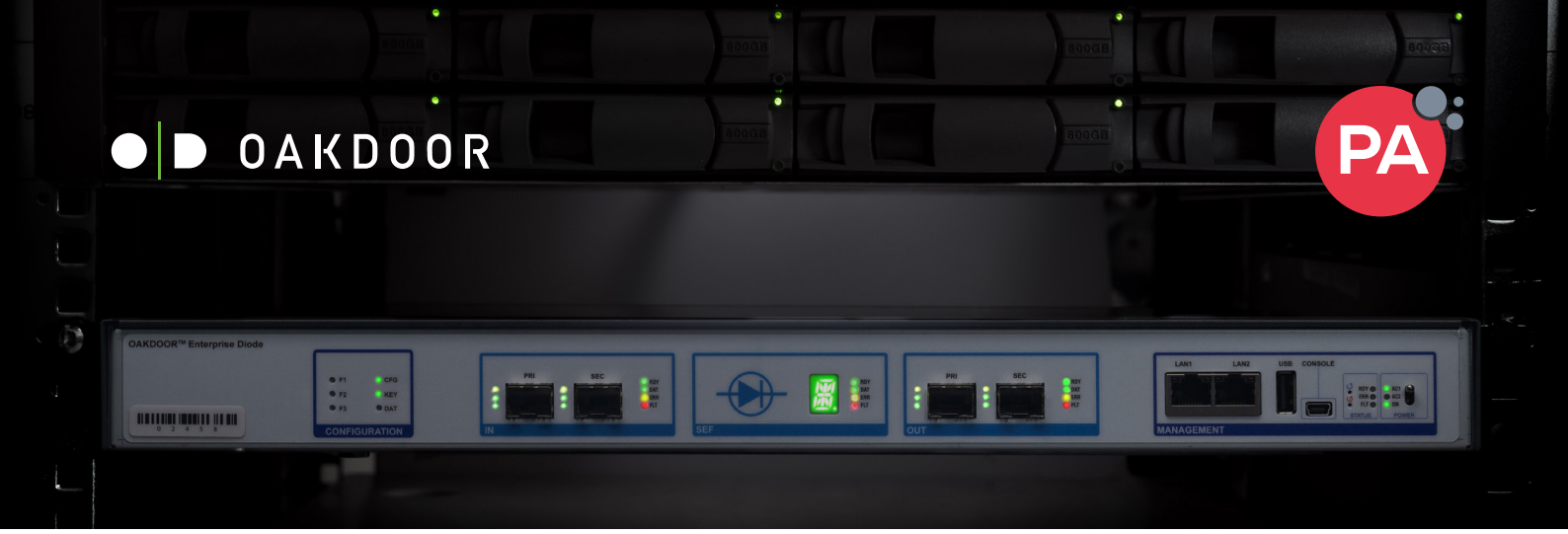


Protecting your SOC/SIEM infrastructure with Oakdoor™ Hardware Security Solutions

A typical SOC/SIEM infrastructure

The security operations centre (SOC) is the core of your organisation's defence against cyber-attacks, which should be closely protected from lower trust parts of the network. When your security information and event management (SIEM) solution detects suspicious activity on the network, it sends data logs to the SOC for analysis.

SIEM software monitors network activity in real-time and flags anything that could be an attack, whether it's an attempt to introduce malware, phishing attempts, or email hacking. Event records must be channelled to the SOC to be dealt with as quickly as possible.

Traditional data transfer methods are not safe

A physical airgap, where data is transferred between network segments using media like CDs or USB sticks, isn't suited to today's fast-moving SOC/SIEM environment.

In addition, hardware-based security has traditionally been inflexible and hard to deploy in existing network infrastructures. Segregating high-security networks using hardware is inherently more secure than relying on software-based firewalls that are more vulnerable to remote hacking and zero-day exploits.

How Oakdoor helps

Oakdoor data diodes, an integral part of Cross Domain Solutions, provide a robust way to maintain the integrity of your trusted and high-security SOC network. They do that by minimising the risk of malicious SIEM data entering your SOC while ensuring data does not escape your SOC from this connection.

Our data diodes function by combining flow control with careful syntactic content inspection and semantic verification of the message protocol. This prevents the 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 potentially malicious data will always be identified and handled safely.

Oakdoor data diodes offer a combined hardware and software solution, which is scalable and reliable so you can implement data diodes at multiple points across your organisation's 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

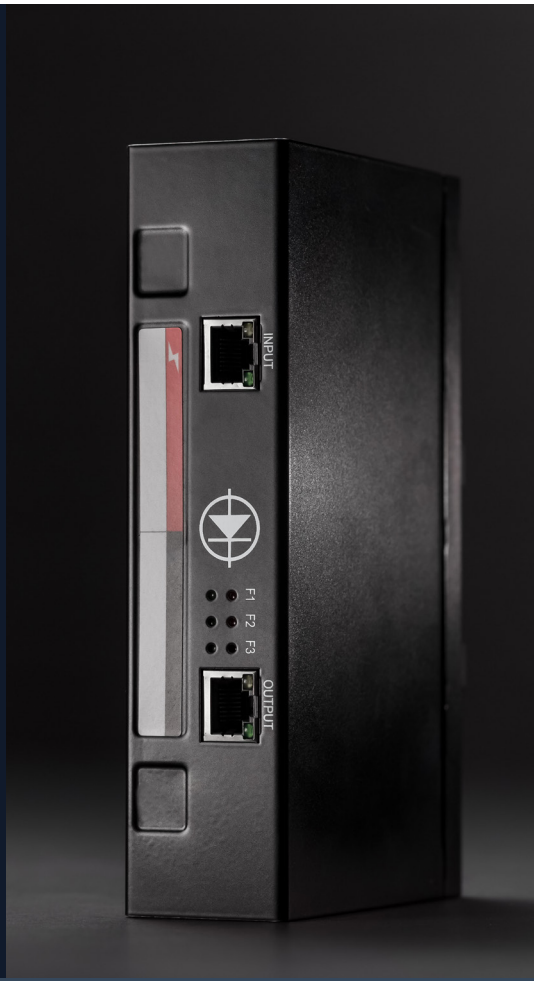
Strong security with a low capital cost, ideal for a variety of cross-domain applications that require flexibility and speed.

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**