conference 2017

CyberSecurity4Rail

October 4th · Hotel Thon EU · Brussels

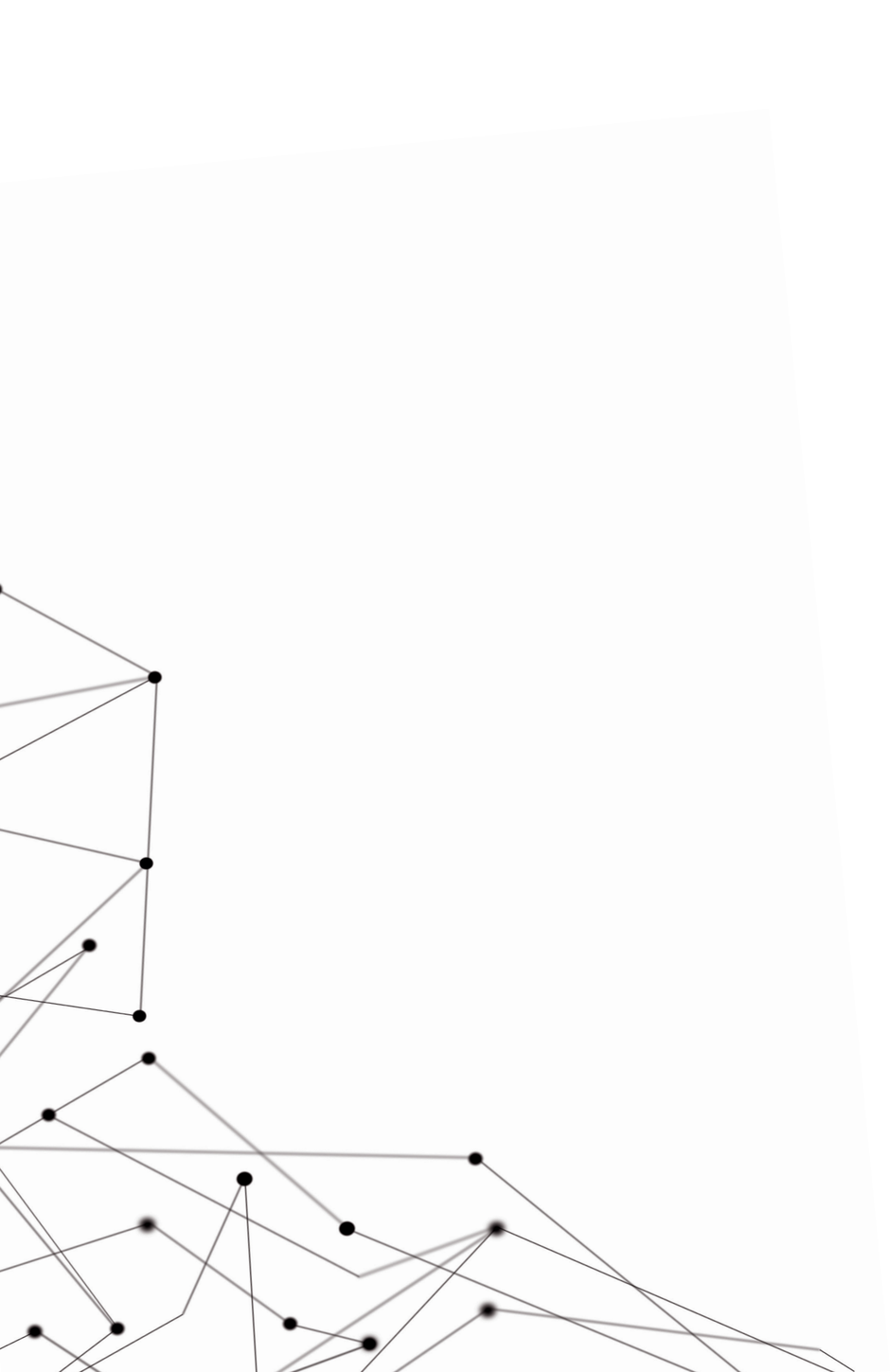
Are your services protected
against cyber criminals?

This Conference will prepare you!

hitrail

european railway IT & data communications

conference 2017
CyberSecurity4Rail

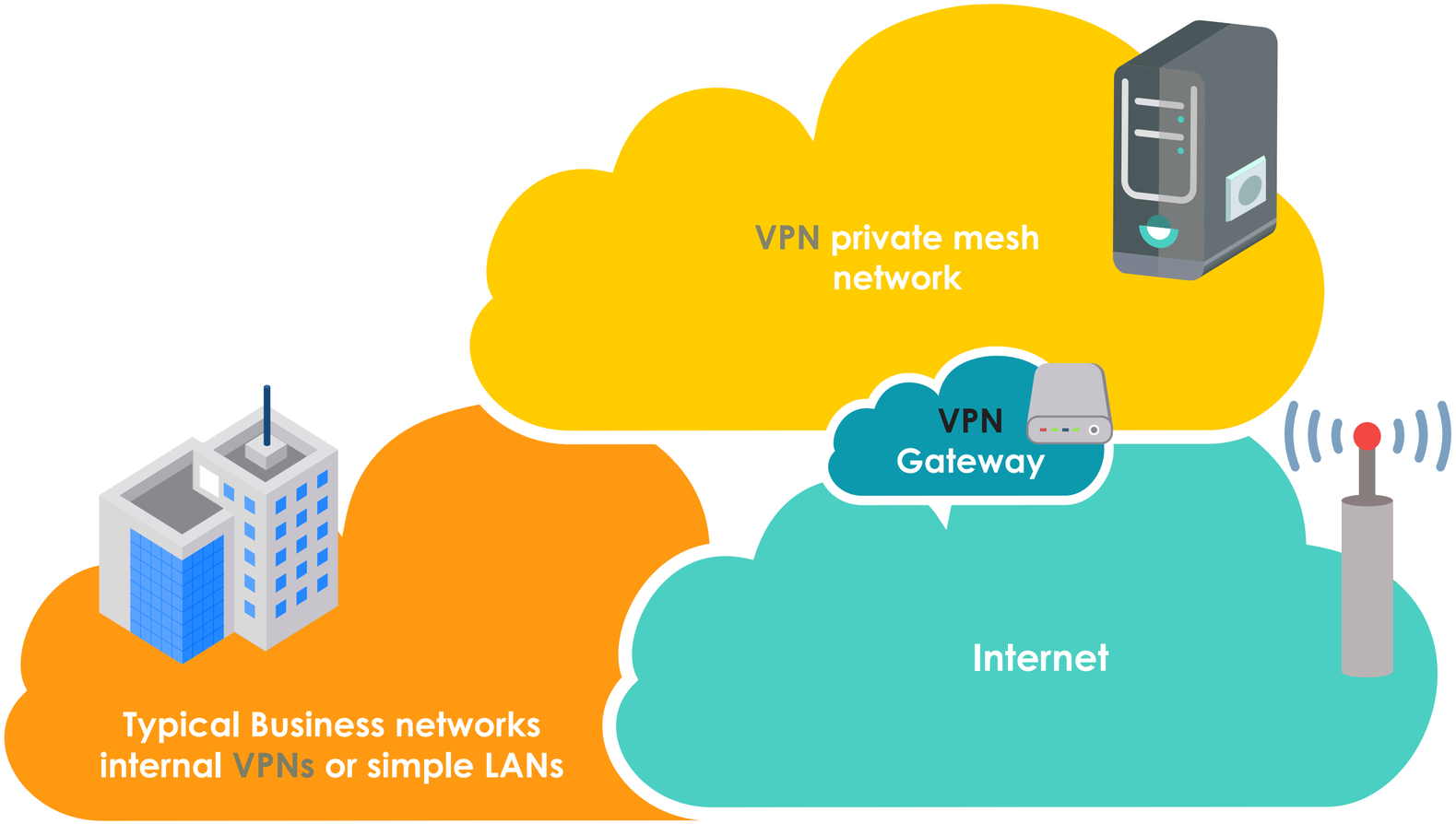


Secure networks for collaborative services

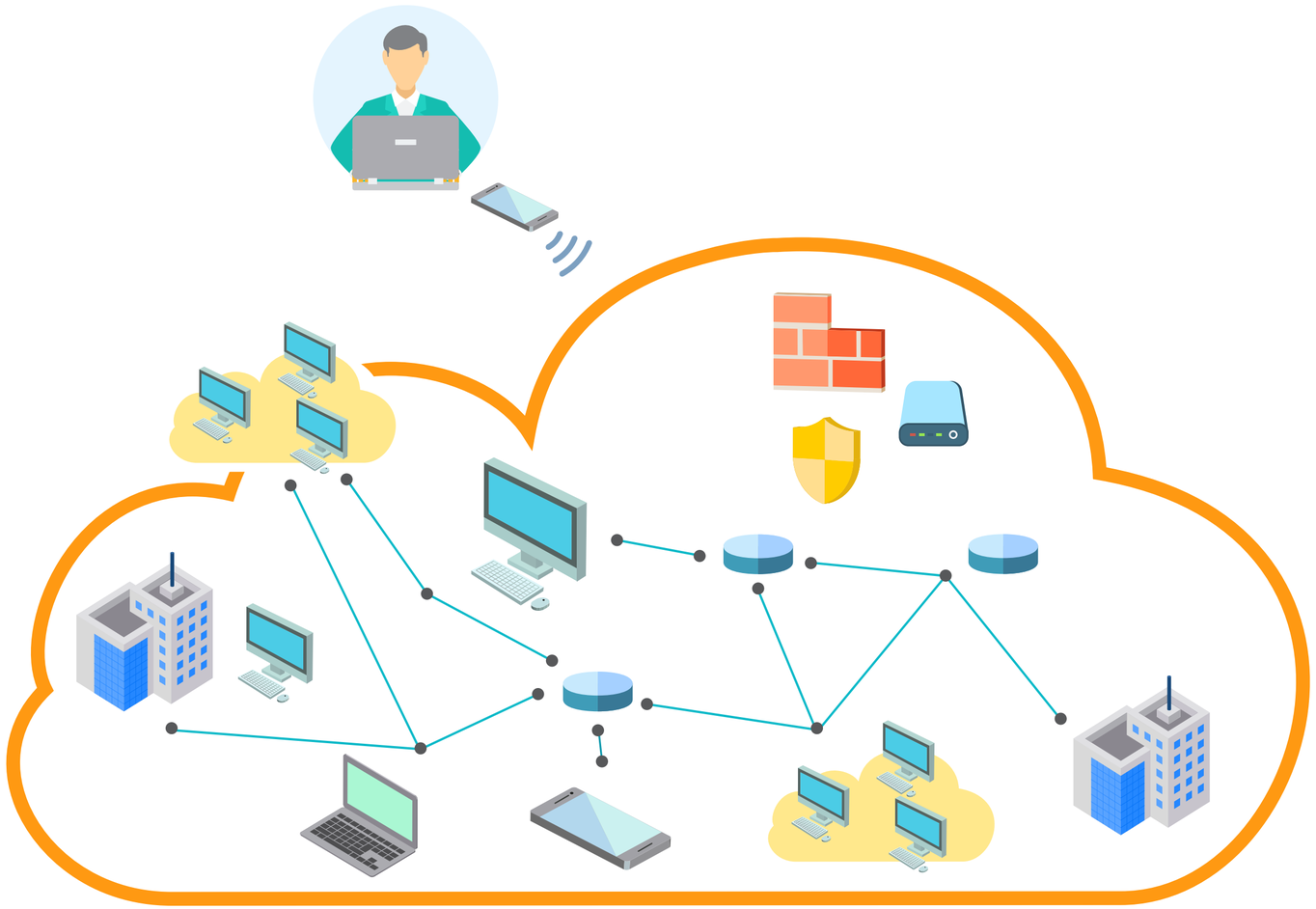
Mick Haynes
Technical Director, Hit Rail

hitrail
european railway IT & data communications

Why are networks a major risk?



