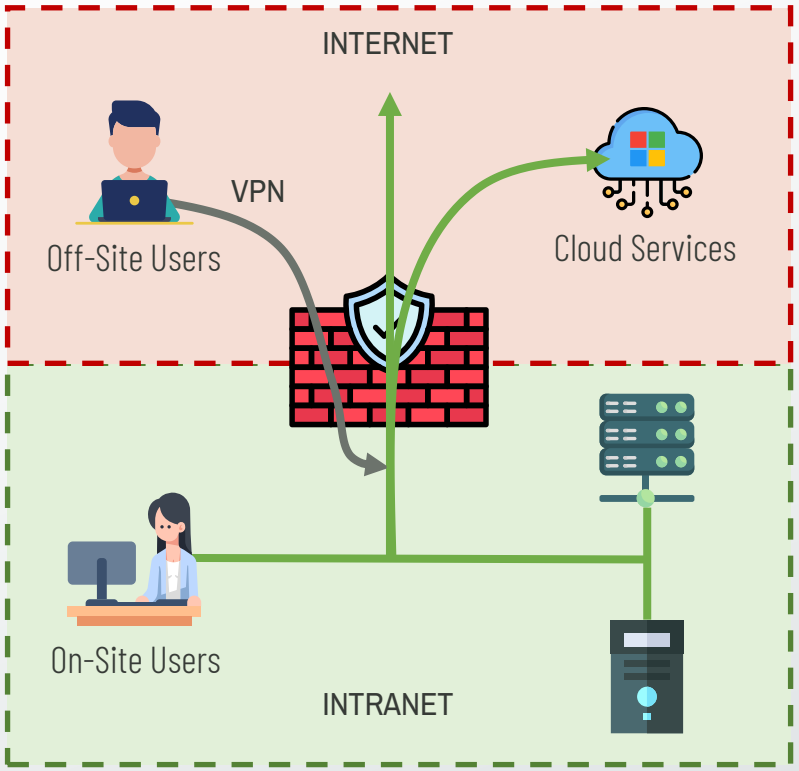
Exploring ZTA Use Cases

VPN-Less Implementation

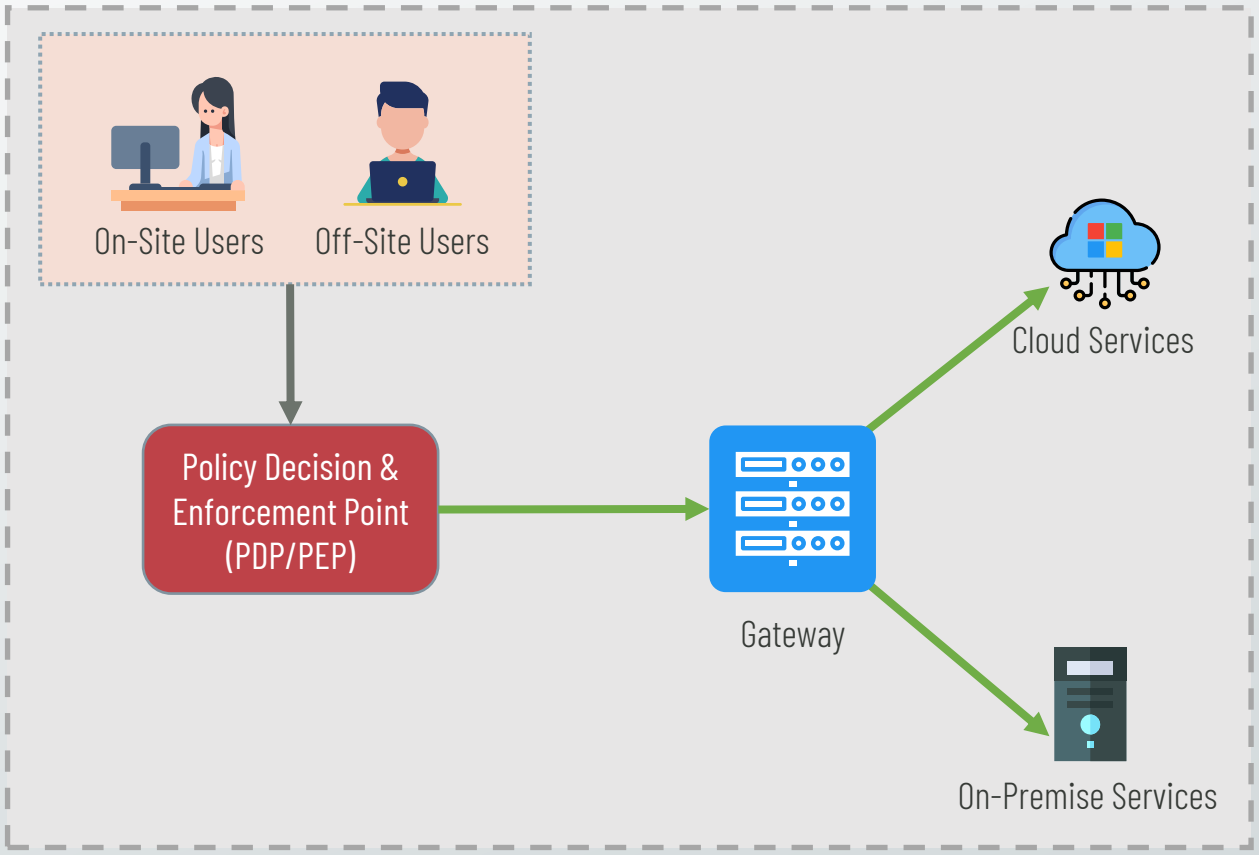
INSTRUCTOR ALTON

Conventional Design



- On-site users have implicit trust.
- VPN users are given full access.

Zero Trust Design



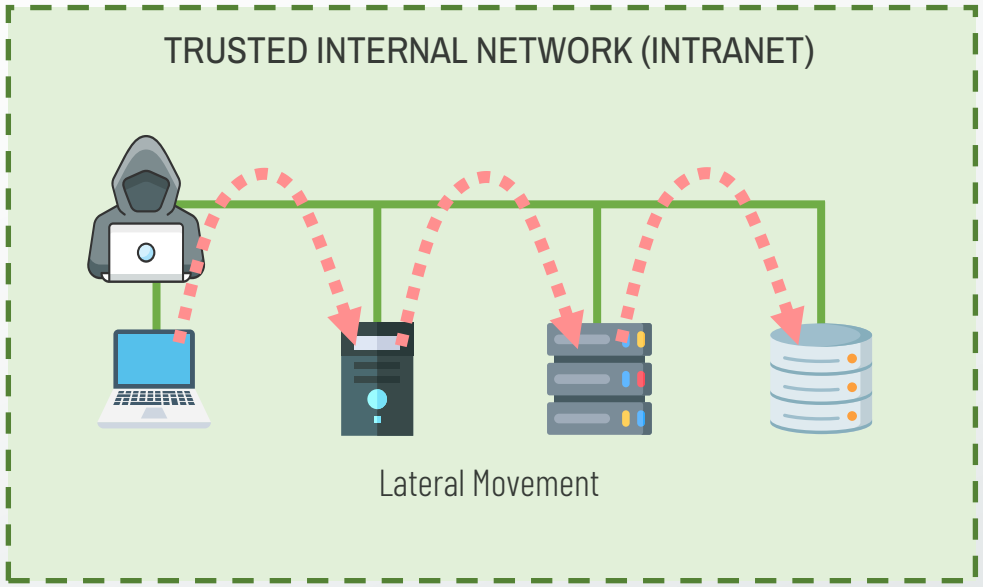
- Follows the same access process for all users.
- Since there's no implicit trust, a VPN connection isn't needed.

