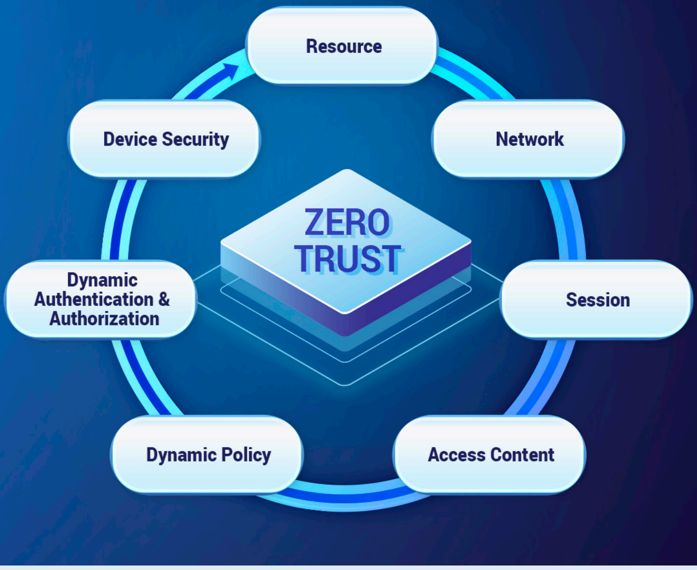
Zero Trust Architecture Readiness

Plan and prepare for your Zero Trust implementation



What is Zero Trust

Zero Trust (ZT) is an IT and cybersecurity strategy that seeks to eliminate or significantly reduce the likelihood of a successful breach. When properly designed and implemented, ZT represents a collection of technologies and processes that remove the notion of implicit user or device "trust," meaning each access attempt must be re-verified. The result is an IT environment where simplified granular access controls and network segmentation eliminate the concept of lateral movement and provide multiple Layer 7 threat protections.

Why your company should apply ZT

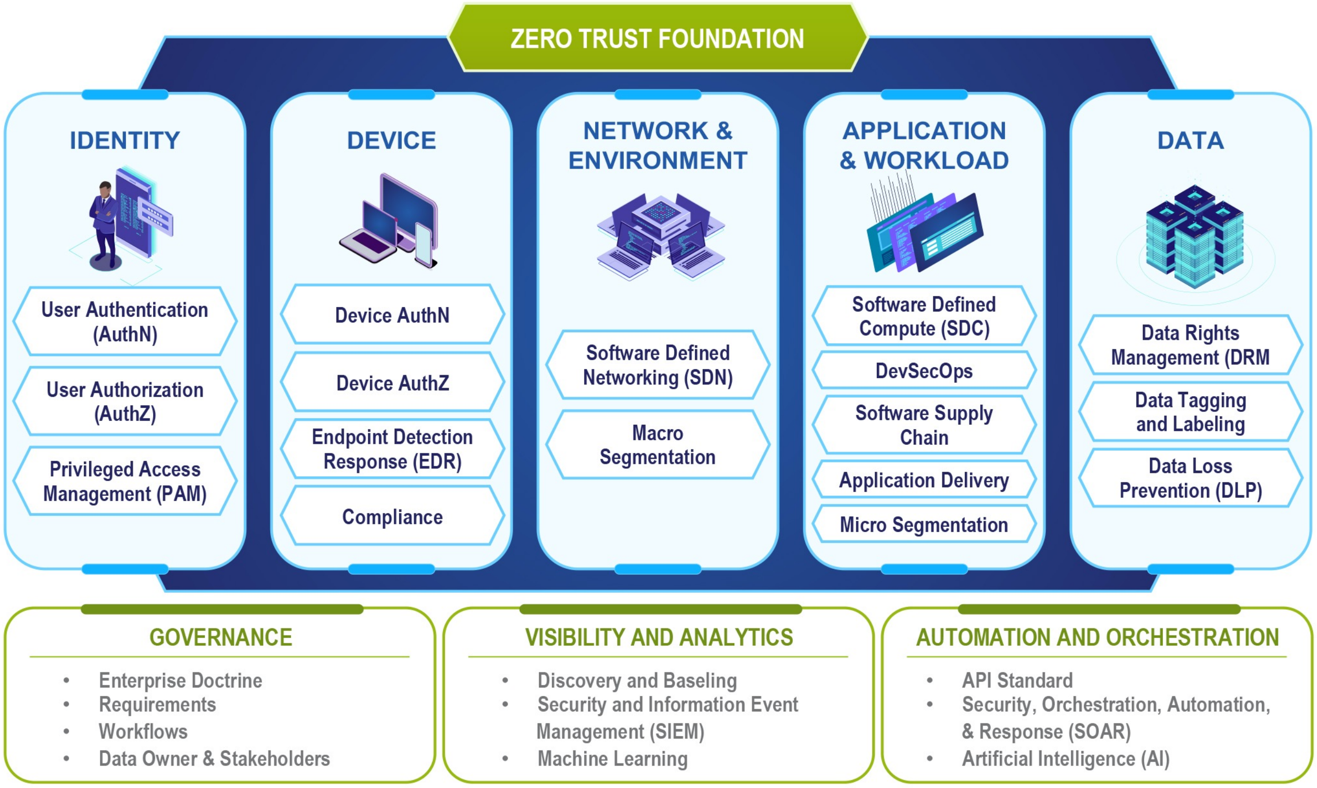
Cybersecurity models of the last 20 years are based on the traditional boundary or perimeter and defense-in-depth types. A significant drawback to these defenses is that they fail to prevent lateral movement once a user has authenticated to the network. As businesses grow, the possible entry points grow, as do the users interacting with the systems and networks. The result is often easy pickings for attackers. With an ever-increasing number of cyberattacks occurring year after year, safeguarding systems against external and insider threats is crucial for ensuring continuity of operations and data security.

