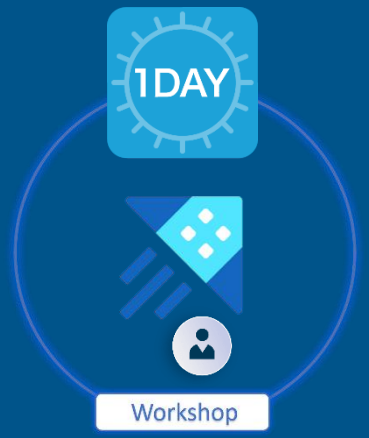
Executive Leadership Series

Zero Trust Security for Business Technology and Security Professionals

Education & Training Services



- CXO's
- Business Executives
- Technology Executives
- Entrepreneurs
- Cybersecurity Professionals
- Cloud Leaders
- Project Managers
- Strategic Planners

Zero Trust Security for Business Technology and Security Professionals

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

Executive Leadership Series

About this Workshop

In a nut-shell, the concept of a Zero Trust Security Architecture has been around for more than a decade, but adoption did not really begin to take hold until the past couple of years. Zero Trust is a framework for securing organizations in the cloud, on-premises and mobile world that asserts that no user or application should be trusted by default. Following a key zero trust principle, least-privileged access, trust is established based on context (e.g., user identity and location, the security posture of the endpoint, the app or service being requested) with policy checks at each step.

Target Audience

- Customers who want to build their knowledge in the space of Zero Trust security technology and are in the process of planning and implementing Zero Trust Security Architecture Framework in their organization.
- CIO/CISO/CTO, CRO, IT Directors/GM IT, Risk and Business Technology Leaders, IT Managers, Application and Development Team Leads, Strategic Technology Planners, Project Managers, Solution/IT/Systems Architects, Enterprise Architects, Network Operation teams , Information Security and Cybersecurity teams, SOC teams and Cloud Leaders.

Zero Trust Architecture is an alternative security model that addresses the fundamental flaw of traditional strategies that data only needs to be protected from outside of an organization. The **Zero Trust** model views data security through a new lens, enabling parameters that dictate access and restrictions.

Understand how **segmentation gateway** provides granular visibility into traffic and enforces additional layers of inspection and access control with granular Layer 7 policy based on the **Kipling Method.**

Zero Trust is an augmentation of your existing architecture, it does not require a complete technology overhaul. Rather, it can be deployed iteratively while allowing you to take advantage of the tools and technologies you already have.

Unit 1 – Zero Trust Security Architecture Framework and Implementation Strategy

- Understanding the Common IT Challenges.
- Identify High Deployment Risks spread over five key Domains.
- A Framework for Zero Trust – Three Key Phases, and the importance of Feedback Loop.
- Certain Myths and Confusions that need Attention from ZT Point-of-View.
- Understanding Zero Trust Architecture.
- Zero Trust architecture services – An Example.
- Putting Zero Trust Architecture into Practice.
- Differentiating between Untrusted Zone and Implicit Trust Zone.
- Zero Trust Architecture – Logical Components.
- Zero Trust Architectural Framework.
- Unleash the role of TCP/IP Session Layer and ZT Implementation.
- The Principles behind Zero Trust Security.
- How to achieve a Zero Trust Architecture.
- Describe Segmentation Gateway – An essential component of Zero Trust.
- Deploying Zero Trust using Kipling Method.
- Implementing Zero Trust Identity Management Principles.
- Following the Zero Trust Model.
- High-level Zero Trust Maturity Model Overview.
- Identity Governance and Administration Strategy.
- Implementing Zero Trust Identity Management Principles.
- ZT Architecture Implementation Example – Before and After.
- A layered Cyber Defense Approach – The bigger picture.
- Recommendations for starting a Zero Trust Journey.
- Digital Enterprise based on Zero Trust adoption – A Bigger View.
- Five Stages Determined Maturity Level for Zero Trust.
- A Checklist to take you from Theory to Zero Trust reality.
- What are the threats to Zero Trust Architecture?
- Steps towards Zero Trust implementation strategy summary.
- Unit 1 Assessment.

