StealthPath™

Datasheet

Zero Trust Capability Model (ZTCM)

Authentication

Verified Membership

Obfuscation

Behavioral Analysis

Component Authenticity

Connection Management

Isolation

Authorization

Traffic Flow

Restricted Functionality

Content Inspection

Tamper-Proof

Configuration Control

Independent Verification

"StealthPath's model will save us two years in our mandated move to Zero Trust"

- DOD

Developed by industry thought leaders, leveraging next generation technologies, and extending current cybersecurity best practices, the ZTCM provides a practical roadmap to the Zero Trust future.

Zero Trust Implementation Services

Organizational Readiness

- Training
- Governance
- Risk Model
- SWOT Analysis

ZT Transformation Mentoring

- Identity critical assets
- ID available resources
- Prioritize initiatives
- Establish Roadmap

Organizational Alignment

- Objectives
- Business case
- Metrics
- Communication Plan
- Change Management

Zero Trust Evolution

- Requirement definition
- Architectural Assessment
- Program Management

Learn More

www.stealthpath.com

Reduces the encyclopedic complexities of NIST 800 configuration standards and controls into a manageable, implementable framework:

Three pillars, 13 Domains, 104 controls`

Pillar	Domain	
Confirmation	Authentication and Authorization	*Continuous verification of identity and privileges*
	Verified Membership	*Confirmation of valid access based on defined roles*
	Configuration Management	*Establishment/integrity of detailed policies for access enforcement*
	Restricted Functionality	*Access and actions limited to those required for roles/responsibilities*
	Independent Verification	*'Watchdog" uncorrelated checks on cybersecurity functionality*
	Component Authenticity	*Hardware/software provenance and integrity*
Connections	Connections Controls	*Limiting network communications to approved interactions*
	Verified Path Flow Control	*Monitoring all direct and indirect connections to ensure consistency with policy*
	Interaction Content Control	*Payload parsing and analysis to detect malware or potentially threatening outliers*
	Behavioral Analysis	*AI/ML deep pattern recognition to detect sophisticated compromise*
Concealment	Obfuscation	*Shielding key components and processes from outside surveillance*
	Isolation	*Physical and logical protection of asserts from outside interference*
	Tamper Proof	*Ensuring components have not been changed from intended state*