Zero Trust Hardware Access

Controlling Access to Hardware Assets

Never trust, always verify – the founding principle of the Zero Trust concept. However, applying this to devices and peripherals is no easy task; gaps in asset visibility prevent the reliable verification of devices.

Bridging the gap

Lenovo customers now have the opportunity to purchase devices with Sepio, a solution that takes care of visibility blind spots. With Sepio, customers benefit from Zero Trust Hardware Access thanks to asset-level visibility and policy enforcement capabilities. Now, the gold standard of hardware security is an embedded function of Lenovo's industry-leading devices, whereby every USB connection request gets verified on a continuous basis.

Sepio drives deeper visibility into hardware assets on USB interfaces, acting as the foundation to its powerful Zero Trust Hardware Access approach.

Learn more at: techtoday.lenovo.com
Learn more at: sepiocyber.com/thinkshield

Trust at the Hardware Level

COMPLETE ASSET VISIBILITY

Sepio's patented technology, augmented by a unique machine learning algorithm, generates an objective DNA profile for every known and shadow asset on USB interfaces, providing component level visibility to accurately identify devices.

RISK SCORING

Each asset, based on its DNA profile, is assigned a risk score in real-time, determined by multiple risk indicators and the enterprise's specific rules, to automate risk prioritization .

POLICY ENFORCEMENT

The system administrator defines granular hardware access control rules for Sepio to enforce based on device characteristics and risk scores, ensuring dynamic device verification and a robust Zero Trust Hardware Access approach.