Zero Trust Maturity Models

NSA Zero Trust Maturity Model

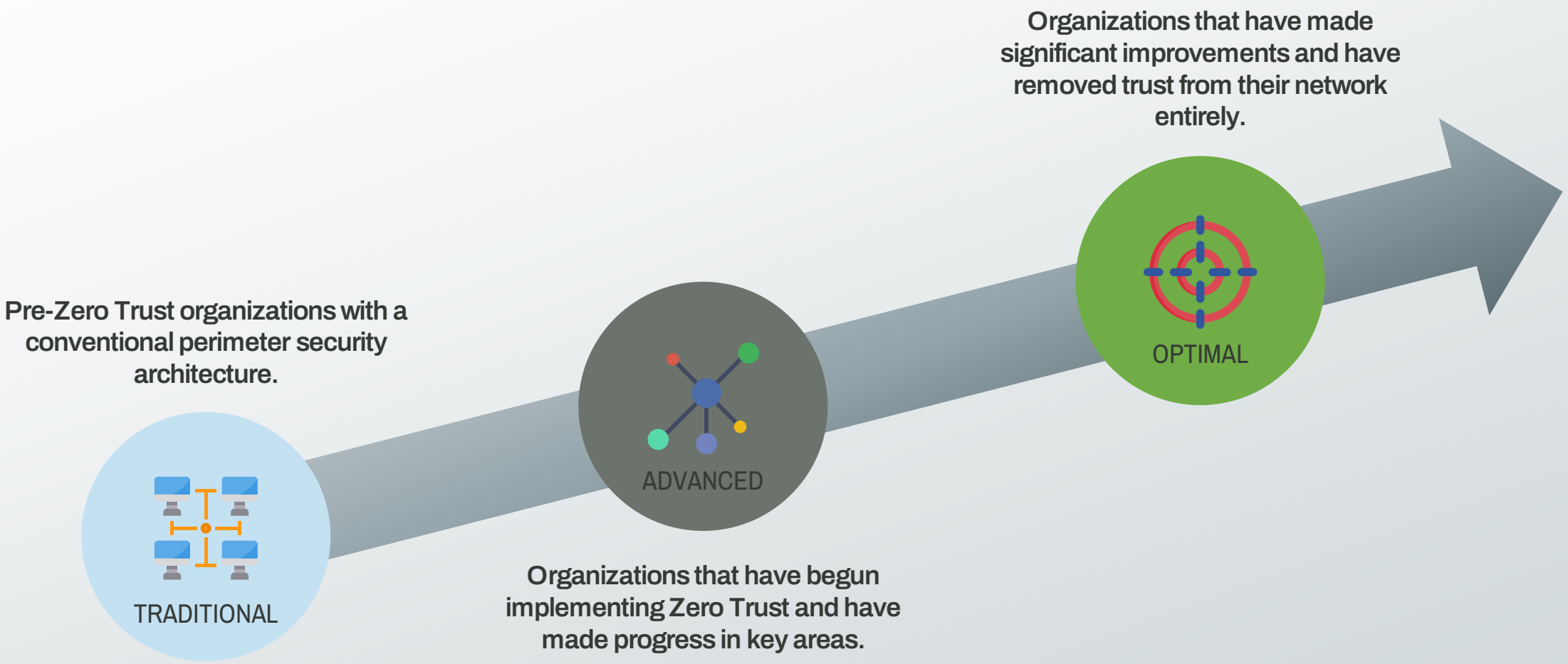
INSTRUCTOR ALTON

WITHOUT ZERO TRUST	WITH ZERO TRUST		
PREPARATION Initial discovery and assessment activities.	**BASIC** Implement fundamental integrated capabilities.	**INTERMEDIATE** Refine capability integration and further refine capabilities.	**ADVANCED** Deploy advanced protections and controls with robust analytics and orchestration.

NSA: Embracing a Zero Trust Security Model

Microsoft Zero Trust Maturity Model

INSTRUCTOR ALTON



Microsoft: Zero Trust Maturity Model

Microsoft Zero Trust Maturity Model

INSTRUCTOR ALTON

	TRADITIONAL	ADVANCED	OPTIMAL
Data	Access is controlled by perimeter-based security, not data sensitivity.	Data is classified and labeled based on sensitivity.	Data classification is improved by machine learning and artificial intelligence.
Identity	Visibility into identity-based risks is very limited.	Data analytics improve visibility into identity-based risks.	User, device, location, and behavior are analyzed in real-time to determine risk and provide ongoing protection.
Network	Designed using minimal network security perimeters with a flat open network architecture.	Designed utilizing ingress and egress cloud micro-perimeters with some network micro-segmentation.	Designed utilizing fully distributed ingress and egress cloud micro-perimeters and deeper micro-segmentation.

