SCATR: The Most Resilient Zero Trust Transit Network Ever Created

SCATR is a resilient, decentralized, and self-healing Zero Trust Transit solution for securing an organization's data in motion. SCATR's patented data camouflage solution combines packet and protocol configuration with a multi-path routing capability that securely routes data across any IP-based transit path. This results in unprecedented security and resilience for an organization's data in motion — even in the face of failures or adverse network conditions.

What makes SCATR so resilient?

- **Decentralization:** SCATR is based on a decentralized IP transit architecture, where the control and management of the data in transit are distributed among multiple nodes, from providers located in most countries worldwide—preventing a single point of failure or adversary from bringing down the entire network.

- **Redundancy:** SCATR incorporates redundancy throughout the entire data transit process, including multiple IP pathways (IXP, ISP, Satellite, Cellular, IoT, etc.) and redundant relay nodes.

- **Self-healing:** SCATR can automatically detect, diagnose, and recover from failures without human intervention. Our intelligent multi-path packet routing uses automatic failover, so packets are automatically rerouted to healthy transit paths when a failure or significant drop in network performance is detected.

- **Adaptive routing:** SCATR employs intelligent routing protocols that can dynamically adapt to changing network conditions, such as link failures or congestion. These protocols find alternative paths to maintain connectivity and optimize network performance.

- **Diversity:** SCATR uses a diverse mix of IP-based transit providers globally to ensure that there is always a path for an organization's data to securely transit through — be that IXP, Satellite, mobile, ISP, or even IoT.

- **Command and Control:** SCATR Command and Control (C2) provides comprehensive monitoring and management tools to continuously track network health and performance of an organization's data in transit, allowing complete visibility and full command and control of multi-path routing, no matter what network the data in motion is running over.

- **Security:** SCATR incorporates strong security measures to protect against cyber threats, such as intrusion detection systems, firewalls, and encryption. These measures help prevent unauthorized access, data breaches, and other security incidents that could compromise network availability.

- **Scalability:** SCATR scales gracefully as an organization's data transit requirements grow in size and complexity - allowing seamless addition of new IP transit providers and new secure relay nodes without compromising resilience or performance.

-

Discover how effortless it is to implement resilient Zero Trust Transit for your organization. Click here to get started!

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