

# Inzet van data diodes in een OT omgeving

Maurice Snoeren



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch



# Maurice Snoeren

Maurice.Snoeren@RWE.com

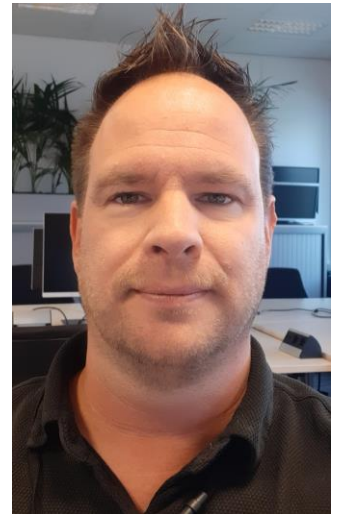
## Background

Electrical engineering, computer science with specialism on control & instrumentation. Always had a passion for cybersecurity.

## Cybersecurity

Since 2009 started with the protection of control systems of critical infrastructures.

**OT Security Officer @ RWE Generation**



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch



# For more than 120 years, RWE has been passionate about generating electricity. Now, RWE is shaping the new energy era.



**1898**  
The future starts today, more than 120 years ago.

Lignite is the key to affordable electricity.  
**1914**



Powering the economic miracle.  
**1950s**



Security of supply thanks to nuclear power.  
**1970s**



Lignite-fired power stations with optimised plant technology help reduce CO<sub>2</sub>.  
**2002**



**1928**  
RWE builds the first cross-regional high-voltage transmission line.



**1955**  
Ludwig Erhard opens the Weisweiler lignite-fired power station.



**1976**  
RWE researches, develops and tests renewables.



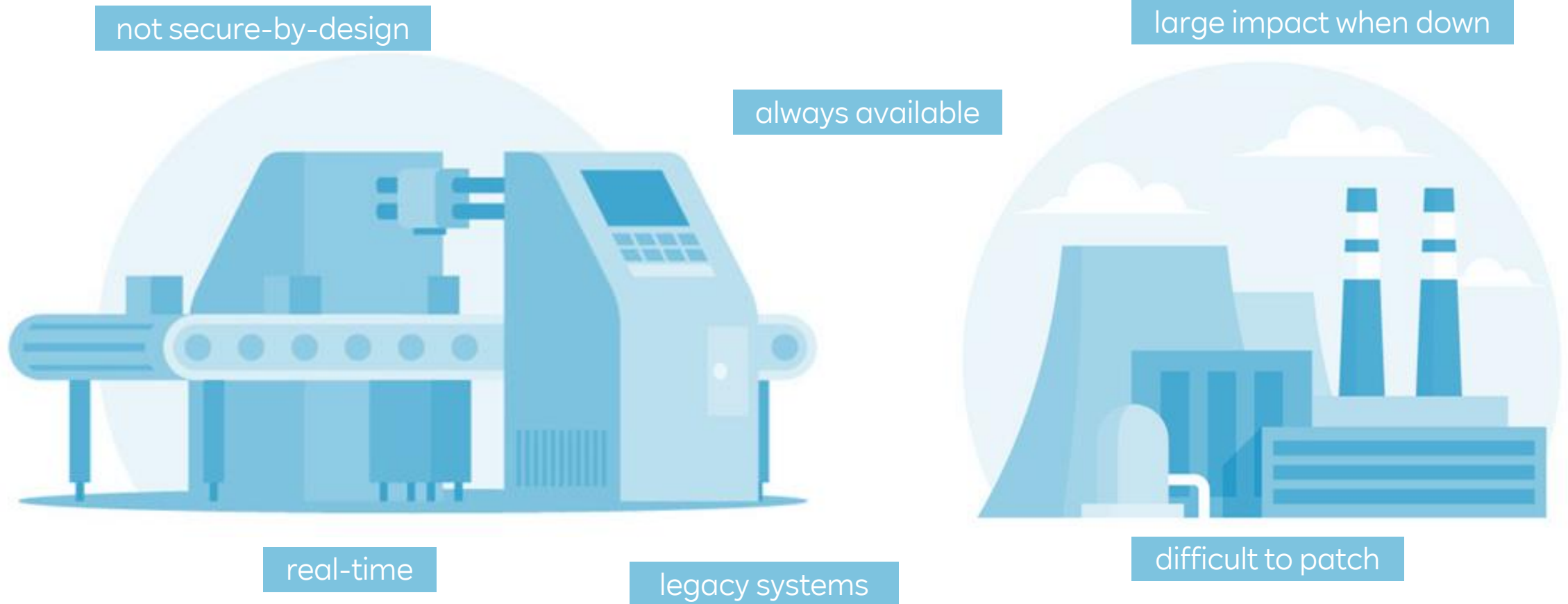
**2016**  
Foundation and stock market launch of innogy SE.



**2019**  
The transaction with E.ON.

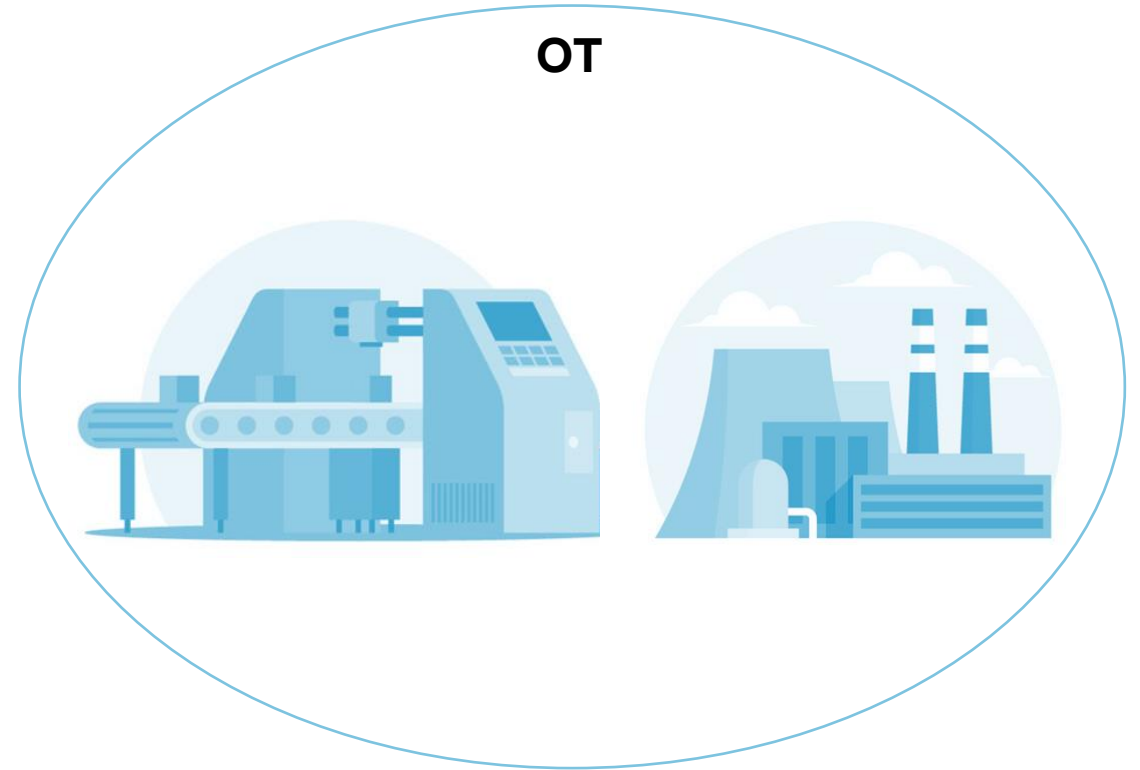
**2019 - today**  
RWE is one of the world's leading generators of renewable electricity.

