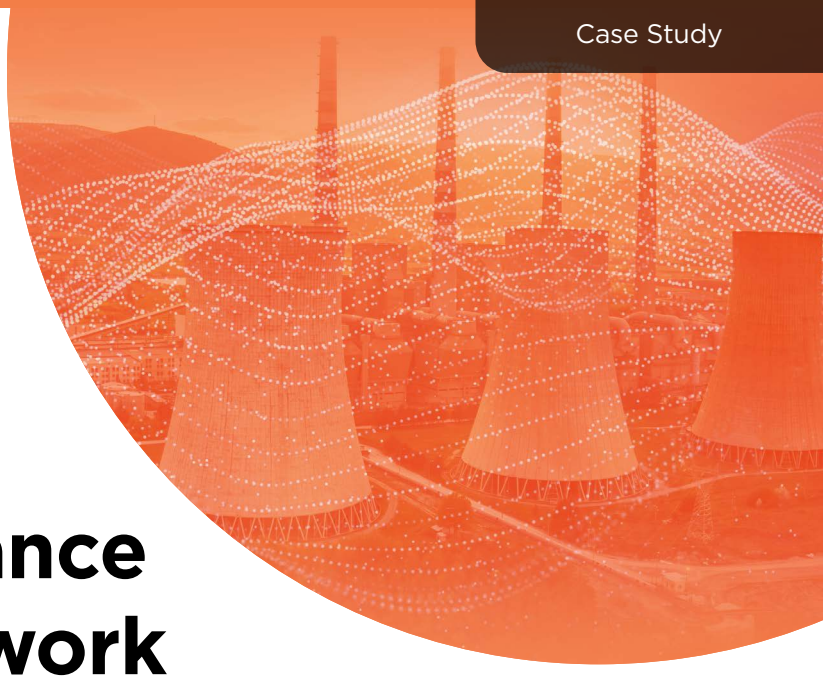
Case Study



Ensure compliance with IT/OT network segregation policies

UK electricity and gas provider selects Skybox Security to ensure policy compliance for segregating their OT networks.

Learn how you can:

- Model the OT network.
- Check that firewalls and routers are correctly configured.
- Ensure IT/OT network separation.

A UK electricity and gas infrastructure provider needed to monitor and maintain network access and separation across their Operational Technology (OT) networks. They chose the Skybox Security Posture Management platform to help them meet their compliance responsibilities.

The exploitation of IT and OT vulnerabilities represented

40%

of initial infection vectors for attacks on organizations connected to OT networks[1]

[1] Attacks on operational technology from IBM X-Force and Dragos Data, 2020

Business challenge

Work with specialist ICS firewalls and switches

The UK electricity and gas infrastructure provider controls the national transmission and distribution of electricity and gas, serving the needs of over 50 million people and more than 5 million businesses.

The organization uses a dedicated Operational Technology (OT) network to manage the delivery of energy via a network of overhead lines, pylons, underground cables, pipes, and transmission substations.

The organization wanted a solution to help them manage access to this network and **ensure compliance with best practices for OT network segregation.** A key requirement was that the solution should work with the organization's installed base of specialist Industrial Control System (ICS) firewalls and switches.

> "We needed to monitor OT network access and ensure compliance with strict segregation polices."
>
> **UK electricity and gas provider**

Solution

Ensure compliance with best practices for network segregation

The organization selected the Firewall Assurance and Network Assurance modules of the Skybox Security Posture Management platform.

Using Skybox, the organization created a network model that emulates the actual OT network. This model is a dynamic, visual representation of the network generated by aggregating and centralizing data from the ICS firewalls and network assets.

The organization uses the model to **analyze network access compliance,** eliminate potential blind spots, and ensure complete visibility for the security team.

Using Skybox, the organization ensures its ICS firewalls are correctly configured in line with industry best practices. The team uses compliance policies to inspect specific rules to identify violations in the configured source, destination, port, or application and to prohibit violating traffic from moving between network zones.

> "Skybox worked with us to ensure the integration with our ICS firewalls and switches worked seamlessly."
>
> **UK electricity and gas provider**

Results

Deliver accurate, up-to-the-minute reports

Using Skybox gives the team a dynamic model of the OT network that illuminates how the various ICS firewalls and networking devices behave. Thereby, the team eliminates the risk that cyber attackers could exploit a blind spot.

The platform collects configuration information from all the network-addressable devices on the OT networks, providing complete operational visibility and an understanding of network separation and the network's compliance levels. It helps the team **ensure good firewall hygiene and deliver accurate, up-to-the-minute reports** demonstrating the actual – rather than theoretical – level of network access and segregation.

> "Using the Skybox platform, we can test, demonstrate and ultimately ensure we comply with network separation regulations."
>
> **UK electricity and gas provider**

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo