EchoStor TECHNOLOGIES

SOLUTION BRIEF

NETWORK SECURITY

Zero Trust Framework

Zero Trust is a security model that operates on the principle of "never trust, always verify." It emphasizes continuous verification of access requests from users and devices both inside and outside the network.

Key Concepts

Continuous Authentication
Implementing constant validation for access requests.

Strict Access Controls
Ensuring only authorized users and devices access specific resources.

Least Privilege Principle
Providing minimal access necessary for functionality.

Implementation

Technologies
Multifactor authentication, encryption, network segmentation, IAM systems, continuous monitoring, and analytics.

Stages of Maturity
Traditional, Initial, Advanced, Optimal

Zero Trust Maturity Model (ZTMM)

Key Pillars for Implementation
Identity, Applications, Networks, Devices, Data

Capabilities
Visibility and analytics, automation, orchestration, governance.

Approach

Planning & Deployment
Review findings, identify risks, validate existing posture.

Review & Deliver
Initial kickoff, read-only access for discovery, and analysis of resources.

Benefits

- Reduced attack surface
- Enhanced granular access control
- Support for compliance initiatives
- Mitigation of attack impacts

Why Choose EchoStor

EchoStor's Zero Trust Framework provides a comprehensive, integrated approach to security, reducing risks and enhancing compliance through continuous validation and strict access controls.

To learn more **contact us** at **echostor.com**

LEARN MORE →