Typical business network(s)

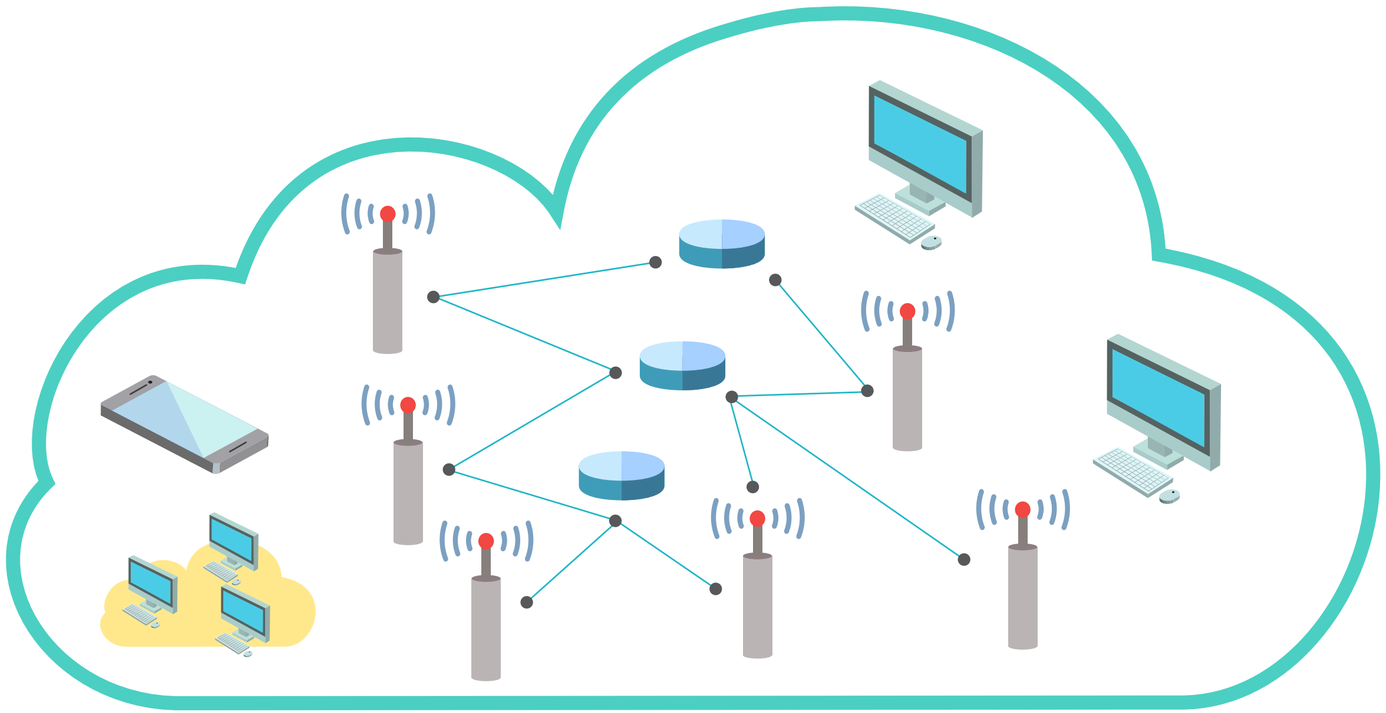


- Some private LANs
- Some private VPNs for larger users
- One main firewall to internet
- Lots of employees working from PCs, phones and tablets over wireless
- Employees using PCs over local LAN (with secure wireless)

Small Businesses

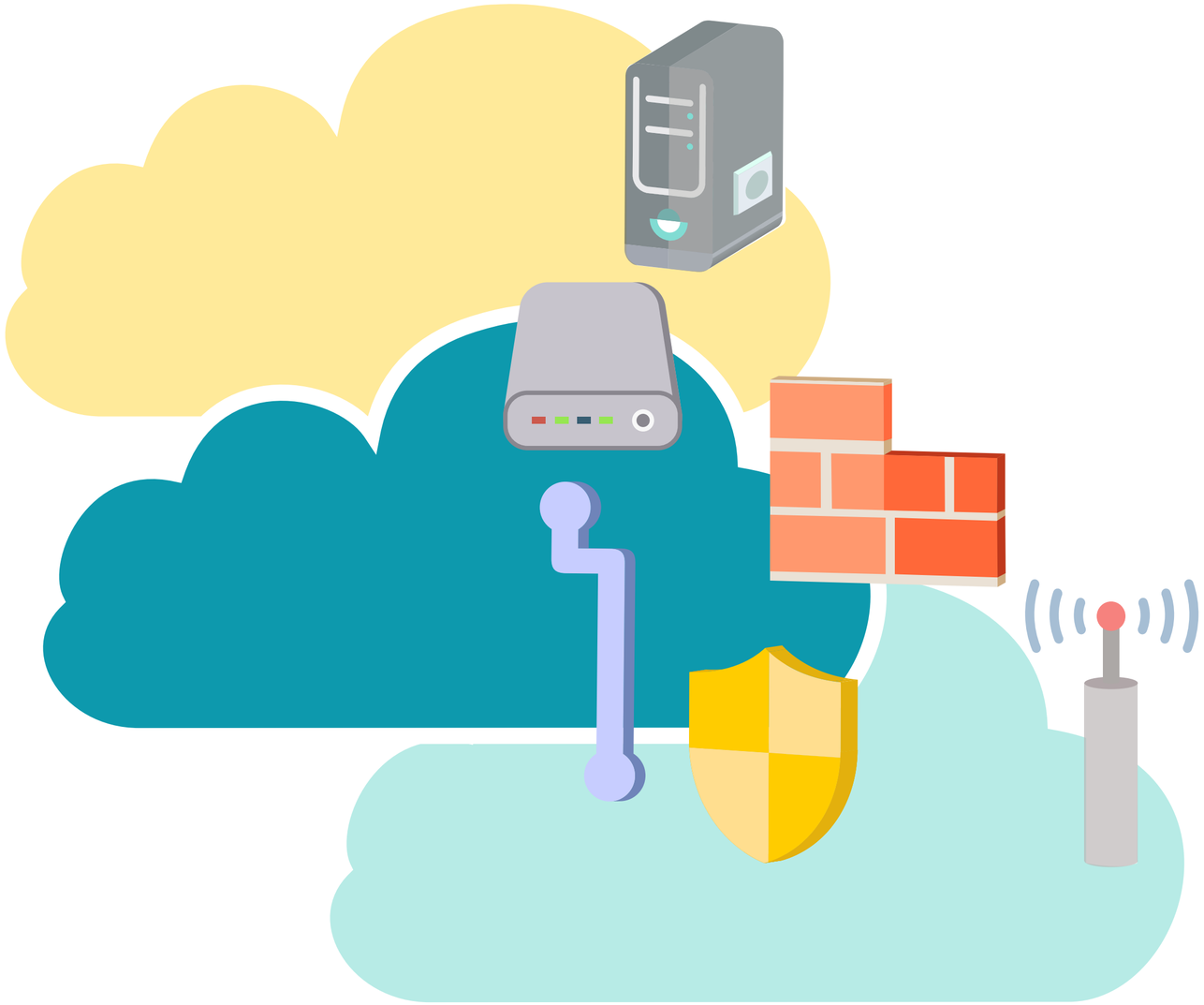
- Laptops with wireless and PC based firewall

Internet



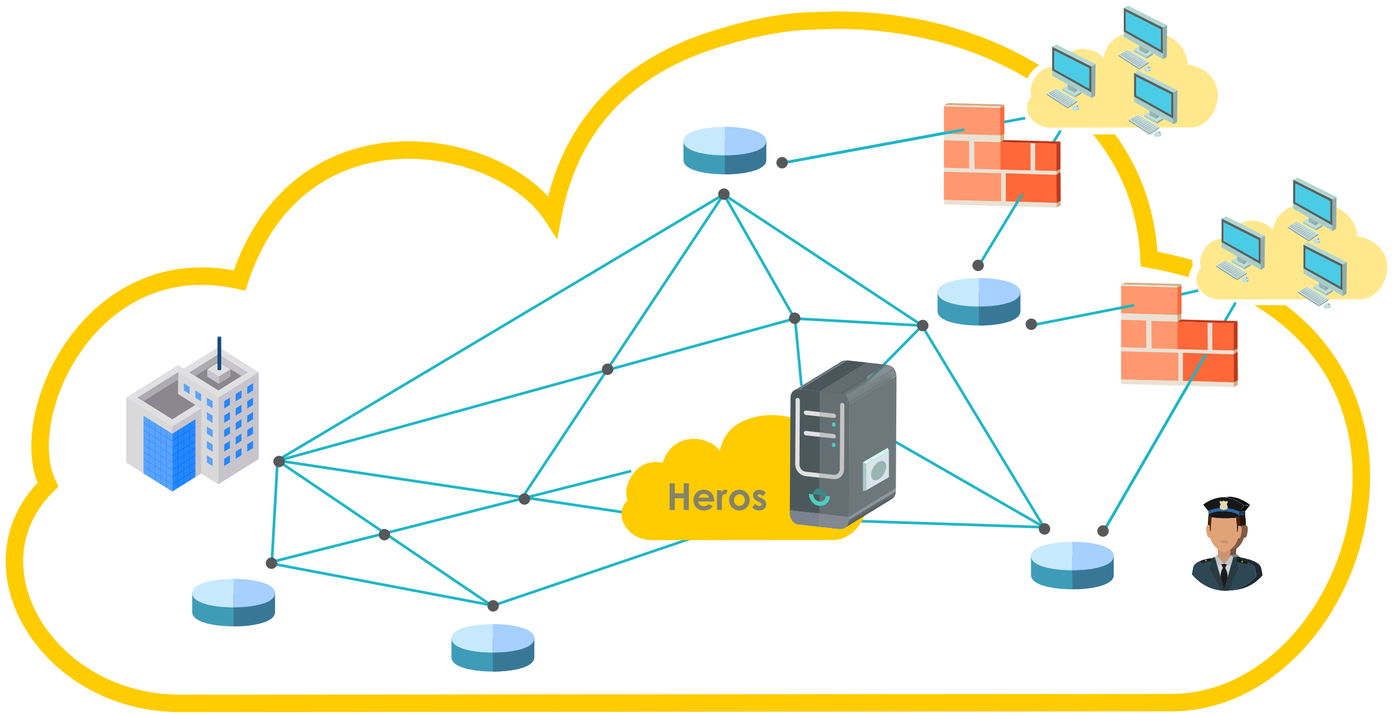
- Ubiquitous
- Attacked continuously
- Fast but with uneven performance
- Fundamentally insecure

