
Zero Trust in Action

Architecting Secure Systems Beyond Perimeters

Samvedna Jha, Senior Technical Staff Member, IBM India
Suneetha Vanjivakam, Senior Software Engineer, IBM India

Introduction

Introduction to Zero Trust

Zero Trust represents a security model moving beyond traditional perimeter defenses to continuous verification.



Why Zero Trust?

Rising insider threats and lateral movement risks, Attackers exploit implicit trust; Zero Trust eliminates this assumption.

Key Drivers

Cloud adoption, SaaS proliferation, Remote workforce, Regulatory compliance and Data protection mandates.

Business Impact

Reduces attack surface and breach impact, Balances security with user experience for productivity.

From Theory to Practice

The session emphasizes actionable strategies for implementing Zero Trust beyond theoretical concepts.

Perimeter Failure vs. Layered Security



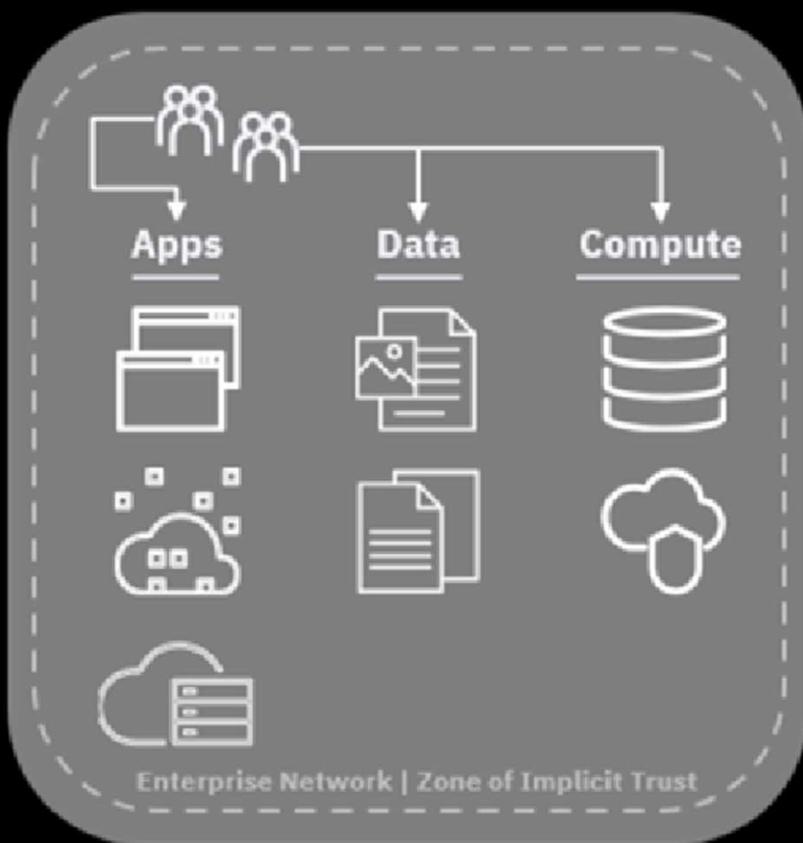
Traditional Perimeter Defense

Crumbling castle walls represent outdated perimeter defenses struggling against modern threats in distributed environments.

