CYBERSECURITY

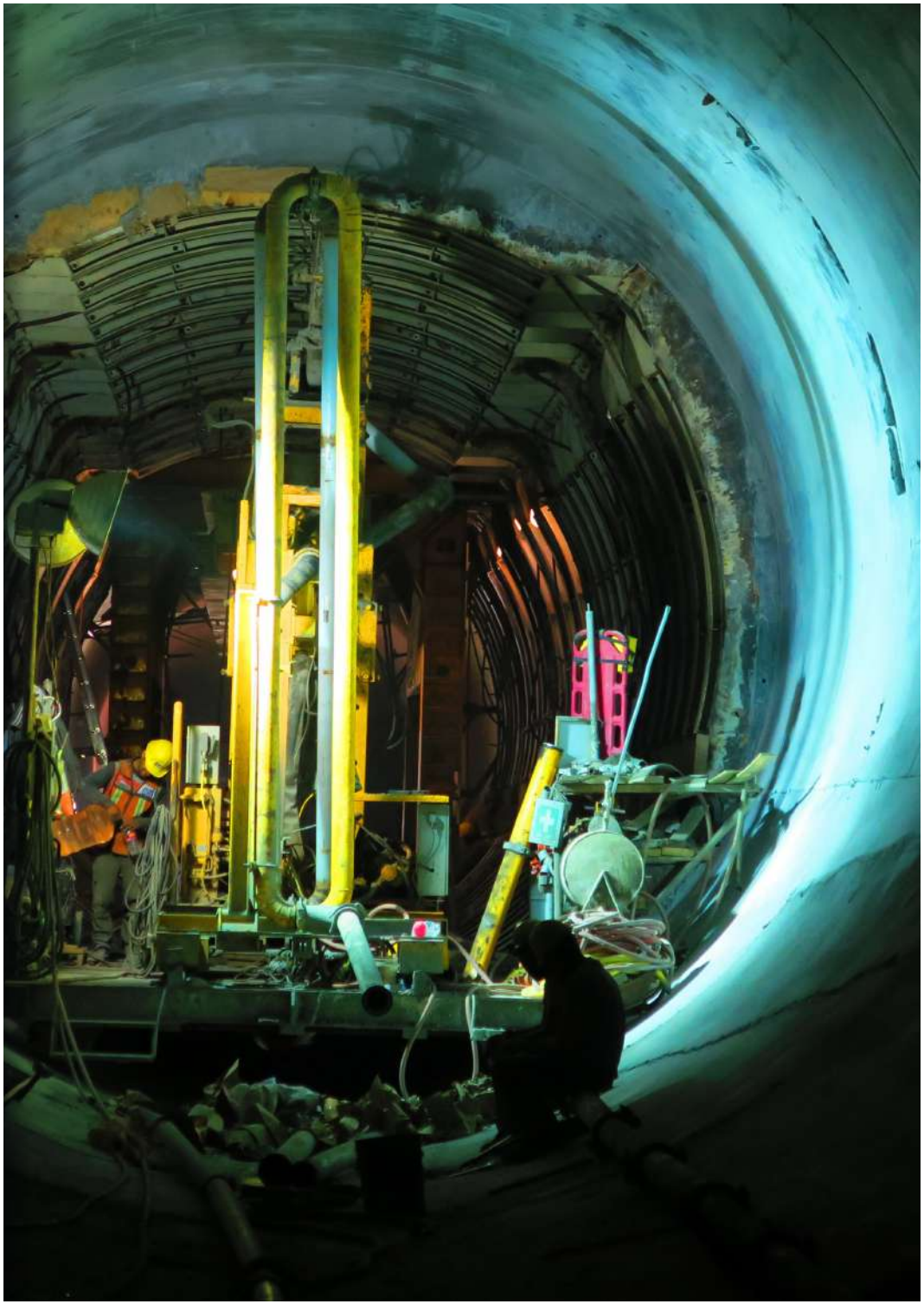
The **Secure Xchange** Story

seclāb

THE PROBLEM

The OT network needs to be highly secured, but...

Lots of **users on the IT network want access to OT** to do their jobs!



