Protecting your IT/OT infrastructure with Oakdoor™ Hardware Security Solutions

The operational control (OT) technology that monitors and controls a range of processes and equipment is becoming more closely linked with organisations' IT systems. Data that passes between the two is valuable, and the connection also provides a potential vector for the sort of cyber-attack that can have a significant financial and operational consequences.

Ensuring that data can travel securely between the OT and IT sides of the network while mitigating the risk of viruses and malicious data is vital to protecting infrastructure.

Typical IT/OT solutions

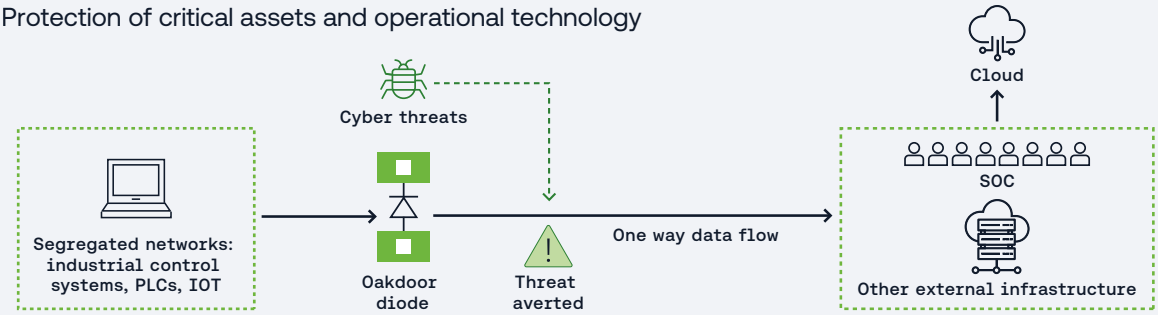
Deployment of real-time continuous sensor-based monitoring across a range of industries creates a need for large volumes of data to be transmitted rapidly between low-security and high-security sides of an organisation's network. Failing to protect the integrity of that link can have serious implications. Aside from the cost of halting operations to deal with a successful cyber-attack and the time taken to get everything running again, there is the risk of reputational damage.

Transferring data between network segments using physical media such as CDs or USB sticks is impractical in today's fast-paced environment. These methods pose significant security risks, as they can easily serve as vectors for malware and other cyber threats.

Software based firewalls are more flexible but require regular updates and are vulnerable to remote hacking and zero-day exploits.

How Oakdoor helps

Protection of critical assets and operational technology



A solution that is established in critical infrastructure and increasingly being adopted in manufacturing uses hardware-enforced protection in the shape of data diodes to create a robust air-gap between OT systems and IT networks.

Data diodes are simple but powerful devices that permit data to move in just one direction. Combined with content inspection they prevent transmission of malware across network boundaries in way that is resistant to hacking. In an IT/OT environment, they have the advantage of a lower power requirement and greater tolerance of harsh environmental conditions than running software on servers.

By combining flow control with careful syntactic content inspection and semantic verification, data diodes prevent transmission of malware from untrusted to trusted parts of a network.

By implementing key stages of the UK National Cyber Security Centre's (NCSC) design patterns for Safely Importing Data and Safely Exporting Data, Oakdoor data diodes are accredited for use in even the most secure environments. They are one of the first data diodes to implement hardware-based syntax verification, which allows structured data to enter while ensuring that potentially malicious data will always be identified and handled in a safe way.

Hardware-based security has traditionally been inflexible and hard to deploy in existing network infrastructures. Oakdoor changes that by offering a combined hardware and software solution that is scalable and reliable for organisations to implement data diodes at multiple points across their network.

Features

- Hardware-enforced unidirectional flow control
- CAPS-approved by NCSC for use in the most sensitive operational environments
- Ideal for cross-domain applications that require flexibility and speed
- Data structure inspection ensures that only structured data can pass
- High data throughput
- More secure and lower maintenance than a software firewall alone

Our products

Oakdoor 1G Data Diodes

Strong security with a low capital cost, ideal for a variety of cross-domain applications that require flexibility and speed.

Oakdoor Enterprise Diodes

Designed for data centre needs, a massively parallel internal architecture supports content syntactic verification at a full 10GbE line rate. Flexibility to route data between thousands of virtual machines in source and destination networks.

Oakdoor Gateway

Single-box solution for applications that require bidirectional data transfer. An import diode and export diode with two integrated servers on either side to accommodate the necessary software for your specific application.

About Oakdoor

Developed at PA's Global Innovation and Technology Centre (GITC), Oakdoor Hardware Security Solutions combine innovative thinking and breakthrough technologies to combat modern day cyber threats.

To find out more about our products, visit us at: **LinkedIn** and **oakdoor.io**