safous | THINK YOUR ACCESS

ZTNA vs. Legacy Security Technologies: Decoding the Differences

As businesses embrace remote work and digital transformation, deploying more robust cybersecurity measures is becoming crucial. That need is fueling the popularity of zero trust network access (ZTNA).

Zero trust security, based on the "default deny" principle, requires users to be authenticated, authorized, and validated before they can access any resource.

Eye-opening statistics about ZTNA:

By 2023, **60%** **of enterprises** will replace legacy VPNs with advanced ZTNA solutions.[1]

By 2024, at least **40%** **of remote-access usage** will be served by ZTNA.[2]

The average cost of a data breach is **35%** **lower for companies** in the mature stage of zero trust deployment.[3]

ZTNA: A Closer Look

ZTNA uses the concept of zero trust security to deny access to a resource unless it's explicitly allowed. It enforces the principles of least privilege and micro-segmentation to prevent lateral movement within a network.

Benefits of ZTNA include:

- Ease of implementation
- Improved adaptability and scalability
- Tighter network security

ZTNA is sometimes used interchangeably with the term SDP, or software-defined perimeter. SDP solutions help establish a one-to-one connection between a user and the resources they want to access. Both ZTNA and SDP are built on the same three core pillars:

Identity-centric
Requires user authentication before granting network access

Zero trust
Applies the principle of least privilege

Cloud-centric
Operates natively in the cloud

Legacy Security Technologies

Traditionally, organizations used legacy technologies like virtual private networks (VPNs) to secure their data and applications. VPNs help establish a private connection for users on a shared network.

Legacy technologies come with risks that businesses can't afford in today's work-from-anywhere environments. They:

- ✗ Are designed to suit the needs of an on-premise workforce
- ✗ Don't protect resources once a user is granted access
- ✗ Don't use advanced technologies like network segmentation
- ✗ Involve higher implementation and maintenance costs

As the world settles into hybrid work arrangements and the attack surface expands, ZTNA is the clear choice over legacy security technologies. Ready to leverage state-of-the-art ZTNA solutions?

Get started with Safous.

Sources cited:

1. https://www.forbes.com/sites/forbestechcouncil/2021/10/01/why-sase-and-ztna-are-even-better-together-when-tightly-integrated/?sh=642158497e97
2. https://www.gartner.com/en/newsroom/press-releases/2021-06-22-gartner-forecasts-51-percent-of-global-knowledge-workers-will-be-remote-by-2021
3. https://www.ibm.com/security/data-breach