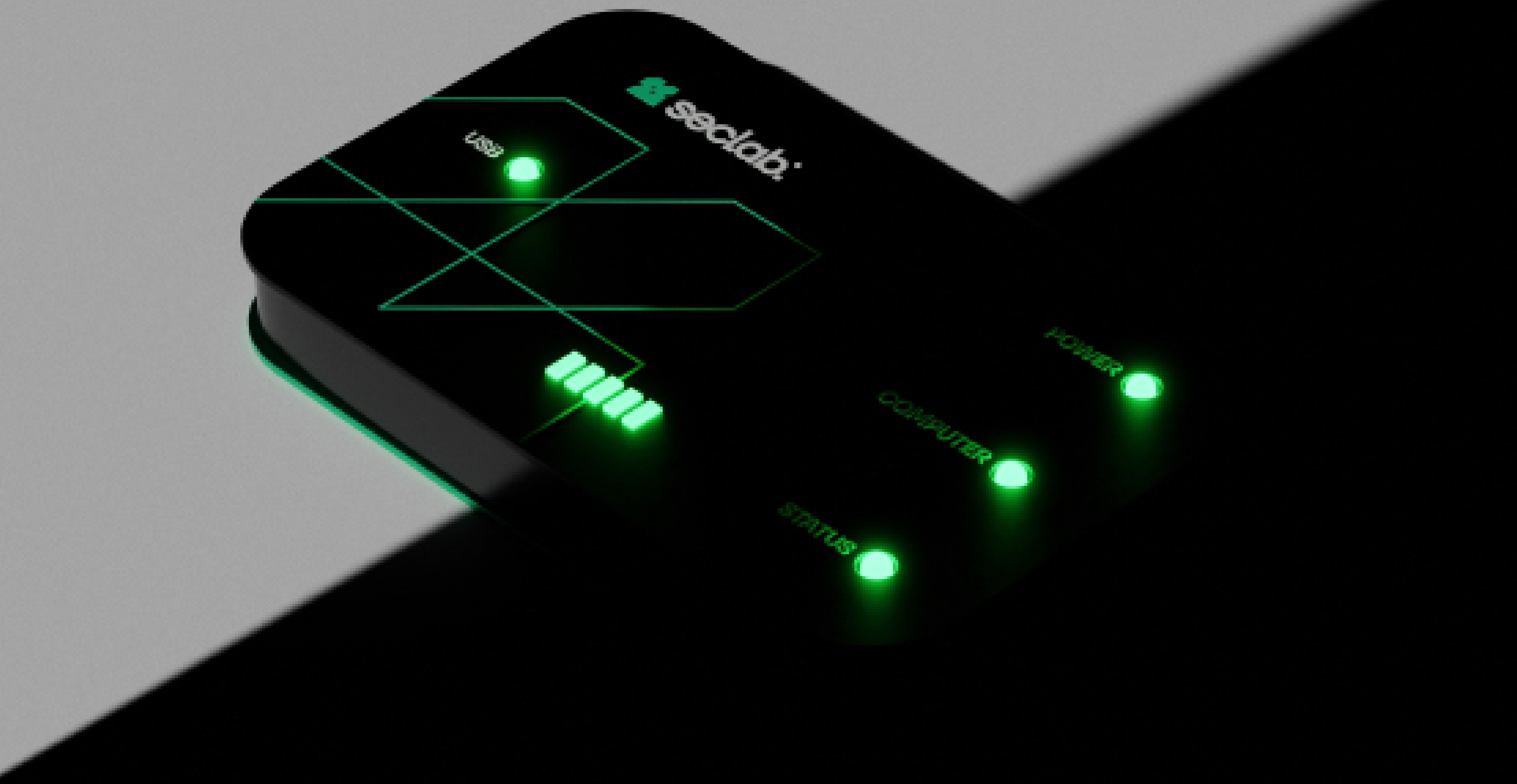


Product datasheet

Xport.

Securing and controlling USB media usage in Critical Infrastructures

Xport.

Securing and controlling USB media usage in Critical Infrastructures.