Microsoft: Zero Trust Maturity Model

CISA Zero Trust Maturity Model

INSTRUCTOR ALTON

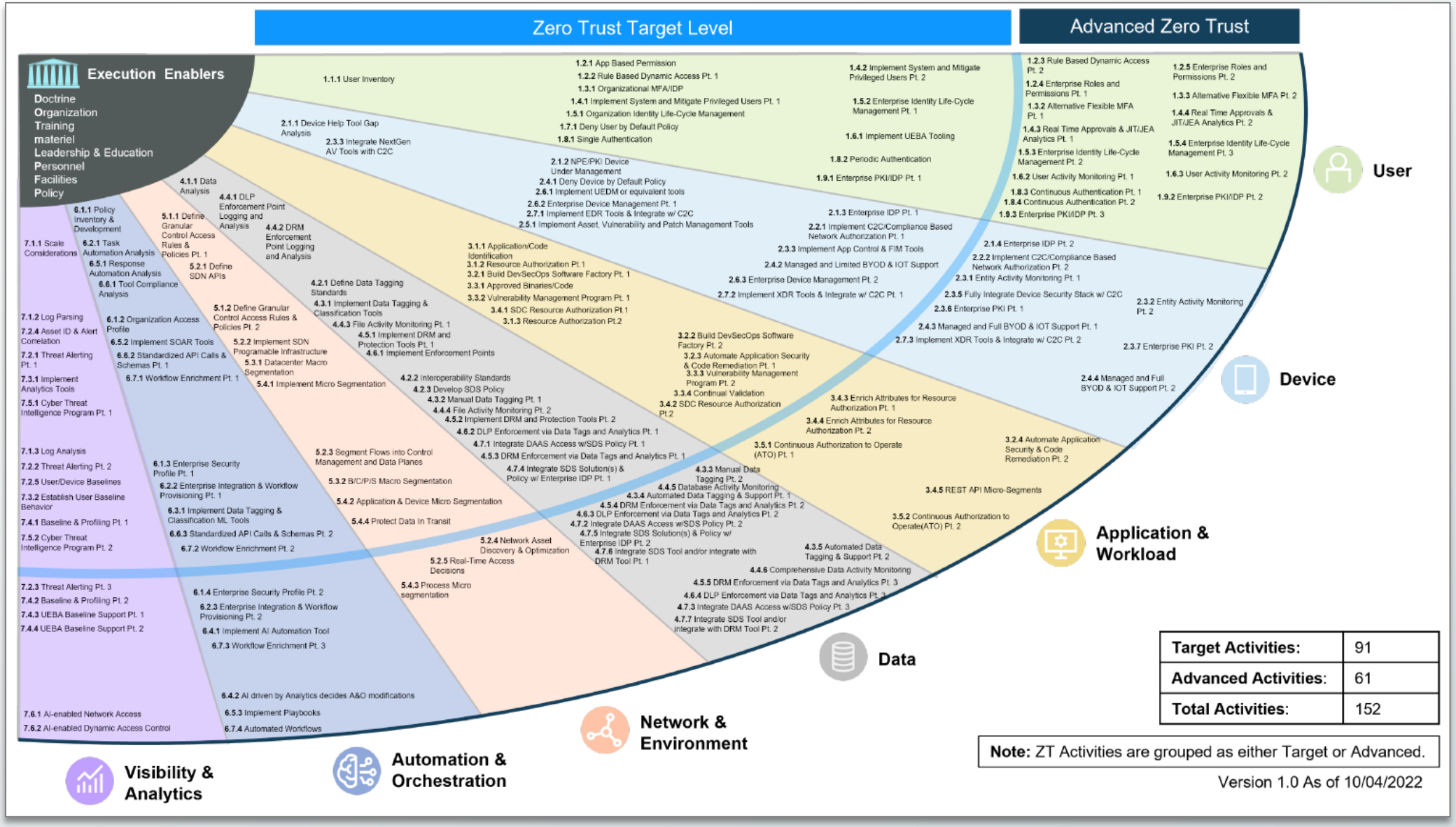
	IDENTITY	DEVICE	NETWORK/ ENVIRONMENT	APPLICATION WORKLOAD	DATA
TRADITIONAL	• Password or Multi-Factor Authentication (MFA) • Limited Risk Assessment	• Limited Visibility into Compliance • Simple Inventory	• Large Macro-Segmentation • Minimal Internal or External Traffic Encryption	• Access Based on Local Authorization • Minimal Integration with Workflow • Some Cloud Accessibility	• Not Well Inventoried • Static Control • Unencrypted
ADVANCED	• MFA • Some Identity Federation with Cloud and On-Premise Systems	• Compliance Enforcement Employed • Data Access Depends on Device Posture on First Access	• Defined by Ingress/Egress Micro-Perimeters • Basic Analytics	• Access Based on Centralized Authentication • Basic Integration into Application Workflow	• Least Privilege Controls • Data Stored in Cloud or Remote Environments are Encrypted at Rest
OPTIMAL	• Continuous Validation • Real-Time Machine Learning Analysis	• Constant Device Security Monitor and Validation • Data Access Depends on Real-Time Risk Analytics	• Fully Distributed Ingress/Egress Micro-Perimeters • Machine Learning-Based Threat Protection • All Traffic is Encrypted	• Access is Authorized Continuously • Strong Integration into Application Workflow	• Dynamic Support • All Data is Encrypted

VISIBILITY AND ANALYTICS | AUTOMATION AND ORCHESTRATION | GOVERNANCE

Cybersecurity & Infrastructure Security Agency (CISA) Zero Trust Maturity Model

DoD Target & Advanced Zero Trust Activities

INSTRUCTOR ALTON



Department of Defense (DoD) Zero Trust Strategy