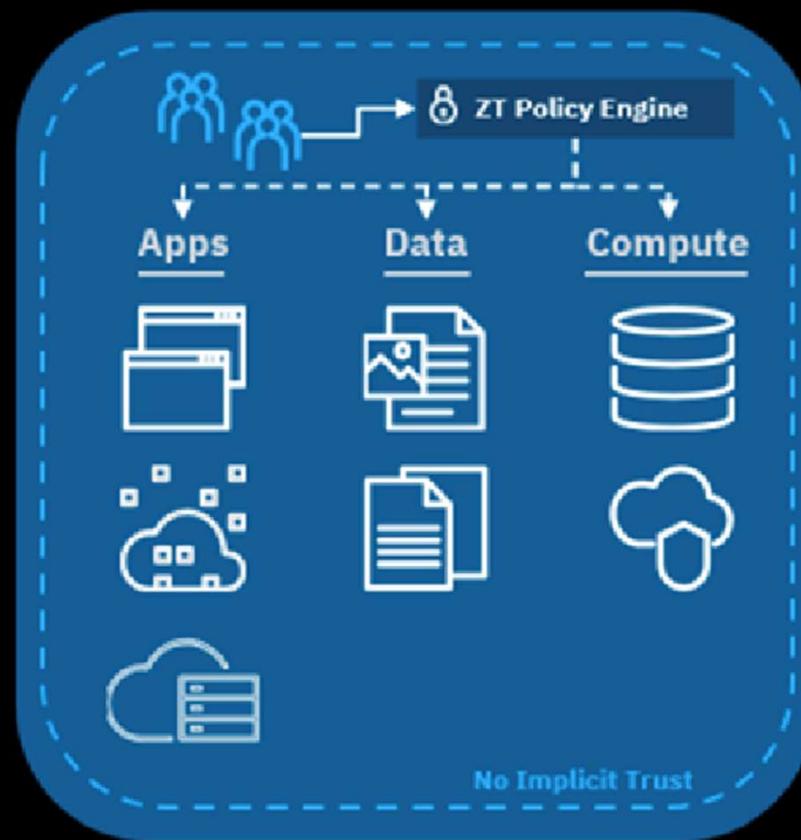
Layered Zero Trust Security

Futuristic airport security checkpoint illustrates layered verification and continuous identity checks in Zero Trust models.

Perimeter Security Model

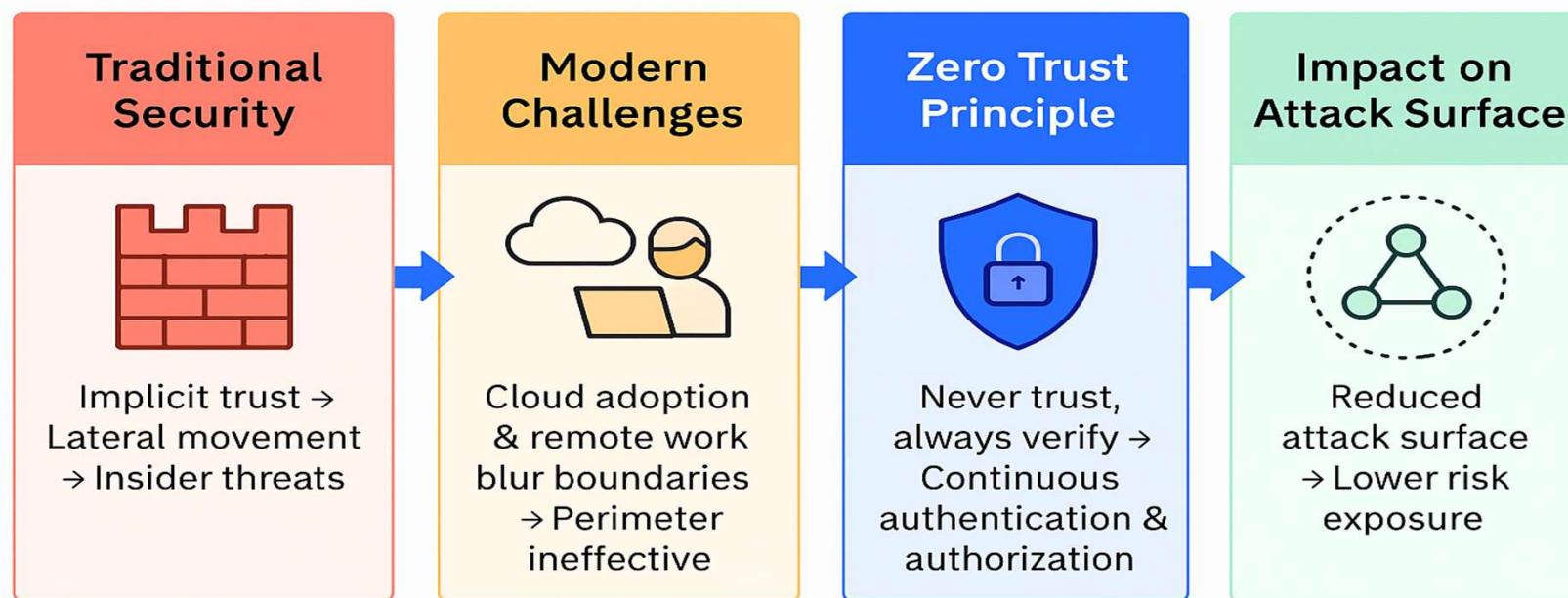


Zero Trust Security Model



Why Zero Trust?