# Industrial process automation environments

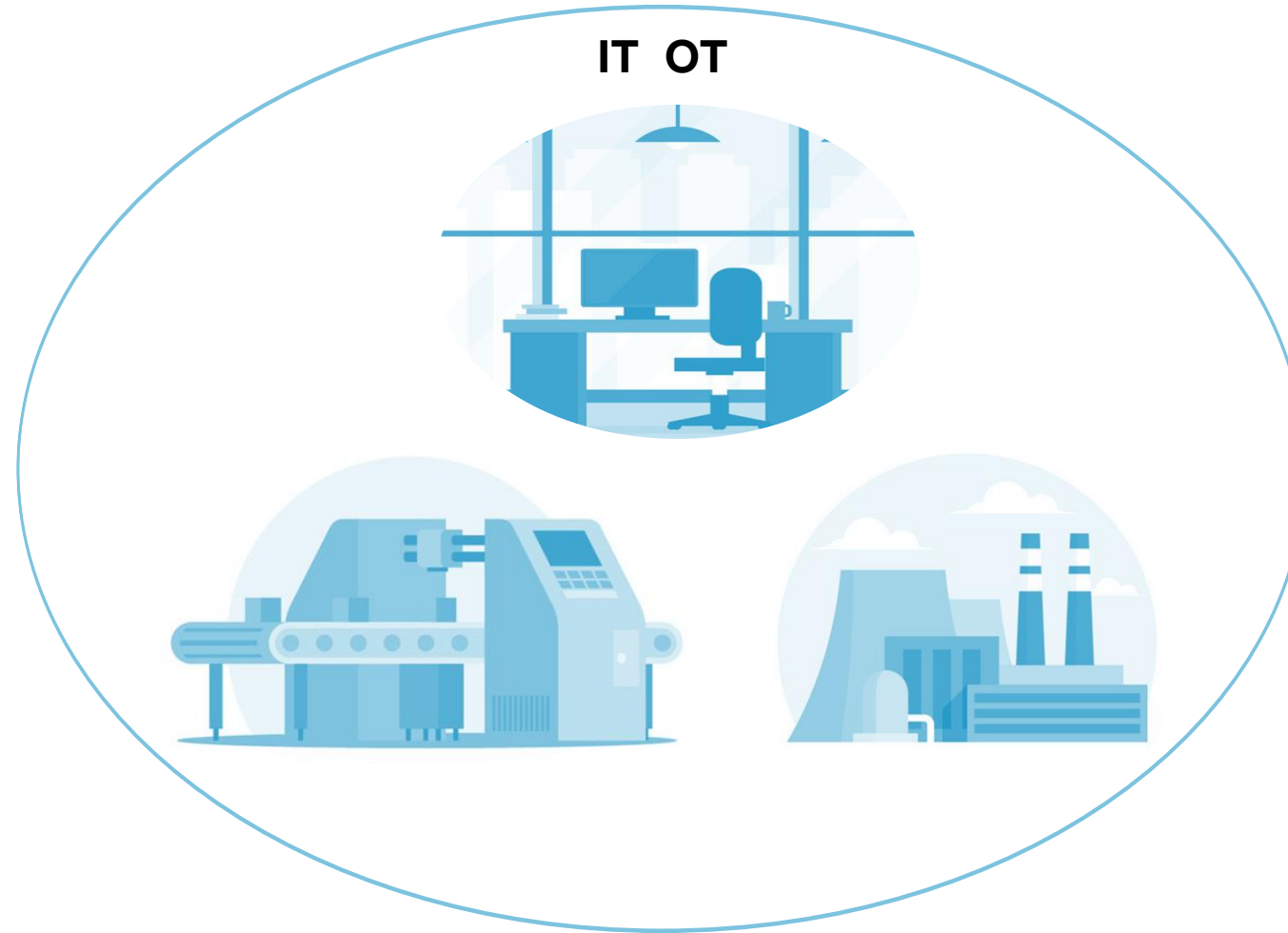




# IT - OT convergence



# IT - OT convergence



# IT - OT convergence

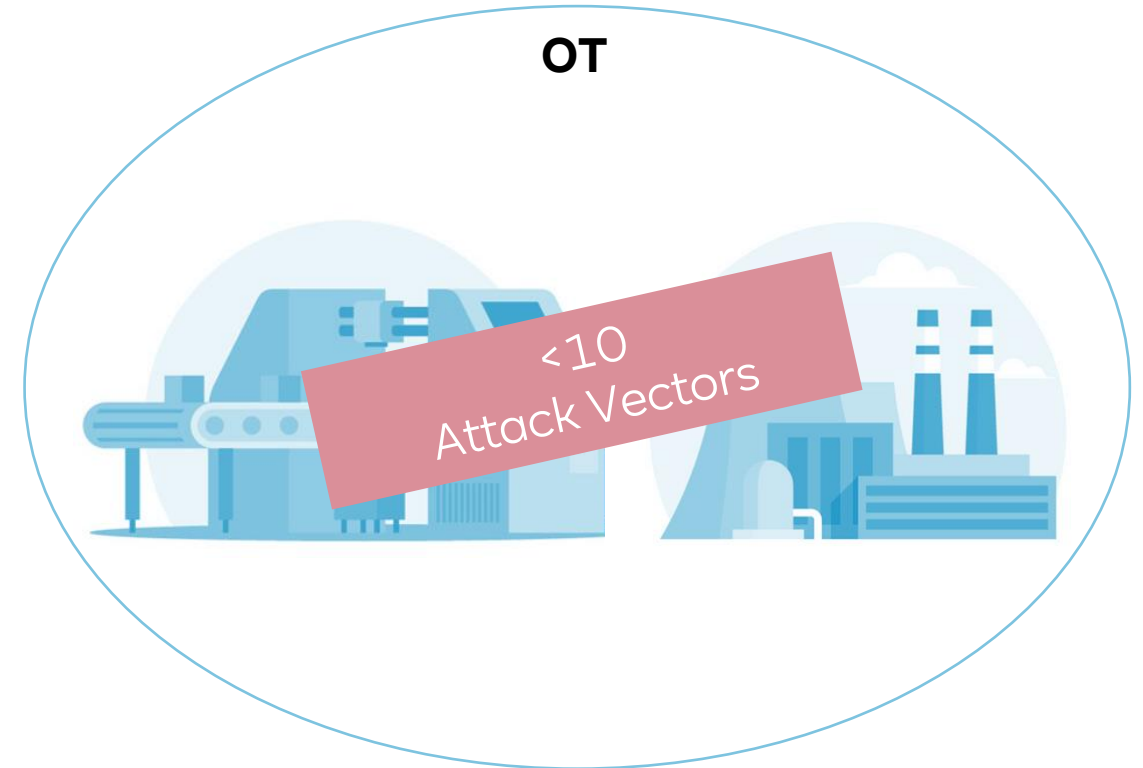


400+  
Attack Vectors

Internet facing services

Active users on internet

Office automation services



<10  
Attack Vectors

Physical access

Remote connections

Software updates

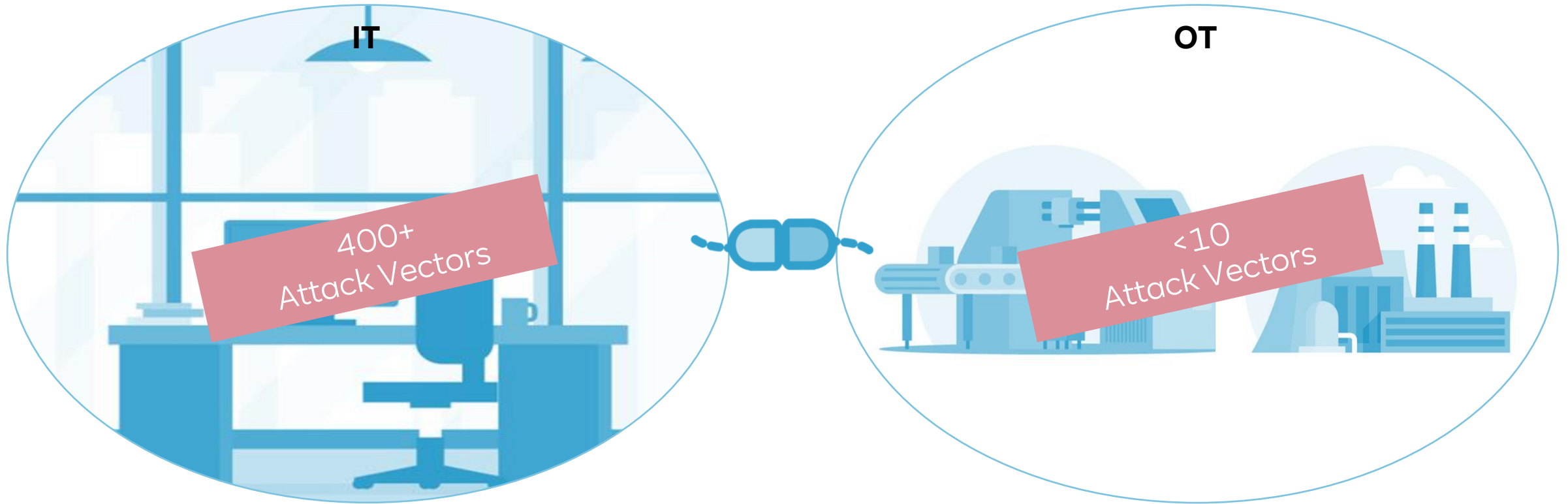


Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

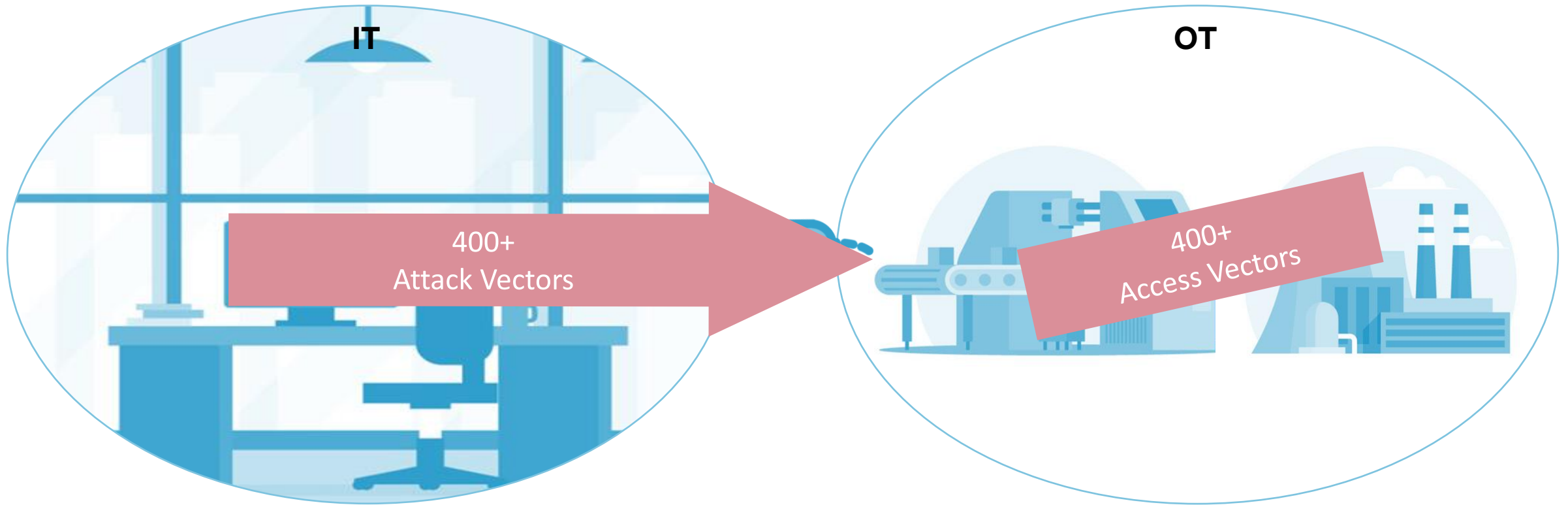


# IT - OT risks

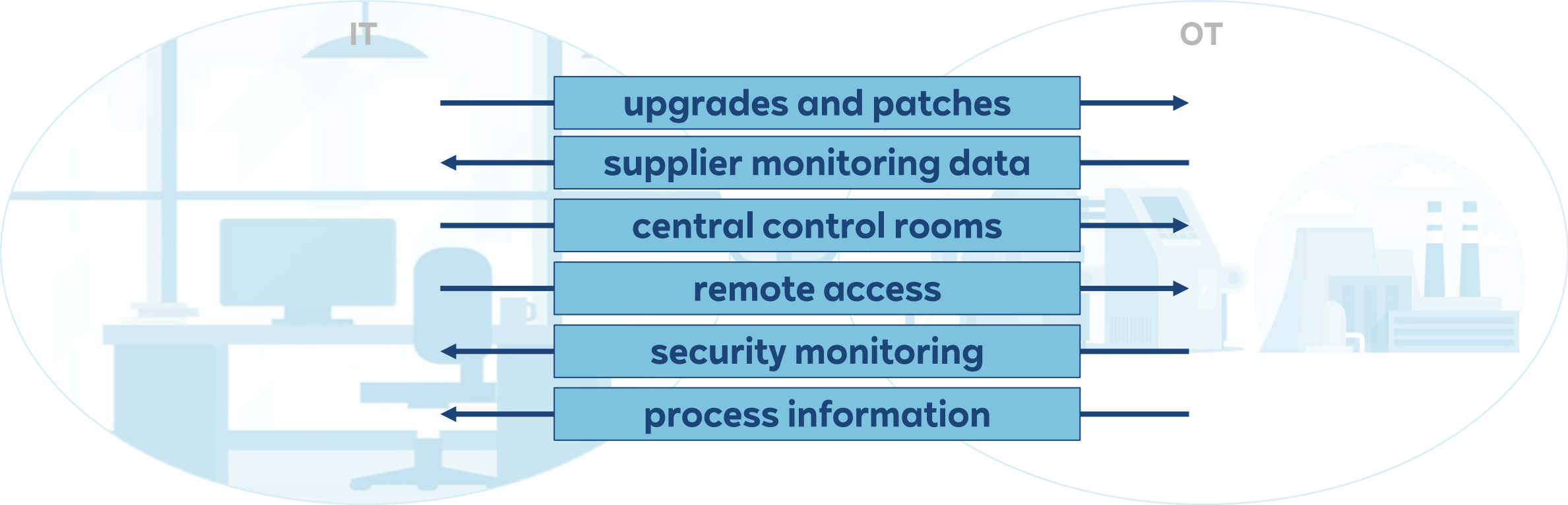




# IT - OT risks



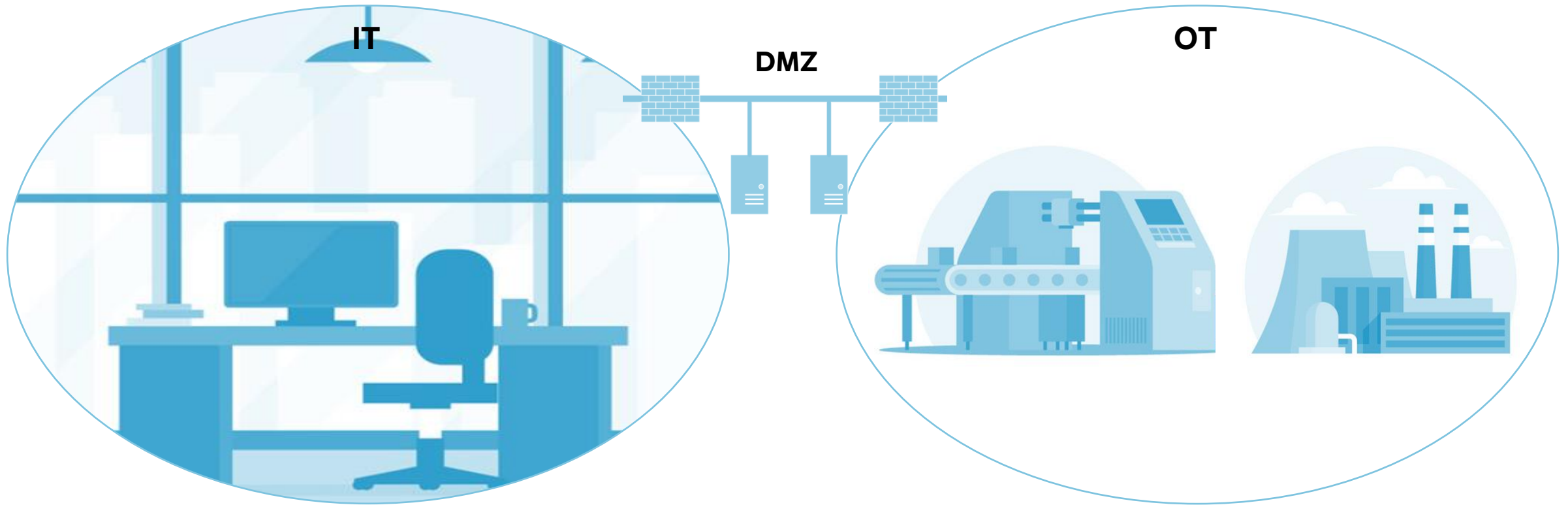
# Digital transformation



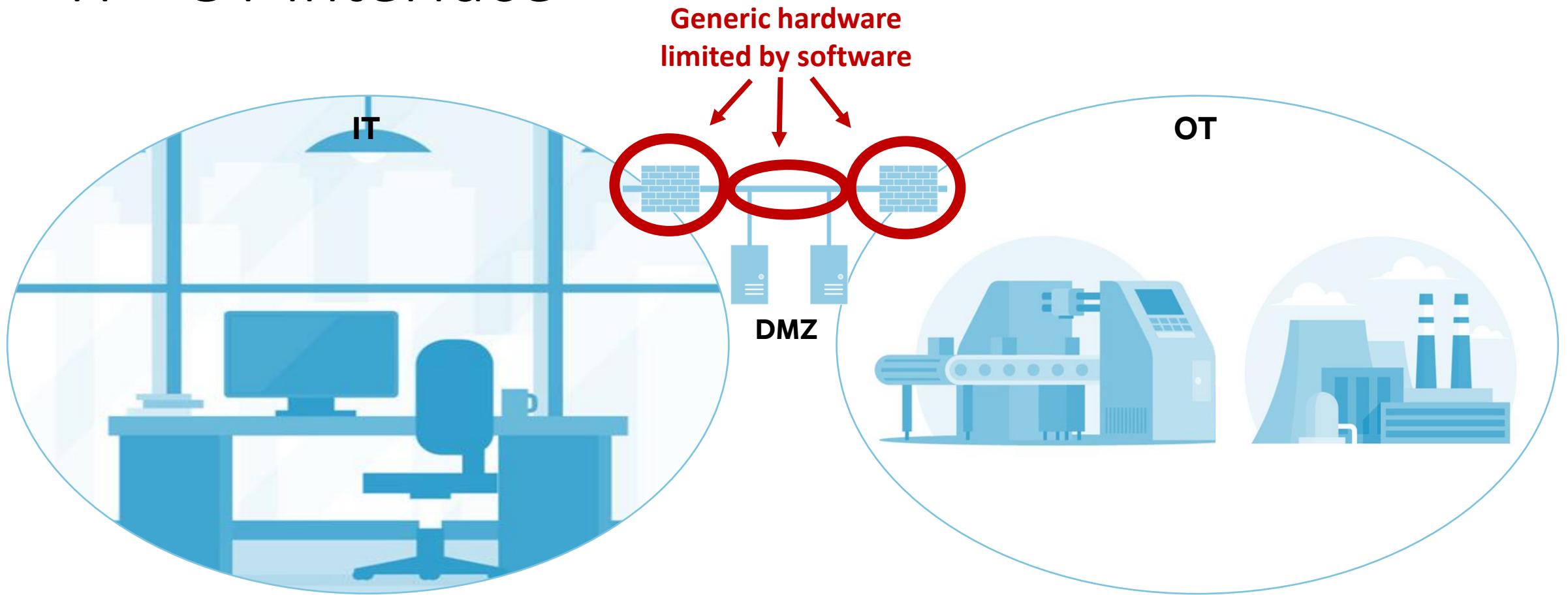
# Digital transformation



# IT - OT interface

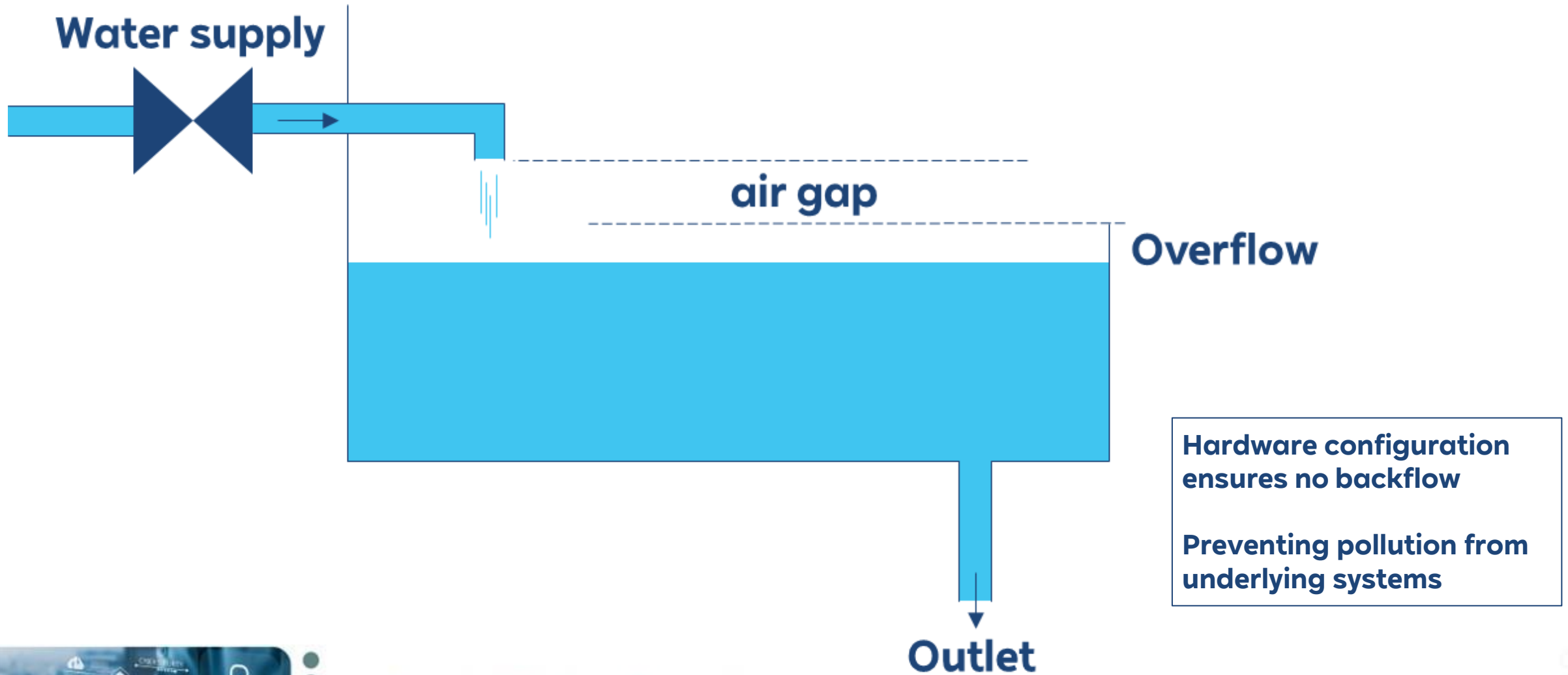


# IT - OT interface

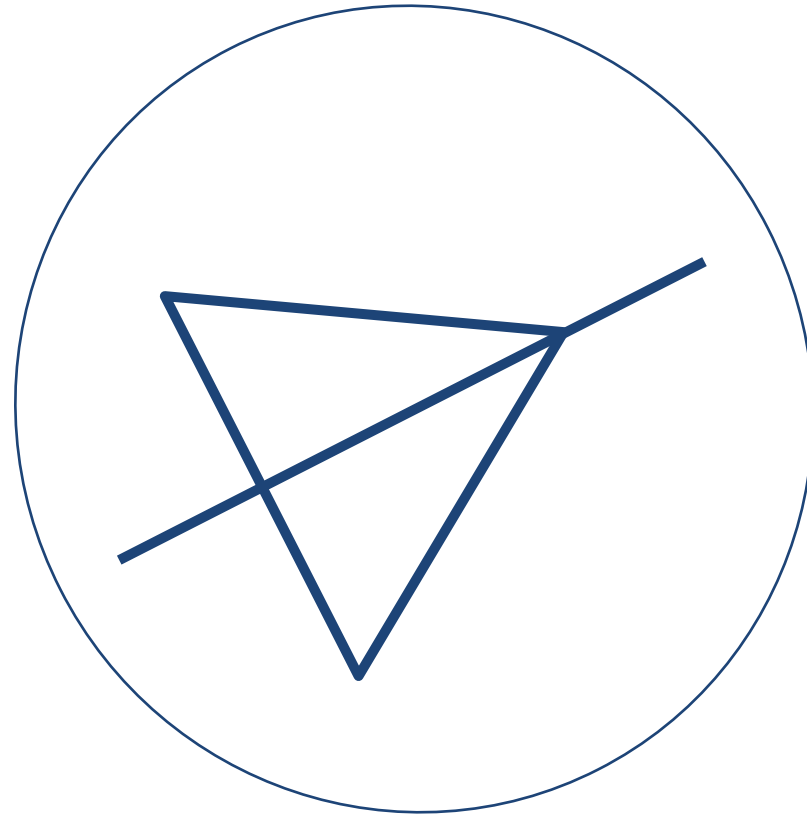




