WHITE PAPER

Network security is not enough for OT data

Cogent DataHub™

Everyone agrees network security is essential for IT systems. And yet, securing OT (operational technology) networks is even more critical. One successful exploit on a production network might halt production, incur huge costs, and even put lives at risk. For OT systems, a secure network is essential—but that's not enough anymore. There's still the question of data security.

Before the days of Industry 4.0, Internet of Things, and digitalization, it was fairly simple to secure OT networks and data—just disconnect them, by air gap if need be. But that is no longer an option for any company that wants to stay competitive. The modern enterprise needs secure access to data from OT to increase efficiency and cut production costs.

The good news is that with the right approach, secure access to OT data does not have to be overly complicated or costly. Whatever level of network security you have, there are easy and affordable ways to access your OT data securely.

Data security: different from network security

Such affordability is possible because data security is different from network security. Although data security can be implemented alongside network security, and be fully compatible with it, the goals of each are not exactly the same. The difference is a little like home security.

Running a system without network security is like leaving a door open, allowing anyone to enter your house. Unwanted visitors can steal things or hold your family members hostage for ransom. You're also exposed to viruses from any infected person who walks in.

Securing the network

To secure the network, a company might implement zero-trust network access—at significant cost. Such a solution often uses VPNs to restrict network access to a limited number of authorized people.

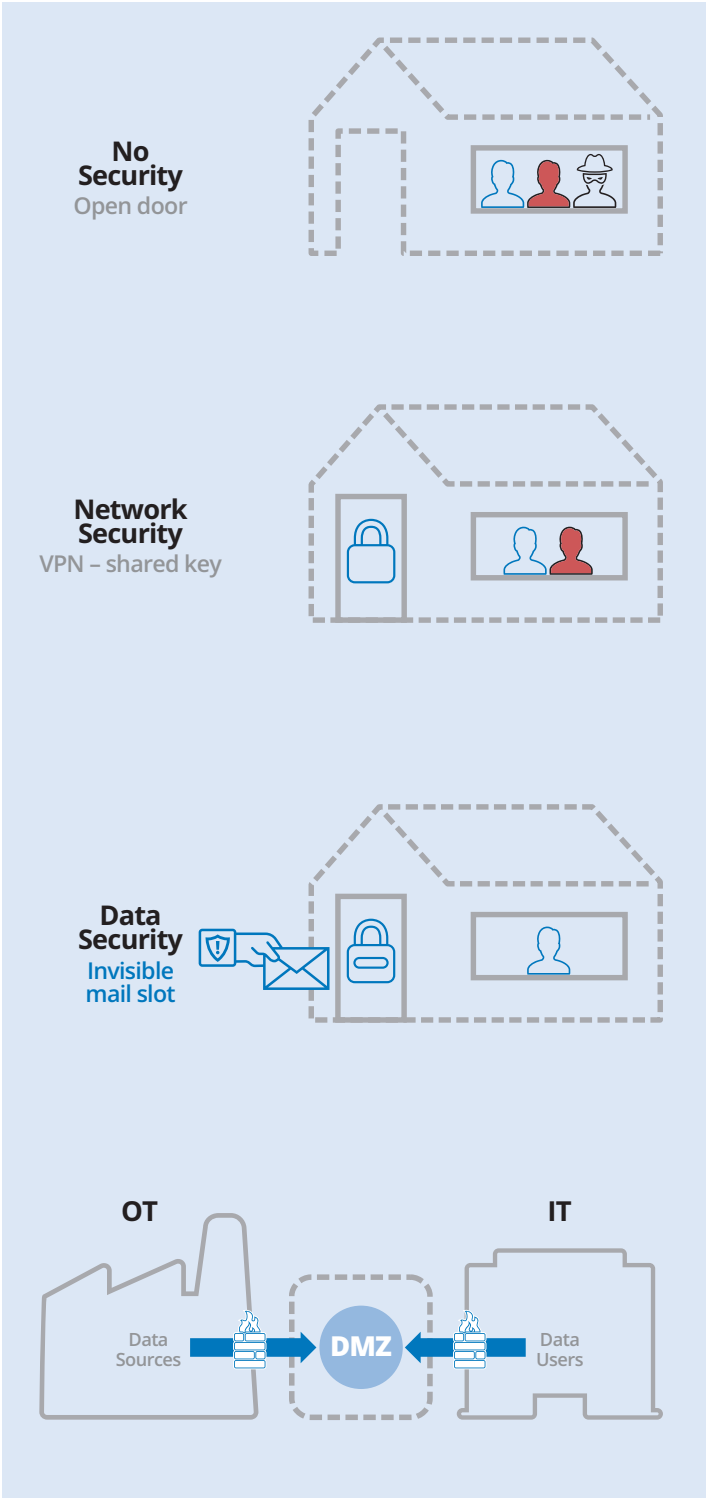
Using a VPN is like allowing only invited guests with a key to enter your house. These guests can still be carrying unwanted viruses that might infect your household. A VPN that extends from the IT network to OT simply extends the security perimeter to enclose OT. Should anyone in IT receive a phishing email or plug in a thumb drive with a virus on board, the malicious code could easily propagate to OT.

An invisible mail slot

For data access, a better solution—which is both cost-effective and secure—is to simply close the network to everyone and set up secure data connections. It's like pushing open an invisible mail slot in your door and exchanging messages with an authorized mail carrier. Nobody enters the house to bring in a virus or hold your family members hostage. When you close the mail slot it blends back in with the door. Only the mail carrier knows it's there and only they can drop off or pick up messages.

For industrial systems, the invisible mail slot is an outbound firewall port at the plant. The mail carrier is typically a tunnelling application or MQTT broker running on-site or in a DMZ. If you are using a DMZ, the IT side can implement the same mail slot interface--and keep all IT inbound firewall ports closed as well.

Using a DMZ is recommended by the EU's NIS 2 Directive and NIST SP 800-82 as the best way to segregate OT and IT networks. Each network must be secure, and any data connection between them must also be secure. Network security and data security should work hand in hand.



Viable options

Whatever level or type of network security you deploy, you need the right software and services to gain secure access to your data. If you simply need to isolate your OT system from IT or the cloud, you can use MQTT or Sparkplug to make outbound connections while keeping all inbound firewall ports closed. Some tunnel/mirroring software, such as Skkynet's Cogent DataHub, can do this and more. Unlike MQTT, this kind of well-designed tunnel/mirroring

solution can pass data seamlessly across a DMZ in both directions, maintaining the connection status and data quality information at every step.

To make an even more secure connection and ensure one-way data flow, you can use a data diode. This is a hardware device that allows and enforces only one-way communication, and prevents any kind of message from the destination getting back to the source. Some tunnel/mirror solutions are fully compatible with data diodes, and can even be used to aggregate data sources on the sending side or to distribute data to various clients on the receiving side.

Working together

The thing to remember is that network security and data security are both important. They may be implemented separately, but they should work together as one unit. No matter what level or type of network security you have, Skkynet provides the technology and know-how you need to fully integrate it with data security.

About Skkynet

Skkynet is a global leader in real-time software and services that allow companies to securely acquire, monitor, control, visualize, network and consolidate live process data in-plant or in the cloud. DataHub™, DataHub™ for Azure, and Embedded Toolkit (ETK) software enable secure, real-time data connectivity for industrial automation, Industrial IoT, and Industrie 4.0. Visit **skkynet.com** for more about the company and **cogentdatahub.com** for more about DataHub.