VPN Gateway



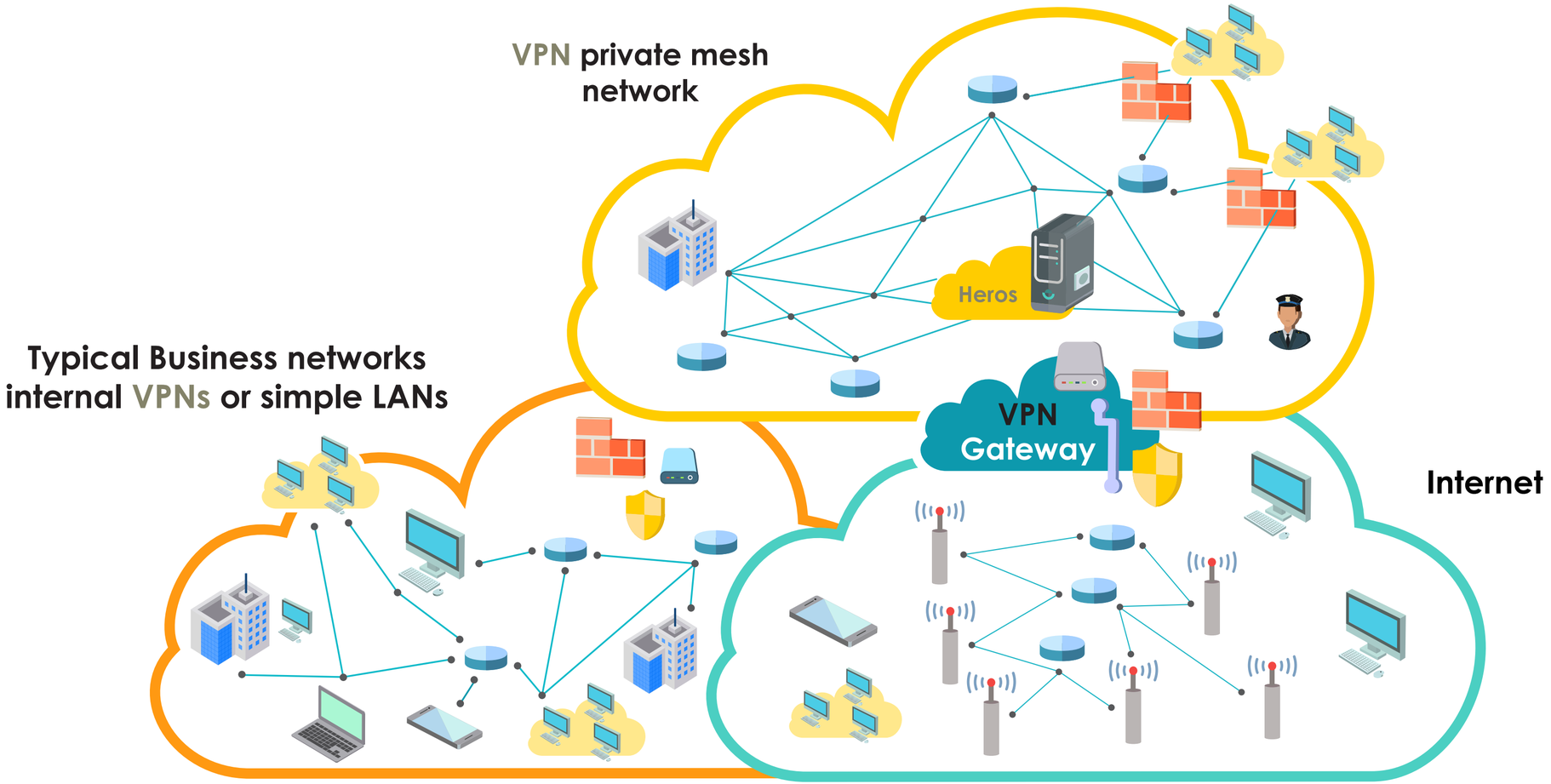
- Hit Rail's secure pipe for internet connections
- IPSec tunnel with backup
- Part of SLA
- Monitored and secure

HERMES Private
VPN

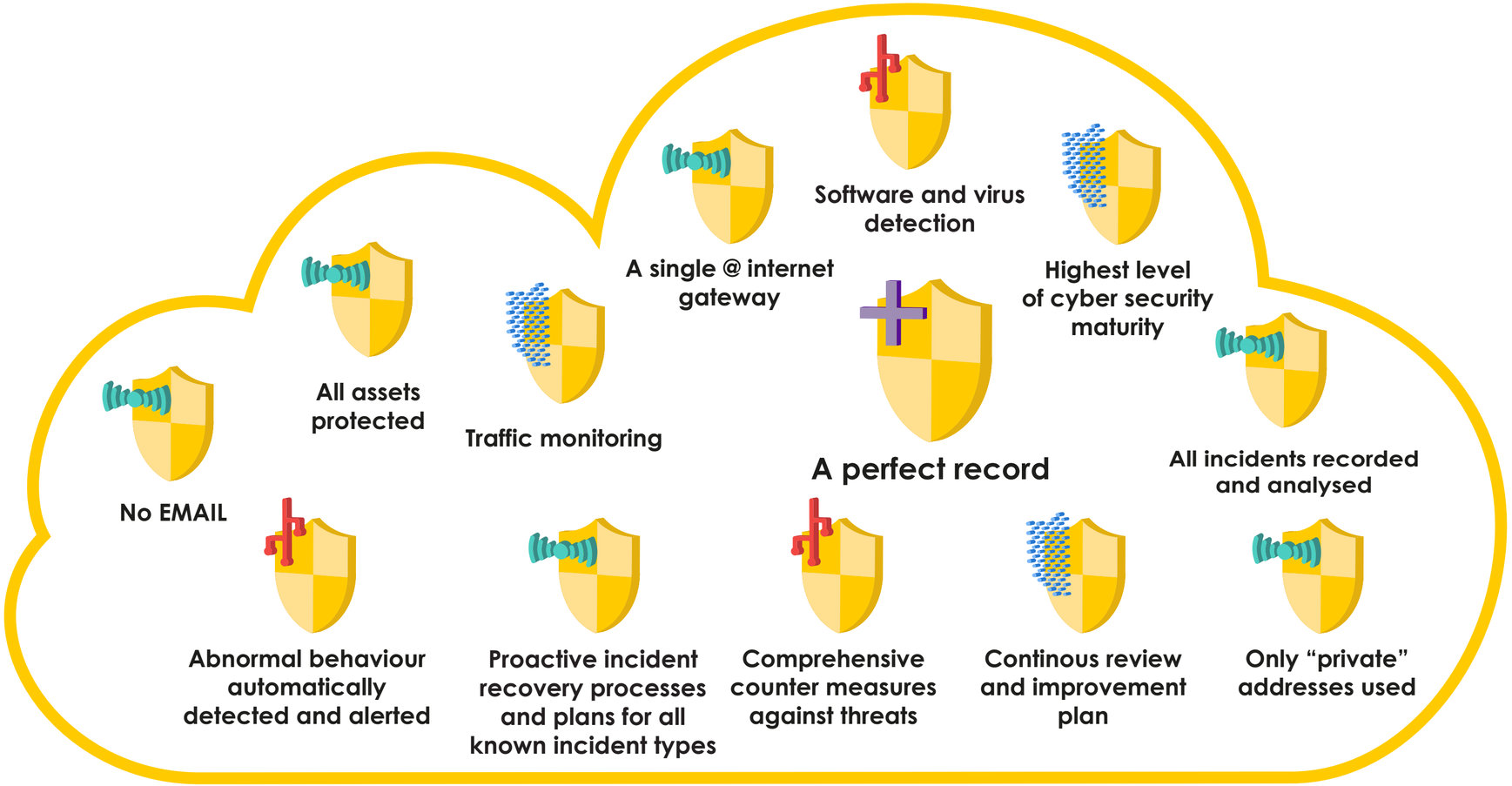


- **Meshed** private rail network
- Rail users make two connections to a private Point of presence
- Rail users have specific firewall policies to ensure no unknown connections or traffic is presented
- **Guaranteed** service levels
- Targested at **mission critical** services

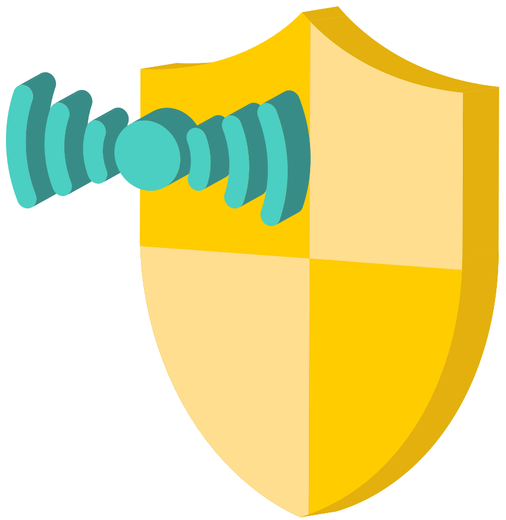
Why are networks a major risk?



The HERMES VPN cyber security shields



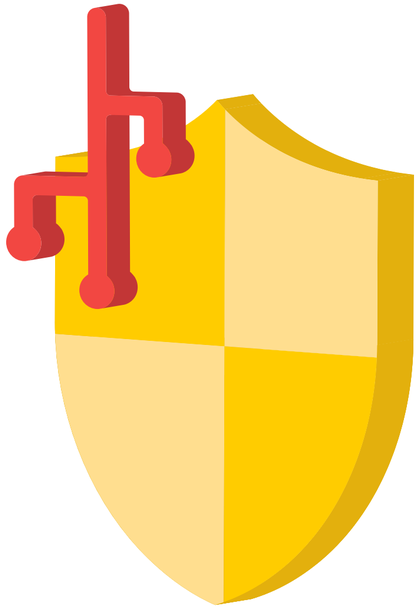
Components of the Hermes VPN Cyber Security Shield



A single @ internet gateway

- **Ability to control traffic entering the network**
- **Measurement**
- **Monitoring**

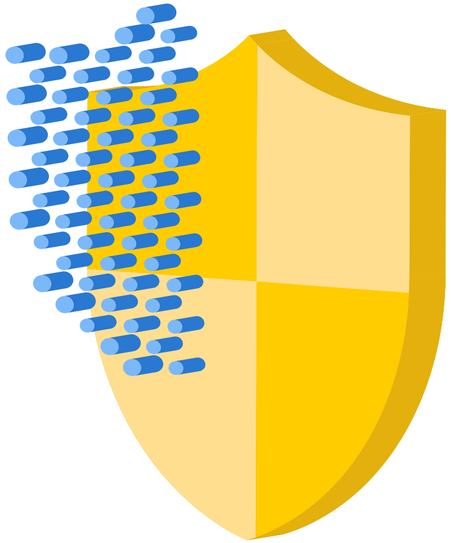
Components of the Hermes VPN Cyber Security Shield



Software and virus detection

- Services are protected and monitored
- Best practice virus protection on all potentially vulnerable connections

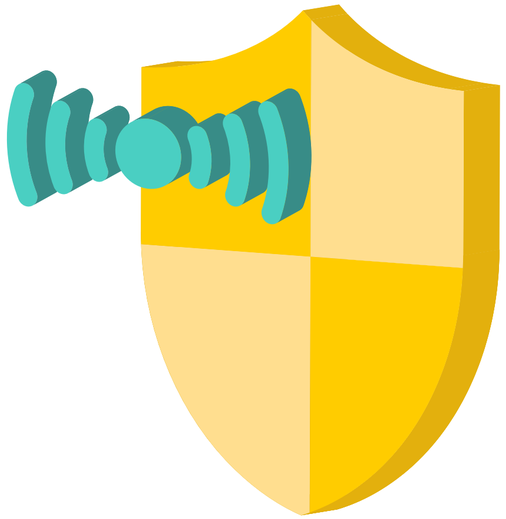
Components of the Hermes VPN Cyber Security Shield