# Example: Break tank to protect the water supply

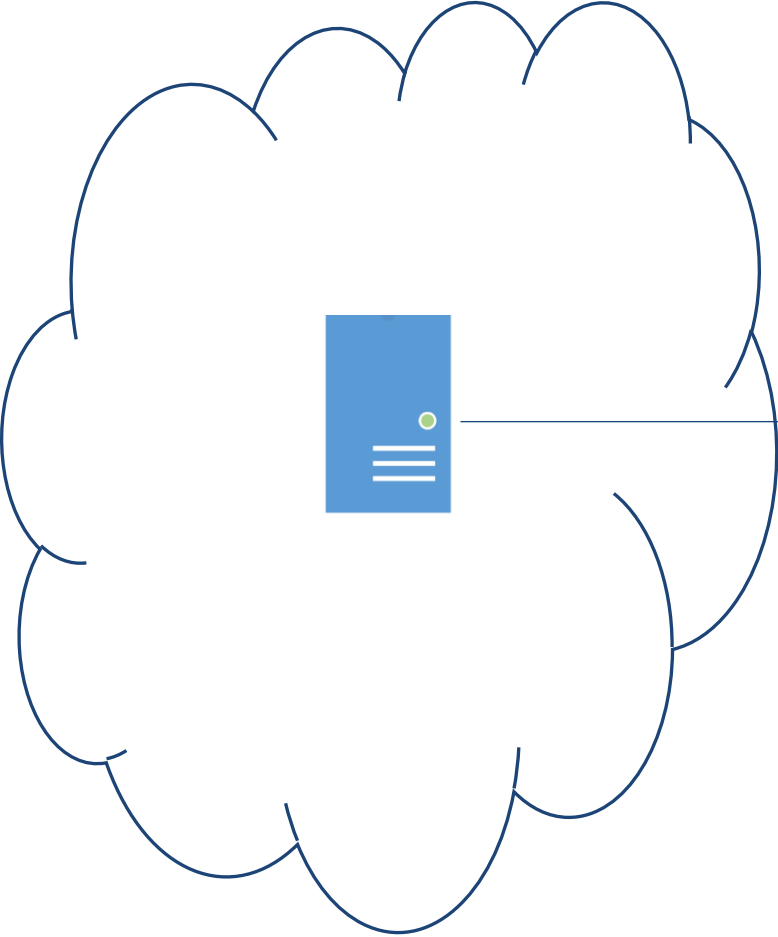


# Data diodes not often used within the industry



# Data diode: The modern air gap

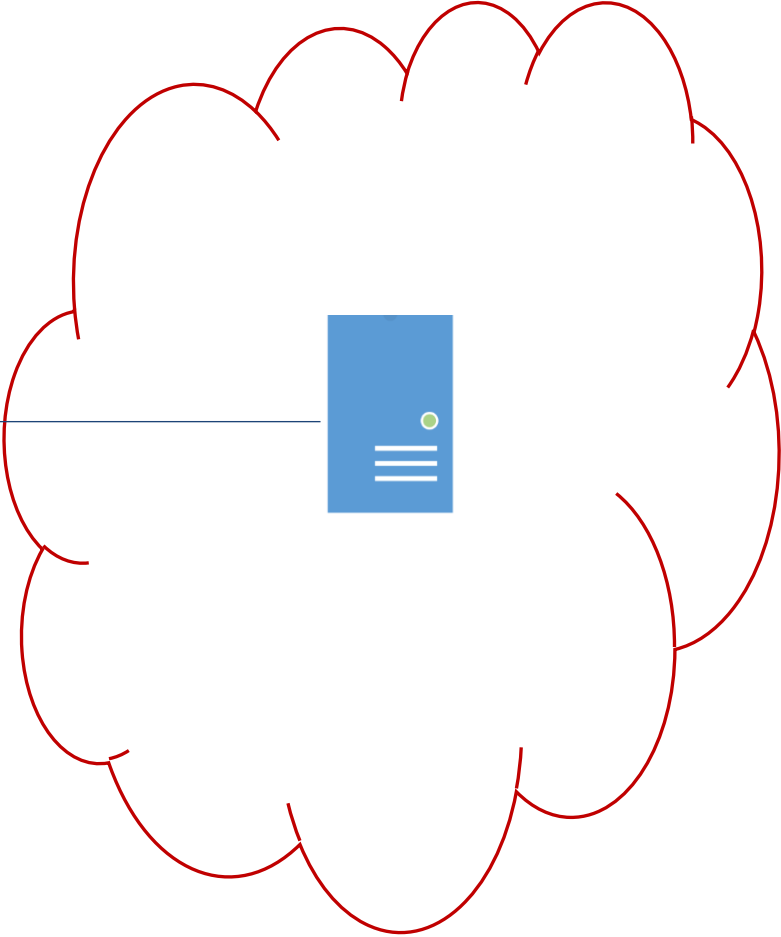
**Central Infrastructure**



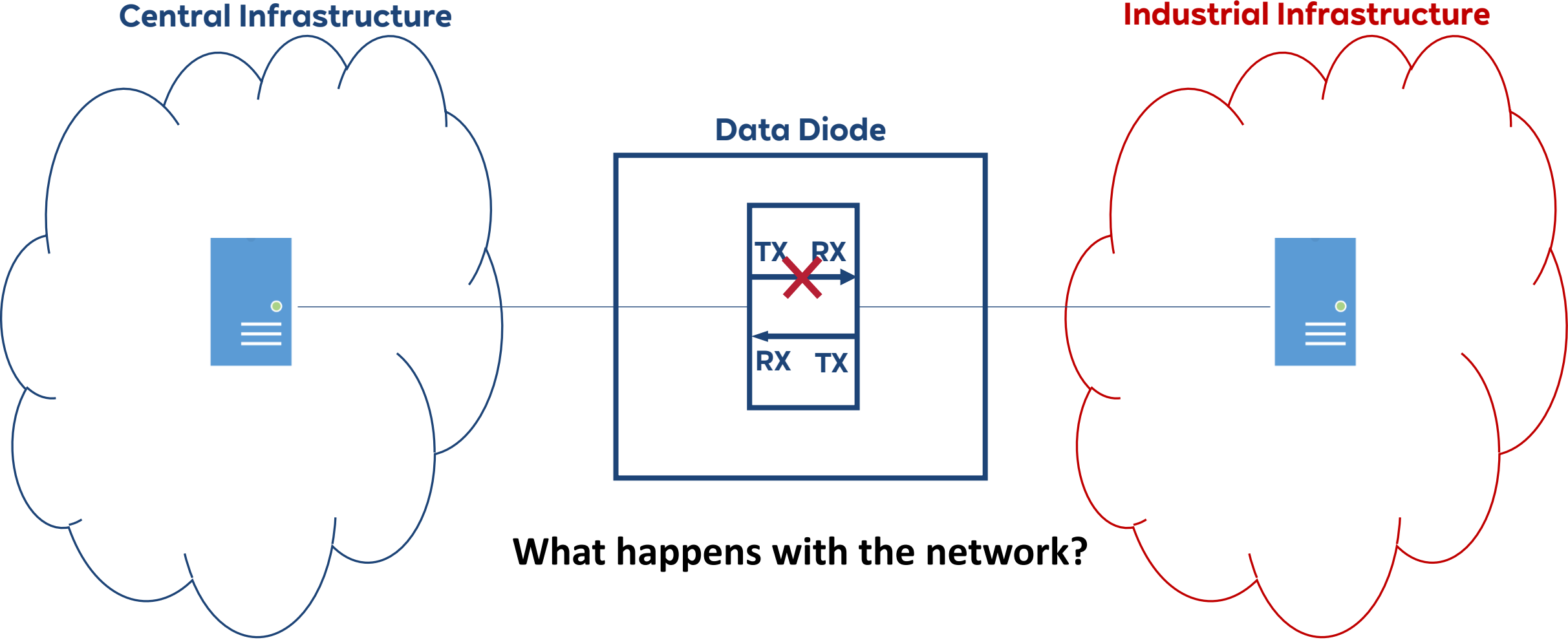
**Data Diode**



**Industrial Infrastructure**



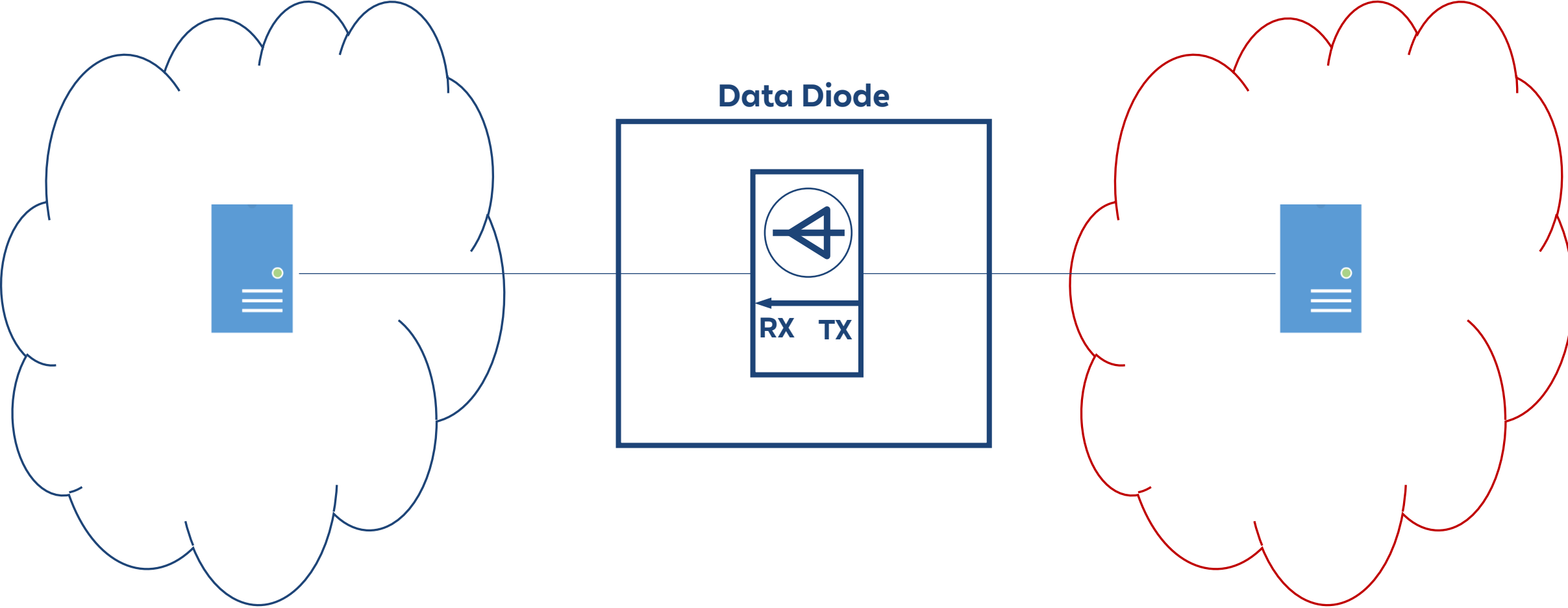
# Data diode: Unidirectional channel (1/2)



