

ZTNA IN CYBER SECURITY

“TRUST NO ONE, VERIFY EVERYTHING”

TUTUL SIDDIQUE ARNOB
COUNTRY MANAGER- BANGLADESH, NEPAL & BHUTAN
ARRAY NETWORKS INC.



What is ZTNA?

- ZTNA is a security framework built on the principle of "never trust, always verify."
- It ensures that every user and device is authenticated, authorized, and continuously validated before gaining access.
- Unlike traditional security models, ZTNA does not assume trust within a network perimeter.



Is ZTNA a Philosophy or a Product?"

1

Philosophy: Zero Trust is a mindset or approach focused on securing access by verifying everything.

2

Product: ZTNA solutions are products developed to implement Zero Trust principles through features like identity management, encryption, and network segmentation

3

Conclusion: ZTNA is both—an overarching security philosophy and a set of products enabling this vision.



"How Does ZTNA Work?"

- 1 User/device authentication before accessing applications.
- 2 Verification of each access request.
- 3 No implicit trust; continuous monitoring of user and device behavior.
- 4 Network segmentation to limit access to only necessary resources.

"ZTNA's Role in the Cybersecurity Arena"

1

Mitigates insider threats and lateral movement.

2

Offers protection against modern threats like ransomware and phishing.

3

Enhances security in remote work environments (post-pandemic trend).

4

Integration with cloud services ensures secure access.

Why Endpoint Users Should Consider ZTNA"



Protection Beyond Network Perimeter: ZTNA secures endpoint devices even in public or untrusted networks.



Adaptive Security: Continuous verification of endpoint devices ensures they comply with security policies.



Zero Trust Extends to Endpoints: Devices are treated with the same "verify everything" approach.



Increased Attacks on Endpoints: Endpoint devices are major targets for cybercriminals.

Benefits of Adopting ZTNA

User can not be trusted

85%

Attack happen from Trust Zone

4%

Of end-users will
click on anything¹

28%

of attacks involved
inside actors¹

17%

Of breaches
had errors as
casual events¹

1



Stronger control
over user access
and data flow.

2



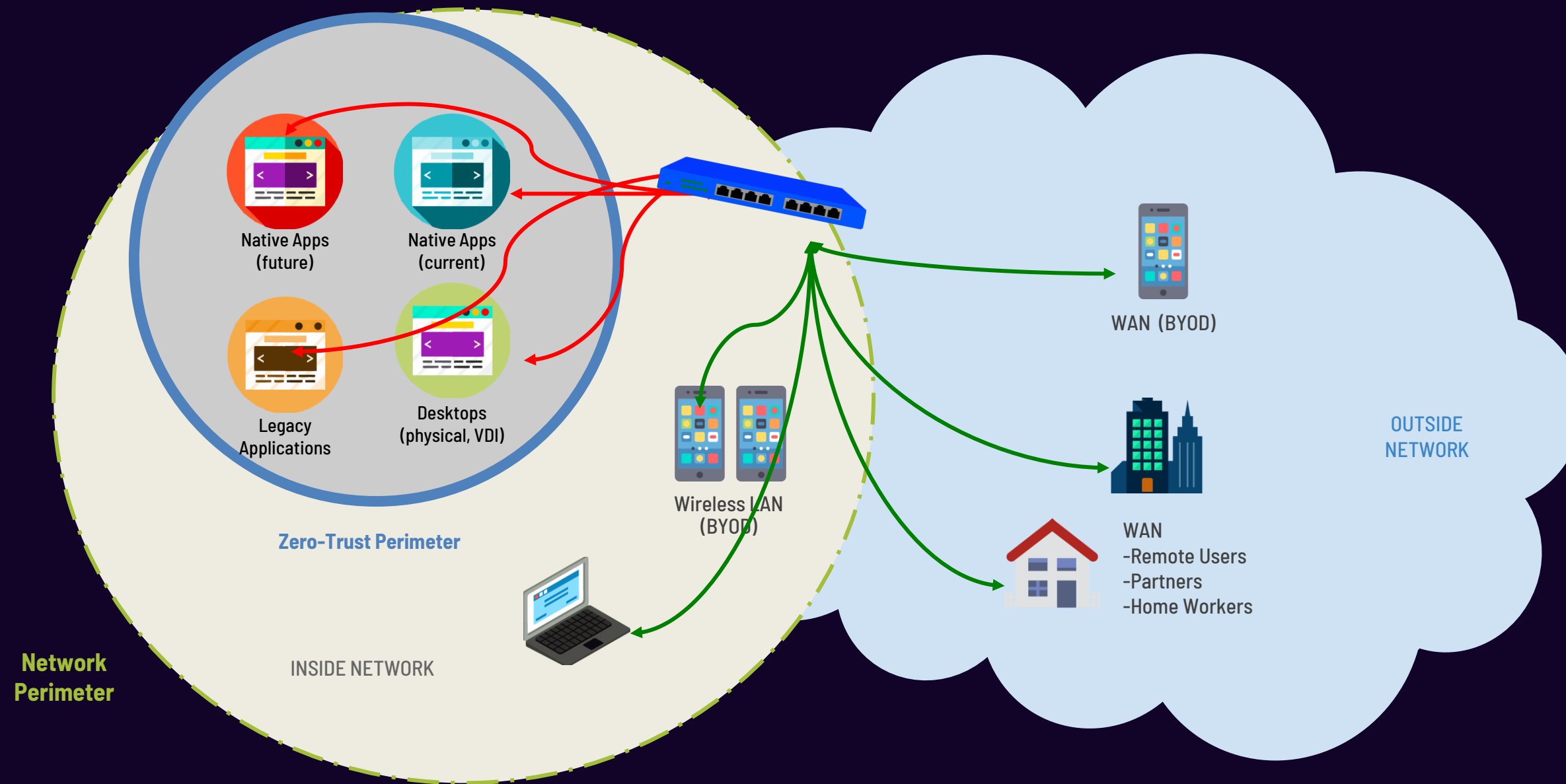
Enhances compliance
with data privacy laws
and regulations.

3



Simplifies securing
remote workforce and
cloud applications.

ZTNA: A Necessity for Modern Security



ZTNA is a crucial strategy and tool in defending against modern cybersecurity threats.

Endpoint users, just like network administrators, must adopt a Zero Trust mindset.

Explore ZTNA solutions today to enhance your organization's cybersecurity posture.



THANK YOU!