Highest level of Cyber Security Maturity Model

- **We follow US and European CSMMs**

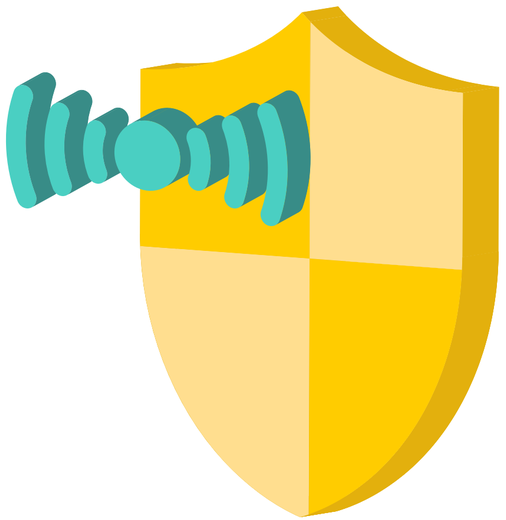
Components of the Hermes VPN Cyber Security Shield



All incidents recorded and analysed

- **Both Hit Rail and users have a process**

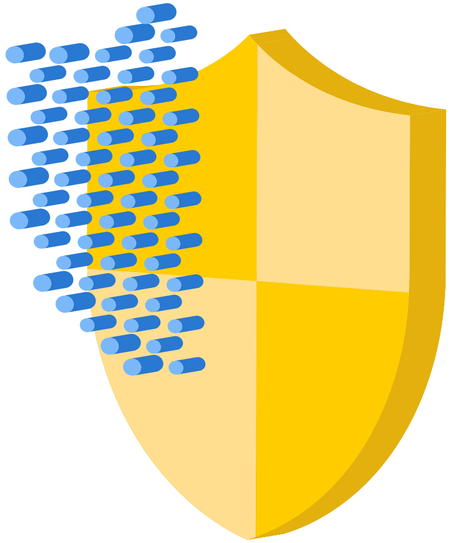
Components of the Hermes VPN Cyber Security Shield



Only “private” addresses used

- **NAT an essential requirement of the architecture**
- **No DNS**

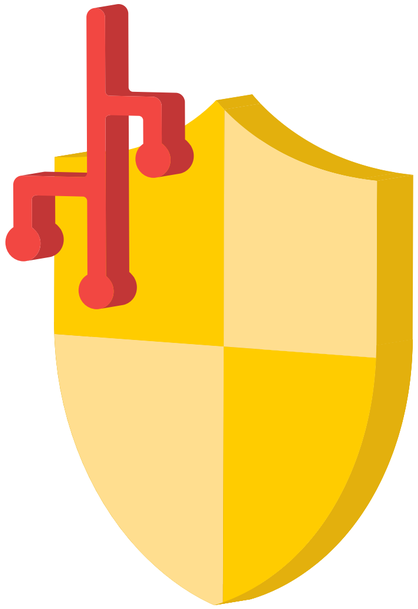
Components of the Hermes VPN Cyber Security Shield



Continuous review and improvement plan

- The Hit Rail team covers roles monitoring possible threats and possible modifications to all of our protection techniques

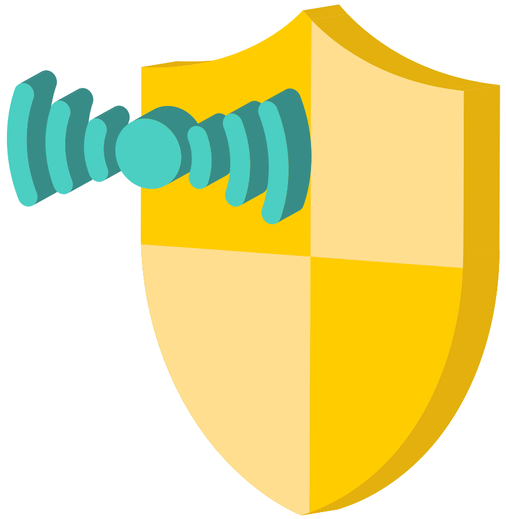
Components of the Hermes VPN Cyber Security Shield



Comprehensive counter measures against threats

- Access lists
- Limited ports
- Valid source and destination combinations
- Encryption
- Traffic pattern monitoring
- Back ups and automatic re-routing

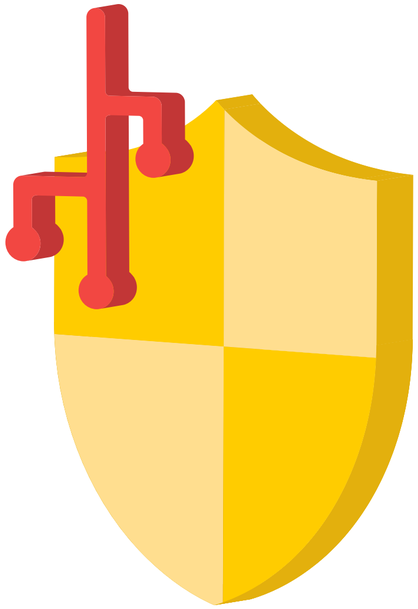
Components of the Hermes VPN Cyber Security Shield



Proactive recovery from incidents

- Automated recovery using back up links
- Tested and documented recovery scripts and data

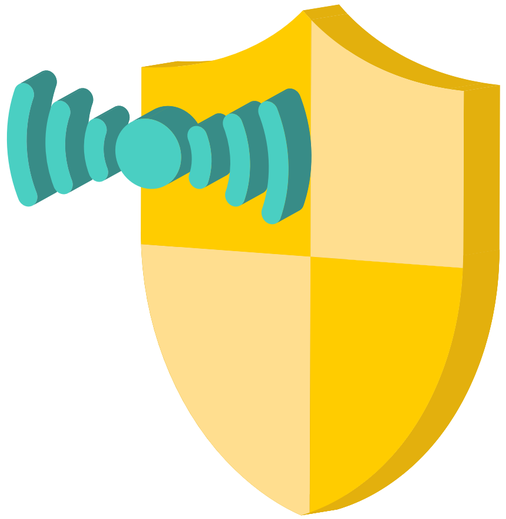
Components of the Hermes VPN Cyber Security Shield



Abnormal behaviour automatically detected and alerted

- **Monitoring sudden excessive activity**
- **Monitoring loss of activity**
- **Monitoring loss of connectivity**

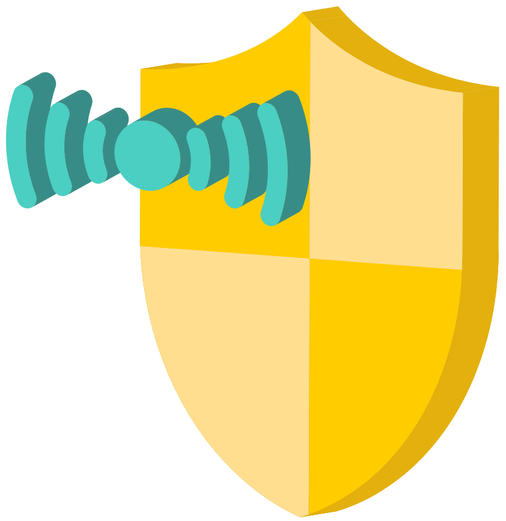
Components of the Hermes VPN Cyber Security Shield



No email

- Email and similar risky traffic is not allowed across the network

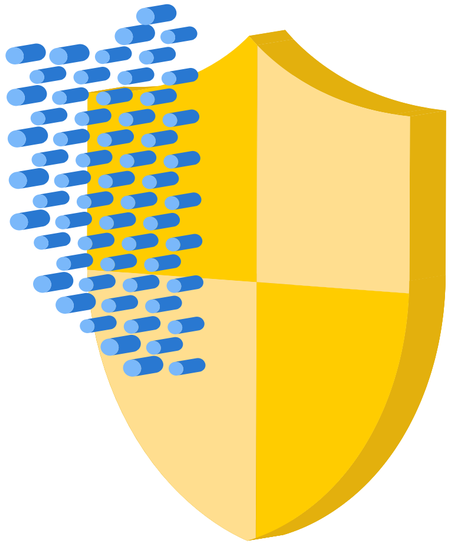
Components of the Hermes VPN Cyber Security Shield



All assets protected

- All nodes have good physical security
- Heros and central site secured
- Customers follow the best security practices

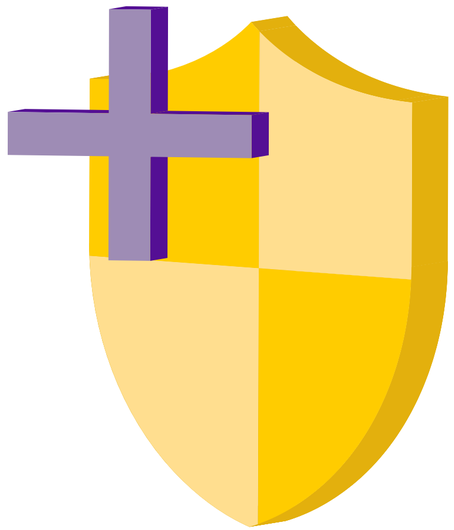
Components of the Hermes VPN Cyber Security Shield



Traffic monitoring

- IP accounting is on all routers
- The data is collected centrally and used to understand patterns of use
- Each traffic type uses a dedicated IP address and is collected to provide application levels volumes
- The variability is understood both within 24 hours and by day of the week and to understand seasonality

