Információbiztonsági megoldások az oktatási szektorban

Never Trust, Always Verify

2025

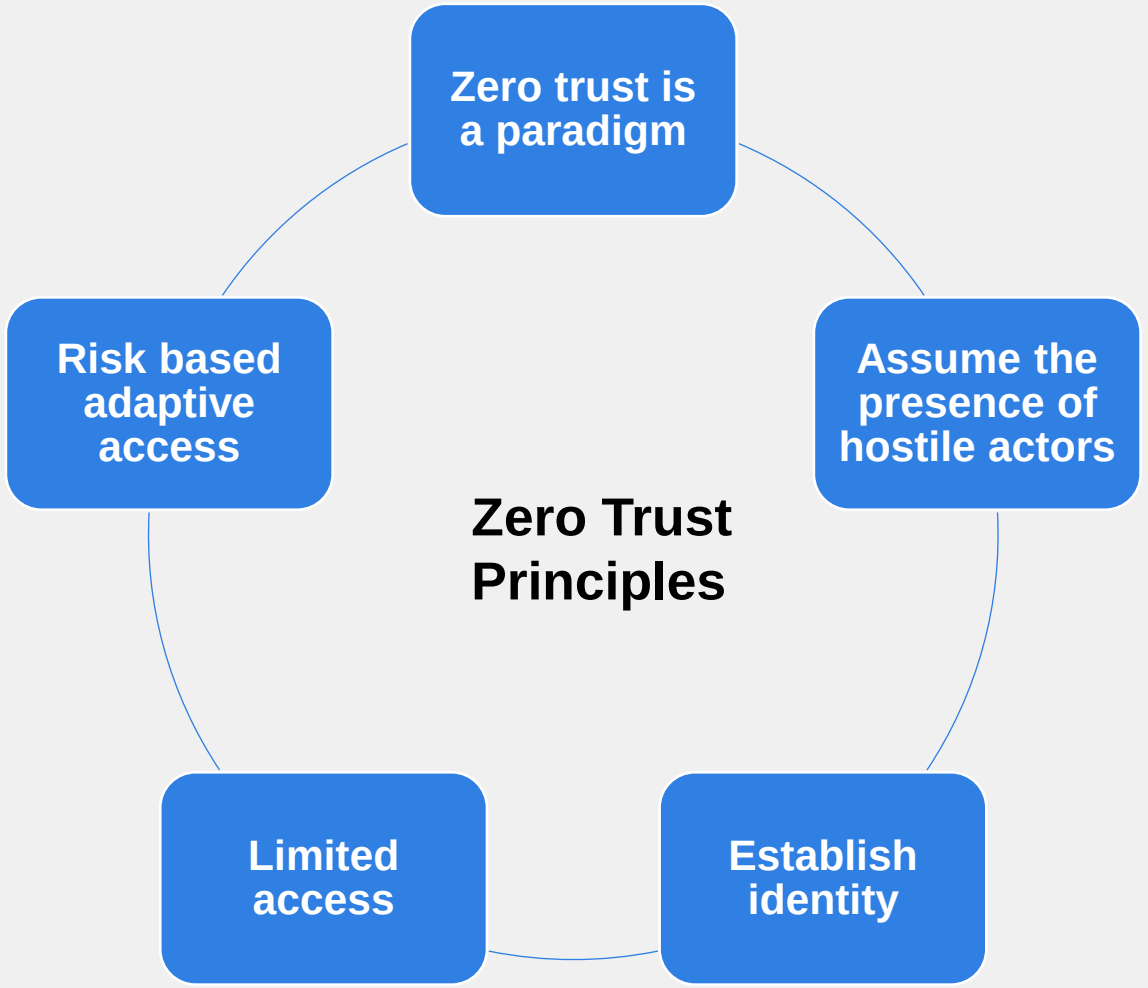
“Credentials are the currency of cybercrime"

- In 2024, over 100 billion records were shared in underground forums, a **42%** increase from 2023.
- The business of corporate infiltration:
  - Corporate VPN credentials (20%)
  - RDP access (19%)
  - Admin panels (13%)
  - Webshells (12%)
- *Well-known groups selling this type of information on the darknet provide the data and streamline these resources to make it easy for a threat actor of any skill level to carry out an attack successfully.*

