Security Forum
Zero Trust Architecture Working Group
Zero Trust Core Principles 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 initially and then refine, based on industry input and feedback, definitions for Zero Trust and Zero Trust Architecture as well as a set of "Zero Trust Core Principles." These core principles should be relatively simple to comprehend, allowing business stakeholders and executives to quickly and clearly grasp their meaning without technical understanding of implementation. The Zero Trust Core Principles document(s) will explain *what* Zero Trust is to key stakeholders and provide groundwork for develop a Zero Trust Reference Model and then Reference Architecture.

B. Goals of this Project

The initial document will develop a set of Core Principles for Zero Trust after explaining the current context of Zero Trust—that is, it is not widely understand in no small part because product vendors have attempted to define it based on product capabilities rather than end user requirements. The initial document will provide drivers, requirements, and capabilities commonly seen as organizations attempt to understand and implement Zero Trust and Zero Trust Architectures. It will provide an initial set of Core Principles as well as a set of scenarios that demonstrate the connection among the drivers, requirements, capabilities, and Core Principles.

The Zero Trust Core Principles White Paper is meant predominately for leaders in business, security, and IT–namely, Executives.

The follow-up document will refine and expand on the initial Core Principles, taking a similar approach to The Open Group Guide: Axioms for the Practice of Security Architecture: clearly and concisely defining the Core Principles and their importance. The Guide is meant to provide more detail on the Core Principles and offer illustrative examples of them.

C. Project Deliverables

A. Zero Trust Core Principles White Paper

a. Provide initial definition for Zero Trust and Zero Trust Architectures
b. Establish relevant drivers, requirements, and capabilities
c. Provide initial set of Zero Trust Core Principles
d. Develop scenarios to demonstrate the connection among the drivers, requirements, capabilities, and Core Principles.

B. Axioms for Zero Trust Guide
   a. Refine definitions for Zero Trust and Zero Trust Architectures from Zero Trust Core Principles White Paper
   b. Refine and expand on Core Principles from Zero Trust Core Principles White Paper
      i. Each Axiom will receive its own page
      ii. Each Axiom will be thoroughly explained and defined
      iii. Each Axiom will receive technical clarity around implementation

D. Project Value Proposition

A. This project will establish a shared industry understanding and definition of Zero Trust and its implications, covering people, processes, and technology.
B. This project will establish a set of Core Principles that will be refined into Axioms and used to develop a Zero Trust Reference Model and a Reference Architecture, which is the ultimate goal of the Zero Trust Architecture Working Group.
C. This project will provide clear documents that can be used to aid marketing efforts for the Zero Trust Architecture Working Group.

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 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. After publishing the initial Zero Trust Core Principles White Paper, The Open Group and project stakeholders will seek industry input and feedback with the goal of refining the initial publication in the planned follow-up document.
B. Roadmap
   a. Develop Zero Trust Core Principles White Paper
   b. Gather/solicit industry feedback and input
   c. Refine Core Principles into Axioms in follow-up document
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.