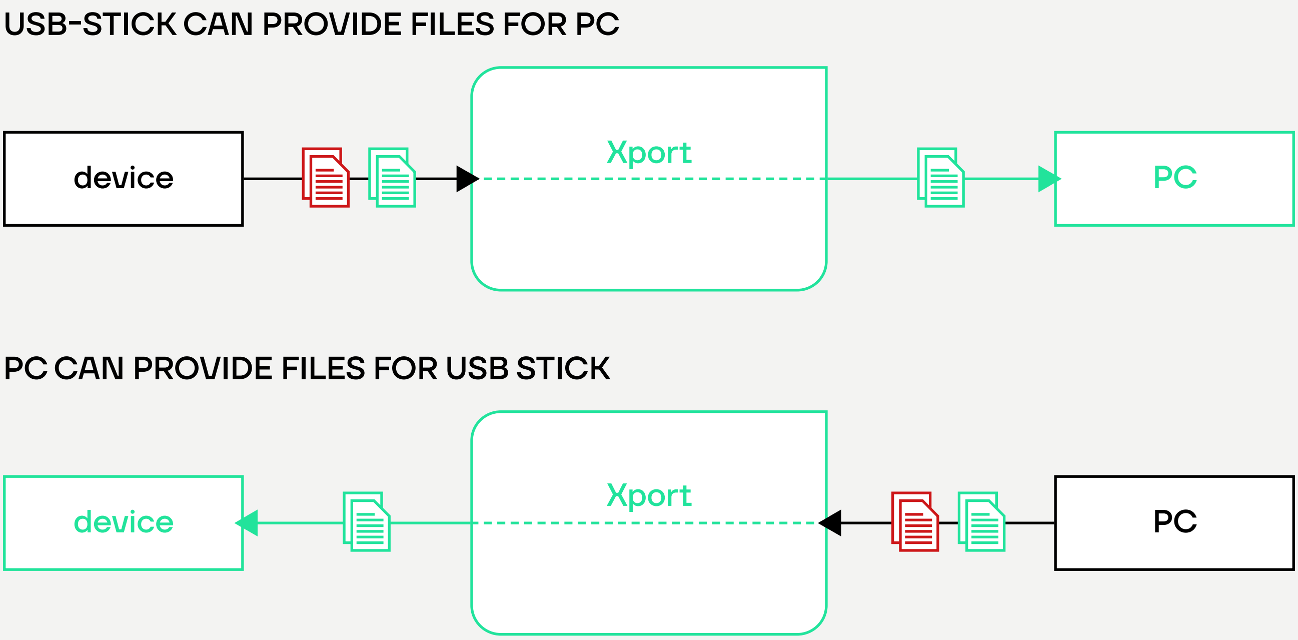
Xport provides a solution for leveraging the advantages of USB media use in OT or Critical environments · without compromising security.

In addition to existing USB auditing and sanitizing solutions, Xport makes sure that only trusted files can be used on specific systems and protects them from advanced USB-based threats. Plug & play, no install, no software.

It's End-to-End USB Security for Critical Systems.

Features

- Blocks untrusted files based on your security policy
- Works with Opswat Metadefender & Kub Cleaner to audit files
- No software install required. Plug and Play on Windows, Linux and MacOS.
- Provides Direction Control: One-Way or Two-Way
- Whitelisting for specific file extensions
- Boot sector protection & Blocks advanced USB attacks (BadUSB)


USB-STICK CAN PROVIDE FILES FOR PC
device
Xport
PC
PC CAN PROVIDE FILES FOR USB STICK
device
Xport
PC

Transfers are secure thanks to the patented seclab technology.

The security policy can be tightened as follows

- Restrict to one direction only (IN / OUT)
- Enable file authenticity and integrity checking
- Blacklist or whitelist file extensions

MAKING THE BUSINESS CARE

Despite the Industry 4.0 market trend, USB media usage in OT and Critical environments remains important for daily operations (configurations changes, manual updates, etc):

- Some systems are not designed to be accessed remotely
- Others can only send data trough a one-way solution (Data diode) 30% USB media usage in OT is up by 30% (1)

As convenient and flexible as it is for productivity, Portable media devices also represent an easy way for spreading malwares and sophisticased attacks.

REQUIRED FIRST STEP

Deploying USB media sanitizing solution on sites as a cornerstone for USB security policy.

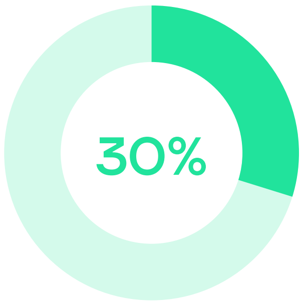
THE MISSING PIECE:

How to ensure that USB media went through analysis before using it on a critical asset? How to prevent additional files from being added after analysis?

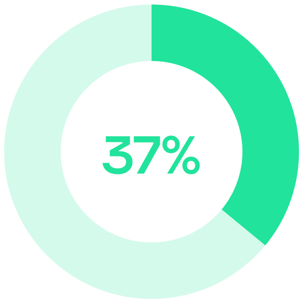
THE ANSWER:

Xport, a hardware USB agent for critical assets.

[1] honeywellforge.ai/us/en/campaigns/cybersecurity-threat-report-2021



USB media usage in OT is up by 30% (1)



37% of OT threats are designed for USB (1)

BENEFITS

- Assists in USB media compliance with security standards (NERC CIP, ISA 62443, NIST 800-53, NIST 800-82)
- USB security policy enforced by End-to-End approach
- Easy to use for field operators
- Secure over time, even with limited patch management resources (Secure-by-Design / Hardware Security)
- Enhanced Business Continuity: in case of network failure, USB-based operations are safely donefile extensions

Technical specifications.

USB Media Type Support

USB Type A

USB 2.0 High Speed

Supported File Systems & Manifests

FAT, NTFS, EXT

USB 2.0 High Speed

Manifests from Opswat and Kub Cleaner

Minimum System Requirements

USB Type-A USB 1.0 or greater

Windows, Linux, MacOS

Physical Characteristics

Dimensions: 125mm x 80mm x 23mm

Weight: 460g

In the Box

Xport

USB power adapter and cable

USB micro to Type A cable

Protective case

Limited Warranty 2yr

Power

Supply: 5V DC via USB wall adapter (minimum 2A)

Active consumption: 1 A @5V (5W)

Standby consumption: 500mA @ 5V (2,5W)

Regulatory Compliance

FCC, CE, RoHS/REACH

seclab®

The Cyber-physical
systems company.

205 impasse John Locke
34470 Pérols, France.

seclab-security.com