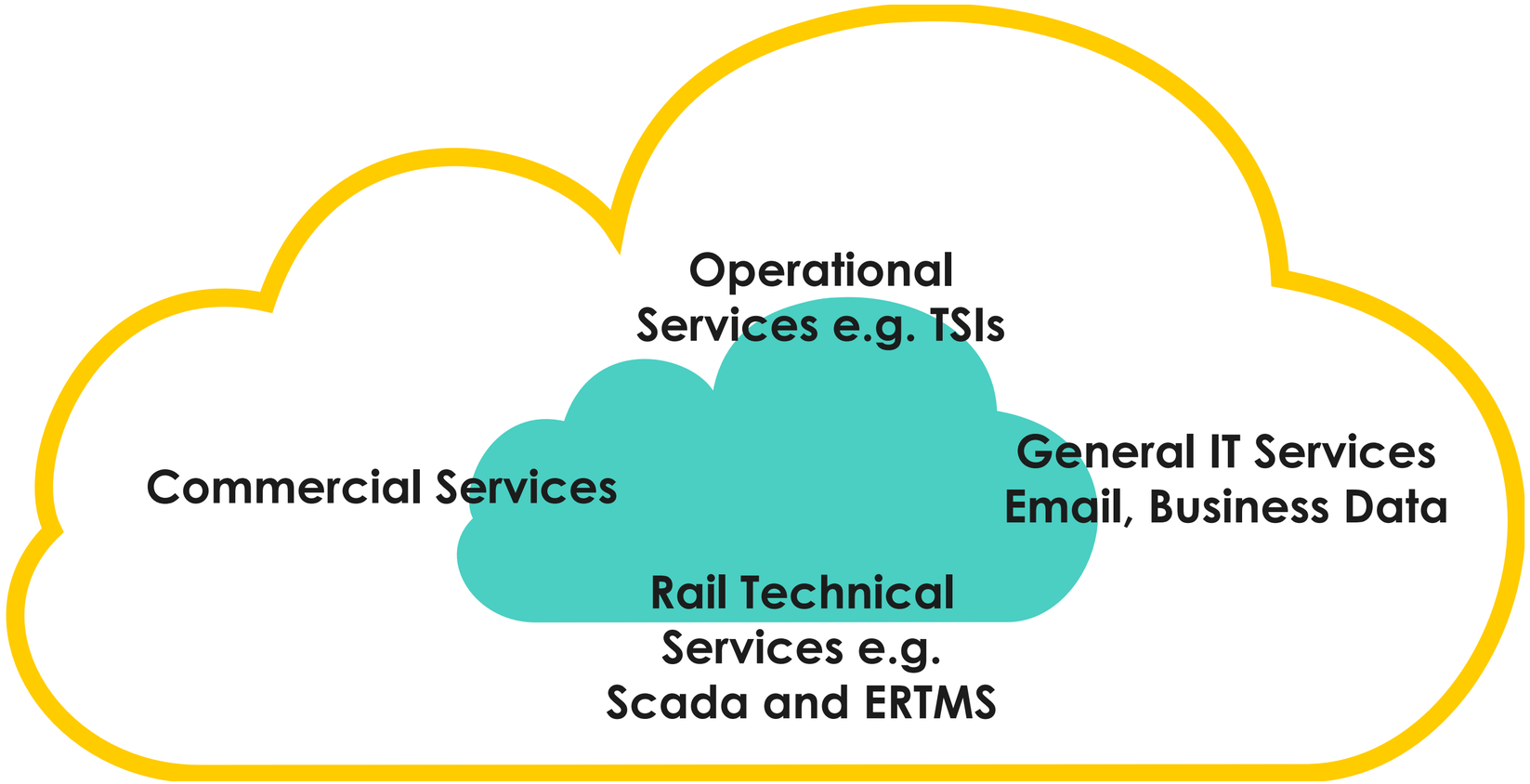
Components of the Hermes VPN Cyber Security Shield



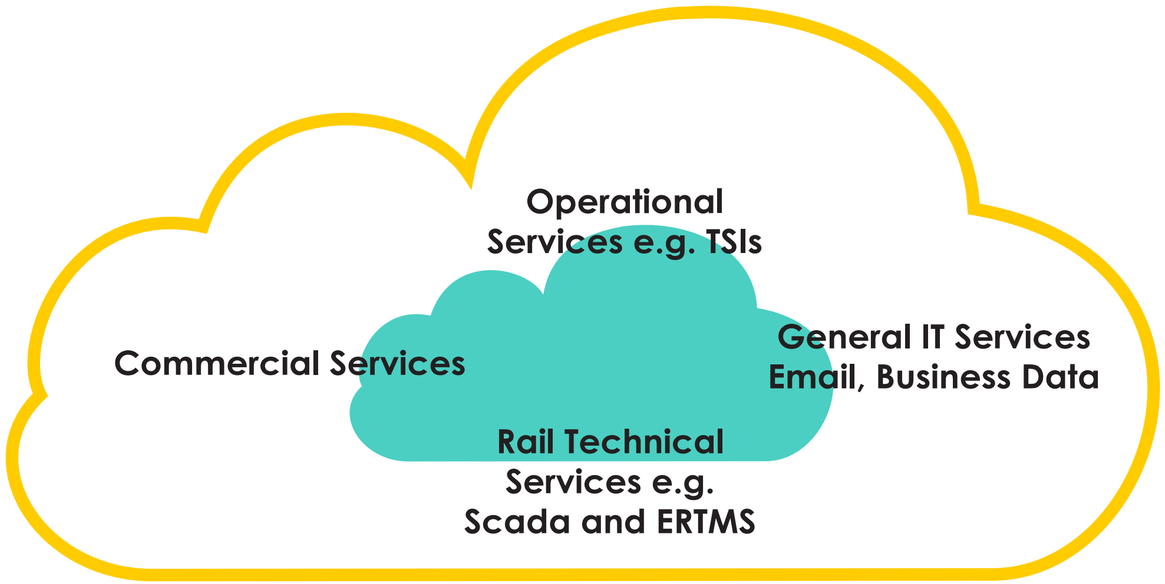
A perfect record

- For over 25 years
- Will be 20 years into the future

Which services justify consideration for network segmentation?

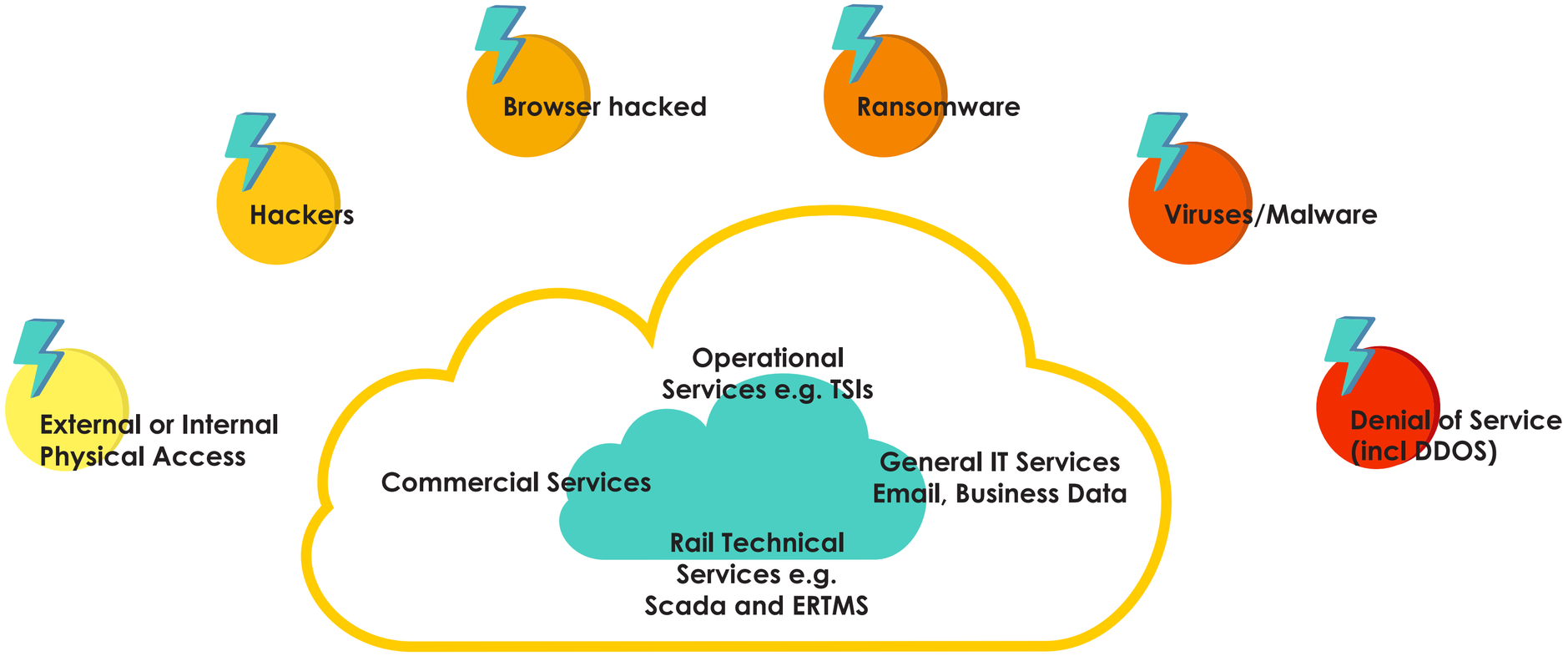


Which are the critical services?

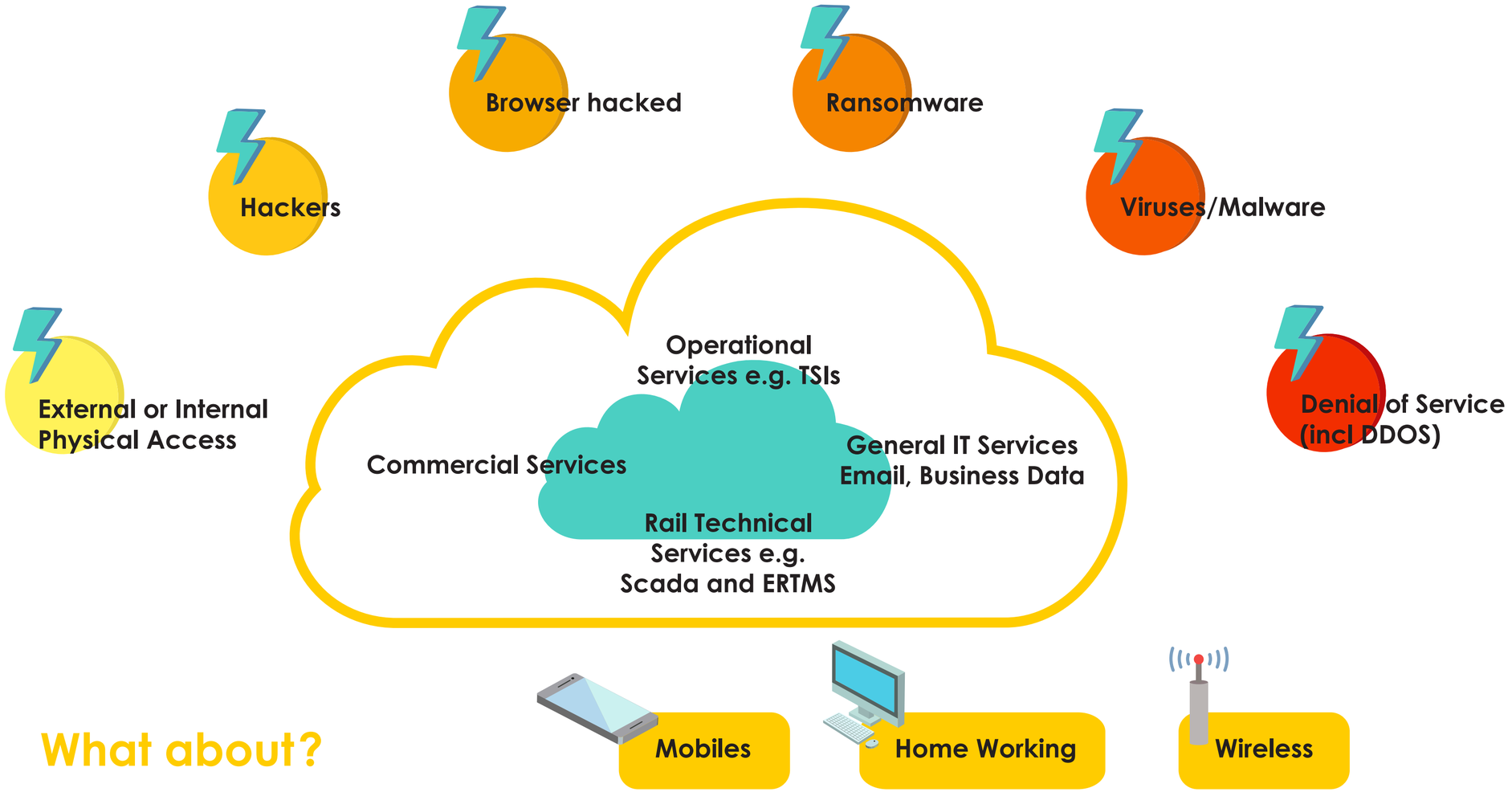


- Control systems including signalling
- Scada networks
- Sales services both passenger and freight
- Infrastructure monitoring
- Communication RU ↔ IM
- International Communication for international services
- Web sites
- Customer communications

