.0	DNS Security	2.1	Network Threat Behavior Analytics	1.0	
Redundancy / Replication	2.3	Privileged Access	2.4	Database Change	1.0	Email Security	3.5	SIEM	2.1	
Business Continuity	2.3	MFA	2.3			Firewall	2.1	Threat Intelligence	2.0	
Disaster Recovery	2.3	Asset Identity	2.3			IPS	2.1	Traffic Visibility	2.1	
Risk Classification Policy	2.3	Configuration (CMDB)	2.9			Proxy	2.1	Asset Monitoring & Discovery	2.1	
Segmentation	2.2	IP Schemas	2.3			VPN / RA	2.1			
						SOAR	2.0			
						File Integrity Monitor	2.3			

Step 3b – Identify Score Card End State Goals

Generate a goal “Score Card” based on requirements

Zero Trust Capabilities- End State Goal												
Policy & Governance			Identity			Vulnerability Management			Enforcement			Analytics	
Change Control	2.5		AAA	5.0		Endpoint Protection	2.0		CASB	3.0		App. Performance Monitoring	2.0
Data Governance Policy	4.0		Certificate Authority	5.0		Malware Prevention and Inspection	3.0		DDoS	5.0		Audit, Logging, and Monitoring	2.0
Data Retention Policy	3.0		NAC	5.0		Vulnerability Management	1.0		DLP	4.0		Change Detection	2.0
QoS	2.0		Provisioning	4.0		Authenticated Vulnerability Scanning	5.0		DNS Security	3.0		Network Threat Behavior Analytics	1.0
Redundancy / Replication	1.0		Privileged Access	3.0		Database Change	4.0		Email Security	0.0		SIEM	2.0
Business Continuity	5.0		MFA	2.0					Firewall	3.0		Threat Intelligence	3.0
Disaster Recovery	1.0		Asset Identity	1.0					IPS	2.0		Traffic Visibility	2.0
Risk Classification Policy	0.0		Configuration (CMDB)	5.0					Proxy	1.0		Asset Monitoring & Discovery	1.0
Segmentation	3.0		IP Schemas	3.0					VPN / RA	5.0			
									SOAR	3.0			
									File Integrity Monitor	1.0			

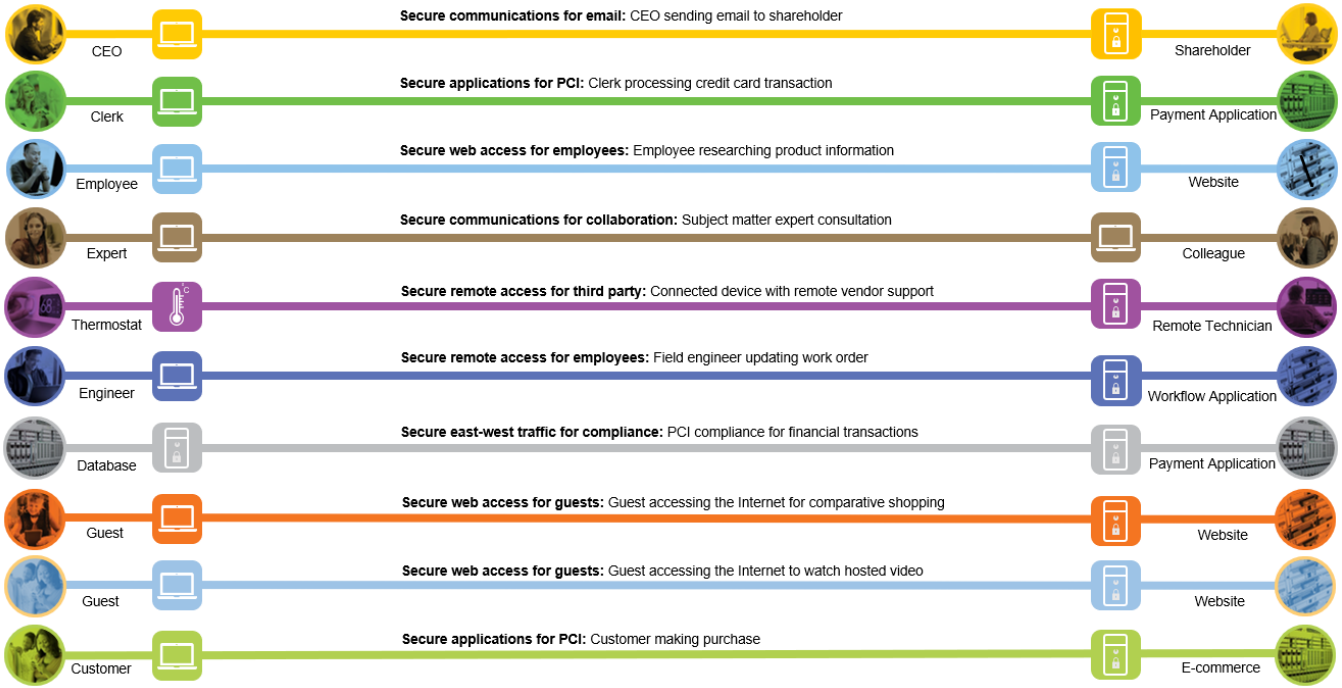
Step 3c – Identify Score Card One Year Goals