Zero Trust Principles

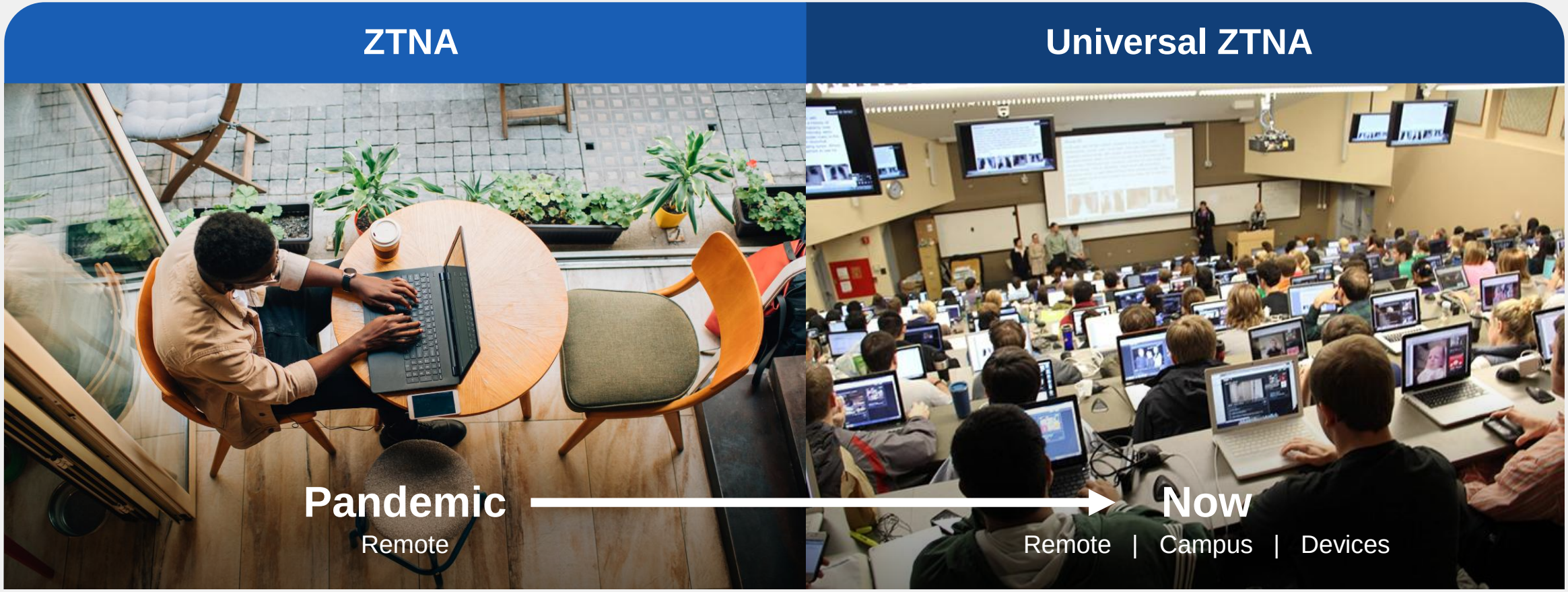
Never Trust, Always Verify for resource protection

- Grants network access only after identity is authenticated and authorized
- Limits network access only to necessary resources/applications
- Continuously adjusts network access in near real time, based on device/user context

