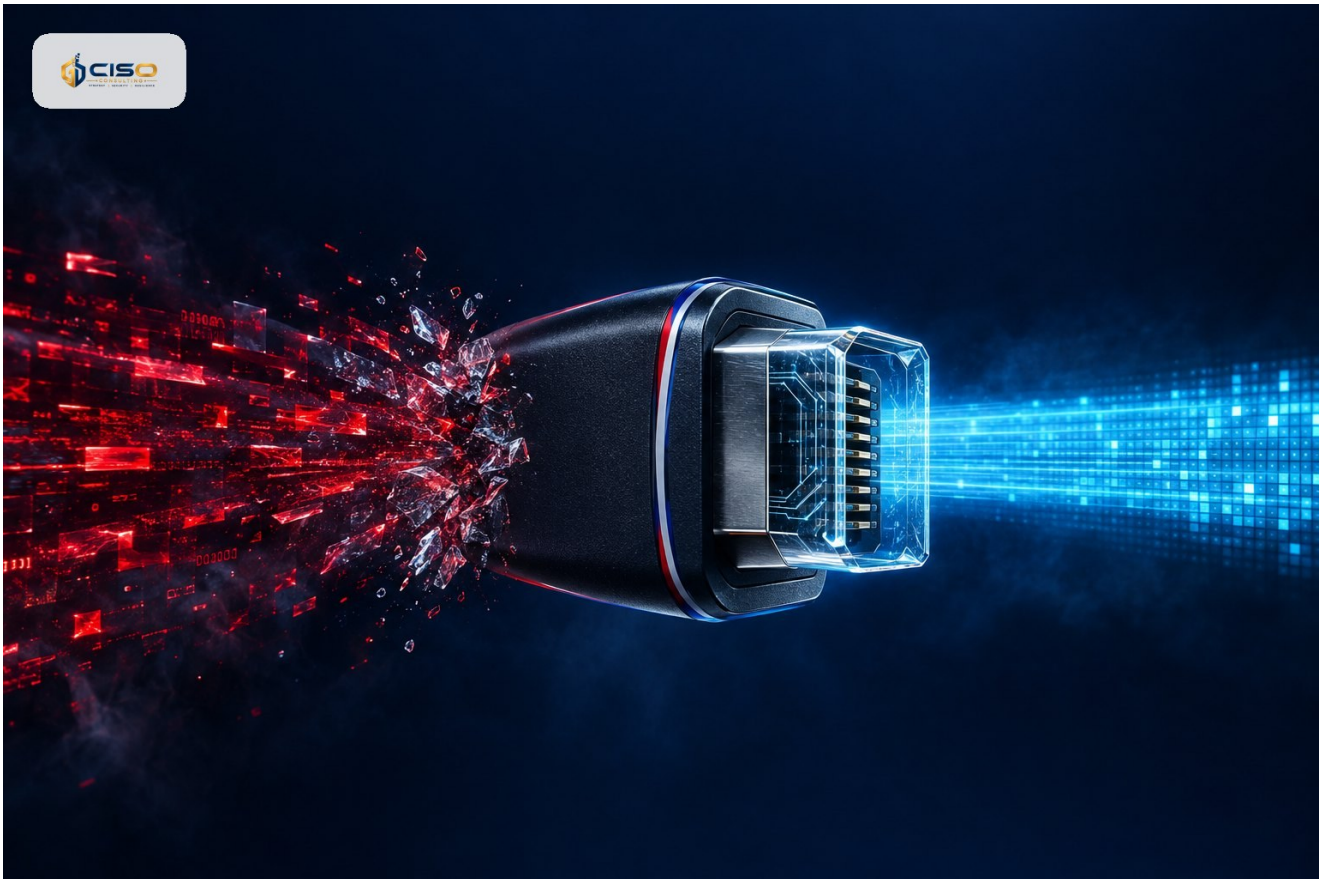


NCSC-designed SilentGlass device aims to block malicious HDMI and DisplayPort links



The UK NCSC has licensed Goldilock Labs to sell SilentGlass, a plug-in device that blocks unexpected or malicious traffic between laptops and monitors. It treats display connections as a security boundary.

- SilentGlass is a plug-and-play device that blocks unexpected or malicious activity on HDMI and DisplayPort connections to screens.
- The NCSC created the intellectual property and licensed Goldilock Labs, working with Sony UK Technology Centre, to sell it globally.
- It is already deployed on UK Government estates and is approved for use in high-threat environments.
- The NCSC assesses monitors as a highly likely route into networks for espionage, disruption or

financial gain.

- Cited risk sources include supply chains, third-party servicing and direct physical access.

The UK National Cyber Security Centre (NCSC) has announced SilentGlass, a device that sits between a computer and its display and blocks anything unexpected or malicious on HDMI and DisplayPort connections. The NCSC created the underlying intellectual property and has licensed Goldilock Labs to manufacture and sell it worldwide, in partnership with Sony UK Technology Centre.

Why display links matter

The NCSC assesses that monitors are an attractive target because they can hold and process sensitive or personal data. It considers them highly likely to be used to gain network access for espionage, disruption or financial gain. It also notes that mitigations are often costly and inefficient.

The agency argues that hardware interfaces have rarely been treated as security boundaries, even though they are exposed through supply chains, third-party servicing and direct physical access.

What the product does

SilentGlass is plug-and-play and has already been used on UK Government estates. The NCSC says it is approved for use in the most high-threat environments and is now available to any buyer, including critical national infrastructure and businesses. The NCSC presents it as a first step towards enforcing behaviour at hardware interfaces before it reaches complex software.

Practical reading

The source does not give technical specifications, pricing or independent test results, so organisations should treat this as a signal about the risk rather than a product endorsement. The broader message is that physical connectivity should be a point of control, not an assumed trust boundary.

What to do now

1. Add display and peripheral ports (HDMI, DisplayPort) to your physical-access and endpoint threat models.
2. Review which high-sensitivity areas, such as trading floors, SOC's and executive offices, rely on shared or third-party-serviced monitors and docks.
3. Require supervision and logging when third parties service or replace display equipment.
4. Ask vendors for independent test evidence before evaluating any hardware port-blocking product, including SilentGlass.
5. Map the findings to your ECC and SAMA CSF controls on physical security and third-party risk.