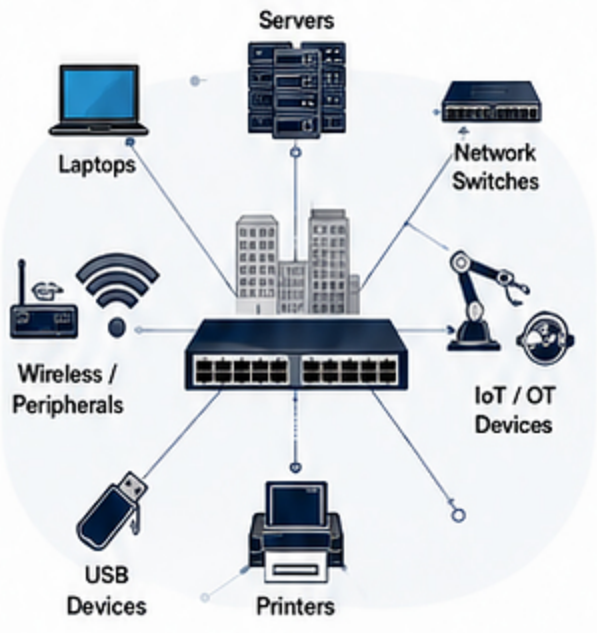
Sepio Solution & Deployment Overview

Zero Trust Hardware Access.
See what you've been missing. Verify before trusting.

1 THE CHALLENGE

Why Organizations Need Sepio



- Traditional tools trust declared identity.
- Unknown, spoofed, rogue, and unmanaged devices create blind spots.
- Hardware supply chain risks, shadow IT, firmware abuse, and rogue peripherals are hard to detect.
- EDR, NAC, and XDR do not verify the true physical identity of every device.

2 WHAT SEPIO DOES

Sepio's Solution

1. Discover
Identify all connected hardware across across endpoints, network, USB, and peripherals.

2. Verify
Validate the true physical identity of devices using AssetDNA and physical-layer intelligence.

3. Assess
Expose rogue devices, unsupported hardware, shadow IT, and policy violations.

4. Enforce
Trigger alerts, define automated workflows, and enable policy-based mitigation.

Sepio extends Zero Trust down to the hardware layer.

3 KEY DIFFERENTIATORS

Why Sepio is Different

- **Trafficless architecture** — no need for traffic inspection or packet decryption.
- **Physical-layer AssetDNA** — verifies real device identity, not just what the device claims to be.
- **Protocol-agnostic** and encryption-independent.
- **Rapid deployment** with fast time-to-value.
- **Actionable visibility** with real identity, location, and risk context.
- **Complements EDR, NAC, XDR, CMDB, SIEM, and SOAR investments.**

4 HOW IT WORKS

How Sepio Works

Infrastructure & endpoints	Sepio Scan Engine/s / Host Module	Sepio Management Platform	Alerts, policies, integrations, response
Collects physical-layer and infrastructure metadata	Builds trusted AssetDNA and device context	Identifies anomalies, rogue devices, and policy violations	Feeds, policies, operations and remediation workflows

5 DEPLOYMENT OPTIONS

Flexible Deployment

SaaS
Preferred deployment for fast onboarding and simplified operations.

On-Premises Virtual Appliance
Deploy on customer hardware using Sepio's virtual appliance.

On-Premises Script-Based Deployment
Install using Sepio deployment scripts on customer-managed infrastructure.

Customer Public Cloud
Deploy in the customer's own cloud environment.

The Sepio Management Platform experience remains consistent across deployment models.

6 ARCHITECTURE / SOLUTION COMPONENTS

Core Components

Network Module
Discovers and validates assets connected through the network infrastructure.

Host Module
Provides endpoint-level hardware visibility and policy support.

HWDR Service
Hardware Detection & Response managed service for organization that want expert and white-labeled support.

7 INTEGRATIONS

SIEM / SOAR · CMDB / Asset Management · NAC · EDR / XDR · Identity & Access · Ticketing / ITSM

Sepio integrates into existing security operations to enhance visibility and accelerate response.

8 BUSINESS OUTCOMES

Outcomes

Reduce hardware blind spots · Strengthen Zero Trust posture · Improve compliance readiness · Accelerate incident response · Lower deployment complexity and operational overhead

9 USE CASES

Common Use Cases

Rogue devices · Shadow IT · Spoofed / impersonated devices · Unknown hardware supply chain attacks · USB and peripheral risks · OT / IoT visibility · Internal abuse

SEPIO

See what you've been missing.