The Need for Zero Trust



Case Study

Case Study 1: Healthcare Sector Ransomware Attack

Date: February 2024

Industry: Healthcare

What Happened: Attackers exploited compromised credentials and weak access controls to infiltrate systems.

Impact: Exfiltration of terabytes of sensitive patient data and disruption of critical services.

Lesson: Lack of identity-centric security and continuous verification enabled lateral movement.

Case Study 2: Research & Development Network Breach

Date: April 2024

Industry: Technology/Research

What Happened: Attackers bypassed MFA using session hijacking and exploited VPN vulnerabilities.

Impact: Breach of sensitive research environments; containment required emergency segmentation.

Lesson: Perimeter defenses and firewall rules were insufficient; Zero Trust segmentation could have minimized impact.

Case Study 3: Critical Infrastructure Attack

Date: May 2024

Industry: Energy

What Happened: Attackers leveraged implicit trust in network connectivity to move laterally.

Impact: Threatened national energy supply; required isolation of systems to prevent catastrophic failure.

Lesson: Zero Trust segmentation and continuous monitoring would have contained the breach.

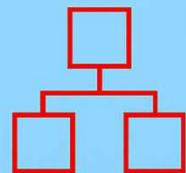
Core Principles and Typical Architecture of Zero Trust

Identity, Segmentation, and Monitoring



IDENTITY-CENTRIC PROTECTION

Identities as modern security perimeter requiring robust Identity Access Management(IAM) systems
Preventing unauthorized access through strong authentication & mechanisms



DYNAMIC MICRO-SEGMENTATION

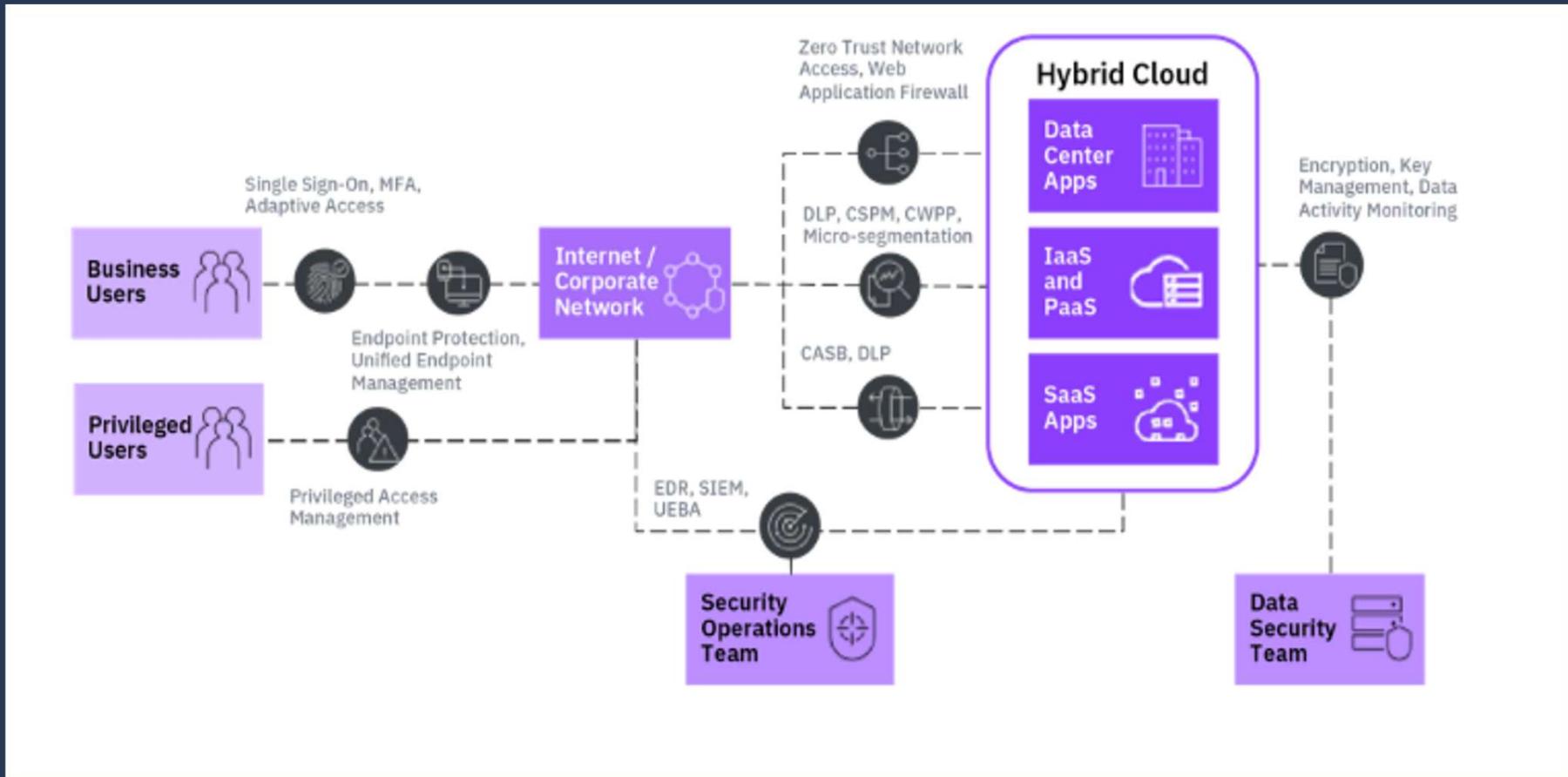
Adaptive segmentation of networks, and applications
Protecting assets by isolating workloads and containing lateral movement