Generate a one year out goal

Zero Trust Capabilities- Year 1														
Policy & Governance			**Identity**			**Vulnerability Management**			**Enforcement**			**Analytics**		
Change Control	3.2		AAA	3.5		Endpoint Protection	3.1		CASB	2.7		App. Performance Monitoring	2.7	
Data Governance Policy	3.7		Certificate Authority	3.1		Malware Prevention and Inspection	3.0		DDoS	2.6		Audit, Logging, and Monitoring	2.7	
Data Retention Policy	3.1		NAC	4.1		Vulnerability Management	3.0		DLP	2.6		Change Detection	1.3	
QoS	2.6		Provisioning	3.0		Authenticated Vulnerability Scanning	2.6		DNS Security	2.7		Network Threat Behavior Analytics	1.3	
Redundancy / Replication	3.0		Privileged Access	3.1		Database Change	1.3		Email Security	4.6		SIEM	2.7	
Business Continuity	2.9		MFA	2.9					Firewall	2.7		Threat Intelligence	2.6	
Disaster Recovery	2.9		Asset Identity	2.9					IPS	2.7		Traffic Visibility	2.7	
Risk Classification Policy	2.9		Configuration (CMDB)	3.7					Proxy	2.7		Asset Monitoring & Discovery	2.7	
Segmentation	2.9		IP Schemas	3.0					VPN / RA	2.7				
									SOAR	2.6				
									File Integrity Monitor	3.0				