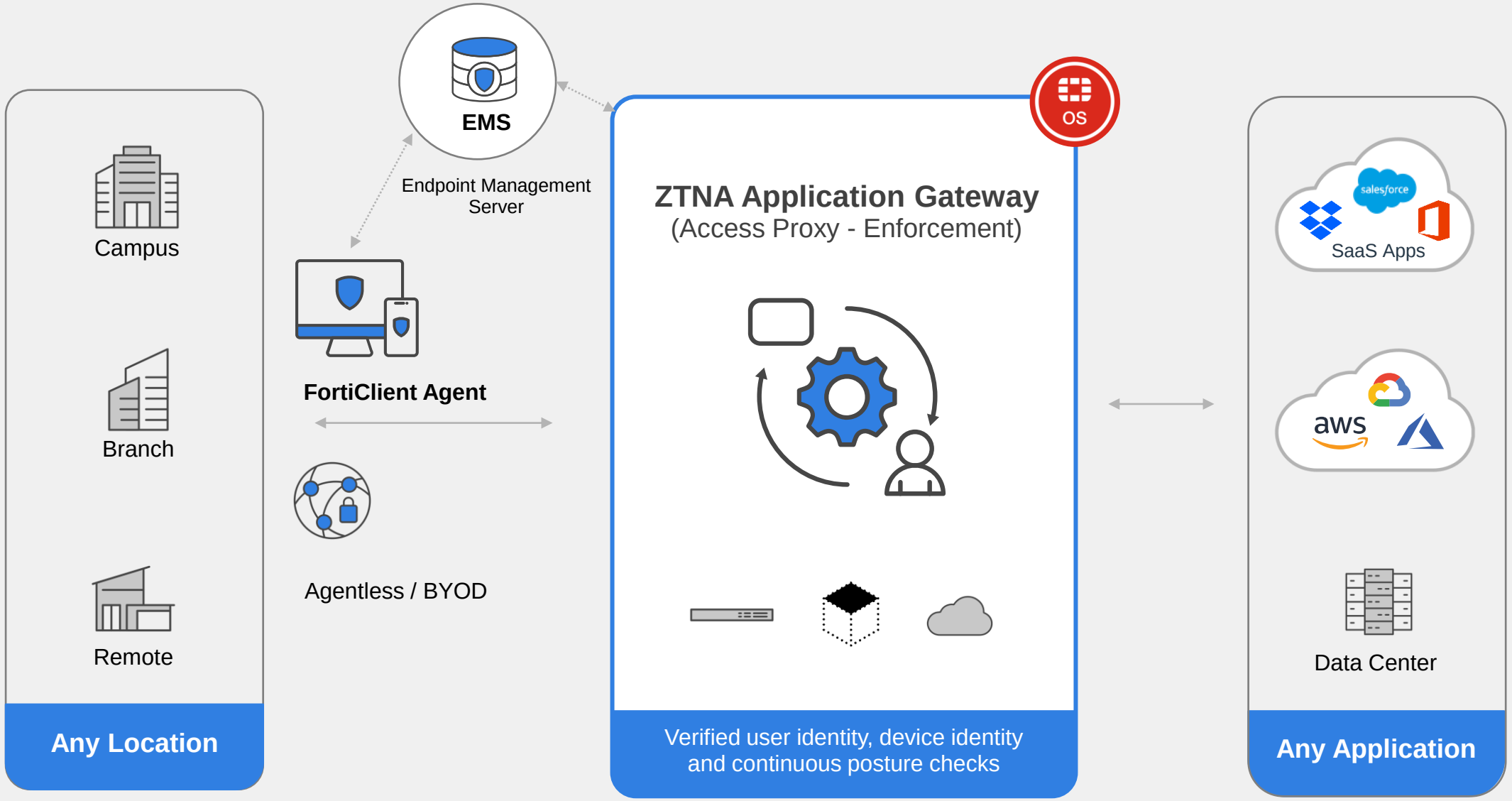


Source: Gartner

ZTNA: Moving to Universal ZTNA



Fortinet Universal ZTNA Solution



Security Posture Tags for Zero-Trust Access

Continuous Posture Assessment for ZTNA

Real-time Endpoints Posture using Tags

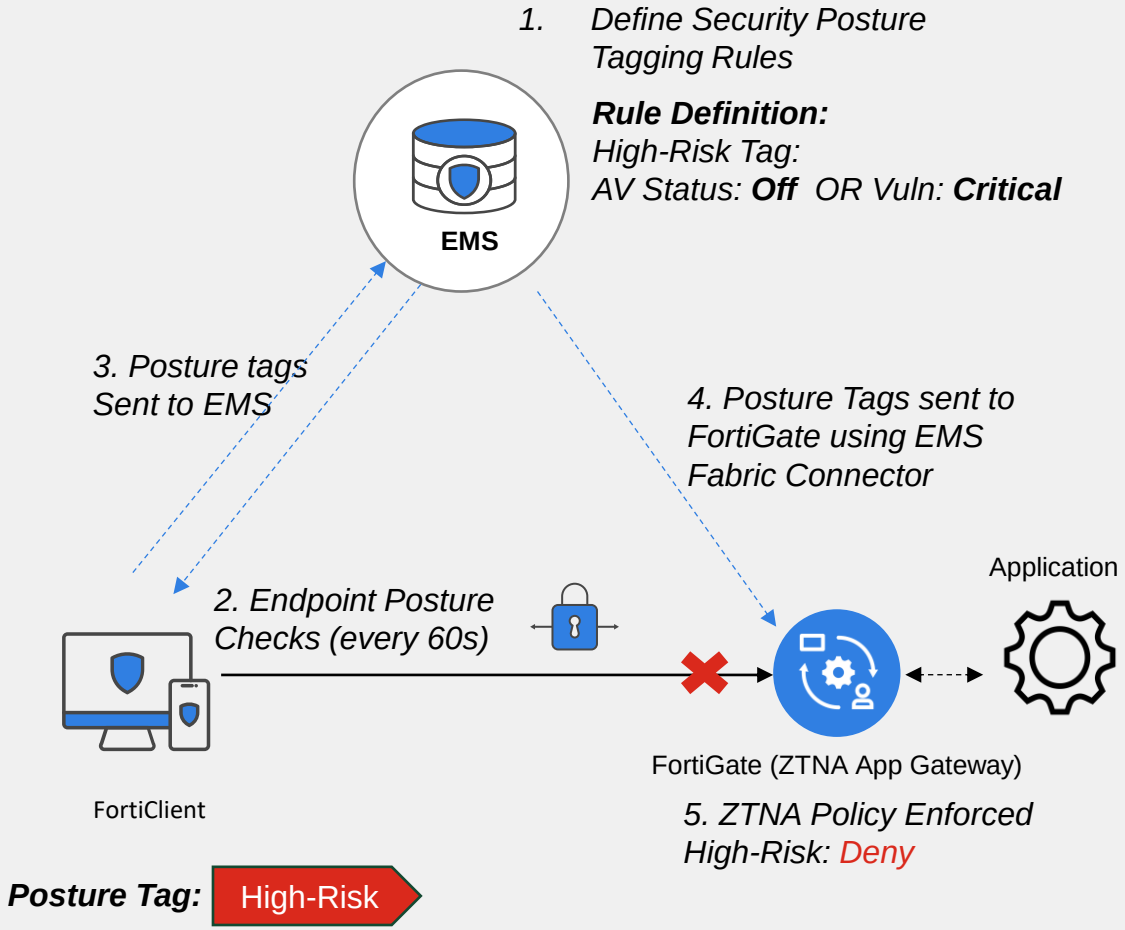
- Posture Tags are labels assigned to endpoints based on endpoint posture checks every 60s
- One or more tags can be assigned per endpoint

Flexible Posture Tagging Criteria

- Posture tagging rules can be based on multiple criteria
- *Example: AD Group, Domain, Endpoint Security (AV, EDR), OS, Vulnerability*

Policies based on Dynamic Posture Tags

- Tags can be used to as a part of ZTNA policies
- Tags also can be used as a part of NGFW/VPN policies to enhance security posture for IPSec VPN



Flexible and gradual transition to zero-trust model

Phase 1

- VPN with posture checks
- Posture checks **even before** VPN connection setup
- Continuous posture checks during VPN session

Phase 2

- ZTNA for select applications
- Target key applications to on-board (e.g., ERP, File servers)
- Continuous zero-trust posture validation per application session

Phase 3

- Expand ZTNA to more applications
- Integrate Endpoint Protection and EDR as a part of unified agent


FORTINET