Department of Defense (DoD) Zero Trust Reference Architecture

East-West Segmentation

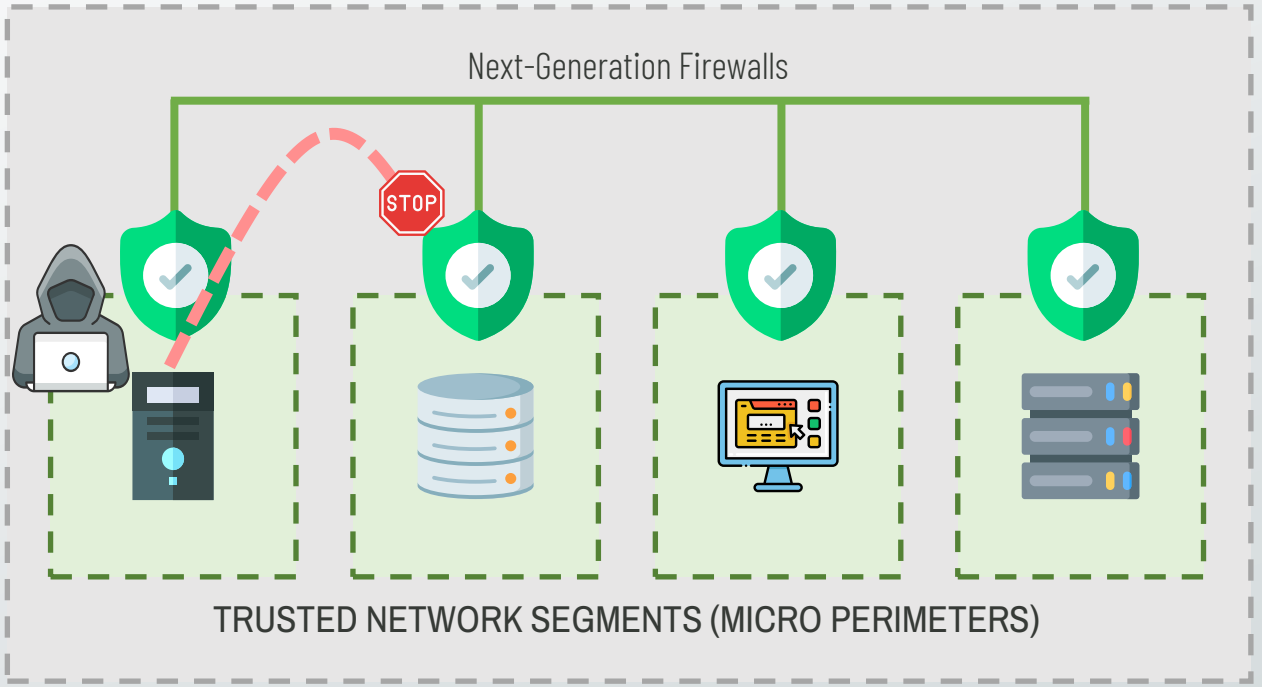
INSTRUCTOR ALTON

Conventional Design



- Intranets generally have a level of implicit trust.
- Implicit trust makes lateral movement possible.