ACTUAL SOLUTIONS – AND WHY IT'S NOT ENOUGH

FIREWALLS

Most industrial organizations start by deploying firewalls between IT and OT networks.

However, there are problems with firewalls.

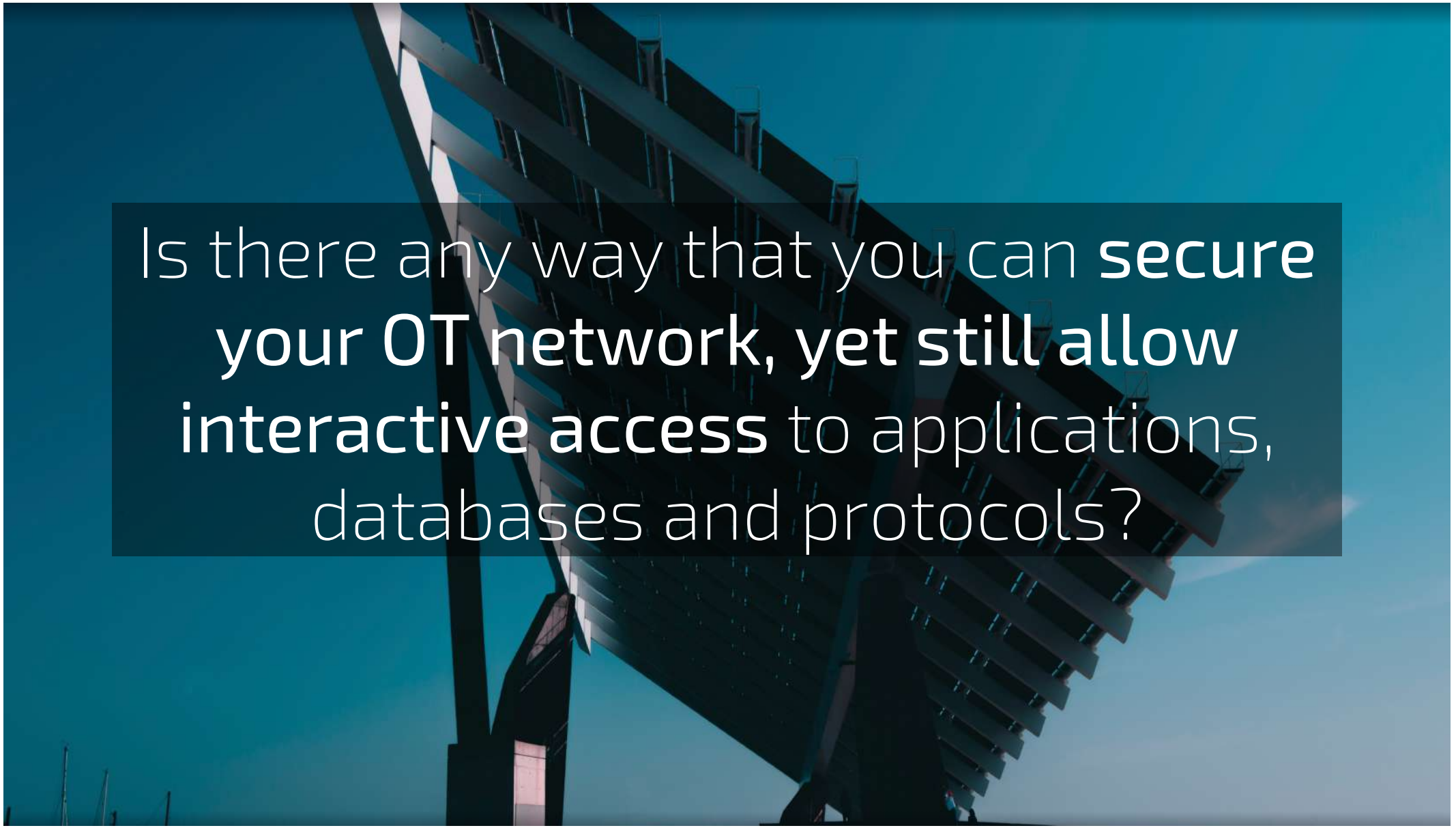
DATA DIODES

They promise total security from any attacks from the IT into the OT network.
But they also **completely cut off any interactive access with OT applications, databases and protocols.**

REPLICATION

Some databases can be replicated to the IT network, where they can be used.

