Zero Trust Security – A Cornerstone to Cyber Defense and Resilience

by **Narayan Sharma,** *Global Head, IAM COE, TCS Cyber Security*

Raghvendra Singh, *Cyber Security Architect, CTM COE, TCS Cyber Security*

Abstract

As organizational security perimeter becomes increasingly porous and data and workloads move across hybrid multi-cloud environments more freely than ever before, shifting towards a contextual, adaptive, risk-aware, and resilient security model has become imperative. The Zero Trust model deems both internal and external entities of an organization 'untrustworthy' and 'eligible to breach the security' and it has been gaining market momentum with escalated adoption rates. Moving up from a moat to an impermeable wall that administers both the in- and outflux of data and controls access without any bias is what an enterprise needs today.

This white paper outlines our views on how enterprises can take a holistic and pragmatic approach to Zero Trust Security and achieve cyber defense and resilience as a valuable competitive advantage.

Zero Trust (ZT) Security – A Business Imperative

No business can survive today by working just within its own organizational boundaries, without opening access to external entities or accessing external systems. It is the era of interconnectedness, digitalization and network parity. There are many trends that drive the highly connected, digital landscape in the current market scenario where security must play a silent yet critical role.

- Pace of digital transformation
- Distributed business-sensitive data
- Data security and privacy regulations
- Convergence of IT and OT
- Emergence of new technologies (5G, cloud, XaaS, IoT, etc.).

The sheer speed and agility with which these trends are consuming the market has led to a growing concern for security and resilience across industries. There are more chances (and cases) of cybercrime, trojan malwares, crypto-ransomware and data misuse. The traditional castle-and-moat approach to security, where everything inside the organization's boundary is trusted - is no more relevant. This security paradigm holds true even if the enterprise has not yet moved its workloads to the cloud.

The need of the hour is an upgraded security model. A model where absolutely nothing is trusted by default and the architecture itself is context aware, risk-driven, and adaptive enough to meet the challenges of the modern threats. Such a security model can enable businesses to confidently pursue digital transformation without the fear of security breaches and achieve shorter time-to-value, and even act as a competitive advantage for them.

Welcome to the Zero Trust philosophy!

Core Principles of Zero Trust Security for an Enterprise

The core premise of ZT Security is to prevent unauthorized access to digital resources through granular and dynamic control enforcement for every access request using a trust broker component, which validates authorization and authentication level. To enable this, enterprises should embrace following principles to achieve Zero Trust Security:

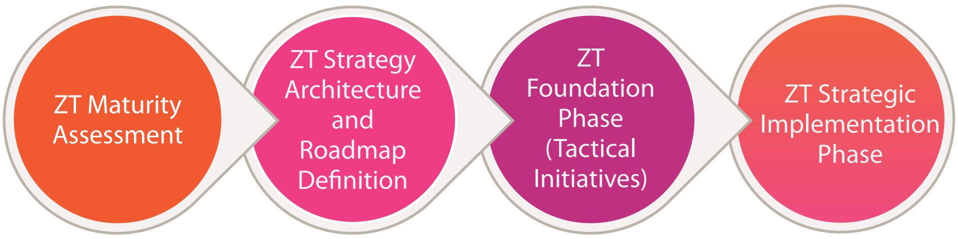
- **Resource visibility:** Ensure sufficient visibility into the resource to be protected – data being at the core. This would eliminate the security blind spots in an organization.
- **Zero attack surface (micro-perimeter):** Ensure zero attack surface for unauthorized access sessions and just enough access surface for authorized sessions. Technologies like micro-segmentation and software-defined perimeter (SDP) can help achieve this.
- **Never trust. Always verify:** Appropriately authenticate and authorize every session in contexts of digital identity (human or non-human), device, and digital resources before enabling access to resources.
- **Principle of least privilege:** Provide just enough access to resources to deliver required business outcomes at any given point. Plus, avoid access conflicts to enforce segregation of duty controls.
- **Data-centric security:** Move the security/privacy controls along with data as it moves across internal and external security boundaries.
- **Risk-driven approach:** Enable dynamic calibration of security/privacy controls in the context of evaluated risk levels.
- **Security visibility and analytics:** To ensure robust detection controls, all the key security events in networks, workloads, and security components must be logged, centrally correlated, and analyzed to derive insights using SIEM (security information and event management) and UEBA (user and entity behavior analytics) technologies. The insights so derived help fine tune the security policies for adaptive security controls and expedite breach investigations.
- **Security Orchestration Automation and Response (SOAR):** Enterprises should automate incident response processes and ability to auto re-configure security devices. While still in its early stages of maturity, SOAR tools and technologies provide the latest weapon in the Zero Trust security armor.

