Executive Summary

Traditional network security models have faced unprecedented challenges in adapting to the demands of a rapidly changing digital environment. As businesses embrace digital transformation and become increasingly cloud-native, mobile, and interconnected, the corporate network perimeter is gradually disappearing, exposing users to malware, ransomware, and other cyber threats. Traditional perimeter security tools no longer provide adequate protection from these threats. But even more so, traditional remote access solutions like virtual private networks (VPN) can no longer ensure the scalability and performance needed for the increasingly mobile and remote workforce.

VPN is a typical example of a technology that was never designed for the purposes it is used nowadays. Besides creating potential bottlenecks by forcing companies to backhaul remote users' traffic to a central location and thus negatively affecting performance and productivity, VPN appliances grant those users full, uncontrolled access to entire local area networks (LANs). This dramatically expands the attack surface of corporate networks, provides easy lateral movement for potential attackers, and enables uncontrolled access to internal resources with implicit trust.

Unlike traditional perimeter-based security models that assume trust within the network, Zero Trust Network Access (ZTNA) adopts a more granular and identity-centric approach. An infrastructure designed around this model treats every user, application, or resource as untrusted and enforces strict security, access control, and comprehensive auditing to ensure visibility and accountability of all user activities. This Zero Trust philosophy has become increasingly relevant as organizations grapple with the proliferation of remote work, cloud adoption, and the growing sophistication of cyber threats. It is also important to emphasize that Zero Trust is not only about networks, but about identities, devices, systems, and applications. It is about ubiquitous and continuous verification of device security and identity authentication.

As a concept, ZTNA is based on the assumption that any network is always hostile, and thus, any IT system, application, or user is constantly exposed to potential external and internal threats. Often expressed as "never trust, always verify," ZTNA is an embodiment of the principle of least privilege, and at its core mandates that every access request be properly authenticated and authorized. Proper access management in service of ZTNA means considering the requesting user's attributes, authentication and environmental context, permissions and roles, source device information, and the requested resource attributes. Zero Trust Architecture implies a concept where clients can access services from everywhere, not relying only on internal network security mechanisms.

This approach ensures that access policies can be defined in a much more granular fashion per individual application or service by establishing secured point-to-point tunnels between clients and services. Each of these sessions is always authenticated and continuously monitored to prevent malicious activities. Access and security policies are managed centrally and enforced across hybrid IT environments (on-premises, multi-cloud, or mobile).

One of the fundamental misconceptions the industry experts are still struggling to explain to the public is that Zero Trust is not an off-the-shelf product, but a journey that begins with a