Getting Started

Properly implementing ZT requires tight coordination between numerous and often disparate disciplines within your organization. Therefore, succeeding with ZT requires much more than just purchasing a ZT platform. Your teams, environments, applications, and end-users must be evaluated and prepared to ensure your ZT project's success.

MindPoint Group's Zero Trust Foundation

MindPoint Group (MPG) approach to ZT starts with a tested and proven foundation of capabilities. Each of the foundational elements represents a functional area of ZT that must be well understood and documented before a ZT platform implementation and is the foundation for our Zero Trust Architecture (ZTA) Readiness Assessment engagement.



ZERO TRUST FOUNDATION

IDENTITY
- User Authentication (AuthN)
- User Authorization (AuthZ)
- Privileged Access Management (PAM)

DEVICE
- Device AuthN
- Device AuthZ
- Endpoint Detection Response (EDR)
- Compliance

NETWORK & ENVIRONMENT
- Software Defined Networking (SDN)
- Macro Segmentation

APPLICATION & WORKLOAD
- Software Defined Compute (SDC)
- DevSecOps
- Software Supply Chain
- Application Delivery
- Micro Segmentation

DATA
- Data Rights Management (DRM
- Data Tagging and Labeling
- Data Loss Prevention (DLP)

GOVERNANCE
- Enterprise Doctrine
- Requirements
- Workflows
- Data Owner & Stakeholders

VISIBILITY AND ANALYTICS
- Discovery and Baseling
- Security and Information Event Management (SIEM)
- Machine Learning

AUTOMATION AND ORCHESTRATION
- API Standard
- Security, Orchestration, Automation, & Response (SOAR)
- Artificial Intelligence (AI)

The Zero Trust Architecture Journey

When designing your ZTA, MPG consultants review documentation and conduct interviews from across the enterprise to understand all supporting aspects of each MPG ZT pillar. When designing your implementation roadmap, we take multiple factors into account:

- Your organization's current cybersecurity framework (i.e., NIST 800-53, FISMA, PCI, HIPAA, etc.)
- Current network design systems, workloads, and architecture.
- Current asset and configuration inventory.

After a thorough analysis, we develop your customized ZTA readiness report, which will arm you with the information and resources needed to identify the best possible ZT platform vendors. It will also make sure you are fully aware of any required work ahead of a platform investment.

Deliverables

Customized MPG Zero Trust Architecture Readiness Report that includes:

- Summary of current enterprise with respect to ZT goals
- ZTA plan and recommendations
- Tailored Implementation roadmap

MindPoint Group, LLC
McLean, VA 22101

(o) 703.636.2033

Learn more

www.mindpointgroup.com
info@mindpointgroup.com

MindPoint GROUP℠