SCATR: Quantum-Proof Zero Trust Transit

SCATR combines advanced data camouflage techniques, a resilient IP network fabric, and a zero-trust security model to provide a comprehensive, quantum-proof solution for protecting an organization's data in motion. Our relentless focus on post-quantum readiness positions us as a future-proof solution for organizations seeking to secure their data in motion in the face of evolving adversarial and technological threats.

Advanced Data Camouflage: SCATR doesn't just obfuscate traffic—it camouflages data-packets and flows to seamlessly blend with the existing IP transit environment. By intelligently mimicking established NetFlow signatures on a packet-by-packet basis, SCATR renders its communications indistinguishable from recognized baseline patterns. This advanced obfuscation technique goes beyond basic encryption or VPNs to prevent any abnormal traffic characteristics from being detected in the first place. By impersonating known NetFlow protocols, SCATR renders an organization's data in motion indistinguishable from all other traffic. This data camouflaging prevents traffic patterns from being effectively identified, analyzed, or leveraged for reconnaissance.

Resilient IP Network Fabric: SCATR creates an unparalleled level of path diversity and resilience by dynamically routing traffic across a mesh of diverse transit providers and paths, in nearly every corner of the globe. Camouflaged data is intelligently split and load-balanced across multiple paths, whether on IP, mobile, or Satellite networks. SCATR intelligently recognizes when a path or paths have gone down or been degraded and re-routes traffic to available paths with the least amount of latency. This maximizes resiliency

and speed, as a significant outage or delay on any single path has minimal impact as packets intelligently reroute across the remaining pathways. The SCATR multi-path capability delivers true route redundancy and fail-safe reliability.

Quantum-Proof: SCATR's obfuscation and path diversity undermine the fundamental requirements for quantum computing's code-breaking capabilities. Quantum's advantage comes from being able to observe complete data flows to then analyze and decrypt them. However, SCATR's data camouflaging and multi-path routing create scenarios where adversaries cannot get a comprehensive observation of the data flows. Without full visibility into the traffic patterns and paths, quantum computing is stripped of the "complete observation" it needs, rendering it ineffective. This quantum-proof design provides security assurance even as quantum computing paradigms evolve.

SCATR camouflages data to blend into normal network activity, splinters data across multiple pathways to ensure resilience, and undermines attack vectors that rely on being able to monitor and analyze full traffic flows. This makes SCATR an incredibly robust solution for secure, available, and obfuscated communications even in the most high-threat and quantum-capable environments.

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