Securing your software updates with Oakdoor™ Hardware Security Solutions

Devices within the most secure segments of your network need access to regular software updates – this involves importing large amounts of unstructured binary data, including executable files. While unavoidable, this creates a potential route for malware to cross network boundaries, with significant financial and operational consequences. Your organisation needs to verify software updates, potentially checking against multiple sources, in a way that isn't labour intensive and doesn't create unnecessary delays.

Typical software update infrastructure

Software updates are traditionally checked using a software firewall or by transferring them across a physical air-gap on removable physical media that can be monitored for malware on a device unconnected to a network.

The multi-gigabyte scale of today's update packages means that CDs and USB sticks are no longer a viable option suited to your fast-moving business environment. Firewalls are more flexible, but still rely on being kept up to date themselves and can be vulnerable to remote hacking and zero-day exploits.

How Oakdoor helps

Data diodes are simple but powerful hardware devices that permit data to move in just one direction. Oakdoor Import Diodes combine hardware content inspection with an extremely safe, automated, and responsive method for handling software updates.

When a software update is sent to the high-security network, the Oakdoor Import Diode flags it as an untrusted binary file, and 'wraps' it into a form that can't be executed. The software update is then held in quarantine, and a copy is routed to a secure testing 'sandbox' or 'blast chamber', where it is carefully unwrapped, and its authenticity is checked using file hashes and digital signatures. Only if these confirm authenticity, is the original unwrapped and released.

Hardware-based security has traditionally been inflexible and hard to deploy in existing network infrastructures. Oakdoor changes that by permitting a combined hardware and software solution that is scalable and reliable enough for organisations to be able to use data diodes at multiple points across their network, following 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 valid data to enter while defending against attacks via malicious encoding and content structure in a way that is extremely resistant to hacking.

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**