When data is not encrypted it can be easily ‘tapped’ or misdirected by cyber-criminals. These criminals can also ‘inject’ data into the link, and potentially override controls on entire systems.

With a signal loss less than 1dB, fibre tapping is practically undetectable.

So, if you can’t prevent or detect fibre tapping, how do you secure your data-in-motion?

You need to **encrypt**.

By using Traffic Flow Security (TFS) you can guard against the risks associated with malicious traffic analysis ensuring your data and metadata are protected.

Compared to IPSec (Layer 3), Layer 2 secure encryption can boost network performance by up to 50%.

Traffic Flow Security (TFS) makes traffic looks consistent without patterns or characteristics.