Common IT Challenges effectively managed by right ZT strategy

Over half of companies are already taking steps to deploy Zero Trust solutions

Security and networking teams globally have implemented or plan to implement soon – Are you ahead of the curve? – *A Ponemon Institute Survey*

62% are familiar with Zero Trust

Zero Trust

20% have deployed

37% plan to deploy

Detailed Information

Course Code	: TN480
Course Duration	: 1 Day Workshop
Course Location	: TLC, Online, and Customer On-site.
Terms & Conditions	:100% payment in advance.
Course Deliverable	: Comprehensive Student Guide and Course Certificate

For additional information:
please write to us at: info@tlcpak.com

Opportunities are made, not found

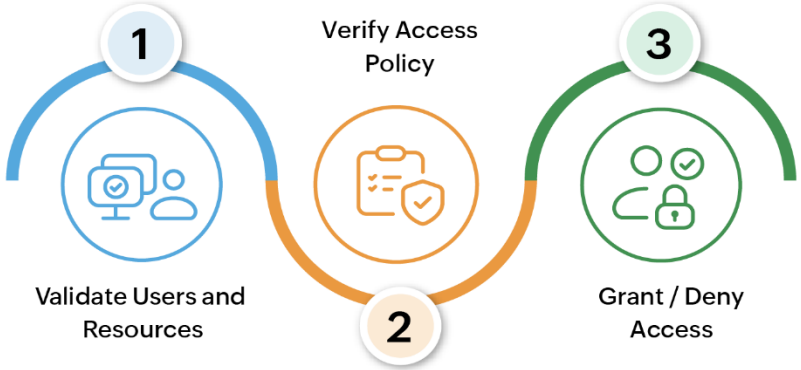
Zero Trust Security for Business Technology and Security Professionals

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

About this Workshop

In a nut-shell, the concept of a Zero Trust Security Architecture has been around for more than a decade, but adoption did not really begin to take hold until the past couple of years. Zero Trust is a framework for securing organizations in the cloud, on-premises and mobile world that asserts that no user or application should be trusted by default. Following a key zero trust principle, least-privileged access, trust is established based on context (e.g., user identity and location, the security posture of the endpoint, the app or service being requested) with policy checks at each step.



Zero Trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. This added layer of security has been shown to prevent data breaches.

A Zero Trust model provides security against ransomware and cybersecurity threats by assigning the least required access needed to perform specific tasks.

A Zero Trust model provides security against ransomware and cybersecurity threats by assigning the least required access needed to perform specific tasks.

Zero Trust: The Role Senior Business and Technology Management leadership Team

Zero Trust Security is a paradigm shift in cybersecurity that challenges the traditional perimeter-based approach. It assumes that no entity—whether inside or outside the network—can be inherently trusted. Instead, trust must be continuously verified based on context, behavior, and risk assessment. Here's why Zero Trust matters and the role of senior business and technology management leadership teams:

Why Zero Trust Matters:

Adaptive Security: Zero Trust adapts to the dynamic nature of modern IT environments. With remote work, cloud services, and mobile devices, the traditional castle-and-moat model is insufficient.

Reduced Attack Surface: By verifying every access request, Zero Trust minimizes the attack surface. It prevents lateral movement within the network, limiting the impact of breaches.

Data Protection: Zero Trust focuses on protecting data wherever it resides—whether on-premises, in the cloud, or on endpoints.

Continuous Monitoring: It emphasizes continuous monitoring of user behavior, device health, and network traffic.

Business Agility: Zero Trust enables secure digital transformation by allowing organizations to adopt new technologies without compromising security.

Applications: Applying Zero Trust to applications removes implicit trust with various components of applications when they talk to each other. A fundamental concept of Zero Trust is that applications cannot be trusted and continuous monitoring at runtime is necessary to validate their behavior.

The Role of Senior Business and Technology Management Leadership:

Championing Zero Trust: Senior leaders must champion the Zero Trust approach. They need to understand its benefits, endorse its adoption, and allocate resources for implementation.

Setting the Vision: Leaders define the strategic vision for Zero Trust within the organization. They communicate its importance to all stakeholders.

Risk Management: Senior management must be briefed about the concept and support the program. They play a critical role in risk management and decision-making.

Cross-Functional Collaboration: Key teams, including architecture, applications, and infrastructure, must be highly engaged. Zero Trust requires collaboration across departments.

Change Management: Leaders drive cultural change. They ensure that Zero Trust becomes an integral part of the company culture.

Monitoring Progress: Senior leaders review progress, assess maturity, and adjust the Zero Trust roadmap as needed.

In summary, Zero Trust is a collective effort involving business leaders, security practitioners, and users. It's not just a technical solution; it's a mindset that transforms how organizations approach security. If you're interested in learning more, explore resources on Zero Trust deployment guidance for identities and consider its impact on your organization's security posture.

With digital transformation accelerating in the form of a growing hybrid workforce, continued migration to the cloud, and the transformation of security operations, taking a Zero Trust approach has never been more critical. If done correctly, a Zero Trust architecture results in higher overall levels of security, but also in reduced security complexity and operational overhead.

Executive Leadership Series