US 20240214377A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214377 A1**

Levin et al. (43) **Pub. Date: Jun. 27, 2024**

(54) **PROVIDING ZERO TRUST NETWORK SECURITY WITHOUT MODIFICATION OF NETWORK INFRASTRUCTURE**

(71) Applicant: **Twistlock Ltd.**, Herzliya (IL)

(72) Inventors: **Liron Levin**, Kefar Sava (IL); **Eran Yanay**, Modiin (IL); **Dima Stopel**, Herzliya (IL)

(21) Appl. No.: **18/600,176**

(22) Filed: **Mar. 8, 2024**

Related U.S. Application Data

(62) Division of application No. 16/939,589, filed on Jul. 27, 2020, now Pat. No. 11,962,584.

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0869*** (2013.01); ***H04L 63/0263*** (2013.01); ***H04L 63/0823*** (2013.01); ***H04L 63/166*** (2013.01)

(57) **ABSTRACT**

Zero trust network security is provided without modifying the underlying network infrastructure. A first entity at a first node in a network environment obtains an entity identifier and host certificate from a second entity installed on a second node. A determination is made as to whether the host certificate is valid based on a firewall policy and an intermediate certificate that was issued to the first entity. A determination is also made as to whether the entity identifier is valid based on a known infrastructure of the network environment. If the host certificate and entity identifier are valid, communications between the first and second entities can be allowed, while communications are blocked if at least one of the host certificate and the entity identifier is not valid.