But many applications, and most protocols, can't be "replicated".


Is there any way that you can **secure your OT network, yet still allow interactive access** to applications, databases and protocols?

THE SOLUTION

Seclab **Secure Xchange** has been **used in Europe for many years**.

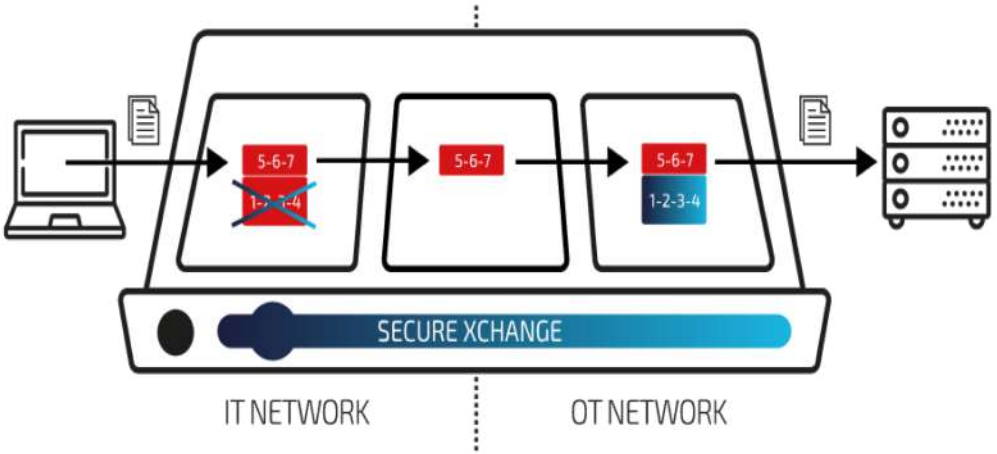
Like data diodes, it provides **total protection from network layer attacks**.

But unlike data diodes, it **adds full bi-directional communications between OT and IT**.

It does this by :

1. **Destroying layers 1-4 of each packet from the IT network**, while leaving layers 5-7 (application) alone.