CONTINUOUS MONITORING

Real-time network and system telemetry combined with behavioral analytics
Promptly uncovering anomalies and identifying emerging threats

Typical ZTA Architecture



Industry Adoption and Trends

Adoption Statistics and Market Movement



Growing Industry Adoption

Over 70%* of organizations now integrate Zero Trust principles into their cybersecurity frameworks, showing rapid acceptance. *Gartner 2024 survey report



Remote Access Deployments

By 2025, 70%* of new remote access deployments will implement Zero Trust principles for enhanced security. *Gartner report

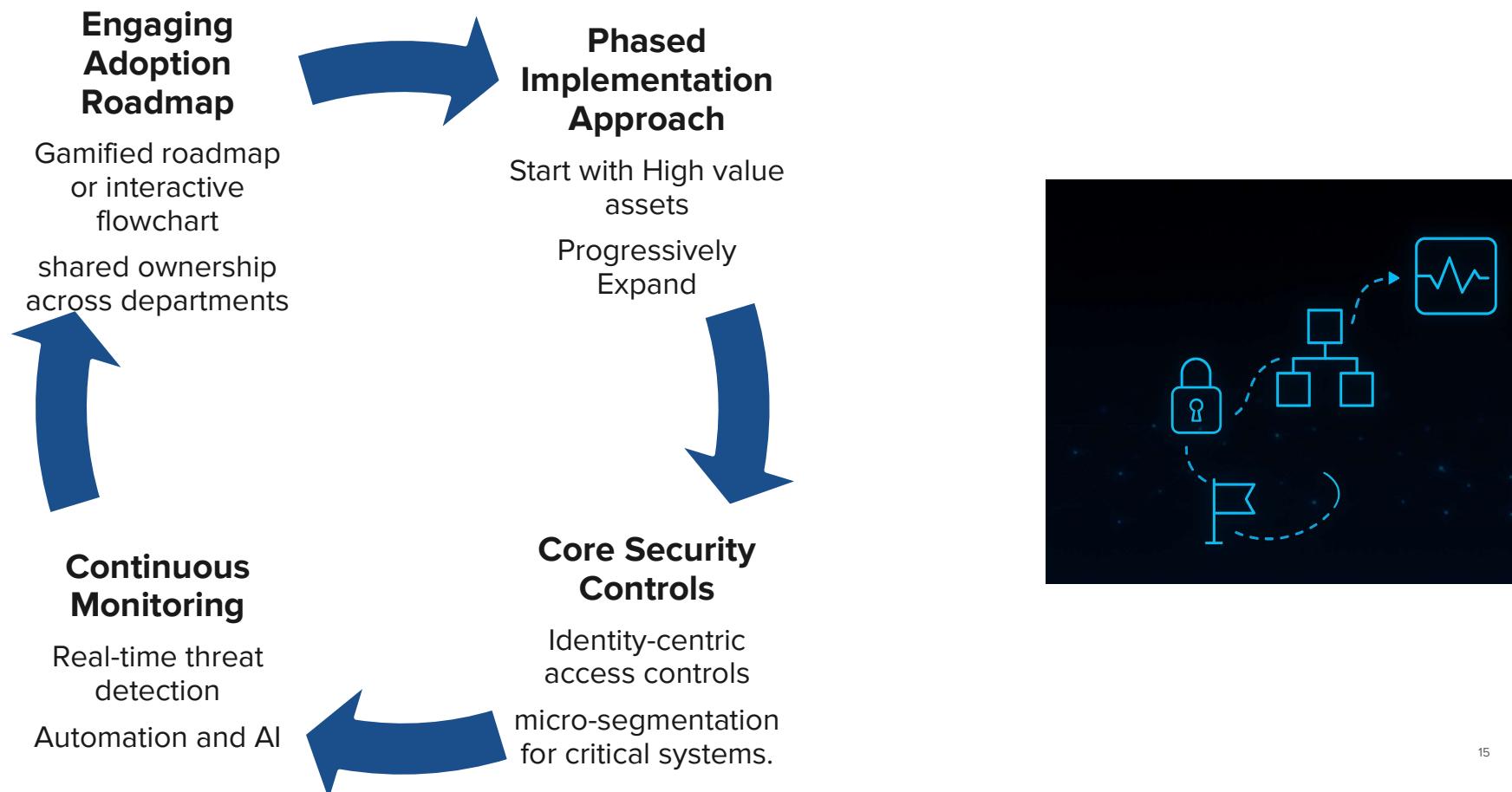


Audience Engagement Prompt

Poll or interactive prompt encourages audience to reflect on their organization's position in the adoption curve.

Implementation Roadmap

From Theory to Practice



Balancing Security and User Experience

Strategies for Seamless Access



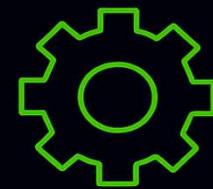
JUST-IN-TIME ACCESS

Temporary elevated credentials →
Just-in-time access grants permissions only when required
Longer access duration → Reduced attack windows
Shorter access duration & minimizing security



ADAPTIVE AUTHENTICATION

Dynamic adjustment of authentication →
Continuous monitoring of user activities and access contexts
Context like user location or device risk



BALANCING SECURITY AND USER EXPERIENCE

Policies tailored to user roles
→ Seamless access to resources and essential applications
Business needs
→ Maintaining user productivity

Common Pitfalls and Future Outlook

Avoiding Implementation Mistakes



Common Implementation Pitfalls

Overcomplicated policies and neglecting identity lifecycle management cause inefficiencies and security gaps.

Strategies to Avoid Mistakes

Simplify policy frameworks, ensure identity governance, and leverage automation for better scalability.

Future of Zero Trust

AI-driven threat detection and automated policy enforcement make security adaptive and proactive.

Reference Open-source Software

Keycloak

Provides single sign-on (SSO), multi-factor authentication (MFA), identity federation (SAML, OIDC), and fine-grained authorization (via policies).

Pomerium

identity-aware reverse proxy that provides secure access to internal applications without the need for corporate VPN.