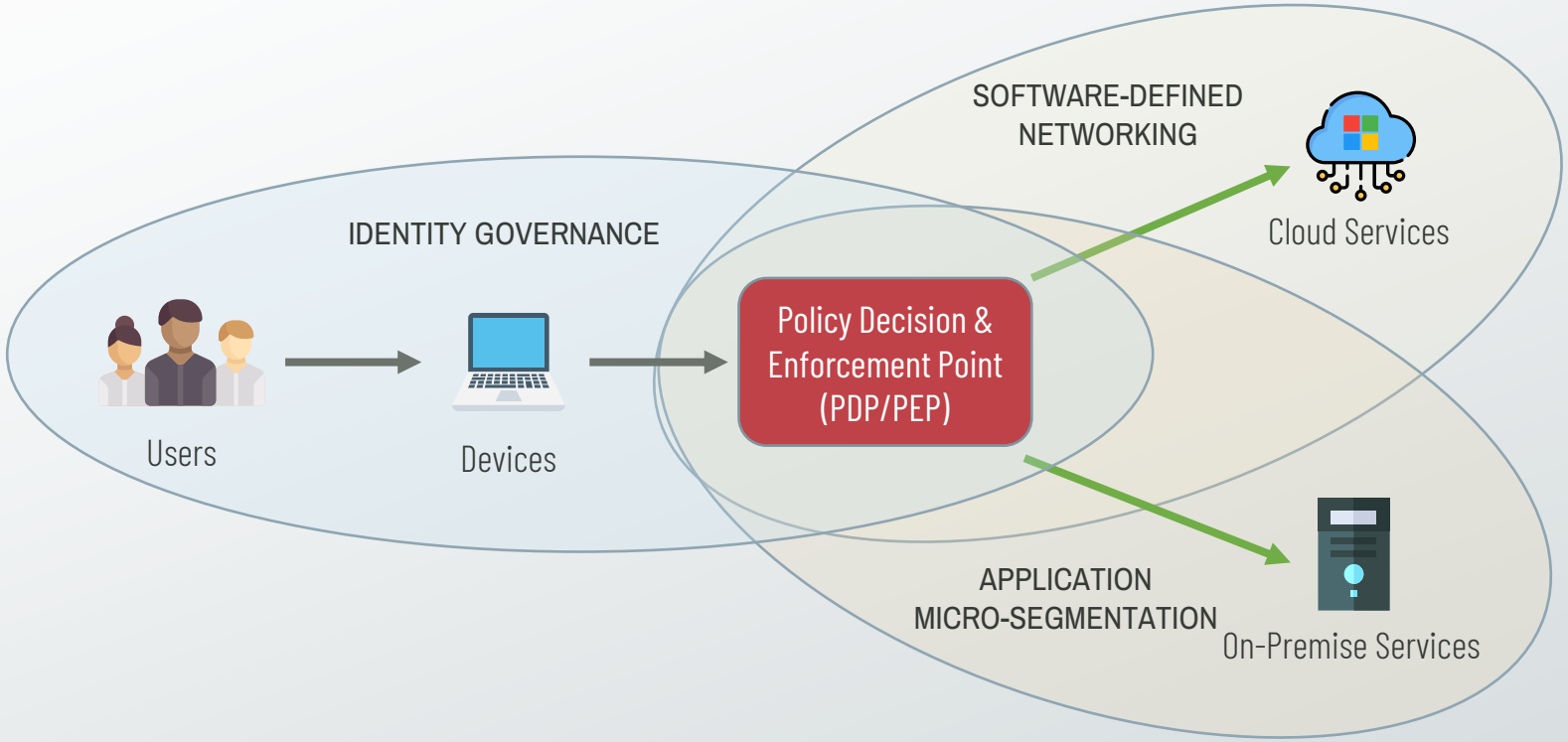
Zero Trust Design



- Designed to prevent lateral movement.
- Limits the blast radius of an attack.

Department of Defense (DoD) Zero Trust Reference Architecture

Secure Access From Anywhere



- **Identity Governance** focuses on identity management and access control.