Step 4 – Segmentation Plan

Map your business workflows



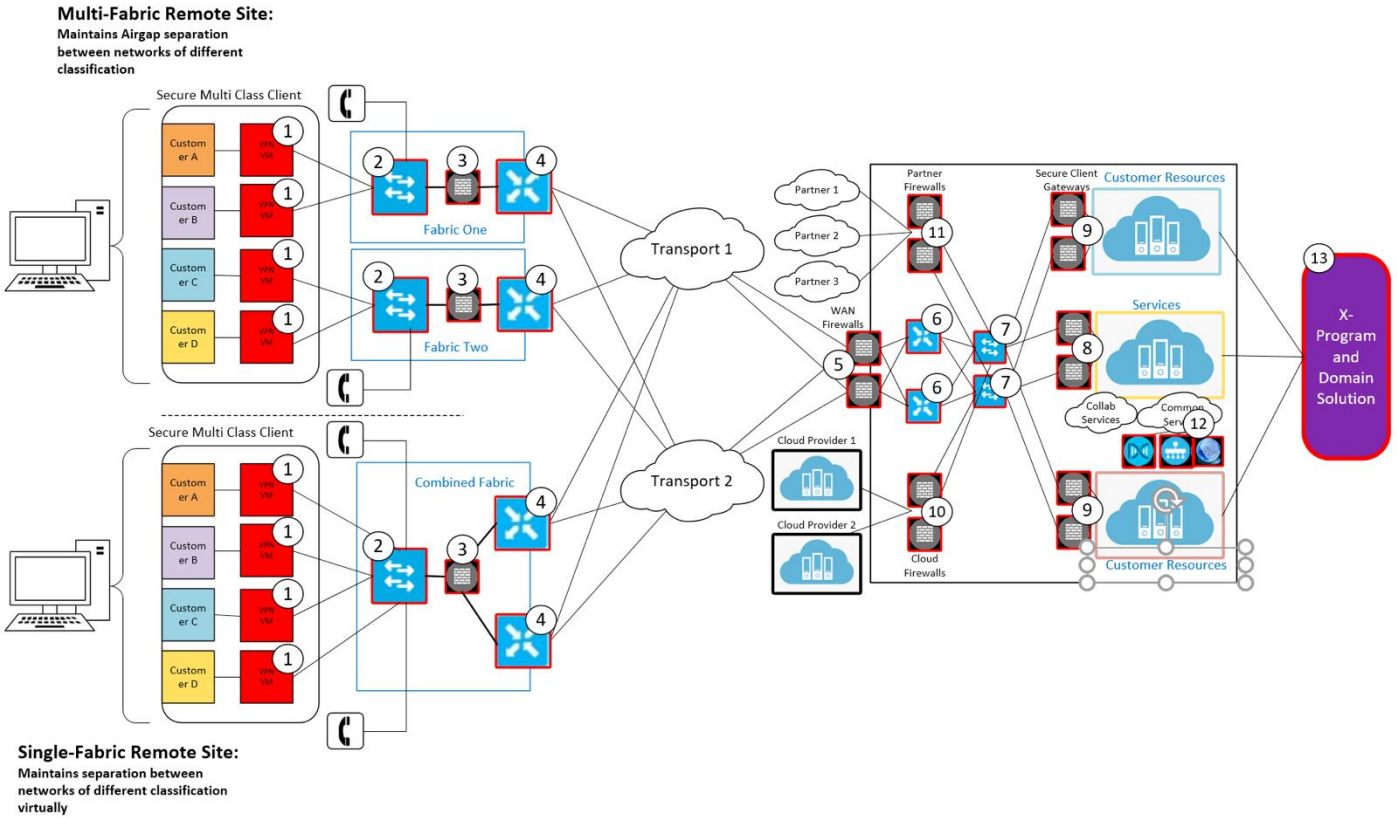
Step 4a – Segmentation Plan

Non Technical Plan aligned to business workflows

	Application Server #1	Application Server #2	Database Server	Call Manager	Print Server	Mail Server	DNS Server	FTP Server	IoT Server #1	IoT Server #2	Network Infrastructure	Server Infrastructure	AWS Infrastructure	AWS: Application #1	AWS: Application #2	Azure: Infrastructure	Azure: Application #1	Azure: Application #2	
Guest User	Yes												Yes		Yes				
Normal User	Yes	Yes											Yes	Yes	Yes		Yes	Yes	
Privileged User #1											Yes					Yes			
Privileged User #2												Yes							
Printer					t9100														Workplace
IP Phone				Yes															
VTC				Yes															
Badge Reader									t14001										
HVAC Sensor										Yes									
Remote User	Yes	Yes												Yes					Workforce
Cell Phone	Yes	Yes											Yes	Yes					

