USE CASE BRIEF

Zero Trust Hardware Access

Printer Man-in-the-Middle Use Case

Industry: Financial Services Institution.

Scenario: A rogue hardware implant is inserted inline with a trusted network printer, creating a hidden man-in-the-middle path into the environment.

Attack Tool: A Raspberry Pi-based transparent bridge is deployed to impersonate a legitimate printer connection, intercept print traffic, and create an unauthorized wireless exfiltration path while appearing operationally normal.

Exposure Window: Because the device operates passively and presents itself as a legitimate hardware path, it can remain invisible to traditional MAC-, traffic-, and software-centric controls for extended periods.

Challenge: Enforcing Zero Trust when hardware identity is assumed rather than verified, especially for unmanaged and embedded devices such as printers, IoT, and OT-connected assets.

Risk: The environment continues to trust the connection because the device appears legitimate, allowing policy bypass, data exposure, and persistent hardware-level access.

Sepio Solution: Sepio enforces Zero Trust Hardware Access by validating the true hardware identity of connected devices at the physical layer, exposing rogue or manipulated assets even when they mimic trusted equipment. This allows security teams to see what is actually connected, apply policy based on verified identity, and reduce hardware-borne risk.

Why Zero Trust Hardware Access Matters

1

You cannot enforce Zero Trust if you do not know what is physically connected to your environment.

2

Rogue and impersonating devices can inherit trust when security tools rely only on declared identity, MAC address, traffic behavior, or software agents.

3

Many hardware threats exist below the visibility of traditional controls, including MAC-less, unmanaged, embedded, and manipulated devices.

> At all times the financial institution shall have the facility to produce a legible paper copy of such records.
>
> BSA 31 CFR § 1010.430(a)

Modern enterprises need more than asset inventory. They need trustworthy hardware identity. In complex IT, OT, IoT, and hybrid environments, hidden, unmanaged, and spoofed devices can create blind spots that undermine segmentation, compliance, and incident response.

Sepio enables Zero Trust Hardware Access by giving organizations verified visibility into connected hardware across network, USB, and peripheral interfaces. By exposing hidden, rogue, and misrepresented devices, Sepio helps organizations extend Zero Trust to the physical edge of their infrastructure.

In as little as 24 hours, Sepio can reveal hidden hardware exposure, validate connected device identity, and strengthen Zero Trust enforcement across your environment.

Zero Trust Hardware Access Benefits

Verified Hardware Visibility: Discover connected assets across IT, OT, IoT, and peripherals based on their true physical identity, not just what they claim to be. This helps uncover hidden, unmanaged, and impersonating devices that other tools can miss.

Policy Enforcement Based on Trusted Identity: Apply security policy using verified hardware context, helping teams control device access, support compliance, and reduce operational friction without depending on a perfectly clean starting point.

Faster Mitigation of Rogue Hardware: Once suspicious or unauthorized hardware is exposed, teams can trigger response workflows through existing enforcement and orchestration tools to contain risk faster.

Why Existing Security Leaves a Hardware Blind Spot

Most security controls focus on software, traffic, or declared network identity. Sepio adds the missing hardware truth layer, helping organizations verify device identity where trust begins.

Why Sepio

Sepio helps organizations implement Zero Trust Hardware Access by verifying the true identity of connected hardware assets. Sepio exposes hidden, rogue, unmanaged, and impersonating devices across enterprise, industrial, and hybrid environments, enabling stronger visibility, policy enforcement, and risk reduction at the hardware layer.

Sepio, See What You've Been Missing™