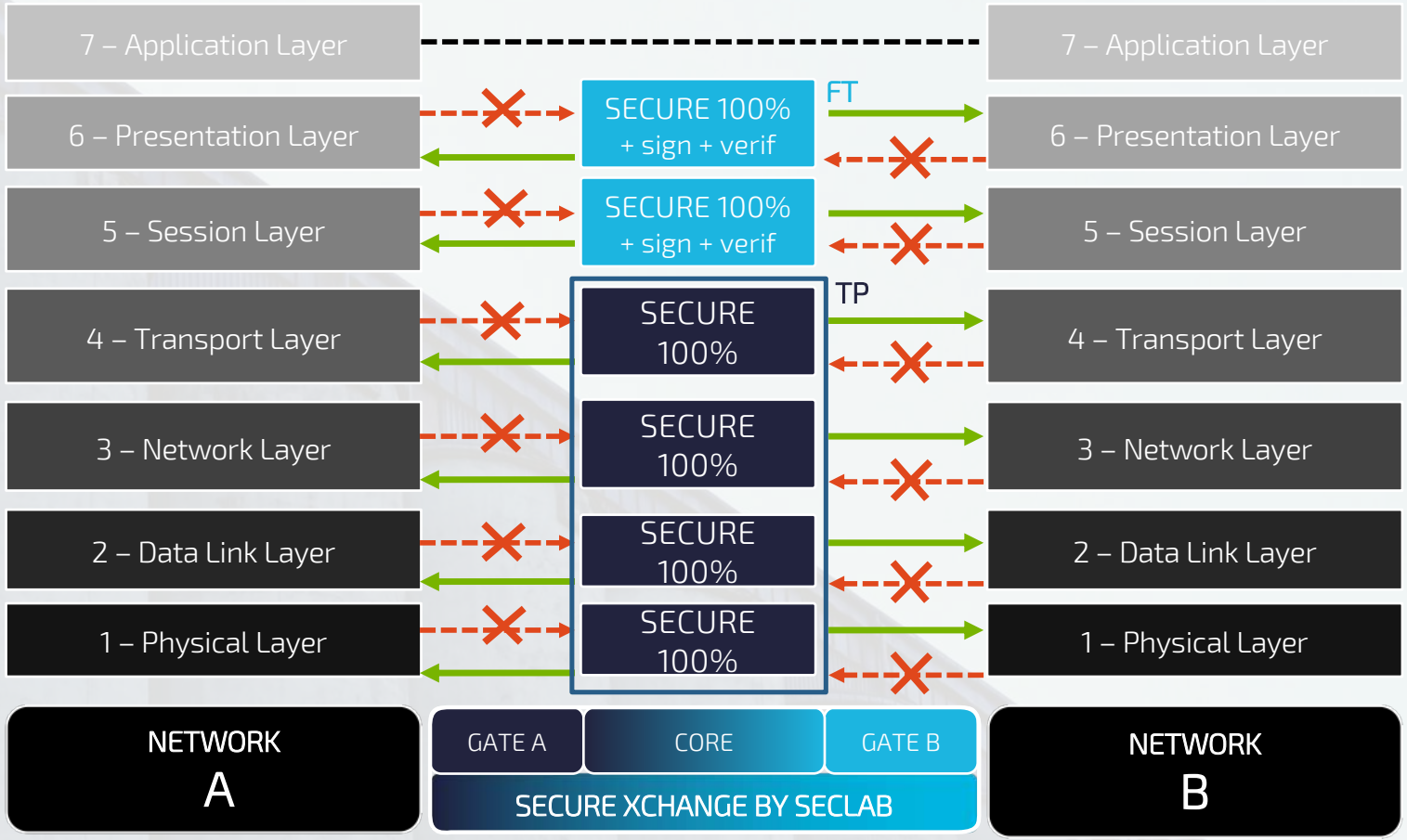
2. **Then re-creates layers 1-4** and inserts the packet **on the OT network**.



IN-DEPTH VIEW:
SECURE TRANSPORT TECHNOLOGY & OSI MODEL

Protection against threats:

- TCP syn flooding
- TCP attack
- UDP flooding
- UDP attack
- MAC flooding
- IP modification
- MAC Modification
- DHCP attack
- ICMP attack
- MAC Attack
- …



SECURE XCHANGE

Most attacks and network reconnaissance occur **on layers 3 and 4** (Network and Transport); **there is no possibility any of these attacks will get through to the OT network**.

It means **your users can continue to use applications, databases and protocols** on the OT network, even though **the level of security has greatly increased.**

APPLICATION-LAYER ATTACKS

There have been **attacks at layer 7**.

Since Secure Xchange passes layers 5 to 7 unchanged from the IT to the OT network, **how does it protect against those attacks?**

In two ways…

APPLICATION-LAYER ATTACKS

First, Secure Xchange offers Direction Control.

This allows you to specify, for example, that all Modbus sessions must originate on the OT network, so no attack on Modbus can ever come from the IT network.

This is a very powerful tool.

Sometimes, Direction Control isn't practical. In those cases, **you can deploy an application-layer firewall "in front of" Secure Xchange**.

You can tune the firewall to block application-layer attacks that apply to the applications in your OT environment.

