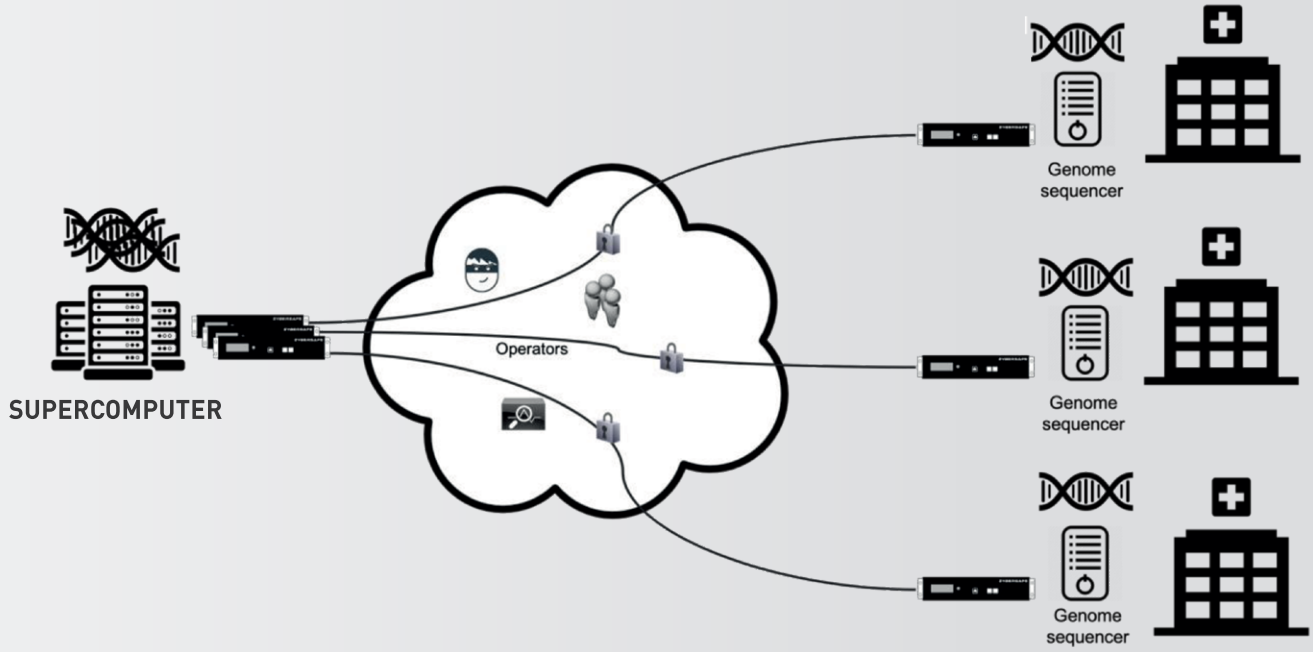

CASE STUDY

Encryption of sensitive Healthcare Data

Background

Most enterprises have very specific lock down procedures for protection of the perimeter. But that is not the case for data transmissions. While there is a strong focus on perimeter security and the protection of local network boundaries, large amounts of sensitive data are still transmitted unprotected through WAN connections. The main reason for this is a general assumption that, if you purchase a dedicated fiber or MPLS connection from an operator, the data is inherently isolated and secure. This is in no way the case.

Although the operators make every effort to protect their customers data, there is no guarantee that a data breach cannot happen inside the operators' infrastructure. This is something that worries the department for genome medicine at Rigshospitalet in Copenhagen. They handle some of the most sensitive data that anyone can come across; complete mappings of patients' genes.

Therefore, when the department for genome medicine at Rigshospitalet, had to connect their genome sequencing machines to the Danish National Supercomputer for Life Sciences (COMPUTEROME at DTU in Risø), they had to use high-speed fiber connections on an independent operator-owned fiber network.

Since they have no control of the data once it resides on the operators' infrastructure, they decided to protect the Genome information by encrypting all data transmissions to and from the COMPUTEROME site.

Because the network infrastructure is managed by the operator, they needed to implement the encryption without having to reconfigure or re-architect the network.

Solution requirements

The encryption solution had to integrate with existing network infrastructure without a need for massive reconfigurations or re-architecting of the network.

Rigshospitalet deployed redundant encryption appliances as an extra security measure.

Redundancy allows for hot failover to a secondary encrypted circuit, guaranteeing that the data will remain protected and available in the rare event of an encryption appliance or network infrastructure failure.

Key benefits

Rigshospitalet needed a scalable encryption solution that was quick and easy to install, simple to manage and did not compromise their network performance.

Based on a successful pilot project, Rigshospitalet implemented the Zybersafe TrafficCloak nCryptor solution, which offered all of the capabilities required for deployment. With its transparent nature and capability of being deployed onto their existing network without any re-architecting, the solution was a natural fit.

Key features

- Strongest cryptography technology, AES 256-GCM
- Designed for security
- Immune to Man-in-the-Middle attacks (Data Integrity control)
- 1, 10 and 100Gbps encrypted throughput
- Low Latency (<5 microseconds)
- Completely transparent to payload
- Embedded and tamper-proof key management

zybersafe.com

About Zybersafe

Zybersafe is an innovative, Danish company that specializes in designing hardware encryption solutions and has many years of proven experience and expertise in securing highly sensitive data. We focus on designing security products that ensure the highest possible level of protection for data in motion. Our objective is to provide products that are easy to implement and can protect our customers' valuable and private information from wiretapping without compromising on performance.