K7

Zero Trust Identity: A Practical Introduction

3 pages • CyberK7 Whitepaper

A practical, jargon-free introduction to Zero Trust principles and a realistic phased approach starting with MFA and least-privilege access.

CyberK7 | Delhi, India | cyberk7.com

1. The Core Principle

Zero Trust means never trusting a user or device by default, regardless of network location.

2. Strong Identity Verification

MFA should apply everywhere, not just administrator accounts.

3. Device Posture & Micro-Segmentation

Verify device health before granting access. Micro-segmentation limits lateral movement.

4. Where to Start

Begin with MFA everywhere and a least-privilege access review — the two changes with highest impact-to-effort ratio.

About CyberK7

CyberK7's IAM consultants help build practical Zero Trust roadmaps. Contact us at info@cyberk7.com or +91 98990 62199.

Quick Reference

Zero Trust Pillar	Quick Win	Maturity Goal
Identity	MFA on all accounts	Adaptive risk-based auth
Device	Basic patch compliance check	Continuous posture scoring
Network	Basic segmentation	Full micro-segmentation

For a tailored consultation, contact CyberK7 at info@cyberk7.com or +91 98990 62199.