SCATR: Protecting Our Warfighters' Data in Motion

The situation: Warfighters across the globe are utilizing traditional NSA Type 1 encryptors to connect to sensitive data in motion.

The problem: Every time a Type 1 encryptor is activated, adversaries can easily detect the location, time, and duration of the VPN connection, leaking valuable information about the warfighters pattern of life and systems that they connect to. Once the connection is established, they can also monitor valuable metadata that accompanies the VPN connection. This provides adversaries with a real-time attack surface to monitor and allows them to prepare for various threats, ranging from DDoS flooding attacks to quantum analysis of encrypted data and kinetic targeting of our personnel.

The solution: SCATR Zero Trust Transit offers a powerful solution to this critical security challenge. By leveraging SCATR's advanced data camouflage techniques and multi-path routing capabilities, SCATR effectively eliminates the signature of our DoD employees and warfighters' connections. This makes it significantly more difficult for adversaries to gather valuable intelligence on their locations, movements, and data in motion.

Key benefits of SCATR:

- **Obscured Connection Signatures:** SCATR camouflages the network traffic generated by Type 1 encryptors, making it virtually indistinguishable from regular traffic. This prevents adversaries from identifying the specific times, locations, and durations of our warfighters' connections.

- **Protected Metadata:** By obfuscating the metadata associated with VPN connections, SCATR MOBI prevents adversaries from gleaning valuable information about our personnel's activities and communications.

- **Mitigated Attack Surface:** With SCATR the real-time attack surface that adversaries can monitor is significantly reduced. This makes it much harder for them to plan and execute targeted attacks against our networks and personnel.

- **Enhanced Data Security:** SCATR's quantum-proof data camouflage techniques ensure that even if adversaries intercept our data in motion, they will be unable to decipher it or use it for malicious purposes.

- **Improved Operational Security:** By safeguarding the digital footprints of our DoD employees and warfighters, SCATR contributes to overall operational security, reducing the risk of compromised missions and personnel.

Implementing SCATR across our DoD networks is a critical step in protecting our warfighters and ensuring the security of data in motion. By eliminating the signature of their connections and protecting valuable metadata, we can significantly reduce the intelligence that adversaries can gather, enhancing the safety and effectiveness of our personnel in the field.

To learn more about how SCATR can protect your organization's data in motion, click here.

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