Workload

Step 5 – Create Reference Architecture



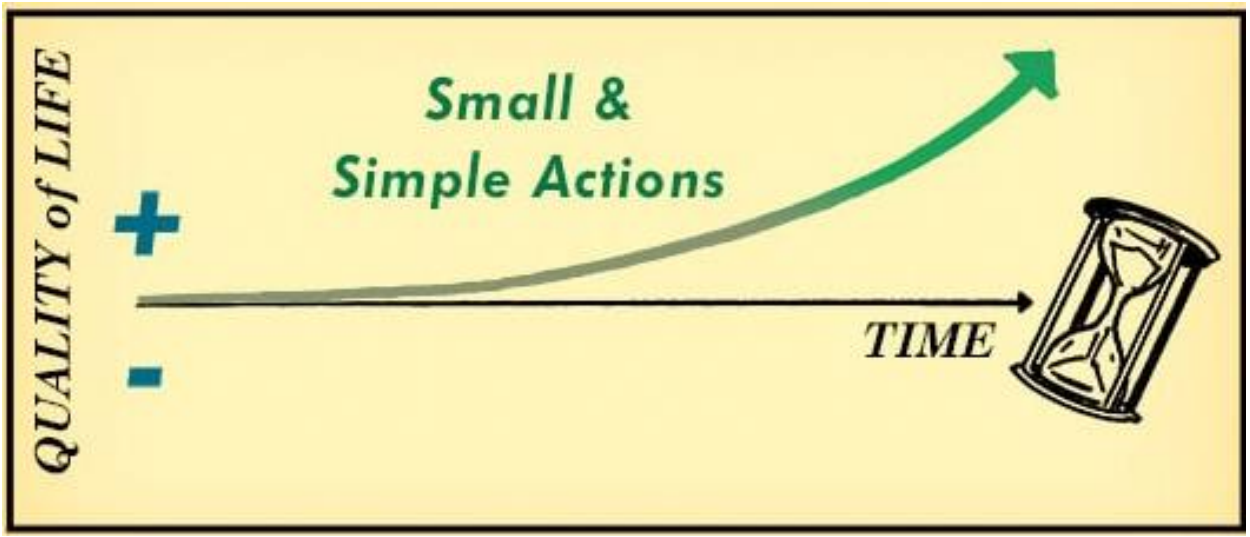
Step 6 – Create the Journey

Create a plan to get to the future state

Immediate (Now)	Short Term (6 – 12 Months)	Medium Term (1 – 2 Years)	Long Term (3 – 5 Years)
13. Remote Access	1. User Inventory	3. Multi Factor Authentication (MFA)	7. Least Privileged Access
10. Device Inventory	5. Software Defined Data Center (SDDC)	7. Software Defined Networking (SDN)	43. Threat Intelligence Integration
39. Log All Traffic (Network, Data, Apps, Users)	30. Macro Segmentation	31. Micro Segmentation	33. Critical Process Automation
	37. API Standardization	36. Security Orchestration, Automation & Response (SOAR)	

Step 7 – Take Small Simple Steps

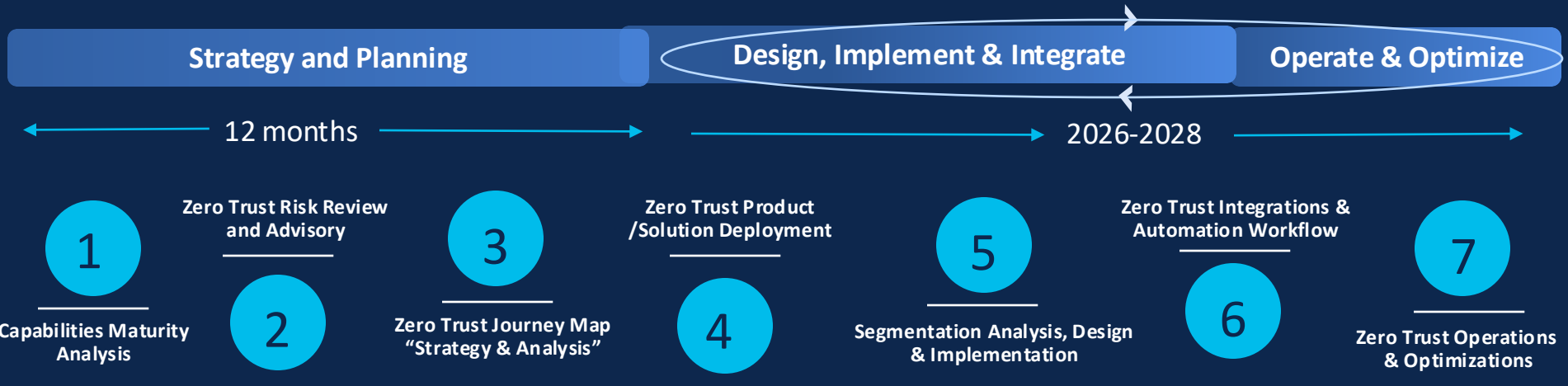
Do Something!



Zero Trust Lifecycle Approach

Zero Trust Lifecycle Approach

Outcome centric approach to mitigate risk and provide advisory support throughout your Zero Trust journey.



In Conclusion

- Understand you will never be finished with Zero Trust
- Understand Zero Trust is NOT a product
- Understand Zero Trust starts with a ZT PMO
- Must break down silos
- Take small steps, one at a time
- No Easy Button

Thank you