Zero Trust Hardware Access

Make Hardware Identity the Foundation of Zero Trust

The Challenge

Most Zero Trust strategies verify users, applications, and sessions - but still assume the device itself is legitimate. That assumption creates a critical blind spot. Shadow IT, rogue devices, dormant implants, unmanaged peripherals, and spoofed assets can persist inside enterprise environments because many security tools focus on traffic, scans, or declared identity rather than the physical truth of the device.

Why It Matters Now

As AI lowers the barrier to exploitation and infrastructure becomes more complex, hardware-level blind spots create more opportunity for attackers. Modern organizations need a Zero Trust approach that starts with the device itself - verifying what is actually connected before it is trusted to communicate, persist, or operate inside the environment.

Sepio's Solution

Sepio enables Zero Trust Hardware Access (ZTHA) by bringing Zero Trust to the physical layer. Using physical-layer intelligence and AssetDNA-based identification, Sepio verifies the true identity of connected hardware assets and continuously validates whether they should be present, trusted, and allowed to operate. Instead of relying on spoofable device claims, Sepio establishes trust based on evidence.

How Sepio Delivers ZTHA

Sepio supports the five operational pillars of Zero Trust Hardware Access:

1

Discover

Gain full visibility of all connected assets across IT, OT, IoT, USB peripherals, unmanaged devices, and shadow assets - including devices that traditional network-centric tools often miss.

2

Verify Identity

Establish device identity based on physical and behavioural evidence, registered attributes, and organizational context - not just what the device claims to be.

3

Validate Posture

Continuously assess whether a device's behaviour, configuration, and compliance align with its intended role, location, and policy requirements.

4

Risk Score

Prioritize action based on exposure, criticality, confidence of evidence, and operational urgency - turning visibility into actionable prioritization.

5

Enforce and Mitigate

Apply policy in real time through alerts, restrictions, quarantine, denial, or automated remediation workflows to reduce exposure before hardware-based threats can operate.

Why Sepio

Sepio strengthens Zero Trust by making hardware trust verifiable. Its approach gives organizations the ability to:

- See all connected hardware assets, including unmanaged and non-traditional devices
- Verify true device identity using physical-layer characteristics
- Detect rogue, vulnerable, spoofed, or unauthorized devices in real time
- Enforce granular hardware access control policies
- Reduce exposure by automating mitigation and integrating with existing security operations.

At Sepio, we believe complete asset visibility is essential to answering the core Zero Trust questions of who, what, when, where, and how access should be granted. That is why we bring this principle down to the hardware level, enabling organizations to verify device identity before trust is given.

Business Outcomes

With Sepio, organizations can:

- Close hardware blind spots across enterprise and critical infrastructure environments
- Strengthen Zero Trust effectiveness from the foundation up
- Improve visibility, compliance, and control over physical assets
- Stop unauthorized hardware before it can bypass identity-based controls or micro-segmentation
- Support proactive security with faster, more accurate response to hardware risk

Zero Trust cannot be complete if hardware identity is assumed

Sepio helps organizations extend Zero Trust to the physical layer - enabling them to discover, verify, validate, prioritize, and enforce trust at the hardware level.