2024 EMA Zero Trust Networking Study

HOW NETWORK TEAMS SUPPORT CYBERSECURITY



ZERO TRUST ZERO TRUST

ZERO TRUST

ZERO TRUST

ZERO TRUST

ZERO TRUST

ZERO TRUST

ZERO TRUST ZERO TRUST

BENEFITS & CHALLENGES

Zero trust (ZT) has resulted from network perimeters alone being no longer viable, especially for hybrid IT environments.

The ZT model brings many benefits:

TOP Benefits



But implementation has proven challenging:

TOP Challenge

Budget constraints

WHY NETWORK TEAMS ARE KEY FOR SUCCESS

The cybersecurity group typically spearheads ZT security.

But network technology & tools like segmentation & observability are foundational components of ZT implementation.

Network teams ensure performance and UX remain optimal in ZT architectures.

What Orgs View as Requirements for Success



Network team is equal partner to security team 44% Observability and monitoring tools 96%

Maintaining optimal network performance 60%

Network infrastructure teams are key enablers of a zero trust strategy.



DO NOT ENTER \\\

DO NOT ENTER

DO NOT ENTER DO THE FUNDAMENTAL ROLE OF DNS

DNS solutions are critical for reducing the attack surface of any organization adopting ZT, bringing value in policy enforcement, segmentation, and threat detection.

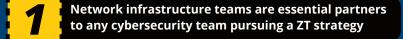
DNS role in ZT strategy

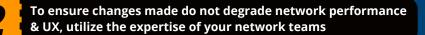
Policy enforcement via DNS filtering/domain blocking

DNS-based network



TOP 3 TAKEAWAYS FROM THE EMA REPORT





Leverage your DNS to optimize ZT network segmentation, policy compliance, and threat detection via observability



GET THE FREE EMA REPORT

