Lenovo | SEPIO

Lenovo ThinkShield

Lenovo's ThinkShield Hardware Defense powered by Sepio extends device protection all the way down to the physical layer, ensuring that organizations have complete visibility and trust in every connected asset.

Building on Lenovo's foundation of security-by-design, ThinkShield Hardware Defense adds patented hardware-level intelligence that identifies, validates, and monitors every device through its unique electrical and signaling characteristics - protecting against spoofed, rogue, or manipulated hardware before it becomes a risk.

With ThinkShield Hardware Defense, Lenovo customers gain the ability to see and secure what traditional software and network-based tools can't.

## Unified visibility across environments

Security begins with knowing what's connected. The ThinkShield Hardware Defense console, powered by Sepio, delivers a single pane of glass view of all connected devices—whether managed or unmanaged, IT, OT, or IoT—providing continuous monitoring and device-level assurance. Native integrations with Lenovo and third-party security platforms simplify operations and ensure end-to-end visibility across the organization.

## Patented intelligence at the physical layer

Sepio's patented AssetDNA technology, embedded within ThinkShield Hardware Defense, detects and classifies devices based on their physical-layer electrical fingerprint. Unlike other analysis tools, this approach is trafficless, protocol-agnostic, and encryption-independent. Physical layer based AssetDNA provides unmatched accuracy in device identification and anomaly detection.

## Proven performance and resilience

The same technology trusted by critical infrastructure, defense, and Fortune 500 enterprises now powers ThinkShield Hardware Defense, delivering reliable visibility and security assurance from the physical asset level. Lenovo customers can operate with confidence, knowing their devices are protected at the most fundamental layer — the hardware itself.

## Security from the physical layer up

With ThinkShield Hardware Defense powered by Sepio, Lenovo extends its leadership in trusted computing by securing what others can't see — the physical foundation of every device. It's a new standard in hardware assurance and visibility, built to strengthen your security posture without adding complexity.

## Simplified management, minimal impact

Complete asset discovery and granular policy enforcement reduce manual effort, while the minimal host footprint and seamless integrations with existing security stacks minimize operational overhead. The result is lower total cost of ownership, faster time-to-value, and stronger protection without complexity.

Lenovo | SEPIO

Lenovo ThinkShield

Sepio's patented, physical-layer visibility makes it easier for security teams to extend protection across every connected asset – IT, OT, IoT and beyond – without adding operational friction. By closing blind spots at the hardware level and integrating with the existing security stack, Sepio helps ensure that every security dollar invested delivers measurable risk reduction and supports the organization's broader business outcomes.

1

### Make every network port and USB count

Sepio turns your existing switches, wireless controllers, and hosts into a real-time hardware security fabric. By avoiding taps, probes, and traffic inspection appliances, organizations can roll out protection quickly across IT, OT, IoT and CPS environments – turning sunk infrastructure cost into immediate risk reduction.

2

### Give analysts a clean, trustworthy hardware inventory

Instead of juggling partial views from multiple tools, teams get a single, consistent picture of every device: what it really is, where it's connected, and how critical it is. Sepio's AssetDNA-based identification and location mapping remove guesswork, helping SOC and OT teams prioritize issues without wrestling with messy spreadsheets or conflicting records.

3

### Let the platform do the heavy lifting on hardware risk

Sepio continuously profiles devices at the physical layer and enriches them with context from CMDB, NAC, SIEM, SOAR and other tools. Policies can automatically tag, score, and enforce controls on risky assets—whether that means blocking a port, opening a ticket, or triggering a playbook—so teams spend less time on manual correlation and more on decisions that matter.

4

### Hear the important signals, not the background noise

By focusing on hardware security aspects—spoofed identities, shadow and dormant devices, and unauthorized connections —Sepio raises fewer but more meaningful alerts. Clear context on "what, where, and why it's risky" allows security teams to act quickly without being buried under low value notifications.

## Let's talk about your security goals.

Lenovo experts can show you how quickly you can gain complete, trafficless visibility into every connected device – IT, OT and IoT – close hardware blind spots, and strengthen your existing security stack against today's evolving threats