Data in Motion: A Blind Spot in Your Zero Trust Security Strategy?

Zero trust security strategies have primarily focused on protecting data at rest and data in use, leaving the security of data in motion reliant on outdated VPN technologies or limited SD-WAN implementations. Data can be classified into three states:

- **Data at Rest:** Data stored on devices, servers, or cloud storage. Typically secured through encryption, access controls, and physical security measures.
- **Data in Use:** Data actively being processed by applications or systems. Secured using techniques like memory encryption, secure enclaves, and runtime application self-protection (RASP).
- **Data in Motion:** Data being transmitted across networks, between devices, or between cloud services. Data in motion isexposed to potential interception, tampering, or unauthorized access during transmission.

Traditional security solutions like SD-WAN and VPN provide some protection for data in motion by encrypting data and securing communication channels. However, as quantum computing advances, the encryption algorithms used by these solutions become vulnerable to quantum attacks, rendering them less effective. Moreover, these solutions do not protect data in motion that moves in and out of these environments over untrusted networks, leaving data at risk of network tapping and encryption threats.

The biggest technical and security risks to your data in motion include:

- **Interception and Eavesdropping:** Unauthorized parties can intercept and access sensitive information transmitted over untrusted networks.
- **Man-in-the-Middle (MitM) Attacks:** Attackers can intercept and alter data in transit, compromising data integrity, confidentiality, and leading to unauthorized access.
- **Untrusted Network Connections:** Transmitting data over untrusted or public networks without protocols, packet obfuscation, and multi-path routing significantly increases the risk of interception.
- **Lack of Encryption:** Unencrypted data transmissions are easily readable by anyone who intercepts the data, exposing sensitive information and violating privacy and compliance requirements.
- **Weak Encryption Algorithms:** Using weak or outdated encryption algorithms with insufficient key lengths or weak encryption protocols makes data vulnerable to decryption by attackers.
- **Malicious Network Nodes:** Compromised or malicious nodes in a network can intercept, modify, or redirect data traffic.
- **Data Leakage:** Misconfigurations, software vulnerabilities, or human errors can expose data to unauthorized parties through unintentional data leakage during transmission.
- **Insider Threats:** Malicious insiders with access to network infrastructure can intercept and steal data in transit – zero trust transit means you cannot trust the humans running the network any more than the network itself.
- **Insufficient Access Controls:** Weak or improperly implemented access controls, Inadequate authentication, authorization, and network segmentation can expose data to unauthorized access.

About SCATR

We are the data camouflage company.
Born out of warfighter requirements, and inspired by the animal kingdom's ability to use camouflage to outsmart its predators, we have developed a patented, quantum-resistant technology that protects data in motion and the enterprises and people who rely on it.

For a demo and more information, contact info@scatr.it