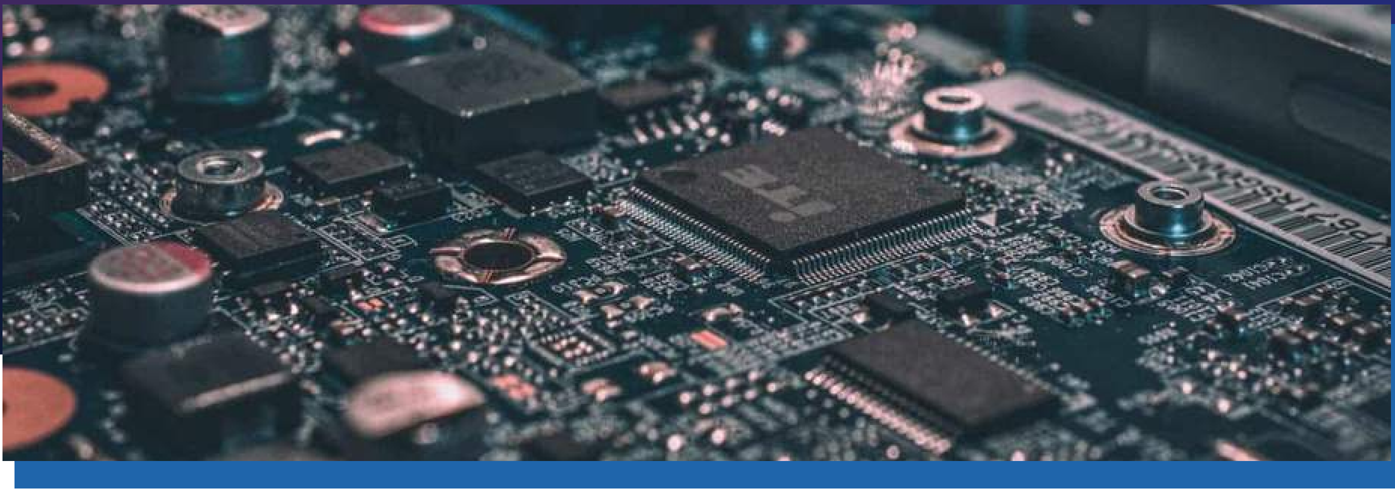
CRYPTO

# *How to:* Combine island mode operations with privileged access management and a DataDiode



Network segmentation is an important cyber hygiene approach – and at times, a vital one. Connecting the OT environment with your IT network can cause vulnerabilities, as the connectivity exposes OT systems to cyber threats that can manipulate or disrupt critical operations. At the same time, there is a need for real time information sharing to know what is happening in the OT environment.

Our DataDiode solves this issue by ensuring a unidirectional data flow at the highest security level. By blocking any data from moving into your OT environment via reverse data paths, you can prevent any external threats from entering the OT network. Combined with a privileged access management (PAM) tool, your organization can safeguard the OT environment while allowing secure data transmission to your IT environment.

## The challenge

Imagine a company with a network consisting of different segments, including a highly secure OT environment and a less secure IT network. The internal OT environment contains critical systems that must not be exposed to external threats.

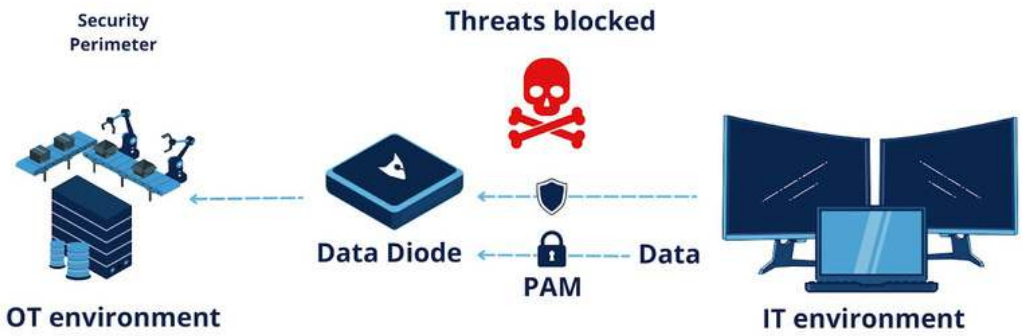
At the same time there is a need for real time information sharing to know what is happening in the OT environment. How do you guarantee the safety, integrity, and availability of the OT system?

## The solution

Organizations can minimize the risk of a security breach in the OT environment by strictly controlling and limiting who has access, in which timeframe and in only specific conditions. This must be done to prevent the risk of data or threats from outside entering the highly secure network.

By combining a PAM solution with our DataDiode the outgoing information flow from OT to IT is protected on a hardware level whilst the incoming connection from IT to OT is heavily regulated and monitored.

# How it works



Privileged Access Management is an approach designed to manage and secure the use of administrator accounts and other privileges within an organization. In the context of using a DataDiode, we can use a PAM approach to ensure that only authorized and verified users have access to the OT environment to provide checks, maintenance, and specific reports.

**Step 1**

**Implement DataDiode:** Configure the DataDiode to enforce one-way data flow, ensuring that data can only move from the OT environment to the IT environment without the possibility of reverse communication.

**Step 2**

**Identification of privileged accounts:** Identify which users or roles within the organization need access to the DataDiode to transfer data. This could include system administrators, security specialists, or specific application managers.

**Step 3**

**Granular access control:** Configure access controls so that only authorized users can perform specific actions for a specific amount of time. For example, to access a turbine in order to troubleshoot.

**Step 4**

**Session monitoring and logging:** Monitor all sessions and activities that occur within the operational network.

**Step 5**

**Just-In-Time access:** Limit the time that privileges are active to only when absolutely necessary. Provide users with temporary access that automatically expires after a certain period.

**Step 6**

**Audit and reporting:** Conduct regular audits to ensure compliance with security policies. Analyze logs and generate reports to quickly detect and respond to suspicious activities.

# The benefits

- **Secure, real-time monitoring:** the DataDiode allows continuous, secure data flow to IT systems for effective monitoring.
- **Operational continuity:** the DataDiode protects the integrity of the OT network, ensuring that critical systems remain unaffected, available and operational.
- **Compliance with regulations:** The DataDiode meets stringent security requirements for critical infrastructure protection.

## Interested? Talk to an expert!

✉ internationalsales@foxcrypto.com

CRYPTO