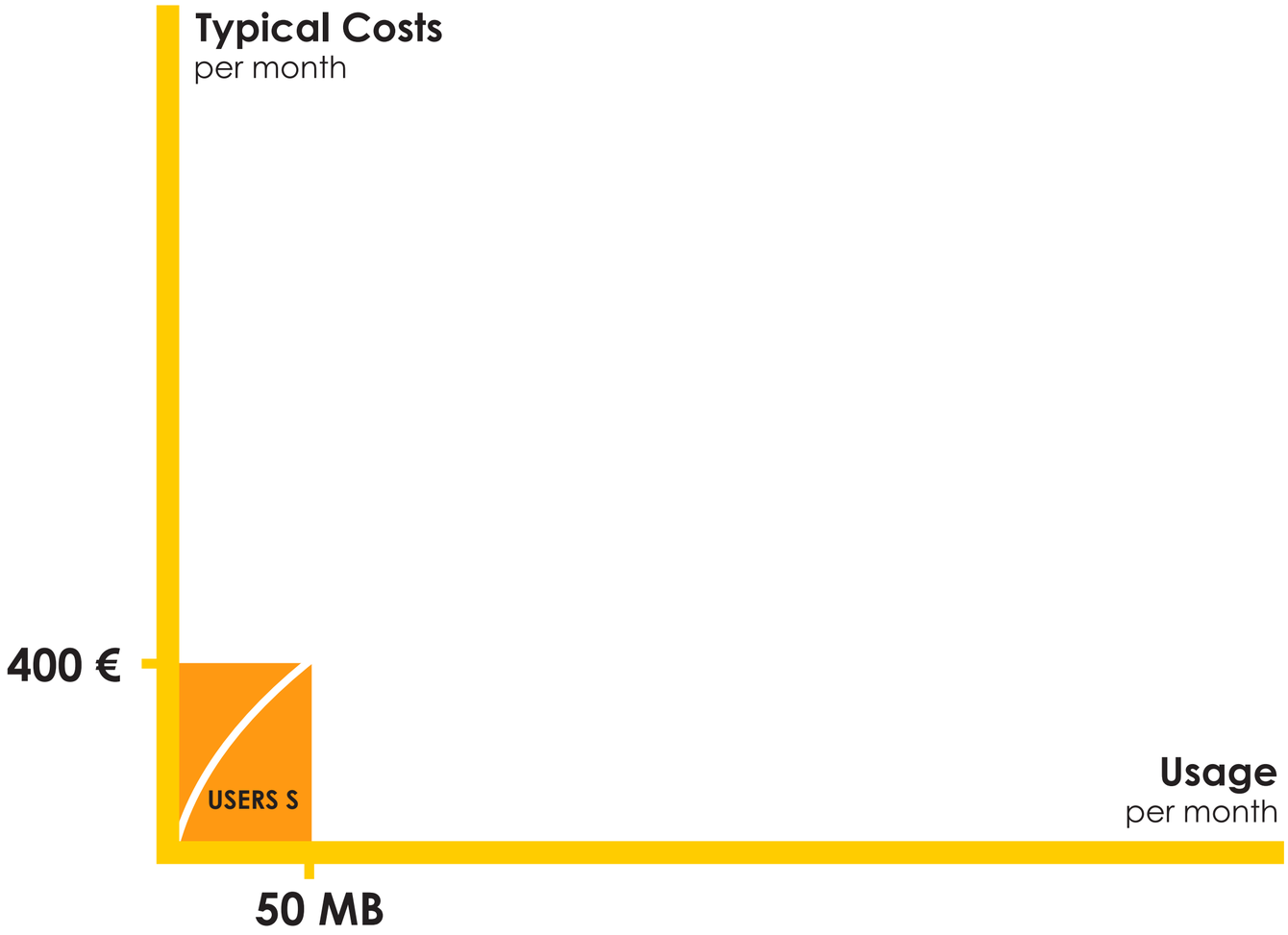
What are the different attack types?



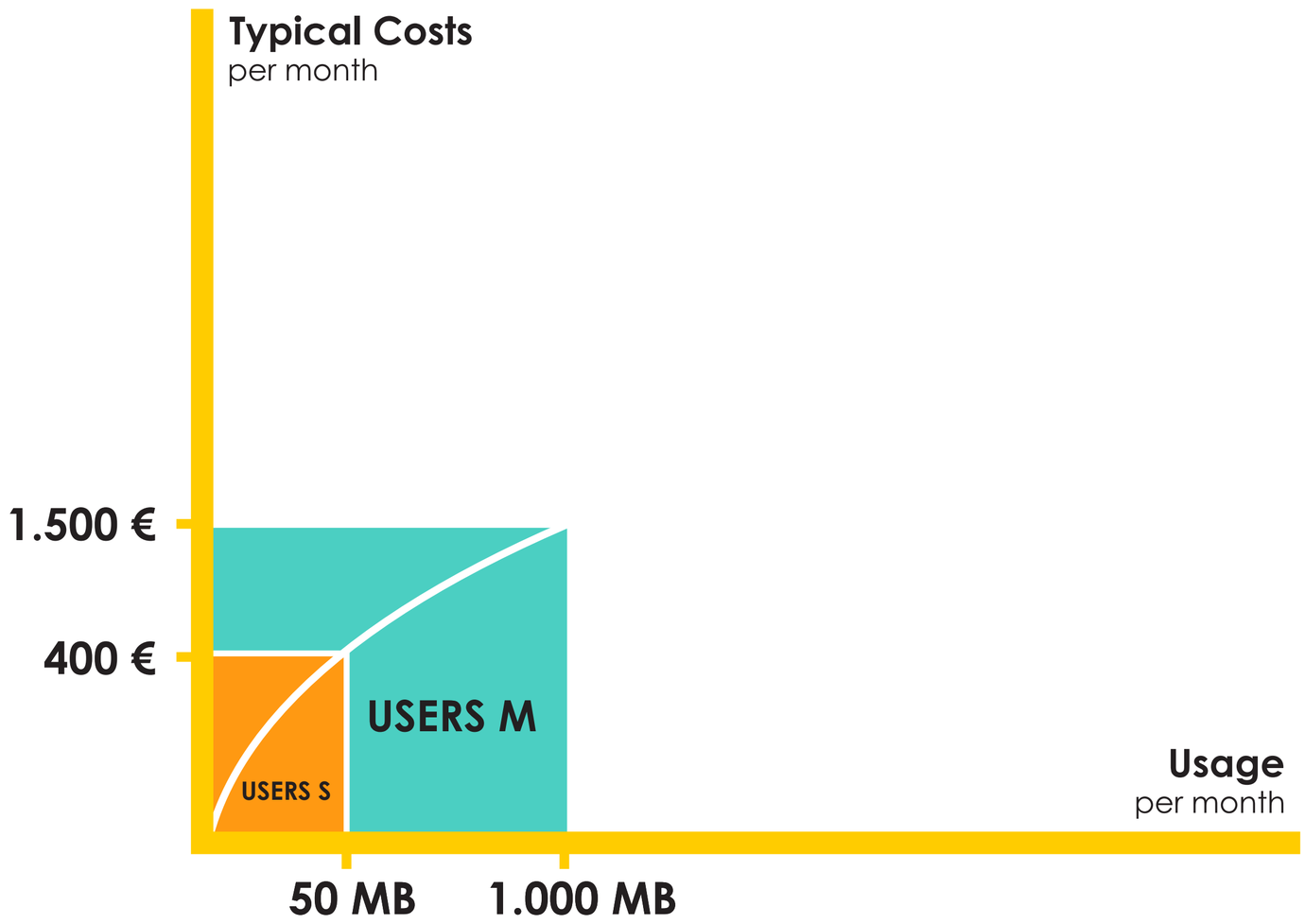
It can’t affect me!



