Establishing Trust for Your Hardware Assets

Verify your assets before trusting them with access to your infrastructure

Every untrusted hardware asset expands your attack surface. With Zero Trust Hardware Access from ThinkShield Hardware Defense Powered by Sepio, Lenovo PCs and their connected peripherals are verified by real, physical identity (AssetDNA)—from day one and every day—so only known, trusted hardware is allowed to operate. This policy-driven control complements the multilayered Lenovo ThinkShield stack and endpoint protection, delivering maximum protection with minimal user friction.

Standardizing on secure PCs integrated with Sepio's hardware identity and access policies eliminates fragmented decisions between IT and Security. Deployment stays simple while protection moves down to the device layer—blocking rogue USB, detecting tampered or vulnerable components, and tracing exact USB port locations for rapid response.

The result: a clearer picture of what's actually connected. By removing blind spots at the hardware layer, Sepio enables teams to trust their assets and manage risks associated with their assets, target spend where it matters, and tighten security budgets without sacrificing protection. Better visibility > smarter decisions > lower total cost of ownership.

Prevent hardware threats with ThinkShield Hardware Defense powered by Sepio

Hardware access control and asset risk management are core to defending against cyber-attacks. Adding Sepio's physical layer-based AssetDNA technology to discover and identify all known and shadow devices provides an additional layer of protection for Lenovo customers and enhances ThinkShield as a significant layer in the cybersecurity stack.

With built-in automation, security teams can setup usage policies, respond to and remediate threats faster than ever, while Sepio's patented technology makes sure that hardware based attacks are prevented.

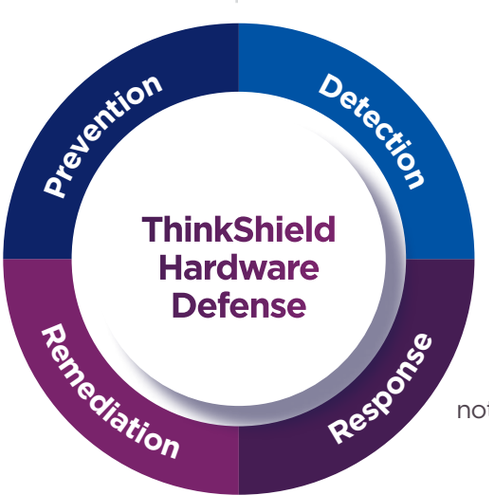
Platform advanced security capabilities

Capability
Enforces Zero Trust Hardware Access at connect-time using AssetDNA

Result
Blocks rogue/unapproved or substituted devices before use

Capability
Continuous discovery and physical identity verification

Result
Spots threats and anomalies that bypass software-only controls



Capability
Forensic timeline and exact device location with guided playbooks or HWDR service

Result
Speeds return to a clean, stable state and reduces MTTR

Capability
Automates isolation and containment (device disable) and notification via EDR/NAC/SIEM/SOAR

Result
Enables action without manual intervention; faster containment

Hardware Truth at Scale
ThinkShield Hardware Defense powered by Sepio

Building on ThinkShield Hardware Defense, Sepio turns raw hardware telemetry into actionable intelligence. AssetDNA gives every device and peripheral a real, physical identity; policy engines then enforce Zero Trust Hardware Access across PCs, docks, USB at scale. Analysts can pivot from a single suspicious connect (e.g., a rogue USB) to the full storyline—device lineage, prior users, switch/port locations, movement across sites, and policy outcomes. With Hardware Watchlists, teams proactively hunt for high-risk vendors and model families, detect known TTPs like HID spoofing, black-box attacks, and rogue modems, and auto-orchestrate containment through EDR/NAC/SIEM/SOAR.

Hardware attacks are here to stay - don't ignore them

Protect against USB Attack Tools

Attackers will always look for the path of least resistance in order to successfully carry out their attacks - whether it's obtaining user credentials through keyloggers, carrying out USB MiTM attacks over biometric measures, ATM "BlackBox" attack or through internal component swap

Complete Asset Visibility

Experience the visibility level that you need in order to meet your IT challenges and efficiently manage IT budgets across all devices - PCs, servers, USB peripherals and internal HW BOM

Granular USB Controls

Enforce specific USB controls based on your preferences. Whether it's based on a specific vendor, model, set of users or specific PCs, you now have the flexibility to provide a better employee experience while still protecting your organization

Low Cost of Ownership

Automated discovery and policy enforcement reduce manual effort, while the negligible impact on host performance and seamless integrations with your existing stack streamline operations and reduce tool overlap. The result is lower operational spend without compromising protection

Verify then trust. Trust your hardware assets with Lenovo ThinkShield and Sepio

One platform for hardware trust—discover, validate, and control every device and peripheral while integrating with your existing ITAM/CMDB and cyber security stack. See What You've Been Missing™

https://www.lenovo.com/us/en/software/sepio/