Security Forum
Zero Trust Architecture Working Group
Zero Trust Core Principles Project Charter

Status: Ballot for Approval
Revision level: V2.0
Date: Sep. 29, 2022

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 initially developed Core Principles and then refined, based on industry input and feedback, definitions for Zero Trust and Zero Trust Architecture before creating the Zero Trust Commandments. The core principles were intended to be 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 explained *what* Zero Trust is to key stakeholders and provided groundwork for develop a Zero Trust Reference Model and then Reference Architecture. The Zero Trust Commandments document presented what Zero Trust *is*.

The next phase of the project is to “promote” and consolidate the Zero Trust Core Principles and Zero Trust Commandments into a single Standard document. This Standard will embrace the notion of Zero Trust being the security approach for the Digital Age.

The new Standard may also act as the basis for a knowledge-based certification program that will complement the in-development Zero Trust Reference Model Standard.

B. Goals of this Project

The initial document developed 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 provided drivers, requirements, and capabilities commonly seen as organizations attempt to understand and implement Zero Trust and Zero Trust Architectures. It provided 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 was meant predominately for leaders in business, security, and IT–namely, Executives.

The follow-up Zero Trust Commandments Guide refined and expanded on the initial Core Principles, taking a similar approach to The Open Group Guide: Axioms for the Practice of Security Architecture: clearly and concisely presenting Commandments.

The final phase of this project is to "promote" and consolidate the Zero Trust Core Principles White Paper and the Zero Trust Commandments Guide. The Commandments were written originally as imperative statements, allowing easy conversion to a Standard. The context, drivers, requirements, and capabilities will be used to introduce the Commandments and ensure consistent understanding of their value. This will also encompass aligning on terminology and vocabulary so that this new Standard may be used as the single source of truth for terms across other publications. The original Core Principles will be published as an appendix in the Standard. The new standard will supersede both the Zero Trust Core Principles White Paper and the Zero Trust Commandments Guide but will align to a separate, top-level document on Security Architecture Principles, ensuring consistency across Security Forum publications.

Upon publication of the new Standard, the project will turn to using the Standard to develop a knowledge-based certification program. This Certification will be at the foundation level, allowing development of higher certification levels as additional materials are published by the ZTA Working Group.

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. Zero Trust Commandments Guide
    a. Refine definitions for Zero Trust and Zero Trust Architectures from Zero Trust Core Principles White Paper
    b. Refine and expand on key concepts from Zero Trust Core Principles White Paper
C. Zero Trust ____ Standard (name undecided)
    a. "Promote" and consolidate the Zero Trust Core Principles and Zero Trust Commandments
    b. Provide a single source of truth regarding what Zero Trust is and related terminology
    c. Act as basis for knowledge-based certification program
D. Zero Trust Foundation Individual Certification
    a. Act as first-of-breed certification on topic of Zero Trust
    b. Provide initial certification for expansion as additional materials are published
    c. Allow individuals to distinguish themselves as clearly understanding what Zero Trust is and why it is important

D. Project Value Proposition

A. Establish a shared industry understanding and definition of Zero Trust and its implications, covering people, processes, and technology.
B. Establish a set of Core Principles that will be refined into Commandments 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. Develop first-of-breed certification program for individuals to distinguish themselves based on consensus-based Standard

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
        iii. The ZTA Working Group 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 Facilitators will be Mark Simos, Nikhil Kumar, and John Linford.

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. Roadmap
    a. Publish Zero Trust Core Principles White Paper
        i. Gather/solicit industry feedback and input
    b. Refine Core Principles into Commandments in follow-up document
    c. "Promote" and consolidate Zero Trust Core Principles and Commandments into a single Standard
        i. Align on terminology in Definitions section and in Glossary
        ii. Complete informal review of document to collect broad comments on body of document
        iii. Complete formal Forum Review and then Company Review to publish as Standard
        iv. Revisit Project Charter to align on approach for developing certification program
    d. Use new Standard as basis for creating knowledge-based foundation certification program
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.