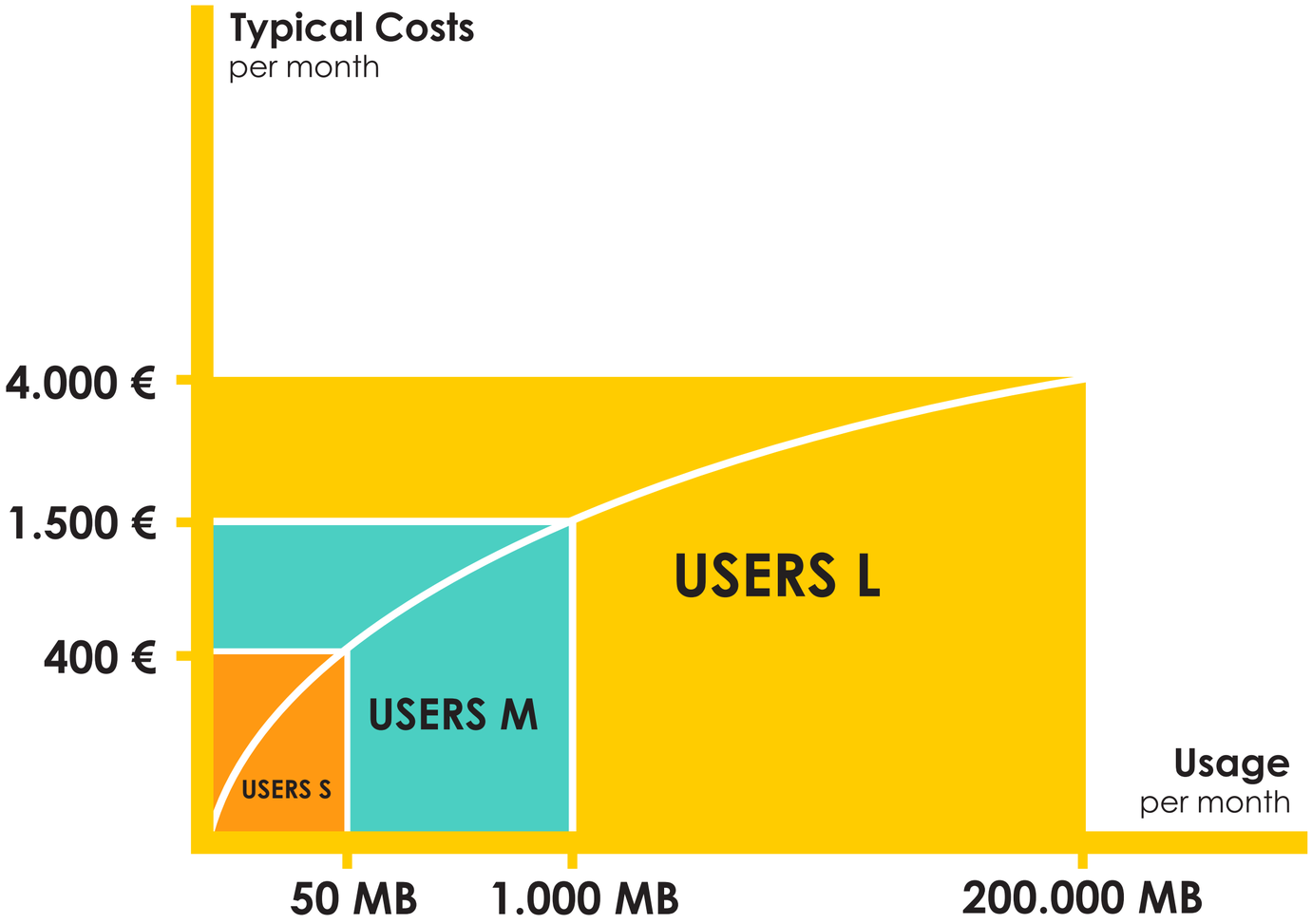
VPN Costs



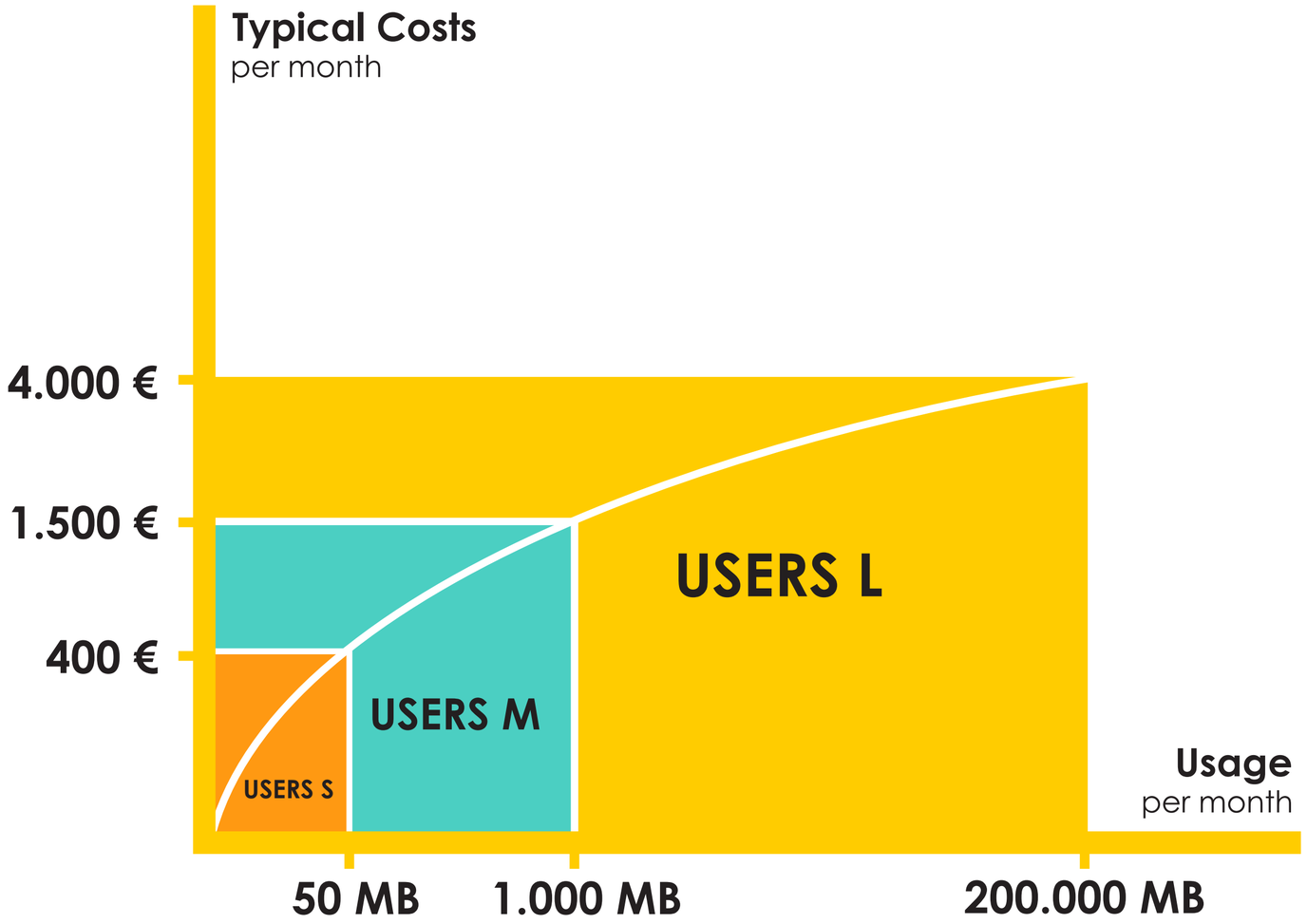
VPN Costs


Typical Costs
per month
1.500 €
400 €
USERS M
USERS S
Usage
per month
50 MB
1.000 MB

VPN Costs


Typical Costs
per month
4.000 €
1.500 €
400 €
USERS L
USERS M
USERS S
Usage
per month
50 MB
1.000 MB
200.000 MB

Risk Cost



Loss of key services (>€1M per day)

- Operations
- Sales

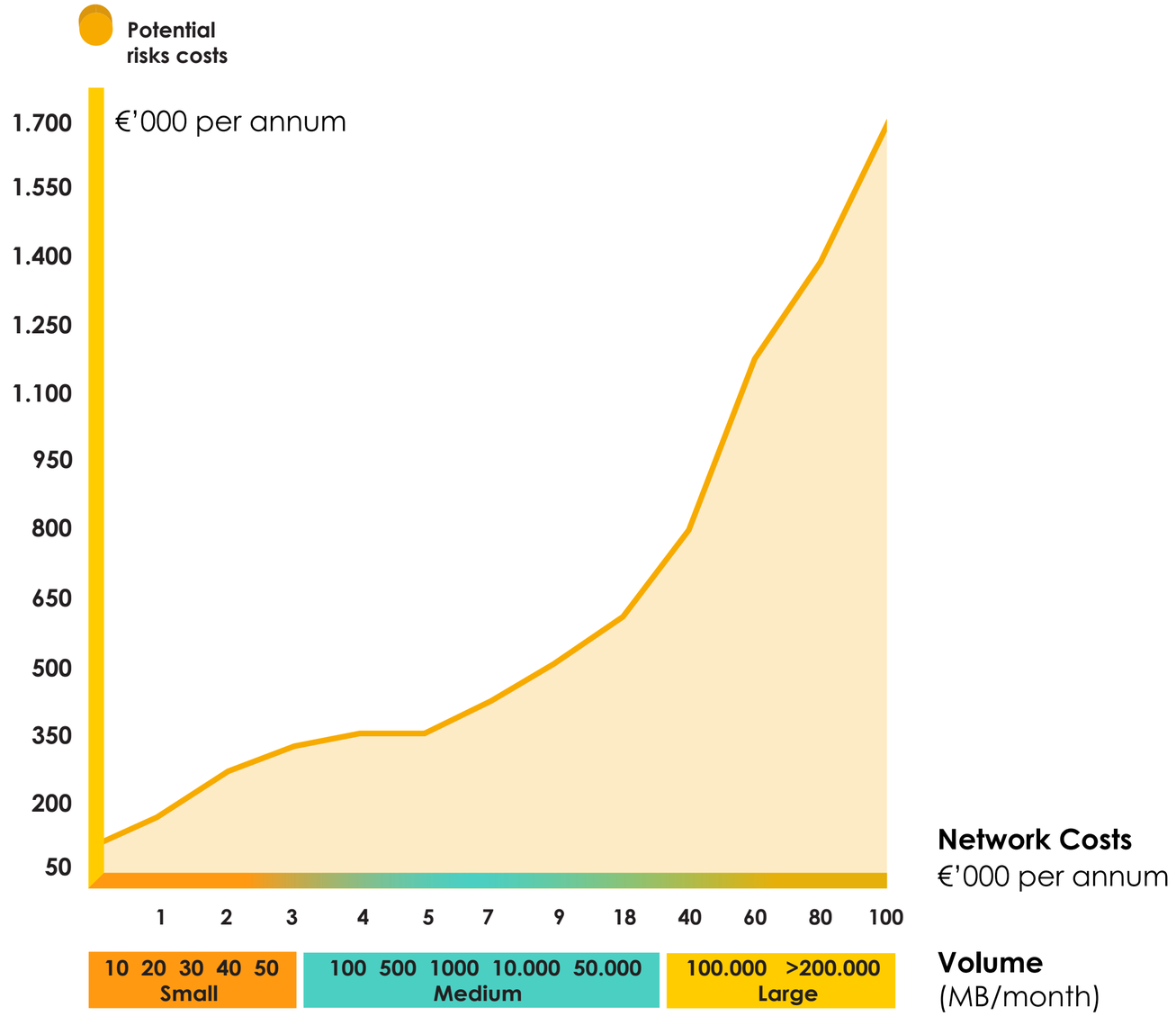
Partial interruption of services (>€100K per day)

- RU ↔ IM connection
- International connection
- Client services
- Business services

Reputation (between €10K and €500K per incident)

- Data breach
- Internal sabotage

Risk Cost



Loss of key services (>€1M per day)

- Operations
- Sales

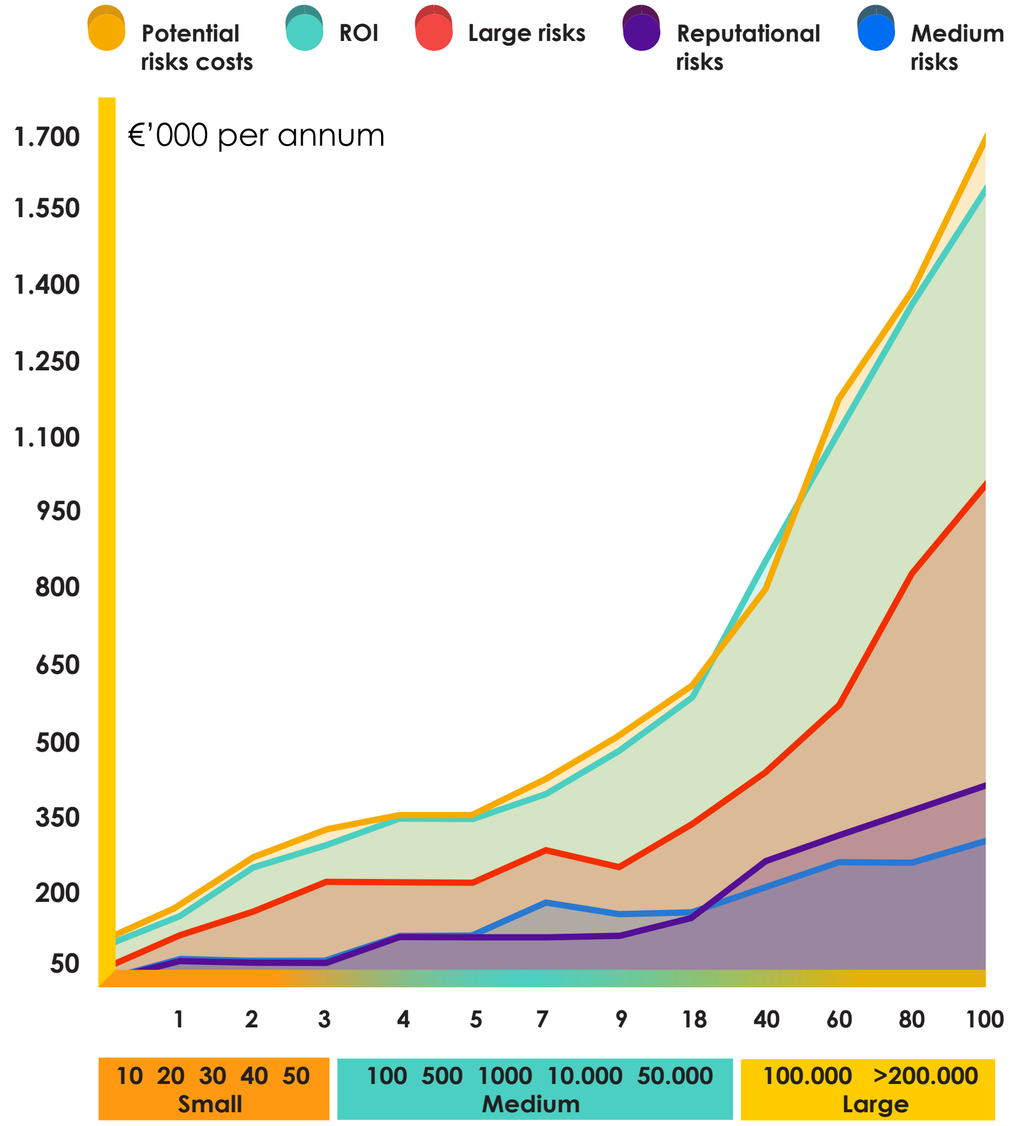
Partial interruption of services (>€100K per day)

