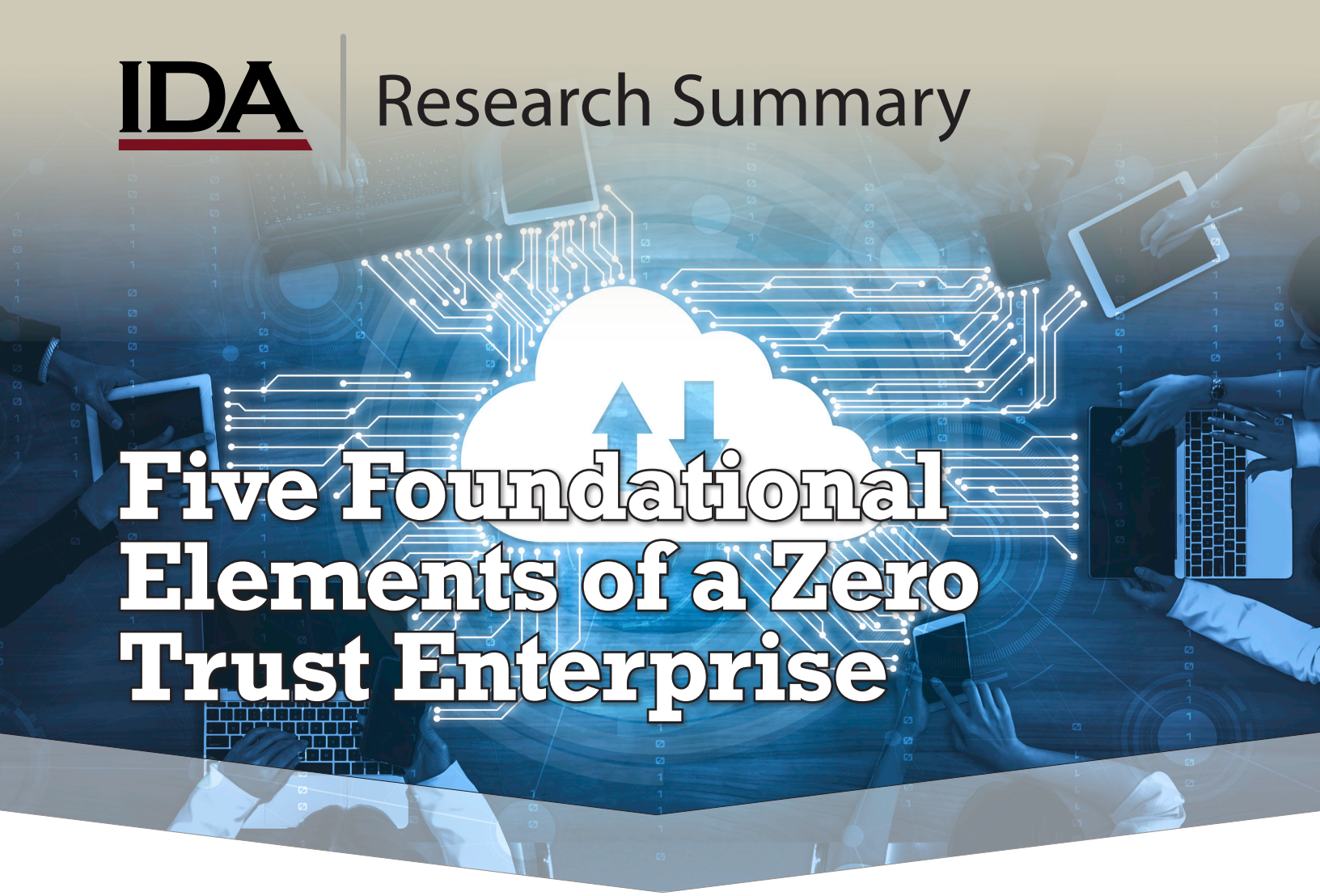
IDA | Research Summary



Five Foundational Elements of a Zero Trust Enterprise

Zero Trust is a relatively new cybersecurity concept that relies on continuous verification of an enterprise's devices, users, and applications. It differs from current security practice in that protections are placed at the resources themselves. This approach is a better match to current enterprise threats, which can break through firewalls and other boundary protections. The vision for Zero Trust is to defend against threats from outsiders and insiders and to block lateral movement within an enterprise.