# Data diode: Unidirectional channel (2/2)

Central Infrastructure

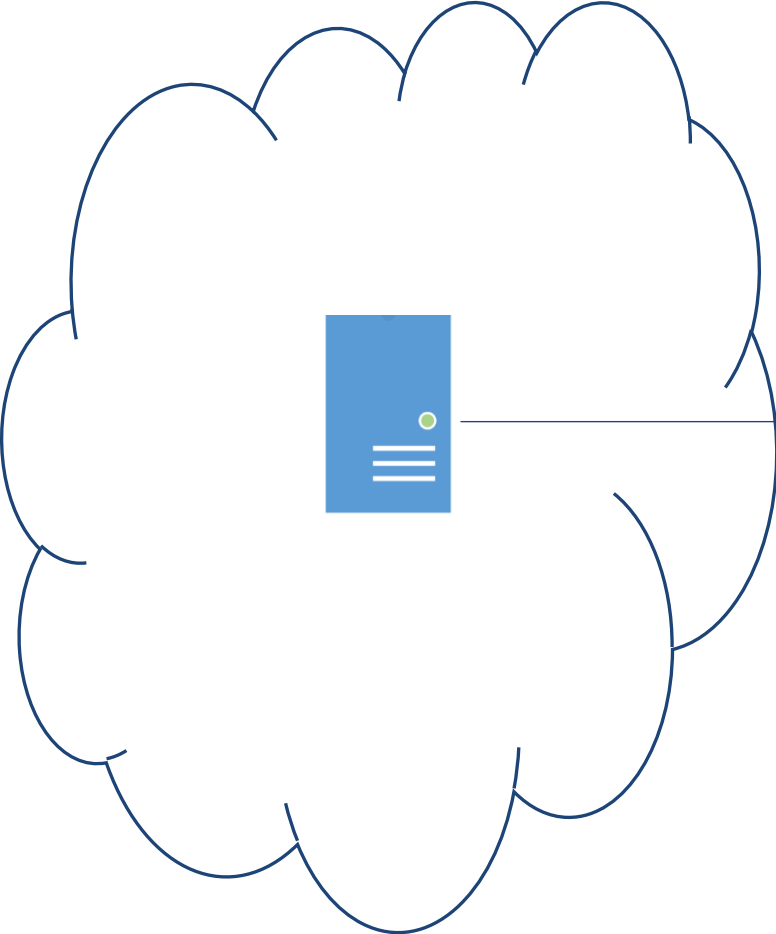
Industrial Infrastructure



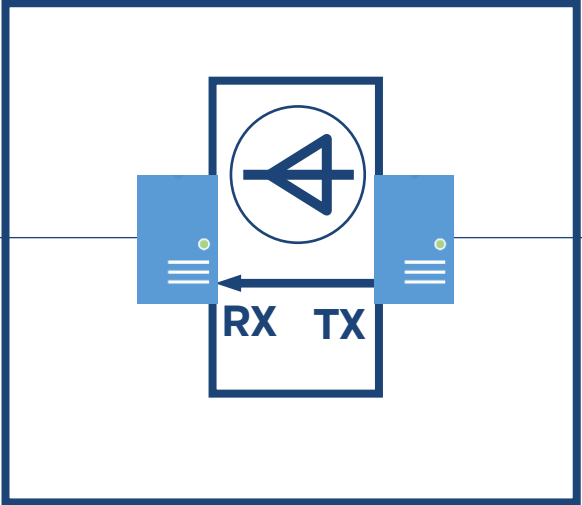


# Data diode: Proxies

Central Infrastructure

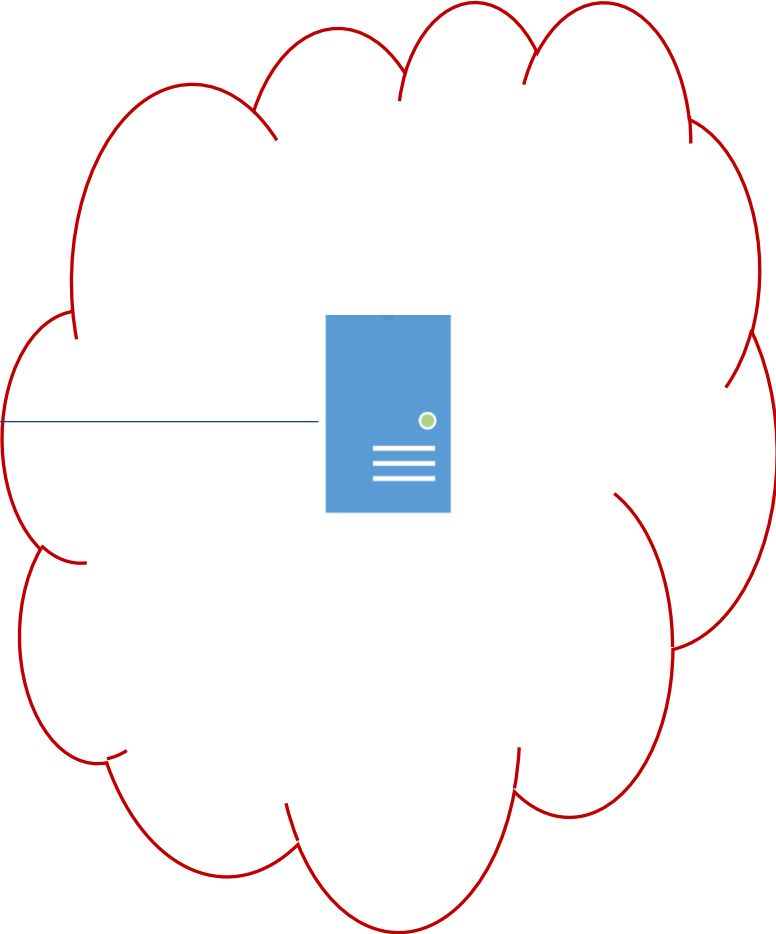


Data Diode



**Proxies can communicate with connected networks AND send data over the