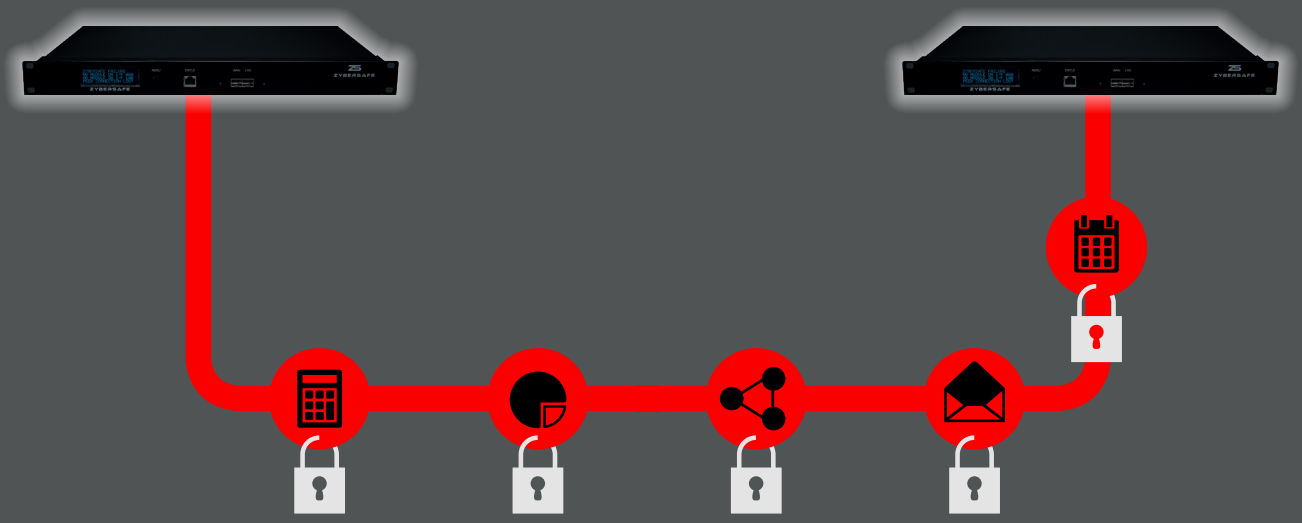
ZYBERSAFE



PRODUCT BRIEF

Zybersafe TrafficCloak – Securing Data-in-Motion

Zybersafe TrafficCloak

At the heart of every communication network today is infrastructure providing connectivity between locations and points. Securing Data-in-Motion, Zybersafe's ethernet encryption products offer a transparent, wire-speed encryption service on fiber or copper links up to 10Gbps.

Risks and dangers

Companies are under increasing pressure to further protect intellectual property rights and privacy against espionage and criminal activities. Criminal organizations and states that want to access private data are becoming increasingly creative in surveying, manipulating and stealing this data. Therefore, securing Data-in-Motion is paramount.

Key Features

- Strongest crypto technology available, AES256-GCM
- Full-Duplex real-time encryption
- Keys are not user manageable/accessible
- Key generation from HW Random Number Generator
- Man-in-the-middle and replay protection of transmitted data
- Authentication and data integrity secured
- Supports 1 G, 10 G or 100 G ethernet point-to-point links
- Encryption of unicast, multicast and broadcast traffic
- Network integration without any change of infrastructure (virtual wire)
- Highly scalable
- No impact on existing redundancy mechanisms
- Designed to comply to FIPS 140-2 L3 and Common Criteria EAL4
- CE compliant

Protective measures

It is impractical to monitor the entire optical fiber network, and as such the only real preventive solution to protect information is to encrypt the data before it goes through the network.

Due to the often sensitive nature of data, particularly from financial institutions, insurance companies, public administration, or from the pharmaceutical and chemical industries, it is paramount that the privacy and reliability of the information carried is guaranteed, as the stakes and risks involved are extremely high.

Wiretapping – a serious threat

Most people take it for granted that if you transfer sensitive data over the public Internet you need to secure the transfer through some kind of encryption. However, there is a general misconception that this does not apply if the data transfer takes place over the company's own fiber infrastructure, as the fiber technology is inherently secure. However, data sent through fiber cables are not automatically protected and can easily be accessed with the right equipment. Therefore, companies need to secure the data traffic that traverses external fiber lines by implementing encryption.

How do they do it?

Hacking a fiber cable is no more difficult than any other type of hack, wired or wireless. Optical network exploits are accomplished by extracting light from the ultra-thin glass fibers.

- The first step is to gain access to the fiber-optic cable
- The second step is to extract light from the cable
- The third step is to extract data from the cable

Bending is the easiest method. By using the clip-on coupler creates a small micro-bend in the cable allowing a small portion of the light to escape from the cable. Once the light has been accessed, the data is captured using a photo detector. It is very difficult to detect, since there is no interruption to the signal.

Corporate Overview

Zybersafe is an innovative danish company specialized within building hardware encryption solutions.
We focus on building security products that ensure the highest level of protection for Data-in-Motion.