Best Practices for Zero Trust Adoption

- While these principles form the building blocks of Zero Trust security, implementing them at an enterprise-wide scale is a complex exercise – particularly while transforming existing cyber security practices and culture. We have identified some best practices from our experience of working with leading organizations across industries.
- **Focus on cyber hygiene:** It is imperative that basic cyber hygiene is maintained before planning for zero trust security adoption. The basic six controls outlined by the Center for Internet Security (CIS) can be a good starting point.
- **Holistic ZT strategy:** The presence and maturity of existing enterprise security solutions must form the basis for defining holistic and comprehensive ZT strategy. Enterprises should carefully assess, reuse, replace, and/or rebuild solution options and their rollout prioritizations.
- **In-built security controls:** Zero Trust adoption should not be an afterthought and bolted in afterwards. It should rather be a part of the overall transformation strategy to derive expected outcomes.
- **Continuous review and enhancement:** Risk is dynamic in nature and so should be the overall strategy. Continuous review and enhancement of ZT security controls is the only way to remain protected.
- **Frictionless user experience:** For seamless adoption of ZT security model, the trust broker solution components should be highly responsive while evaluating complex access policies in real time.

Journey to Zero Trust Security

Since every enterprise is unique in itself with varied security needs, maturity of controls, and technology/tools landscape, there cannot be a one-size-fits-all approach to ZT security implementation. However, a structured and phased approach is essential to ensure a secure and seamless transition. The journey to Zero Trust security can be broadly divided into four phases.


ZT Maturity Assessment
ZT Strategy Architecture and Roadmap Definition
ZT Foundation Phase (Tactical Initiatives)
ZT Strategic Implementation Phase

Zero Trust Maturity Assessment

As the Zero Trust model is built on the foundations of enterprise's security strategy, standards, policies and procedures, a ZT maturity assessment of aspects such as resource visibility, maturity of basic security controls, etc. helps in understanding the starting point of the ZT journey – at a business unit, IT department, or even enterprise level.

Zero Trust Strategy, Architecture, and Roadmap Definition

Post the Zero Trust maturity assessment, a broader strategy and planning around the following should be created.

- Architecture blueprint to meet target state maturity
- Reuse versus acquisition of new tooling
- Evaluation of new tools (if necessary)
- Business case preparation
- Overall program view – phases and timelines
- Prioritized implementation roadmap – both tactical and strategic

Zero Trust Foundation Phase (Tactical Initiatives)

The core focus of this phase is to address the gaps in Center for Internet Security (CIS) basic six controls and to pick up on low hanging fruits from the strategic stream. Following activities can be undertaken as a part of the foundation phase:

- Data discovery and classification
- Data flow paths
- Asset inventory
- Log monitoring and analytics – fine tuning of SIEM
- Secure configuration of end- points, servers, network, and security devices
- Continuous vulnerability management

Zero Trust Strategic Implementation Phase

Strategic tools and controls implementations to achieve ZT security are taken up during this phase. The duration and extent of change during this phase depends upon the reuse verus acquisition of new tools, the coverage to be achieved across user types, access channels, application types, and the spread of workloads across disparate environments (for example, hybrid multi-cloud). Some strategic initiatives that organizations can undertake include:

- Micro-segmentation and software-defined perimeters (SDP)
- Endpoint and server privilege management
- Risk-based strong authentication and authorization
- Comprehensive data protection controls
- NextGen security analytics

Conclusion

Zero Trust provides a blueprint for an enterprise's cyber security architecture to achieve risk-driven, context-aware, and adaptive security posture. If approached correctly, it prepares organizations for better cyber defense and resilience. For example, during the ongoing COVID-19 crisis, organizations who had mature ZT security controls seamlessly enabled secure remote access for their employees to ensure business continuity.

However, if the basic security controls are not in place or are not mature enough then the focus must be on addressing those first before venturing towards ZT initiatives. Organizations must take a holistic (but pragmatic) approach to achieve their target maturity state. Built on top of a robust cyber hygiene, we recommend a staggered, holistic, and pragmatic approach to achieve target state maturity of Zero Trust security in a quickest possible time frame.

About The Authors

Narayan Sharma

Narayan Sharma is the Global Head of Identity and Access Management (IAM) practice of TCS’ Cyber Security unit. With over 20 years of industry experience, he has deep expertise in cyber security consulting, solution architecture, implementation, and delivery oversight across banking, financial services, insurance, and healthcare industries. He has an M. Tech. in Machine Design from IIT Delhi, and holds CISSP, Architecture Concentration (ISSAP), CISA, CEH, and CCNA certifications.

Raghvendra Singh

Raghvendra Singh is an Enterprise Security Architect working with the Cyber Security unit at TCS. He has over 11 years of experience in enterprise security and leads the consulting and advisory services in Cognitive Threat Management CoE. He has led various engagements in IT security service transition, IT security assessment, roadmap definition, cloud roadmap and migration definition across retail, life science, utilities, media and aviation industries. He holds a Bachelor of Engineering in Electronics and Communication from RGTU, Bhopal.

About Tata Consultancy Services Ltd (TCS)

TCS Design Services I M I 07 I 20