unidirectional channel**

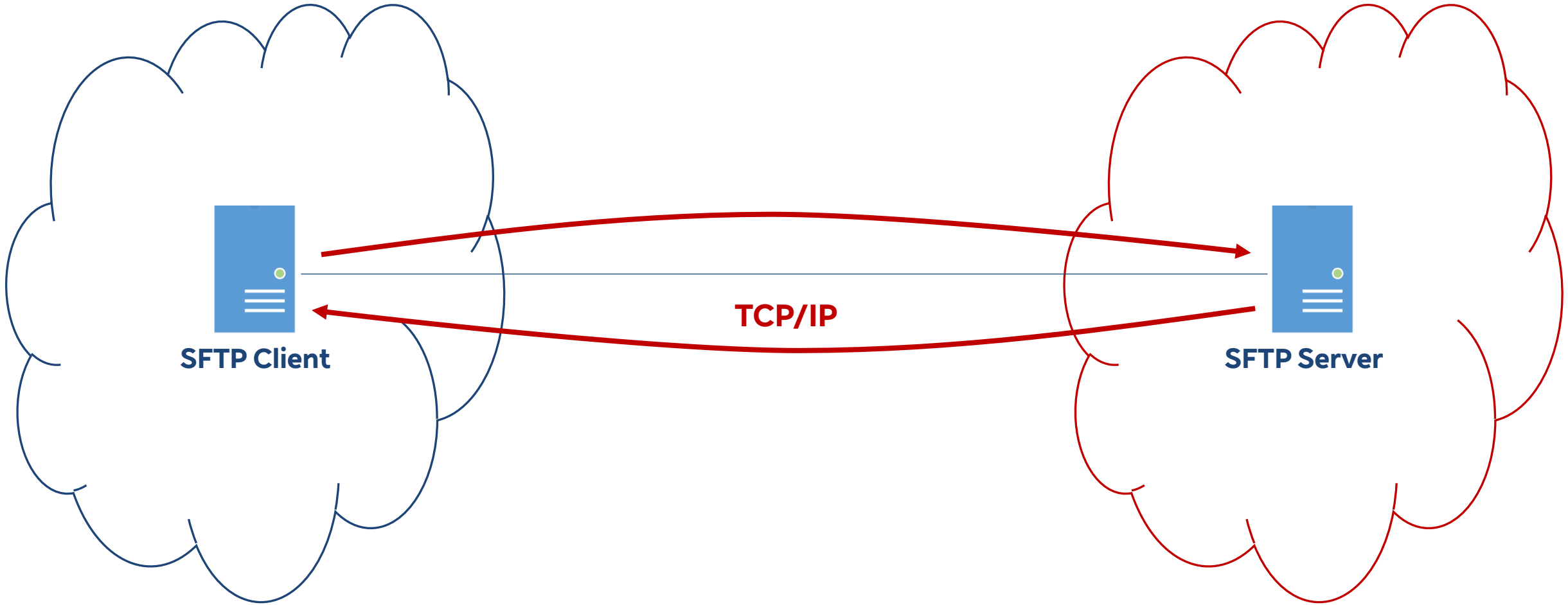
Industrial Infrastructure



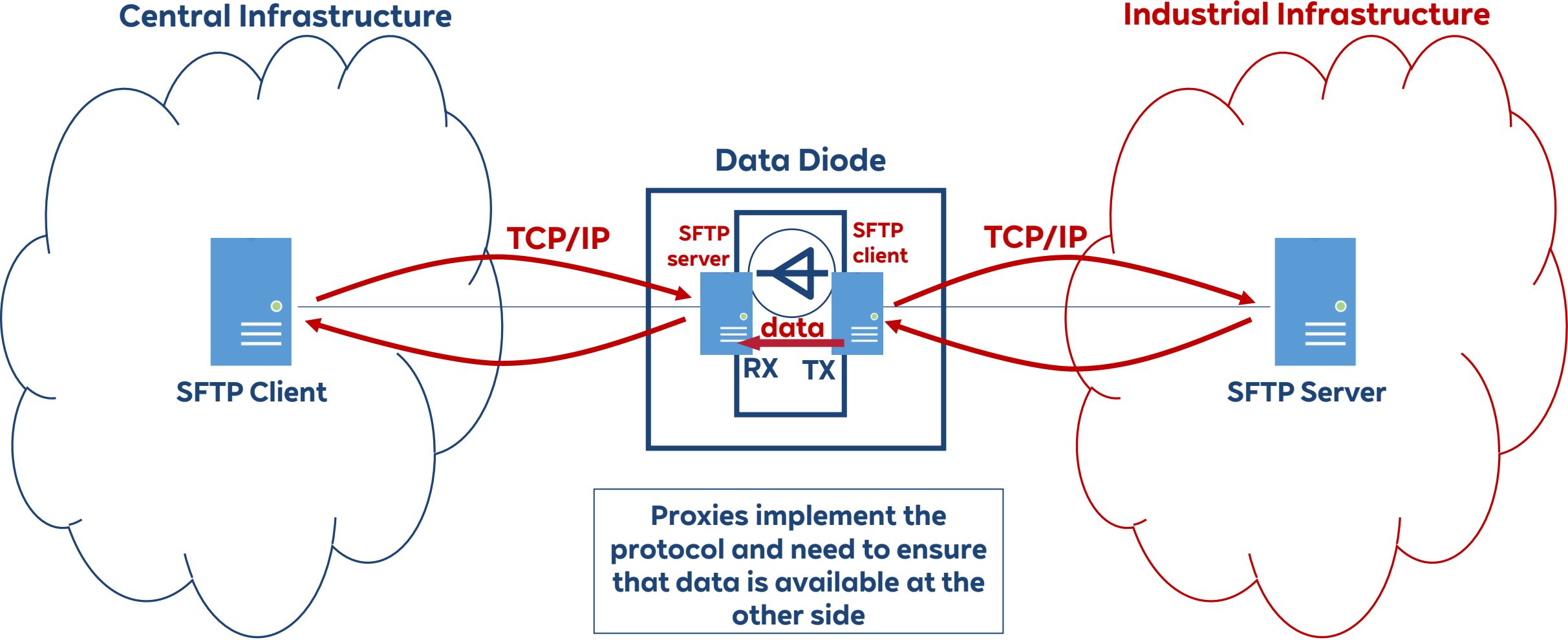
# Data diode: Example SFTP server (1/2)

Central Infrastructure

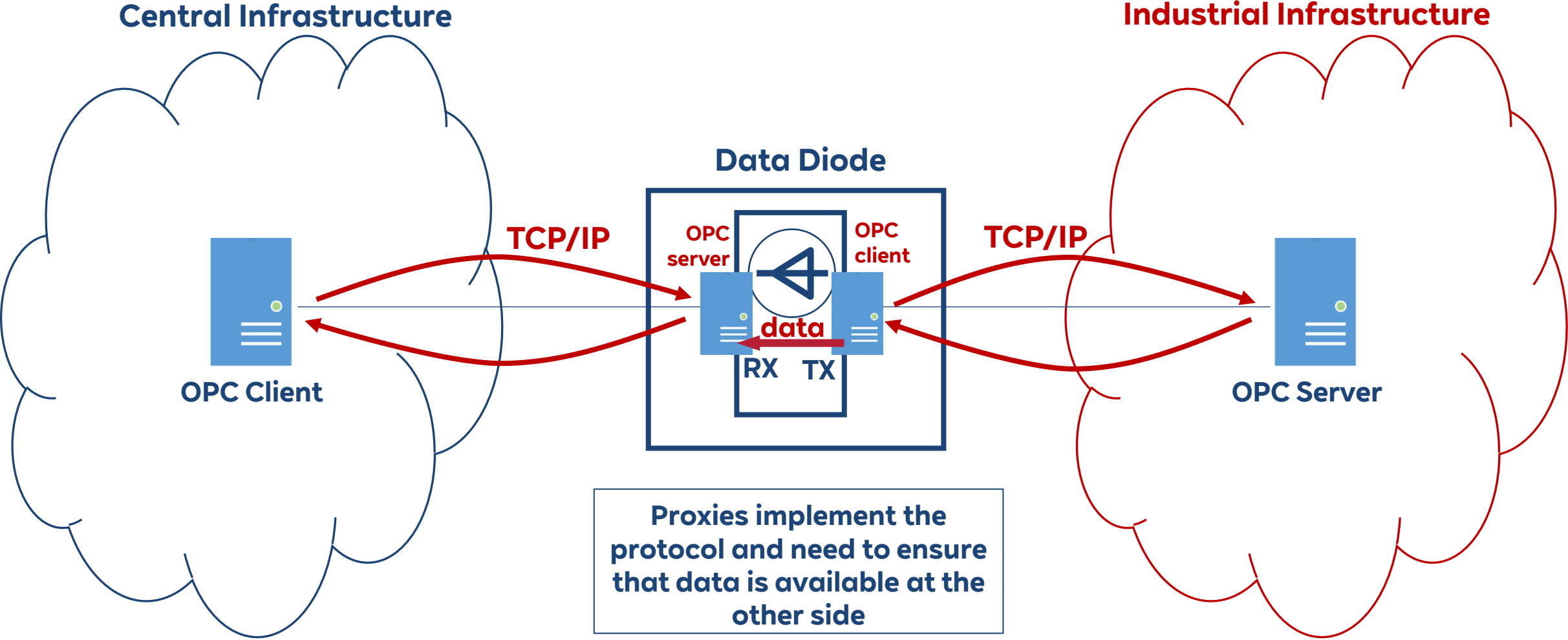
Industrial Infrastructure



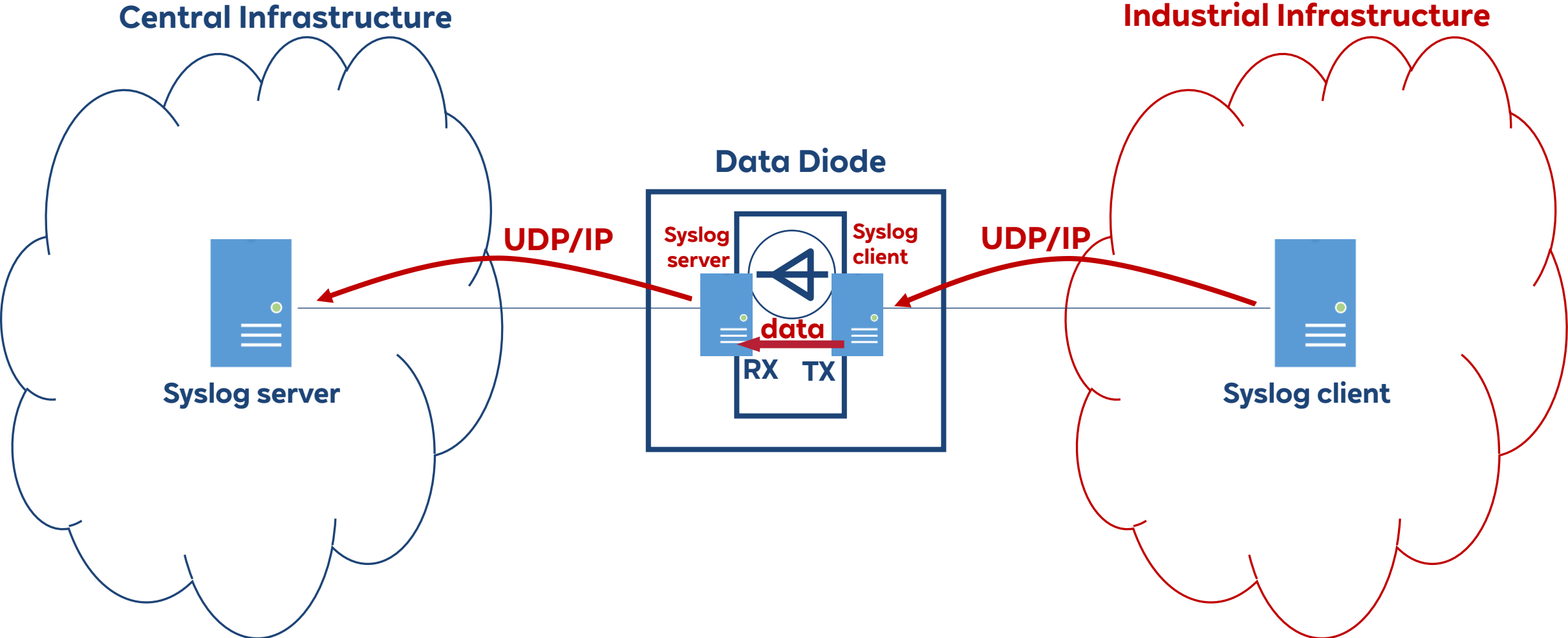
# Data diode: Example SFTP server (1/2)