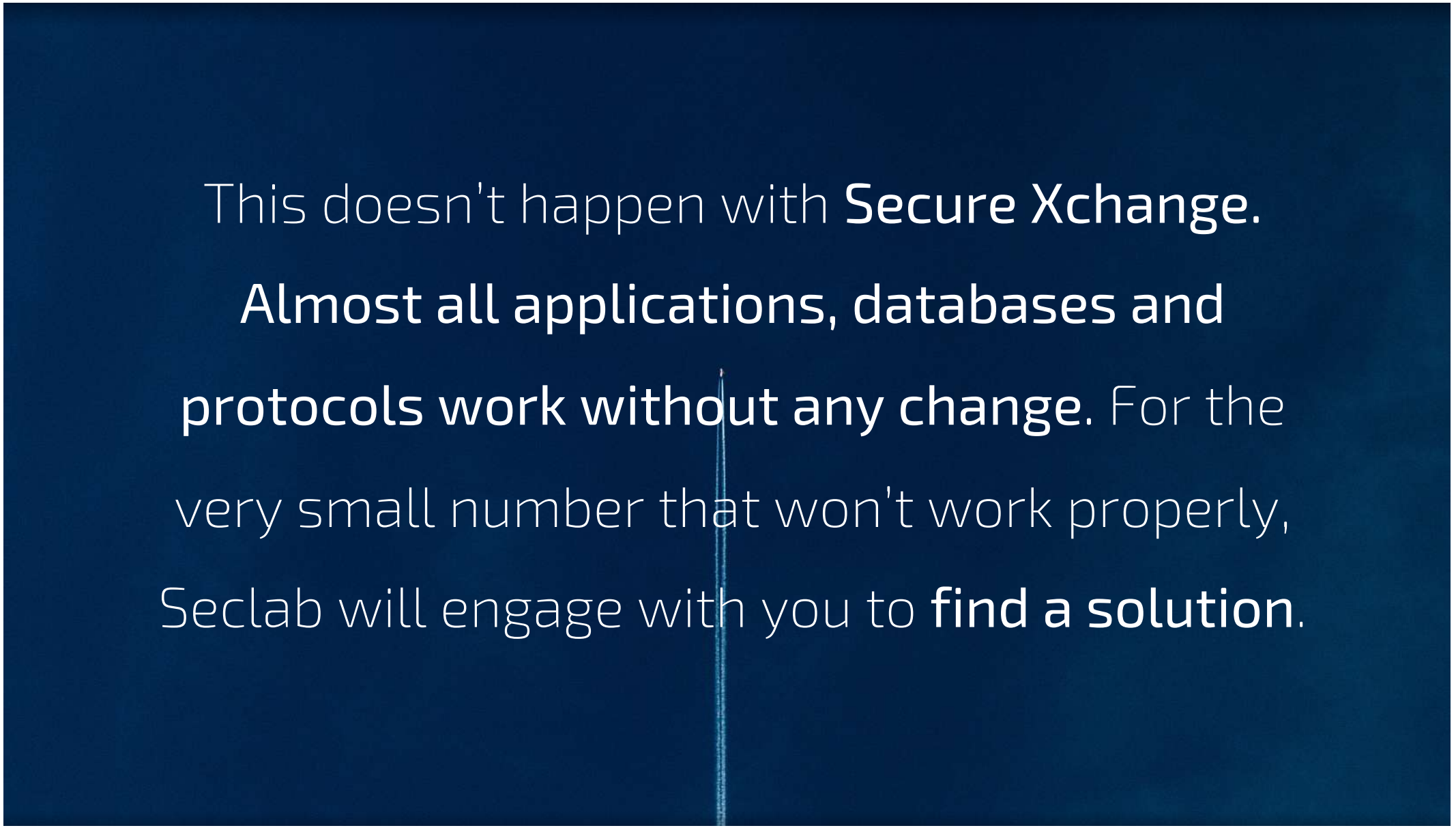
The firewall protects layers 5 to 7, while Secure Xchange protects the rest.

WHICH APPLICATIONS WORK?

All applications, databases and protocols are developed under the assumption that the user will **have interactive (bi-directional) access**.

Since **data diode solutions block interactive access**, there always **needs to be a special workaround for any application** that your IT network users still need to use – e.g. database replication.

But many applications, and most industrial protocols like Modbus, **can't be "replicated"** to the IT network. **With a data diode, there is no solution for this, other than moving physically to the OT network.**


This doesn't happen with **Secure Xchange.**
Almost all applications, databases and protocols work without any change. For the very small number that won't work properly, Seclab will engage with you to **find a solution**.

For more information

www.seclab-security.com

contact@seclab-security.com

(+33) 411 930 859

seclāb