Security Forum
Zero Trust Architecture Working Group
Zero Trust Reference Architecture Project Charter

Status: Final
Revision level: V1.0
Date: Feb. 24, 2021

A. Project Description

In recent times, the security concept known as "zero trust architecture" (ZTA) has become a hot topic. Key drivers have been on both the end user side and the supply side. Zero Trust in the modern environment constitutes a holistic capability addressing components in the entire IT ecosystem. However, traditional, perimeter-based approaches are unable to support moderns rate of change and the transition to cloud environments. The vendor community has shown particular interest because (a) they see an opportunity to develop, market, and sell new products, and (b) some interpretations of the concept threaten to disrupt the network security industry, leaving some vendors without a meaningful offering in network security. The situation is a classic case of "digital disruption," leading to opportunities for digital evolution to meet the perpetual state of business and technology disruption.

This project is intended to develop a reference architecture for implementing Zero Trust. The reference architecture will build on other, previous deliverables from the Zero Trust Architecture Working Group, predominately the Zero Trust Core Principles White Paper and the Zero Trust Landscape White Paper, in order to define common characteristics and identify requirements and desired capabilities.

B. Goals of this Project

This project will ultimately create a Zero Trust Reference Architecture (a standard) that demonstrates and defines how to implement Zero Trust. The project will begin, though, by creating an initial conceptual Zero Trust Reference Model based on industry input and use cases. The Reference Model will be a higher-level document focused more on strategic direction and conceptual guidance and will allow for reference implementations to be contributed. These reference implementations will aid in the creation of the Zero Trust Reference Architecture.

This project will utilize The Open Group Snapshot process, publishing regular updates as progress is made and soliciting input from both Members and non-Members of The Open Group to ensure the Zero Trust Reference Model and eventual Zero Trust Reference Architecture meet industry requirements and desires.

This project will also aim to develop complementary documents in order to aid those implementing Zero Trust. Among these are a Business Guide, which will be intended for senior and C-level executives and enterprise architects, that explains what Zero Trust is, its impact on business, and the reasoning for implementing it, as well as a Practitioners Guide, which will be intended for those implementing Zero Trust, that provides a process framework and develops an ontology for Zero Trust.

By developing a Reference Architecture based on accepted definitions, requirements, and capabilities for Zero Trust and Zero Trust Architectures, end users will be able to focus on improving

speed-to-market and Agile practices while vendors will be able to compete without dealing with interoperability concerns from users.

C. Project Deliverables

A. Zero Trust Reference Model
  a. Develop complete outline first
    i. Clarify distinction between Model and Architecture
    ii. Normative model (i.e., Standard)
  b. Provide high-level conceptual guidance
    i. Leverage Zero Trust Core Principles and Axioms for Zero Trust
  c. Develop community around Zero Trust
  d. Allow for contribution of reference implementations
B. Zero Trust Practitioners Guide(s)
  a. Develop ontology of Zero Trust concepts, terms, and relationships
  b. Provide actionable steps for implementing Zero Trust
  c. Leverage Zero Trust Reference Model
  d. Include Governance, Risk, & Compliance practices
  e. Bridge gap between policy and procedure
    i. Distinguish between definition and operation
C. Zero Trust Reference Architecture
  a. Define capabilities
    i. Separate required capabilities and desired capabilities
    ii. Separate guidance on implementing capabilities
  b. Define implementation and interoperability requirements
    i. Architectural components
  c. Refine Reference Model concepts based on industry input
D. Zero Trust Reference Implementation
  a. Creating this deliverable will lean heavily on to-be-created and -formalized The Open Group Policies
    i. Take inspiration from the OSDU Forum
E. Zero Trust Business Guide
  a. Provide guidance to senior and C-level executives on Zero Trust
  b. Describe Zero Trust ecosystem
  c. Elaborate on Zero Trust drivers

D. Project Value Proposition

A. End users will have an industry standard and guidelines on interoperability that will allow them to remain focused on improving business outcomes
B. Vendors will have clear guidance on developing products without encountering interoperability woes
C. Those interested in Zero Trust will have clear guidance and a thriving community of practitioners to answer lingering questions/concerns.

E. Project Personnel

A. Stakeholders
  a. The governing stakeholders of the project are:
    i. The Open Group

           ii.   The Open Group Security Forum Steering Committee
- B. Team
    - a. The project team will be drawn from members of The Open Group Security Forum and Architecture Forum. The project leadership will be selected through the normal procedures of The Open Group.
    - b. The Project Facilitator will be Kenneth Street and Nikhil Kumar.

F. Project Methodology

This final section describes the project methodology, which includes:

- A. Approach
    - a. This project will be managed by the Co-Chairs of the Zero Trust Architecture Working Group, who will report regularly to the Security Forum Steering Committee.
    - b. The Zero Trust Reference Model will act as the first step, building on previous publications and continuing to grow the community around Zero Trust.
- B. Roadmap
    - a. Define an initial outline of the Reference Model
        - i. Use this process to clarify…
            1. Definition/requirements for Reference Architecture
            2. Requirements testing and feasibility of this
            3. Logistics for requirements testing
    - b. Develop Zero Trust Reference Model
        - i. Establish process for contribution of reference implementation
        - ii. Determine feasibility of using community contributions
        - iii. Utilize Snapshot process
    - c. Develop Practitioners Guide
        - i. Plan to publish updates as Snapshots are published
    - d. Develop Reference Architecture
        - i. Establish standard and conformance requirements
    - e. Develop Reference Implementation
    - f. Develop Business Guide
- C. Governance
    - a. Governance of the initiative will be The Open Group standard policy and procedures.
- D. Approval
    - a. Project deliverables will be approved by The Open Group. The project charter will be approved through the normal mechanism of The Open Group.