# Data diode: Example OPC

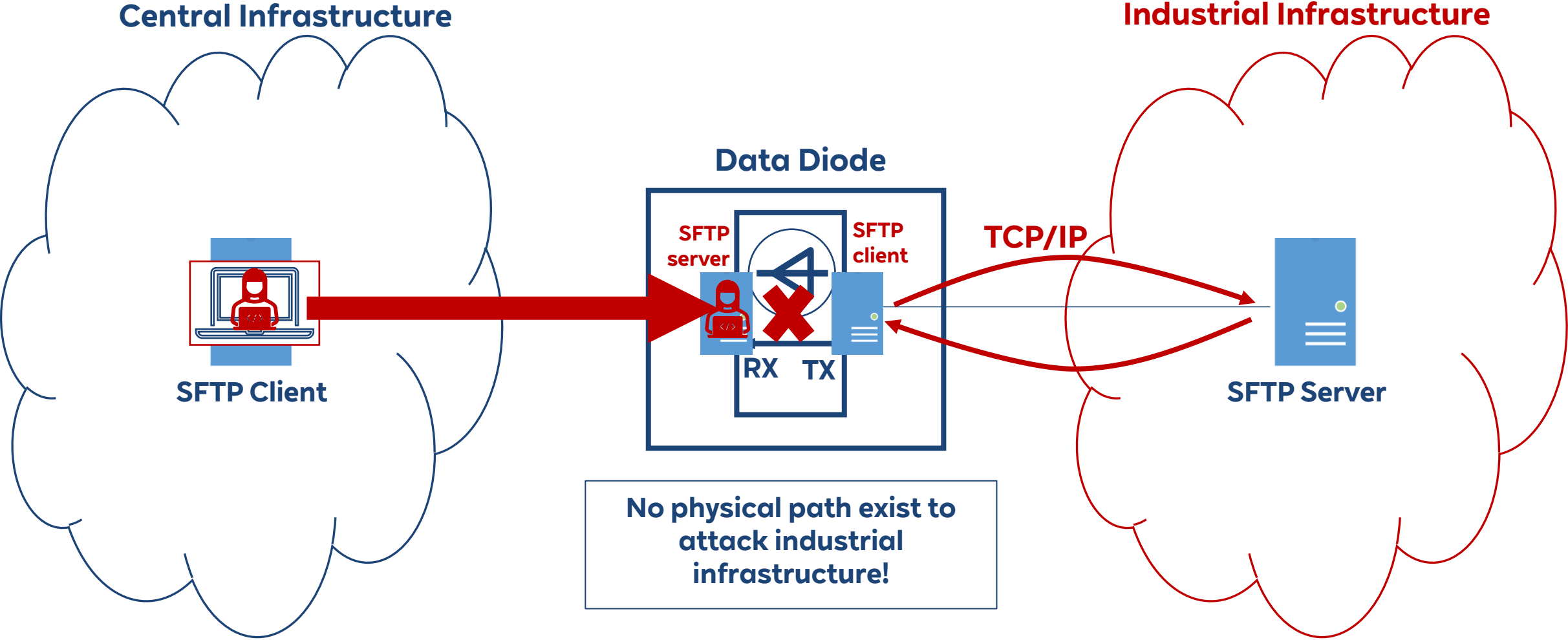


# Data diode: Example Syslog (UDP/TCP)

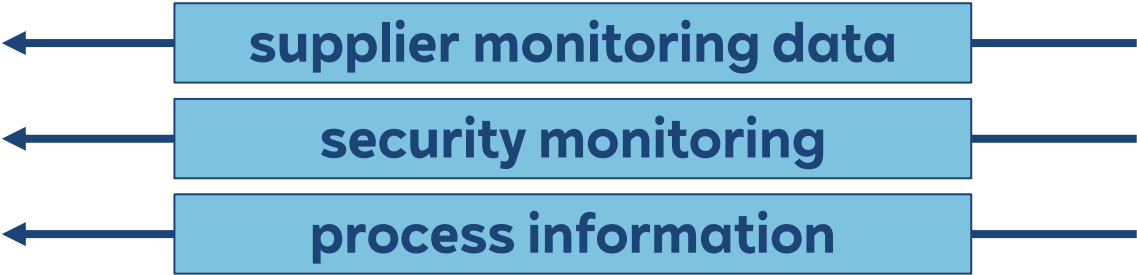




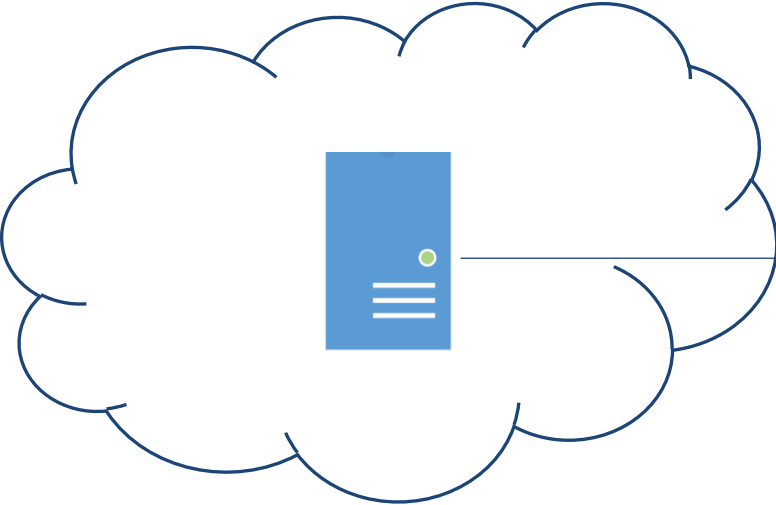
# Data diode for getting data: Ensures no attack vectors back



