Zero Trust Architecture

Refocused Security

Zero Trust Architecture is growing in popularity as a strategic response to growing cybersecurity challenges.

Zero Trust Architecture (ZTA) is growing in popularity as a strategic response to growing cybersecurity challenges and more than 12 billion devices on the Internet of Things. The (IoT) includes issued devices, BYOD, cloud integration, and other mobile technologies that present a new threat each time they are used to remotely access the internet. Challenges multiply exponentially once a network in penetrated, weakening defenses each time a perimeter is compromised. As a *Security Refocused Service*, ZTA fortifies cyber defenses by using granular controls at a pre-determined data level.

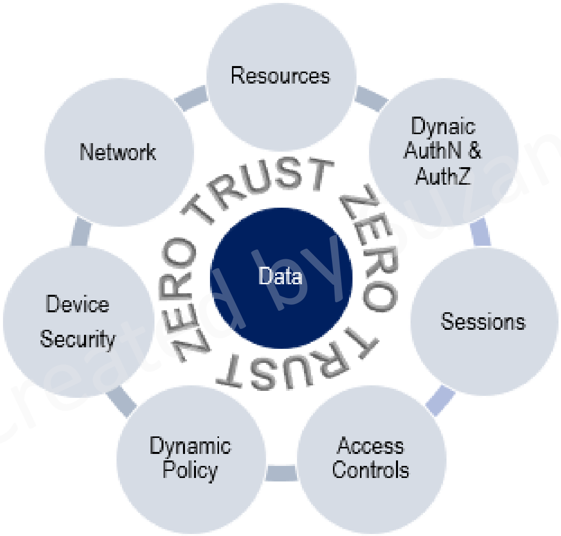


Figure created from NIST 800-207 Guidelines: Zero Trust Architecture

ZTA locks down data with micro-segmentation and additional controls

Starting at the DATA working outwards and guided by NIST 800-207, access controls and network access controls are strategically implemented in-line with, parallel to, or in place of an existing network infrastructure so you can architect a relevant solution with an up-to-date, robust, compliant Zero Trust framework.

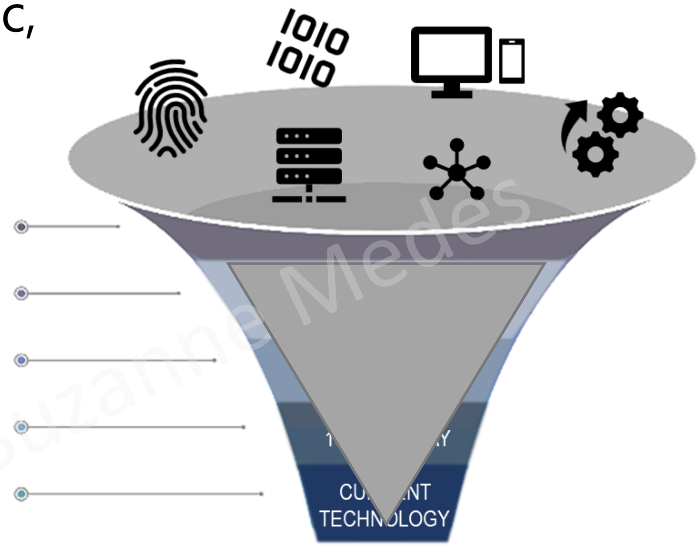
The XYZ TECH ZTA Implementation Approach

Preparation → Architecture → Integration

Through a self-paced, phased implementation, XYZ TECH affords enterprise owners flexibility to reach Zero Trust maturity with minimal risk and a controlled time investment.

www.WORDMECCA.com GENERIC SAMPLE ZTA SLICKSHEET

XYZ TECH has done their due diligence and developed a ZTA strategy that is holistic, secure, and compliant.



ZERO TRUST PILLARS + Automation & Visibility
Users, Devices, Data, Applications, Networks

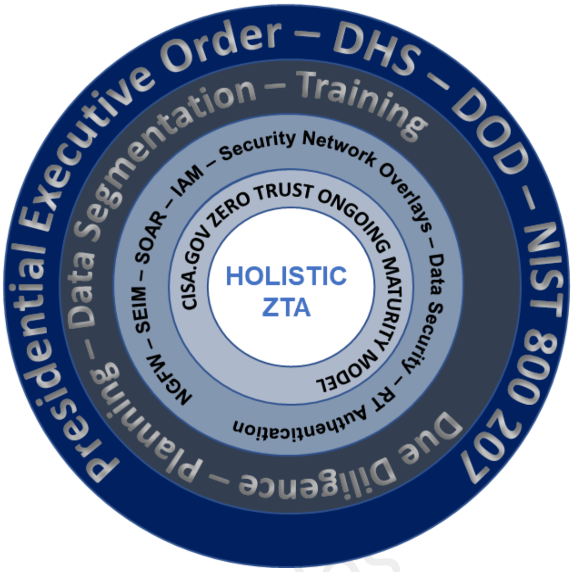
50 YEARS INDUSTRY EXPERIENCE
Half Century Foundation of Cyber Adaptation

INCREASED COMPLEX THREATS
Malware, Ransomware, IoT, AI, ML, Cloud Access

SOPHISTICATED INTERNATIONAL ATTACKS
Russia, China, Iran, Organized Crime, Black Hats

EXISITING INFRASTRUCTURE
Hardware, Software, Storage, Locations, Users

History, current trends, and threat predictions, along with new federal regulations and best practices, fuel the XYZ TECH Zero Trust Architecture approach. With XYZ TECH guiding your ZTA learning curve or implementation, you are guaranteed to receive the most robust, powerful security strategy, realizing maximum ROI for your time.


Presidential Executive Order – DHS – DOD – NIST 800 207
Data Segmentation – Training
Due Diligence – Planning
Security Network Overlays – Data Security – RT Authentication
NGFW – SEIM – SOAR – IAM –
CISA.GOV ZERO TRUST ONGOING MATURITY MODEL
HOLISTIC ZTA

Protect your data dynamically, one request at a time.

Opportunity Cost arises when the choice of one alternative is weighed against another by considering resources and risks. While *Opportunity* forces a business to ask, “Can we afford to do this?”, *Opportunity Cost* begs the question, “Can we afford NOT TO?”

For a Zero Trust implementation journey, the greatest resource investment is time. Decisions if or when to integrate ZTA with existing infrastructure should be measured by how much time it would take your organization to reach compliance vs. the degree of risk that would be mitigated by doing so. Another measurement should be how much risk would increase with a time if the journey were delayed.

Opportunity

- Matching industry standards and regulations
- Proactive security posture
- Business enablement with security refocused
- Quicker incident response
- Reduced costs of incident recovery
- Improved trust from stakeholders, clients, and users

Opportunity Cost

- Costs of renewing existing/outdated security licenses
- Higher spending on incident response/recovery
- Remaining in a reactive security posture
- Increased data loss from network breach/compromises
- Incurred fines for failure to comply with mandates
- Loss of trust from stakeholders, clients, and users

www.WORDMECCA.com GENERIC SAMPLE ZTA SLICKSHEET