See what you've been missing

Visibility. Security. Trust. Control.

The proliferation of connected devices within large law firms presents significant challenges related to data privacy, breaches, and regulatory compliance. The sheer volume of these devices can lead to uncontrolled risks if not properly managed, posing severe threats to compliance with global regulations, audit requirements, and security standards. Achieving complete visibility into all connected assets and applying appropriate control policies are essential for addressing these challenges effectively.

Complete asset visibility eliminates blind spots, providing law firms with an accurate account of every connected device and its associated attributes. This comprehensive overview is crucial for conducting reliable risk assessments, ensuring that appropriate policies and controls are enforced to meet stringent regulatory requirements and customers' expectations.

However, existing solutions often fall short in safeguarding against sophisticated hardware-based attacks, such as those that spoof legitimate devices, execute Man-in-the-Middle (MiTM) attacks, or deploy passive taps or remote Wi-Fi key-loggers to compromise sensitive data. As a result, law firms remain vulnerable to risks that can jeopardize their compliance efforts and expose them to significant legal, reputational, and financial consequences..

True asset identity

Sepio analyzes the physical layer to generate an AssetDNA profile based on physical layer data for every asset, introducing a new dimension of visibility that current solutions lack. By examining electrical and functional characteristics, Sepio provides agnostic visibility and an objective truth, enabling law firms to determine the true nature of each asset—whether legitimate or rogue—before placing trust in it.

This physical layer assessment ensures that Sepio remains unaffected by misleading profile perceptions or behavioral assumptions. Every asset, regardless of its functionality, operability, or location, is detected and identified for what it truly is, eliminating blind spots and providing greater reliability in maintaining data privacy, preventing breaches, and achieving regulatory compliance.

Protect against Hardware Attack Tools

Attackers will always look for the path of least resistance in order to successfully carry out their attacks – weather it's obtaining user credentials through Wi-Fi keyloggers, USB "RubberDucky" or carrying out Network MiTM attacks using MAC spoofed devices.

Granular Controls

Enforce specific controls based on your preferences.

Whether it's based on a specific vendor, model, location, VLAN, MAC address, set of users or specific PCs, you now have the flexibility to provide a better asset usage entitlement, at scale, while still protecting your organization.

Complete Asset Visibility

Experience the visibility level that you need in order to meet your IT/IoT/OT challenges, keeping your CMDB up-to-date and efficiently manage IT budgets across all connected devices - internal HW BOM , USB, wired and wireless Ethernet.

Sepio's Benefits

Protect your private data and prevent breaches caused by malicious hardware attack tools.

Enforce granular asset usage entitlement at scale.

Easily meet regulatory compliance requirements.

Better budget and resource planning.

Reduce clutter and improve the data quality of your CMDB.

Learn more at: **www.sepiocyber.com**