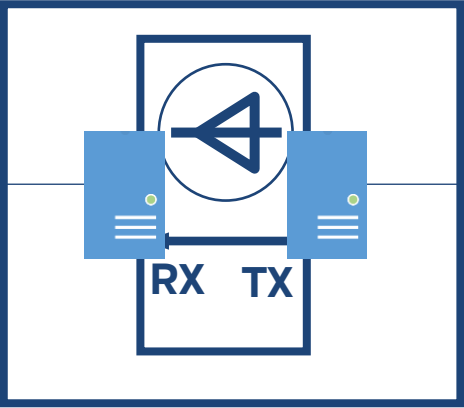
# Data diode: Common applications



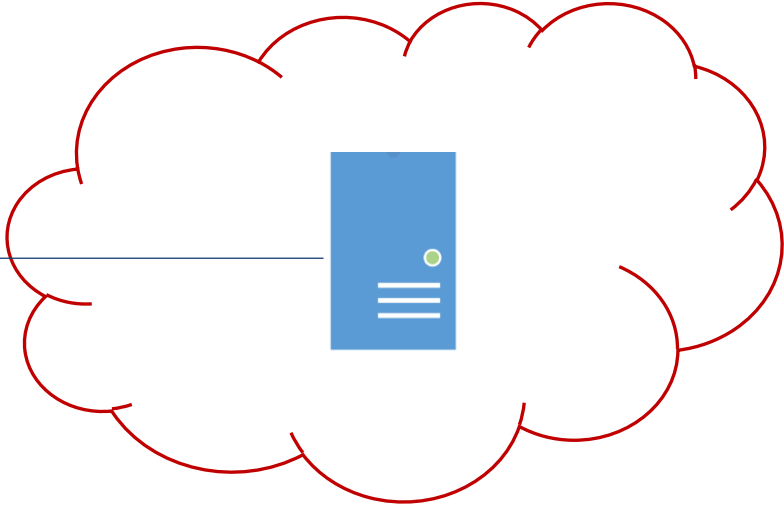
**Central Infrastructure**



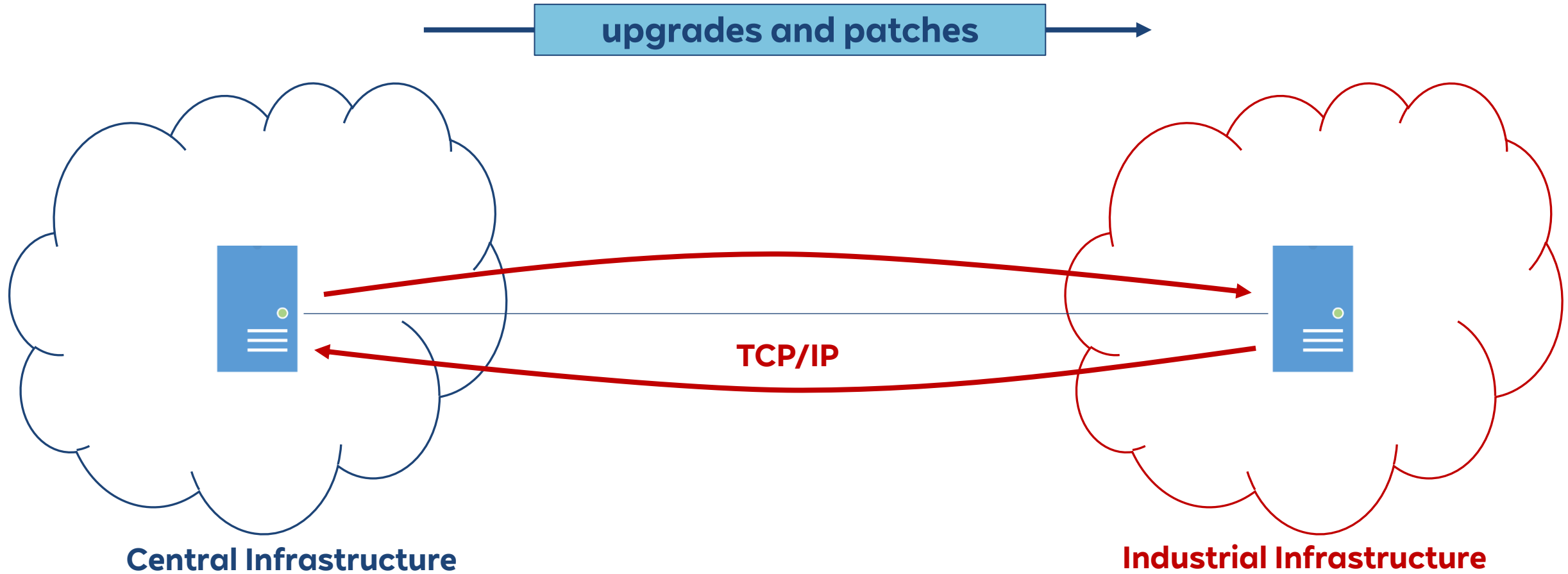
**Data Diode**



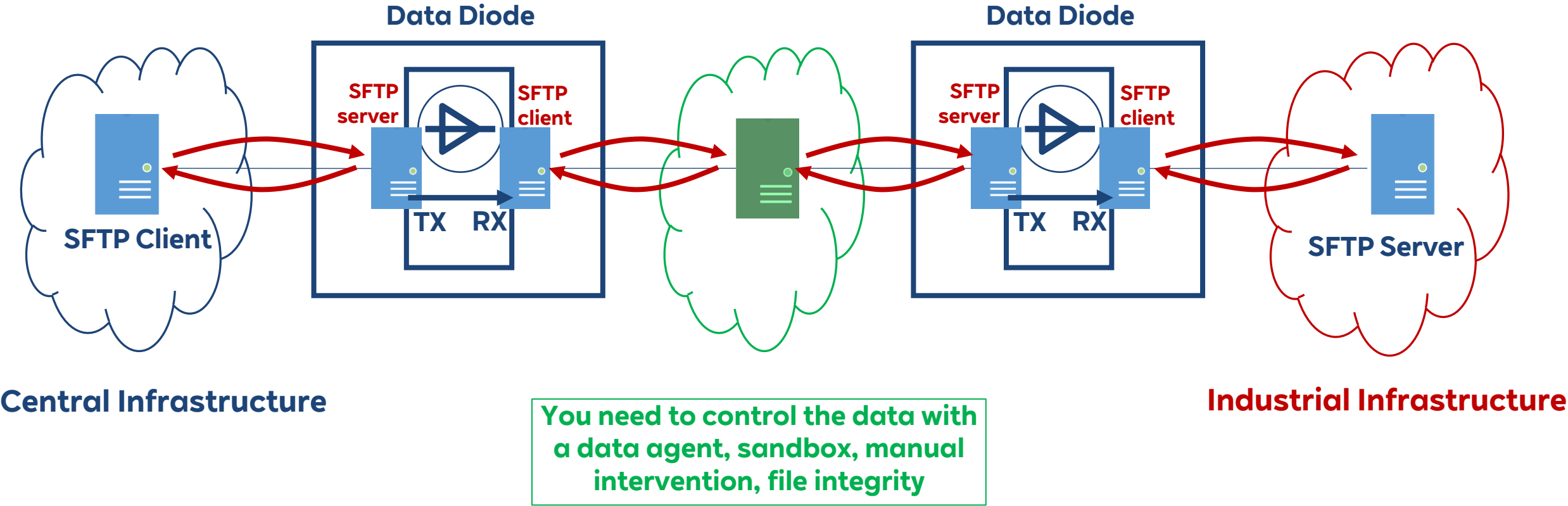
**Industrial Infrastructure**



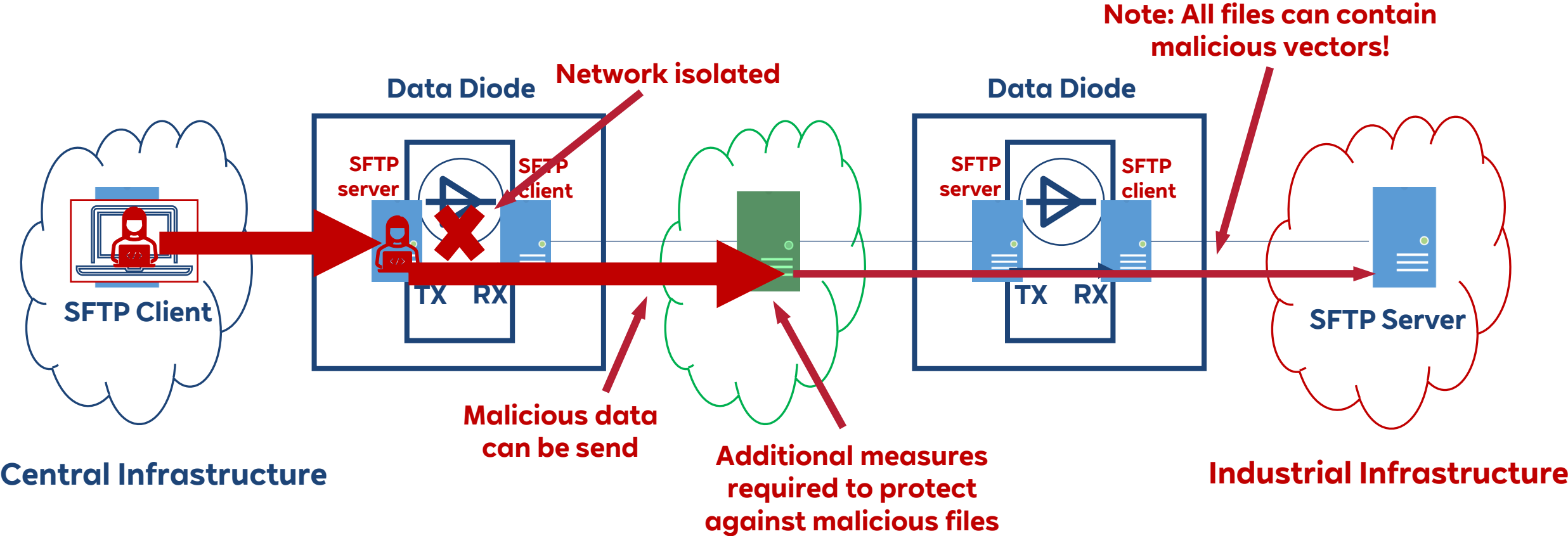
# Data diode: Example automatic updates (1/4)



# Data diode: Example automatic updates (2/4)

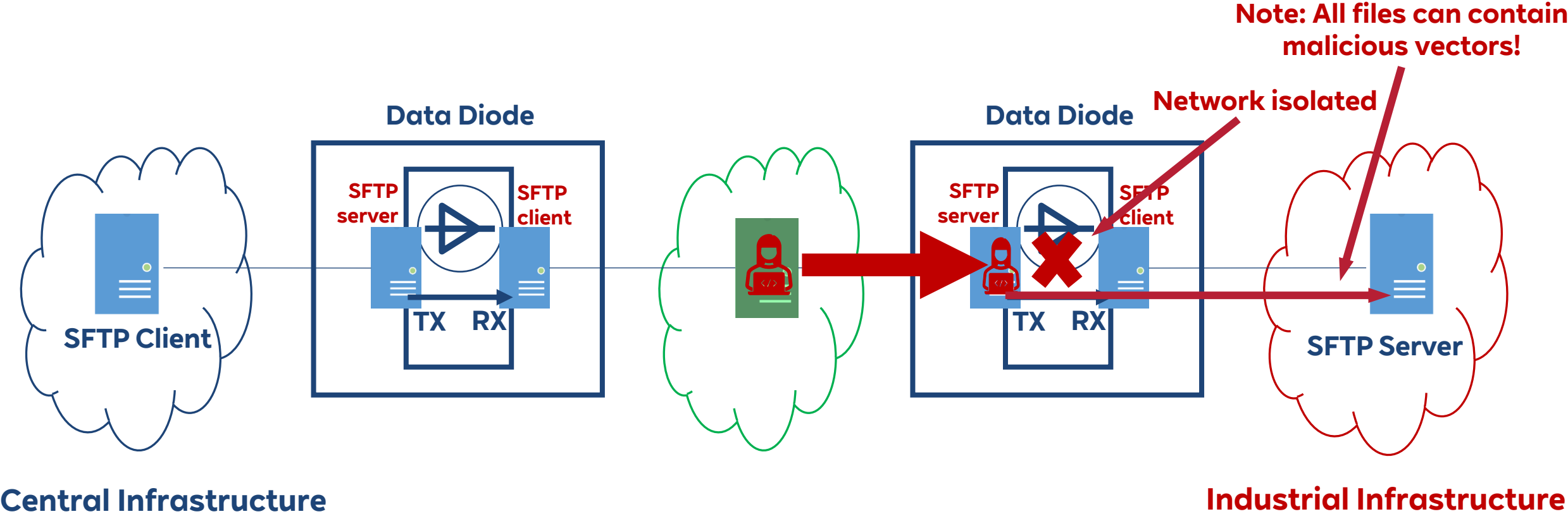


# Data diode: Example automatic updates (3/4)

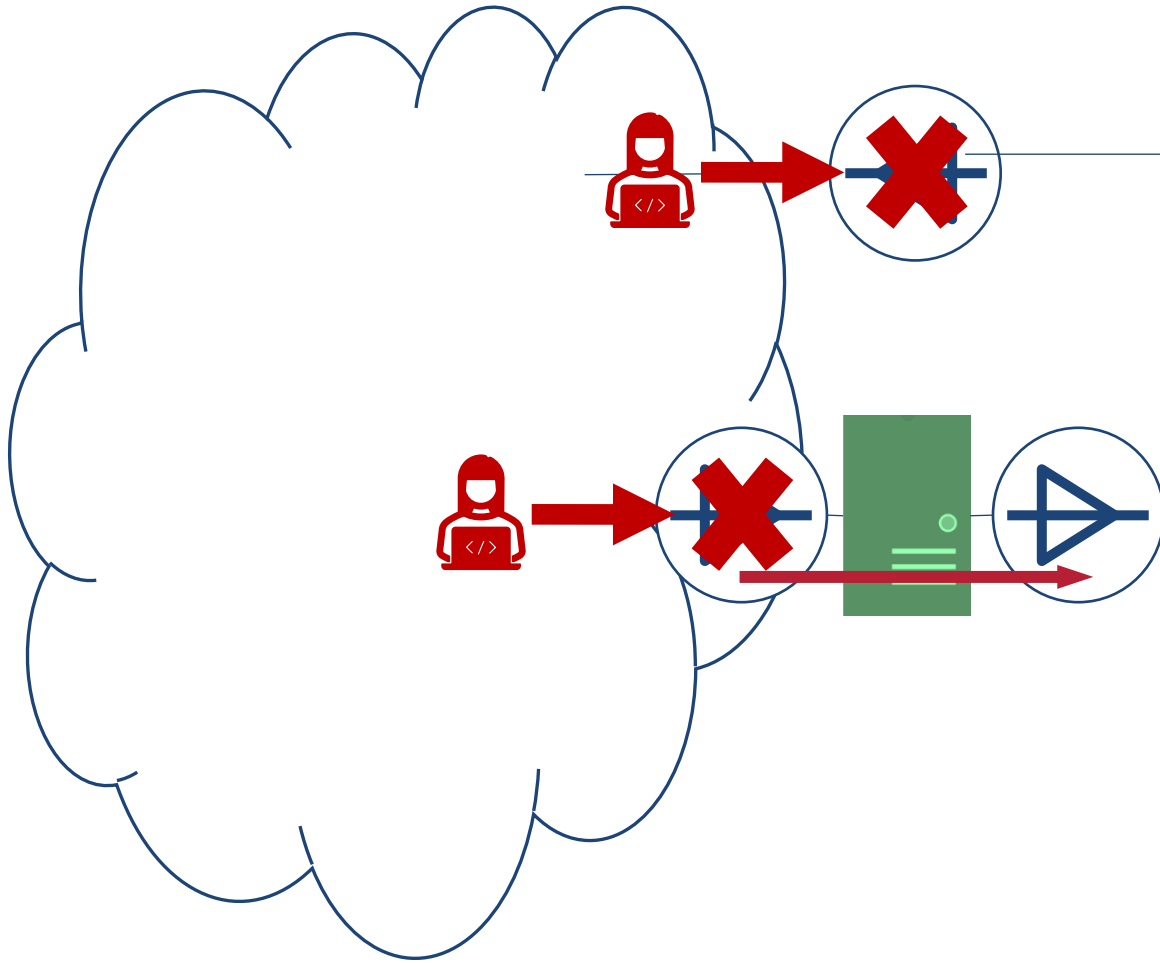




# Data diode: Example automatic updates (4/4)



# Summary



**1. Data diodes ensure no backward attacks possible**

**2. Data diodes isolate networks: modern air gap**

**3. Reversed direction require control of data possible with two data diodes (residue risk)**

**4. Data diodes increase protection to industrial networks significantly**

**5. Do not combine IT-OT and segregate. Respect OT and create secure-by-design IT-OT interfaces.**