- **Application Micro-Segmentation** places micro perimeters around trusted resources.
- **Software-Defined Networking** forms context-aware virtual networks for our assets at the network layer.

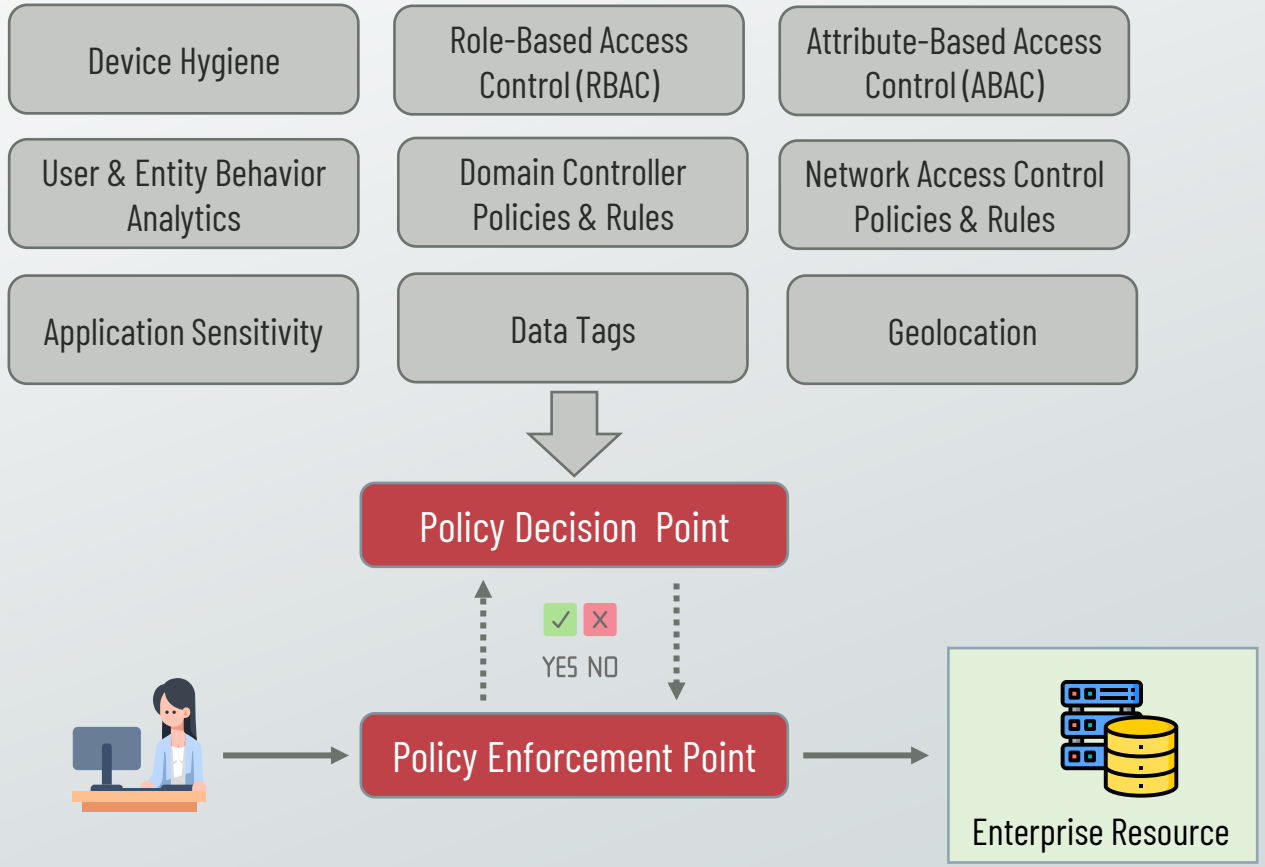
Conditional Authentication & Authorization

