Computer Defense Force LLC

Zero Trust Implementation & Security Design

Computer Defense Force LLC – Core Service Overview

Overview

Zero Trust Architecture (ZTA) is a foundational pillar in modern cybersecurity strategy. Our team helps organizations adopt and implement ZTA by designing segmented, identity-driven, and context-aware access controls. We ensure that no user or system is inherently trusted—security is continuously verified, not assumed.

Key Features

- Tailored Zero Trust network segmentation strategies
- Integration with existing security architectures and identity systems
- Secure application access policies for on-prem and cloud environments
- Identity and device trust modeling with real-time context assessment
- Continuous verification of user and device posture

Client Benefits

- Minimize lateral movement risk from compromised credentials
- Enforce policy-driven access at every layer
- Improve visibility and control over user/device access
- Increase resilience against insider threats and supply chain attacks

Why Choose Us

Our experts have designed Zero Trust systems for national security customers and complex enterprise networks. We guide implementation based on CISA, NIST SP 800-207, and DoD ZTA reference architecture standards.