- RU ↔ IM connection
- International connection
- Client services
- Business services

Reputation (between €10K and €500K per incident)

- Data breach
- Internal sabotage

Risk Cost



Network Costs
€'000 per annum

Volume
(MB/month)

Loss of key services (>€1M per day)

- Operations
- Sales

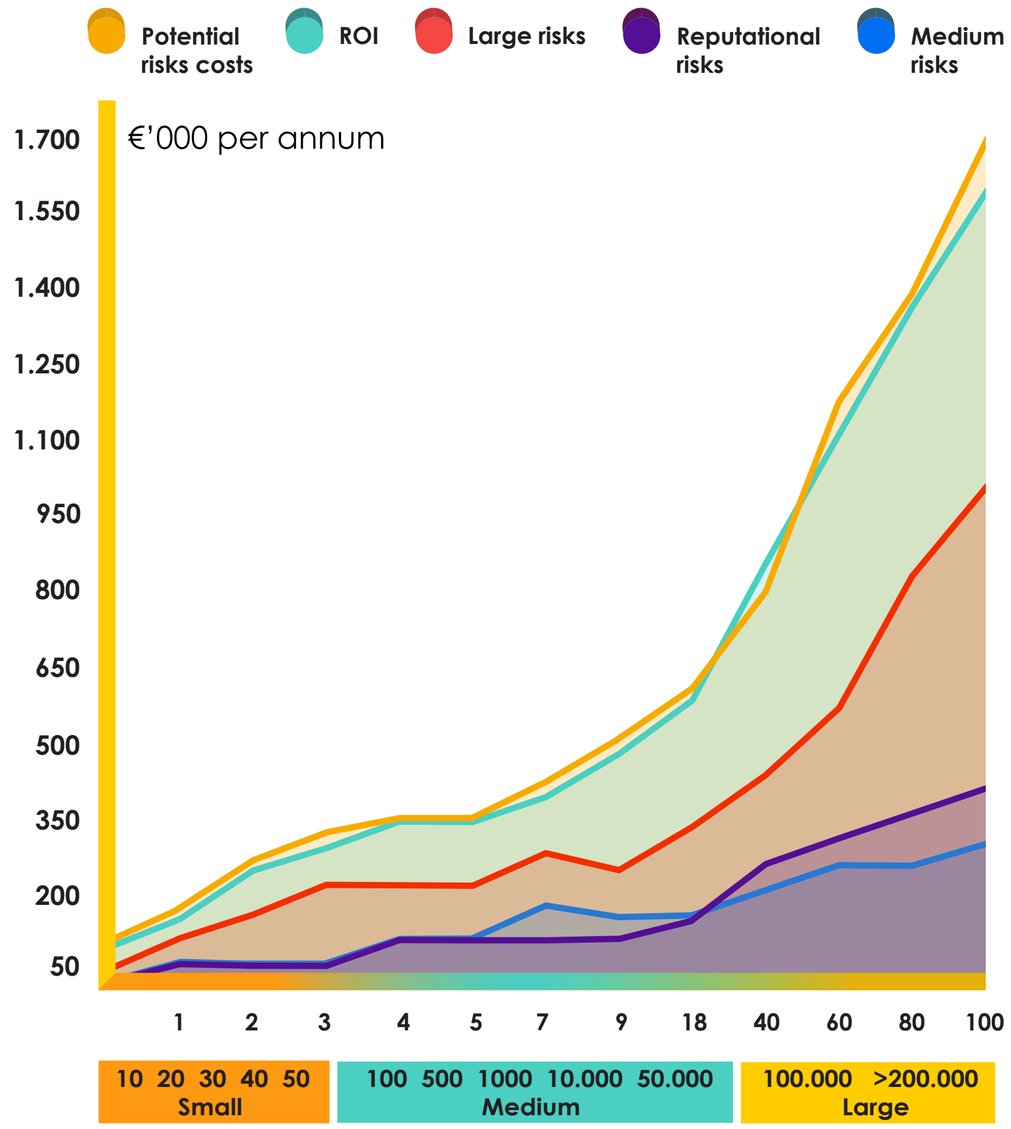
Partial interruption of services (>€100K per day)

- RU ↔ IM connection
- International connection
- Client services
- Business services

Reputation (between €10K and €500K per incident)

- Data breach
- Internal sabotage

Risk Cost

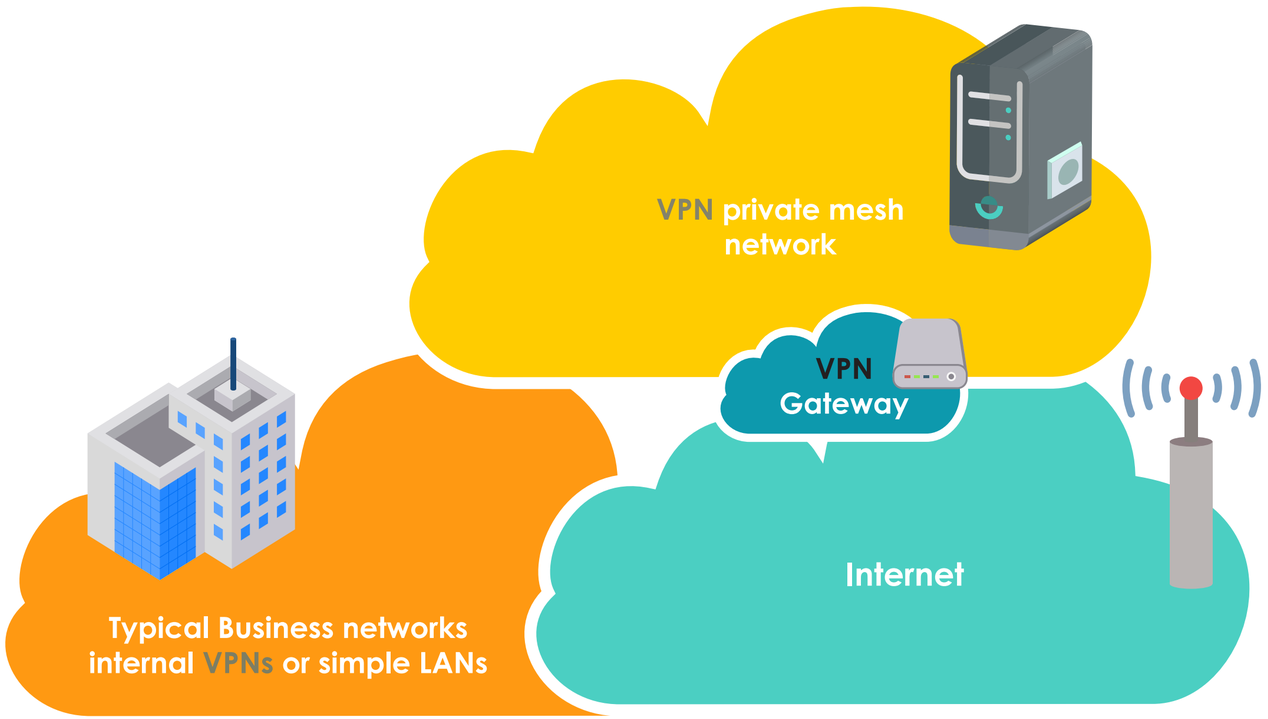


Network Costs
€'000 per annum

Volume
(MB/month)

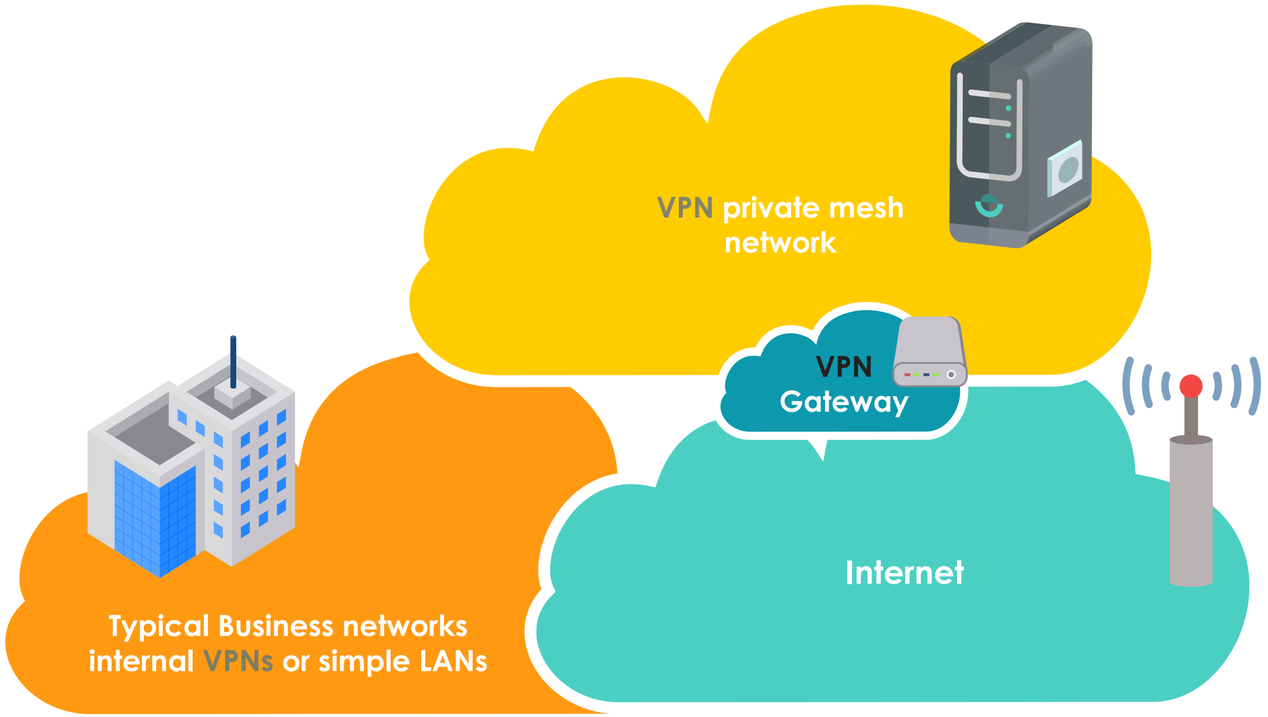
- **Saving one incident per year will give a return on investment**

To summarise



Now you know the answers to:

- What is a VPN?
- What are your cyber security risks?
- How does a VPN provide protection?
- Which services are critical?
- Typical VPN costs?
- What could be a business case?



Any questions?