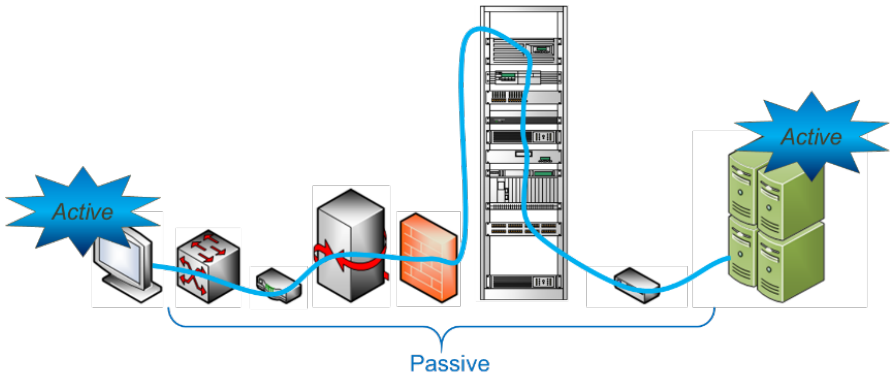
IDA developed five foundational concepts for the Zero Trust Enterprise (ZTE) based on an approach taken in a long-term U.S. Air Force effort called Enterprise Level Security.

Two-Way Authenticated Communication. To provide dynamic, per-connection, policy-based secure communication, entities must know who their partners are. This requires two-way credential-based authentication prior to each access for devices and requesters. Multi-factor authentication can increase security and provide more options for authentication in different situations. However, authentication must be between the two communicating entities. Solutions that utilize a third-party single sign-on provider to issue static authentication tokens are not suited to a Zero Trust solution.

Endpoint Device Management. Authentication is initiated by an individual, but a device is ultimately responsible for sending the data for authentication and other requests. To ensure user intentions are executed properly, such devices must be operating correctly. This is accomplished using endpoint device management that is tied to a verifiable hardware root of trust in the device.

May 2021
NS D-22632

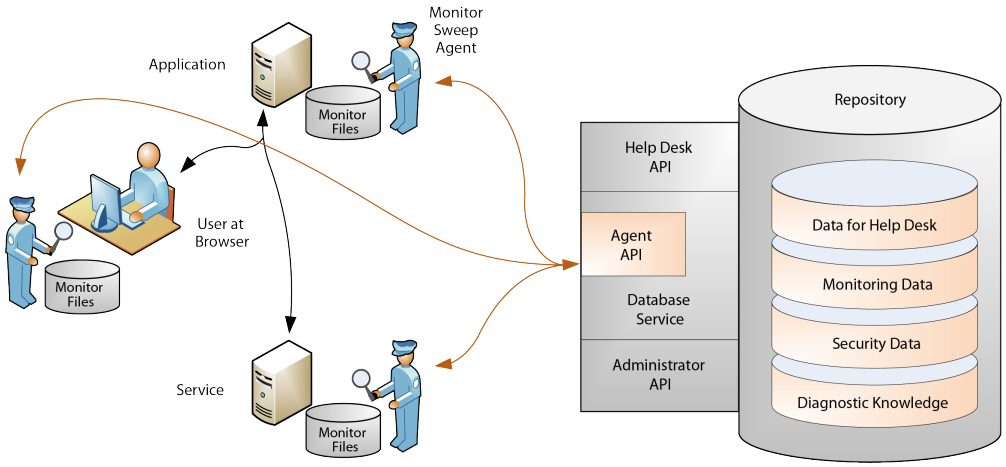
End-to-End Encryption and Integrity. Attackers don't only target endpoint devices. Firewalls and other gateway appliances offer bigger targets due to the high volume of traffic they process. Encryption prevents malicious entities on the network from intercepting and deciphering information, and integrity protections block attacks that modify content. However, such protections only work if they are end-to-end, as illustrated. For Zero Trust, the network elements are passive and the endpoints are active, with embedded security agents performing scans directly on the devices.



End-to-end security is performed at the endpoints instead of in the network.

Policy-Based Authorization. To provide scalability and consistency, access to enterprise resources is determined by policy. The policy is based on entity attributes that are updated regularly. This provides quick access when needed and, more importantly, quickly disables access when no longer needed. The access policies are also determined by environmental information, such as external information about an entity and its veracity; information about the machine, location, and time of their access request; and special conditions as determined by the resource provider.

Accountability for Actions. Zero Trust focuses on preventing attacks, but its basic assumption that networks are not secure implies that attacks will happen. Accountability helps to protect the innocent and identify the guilty when such acts occur. The idea of end-to-end security also relies on accountability of the endpoints. This is provided by endpoint security tools that monitor activity on the endpoints and report suspicious activity.



Automated systems continuously review log files that are uploaded to a central repository.

Kevin E. Foltz (kfoltz@ida.org) and **William R. Simpson** (rsimpson@ida.org) are members of the research staff in the Information Technology and Systems Division of IDA's Systems and Analyses Center.

Based on K. E. Foltz and W. R. Simpson, *Enterprise Level Security 2: Advanced Techniques for Information Technology in an Uncertain World*, Boca Raton: CRC Press, 2020.