INSTRUCTOR ALTON

Conventional Design

- Authentication and authorization is granted based on location, role, username/password, PKI, and two-factor authentication:
  - ✓ Virtual Private Network (VPN)
  - ✓ Trusted Network Location (Intranet)
  - ✓ Role-Based Access Control (RBAC)

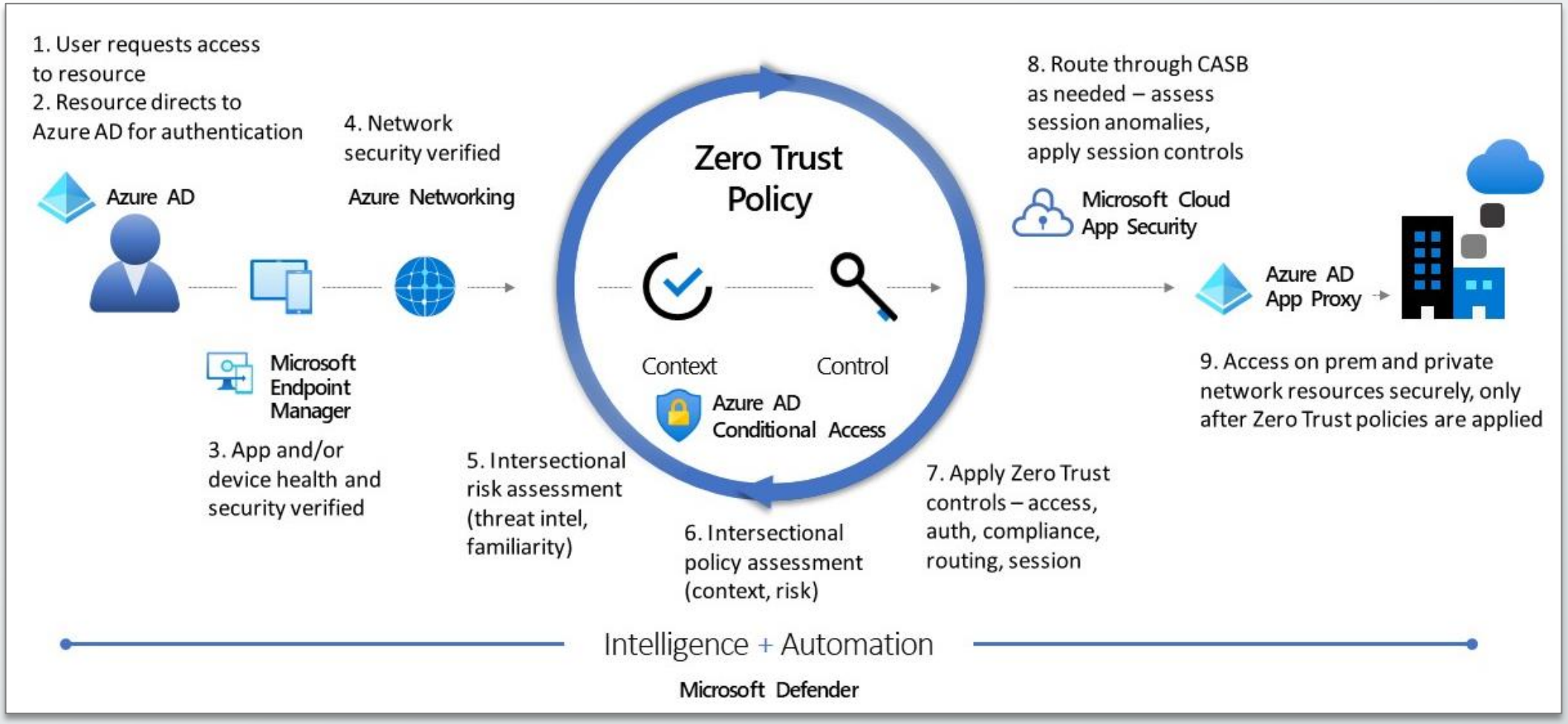
Zero Trust Design



- Utilizes a much more robust dynamic and contextual process.
- Considers device health, location, time, behavior, etc.

Department of Defense (DoD) Zero Trust Reference Architecture

Microsoft Zero Trust Step-by-Step



Microsoft: Using Zero Trust principles to protect against sophisticated attacks like Solorigate