OpenZiti

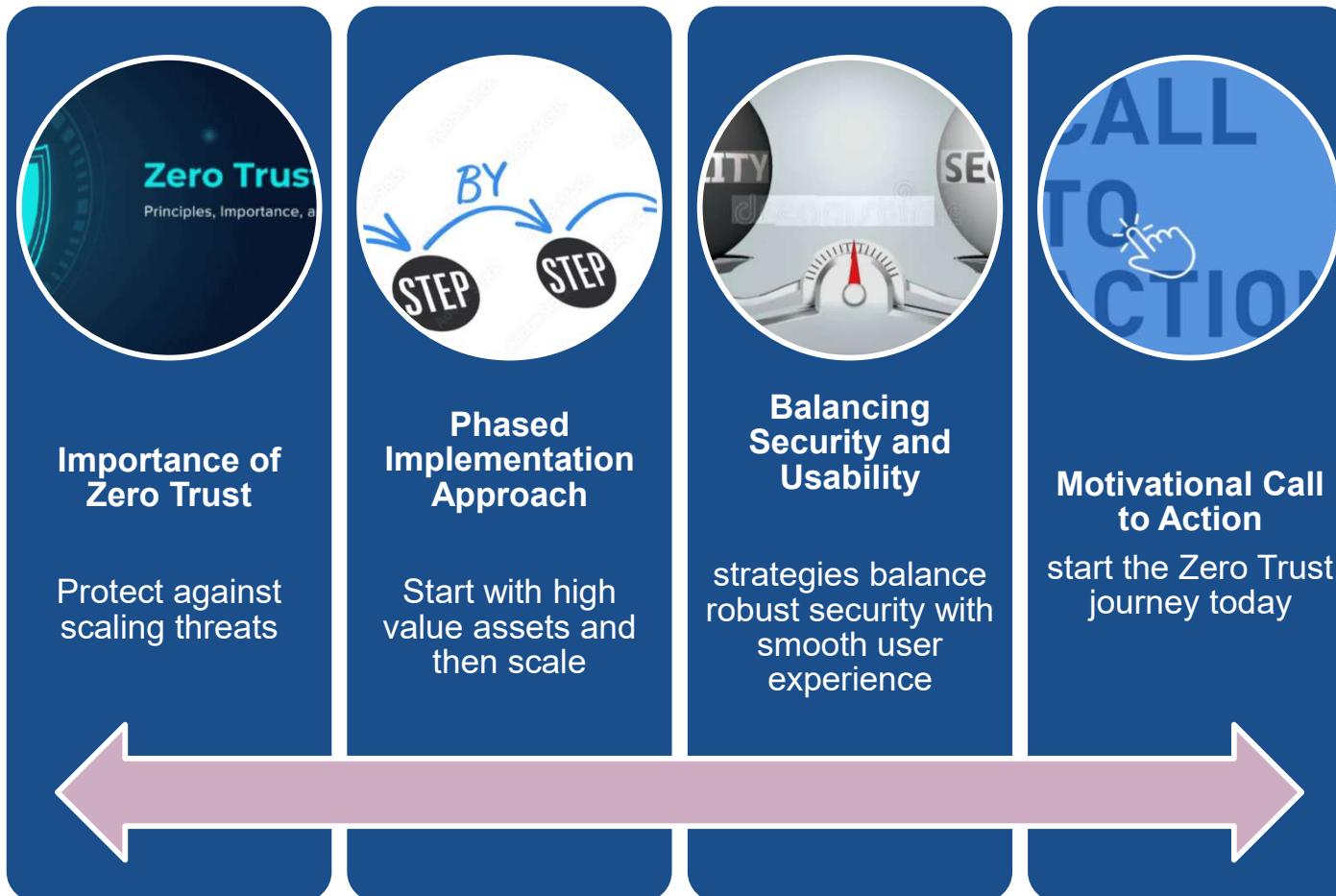
Creates secure, overlay networks (zero trust networks) where applications are hidden (dark) and access is granted only after stringent identity and context checks.

ELK Stack (Elasticsearch, Logstash, Kibana) and PLG Stack (Promtail, Loki, Grafana)

Essential for aggregating, analyzing, and visualizing logs and telemetry from all ZTA components (Keycloak, Wazuh, network devices, endpoints).

Conclusion and Call to Action

Next Steps for Your Organization





Thank you