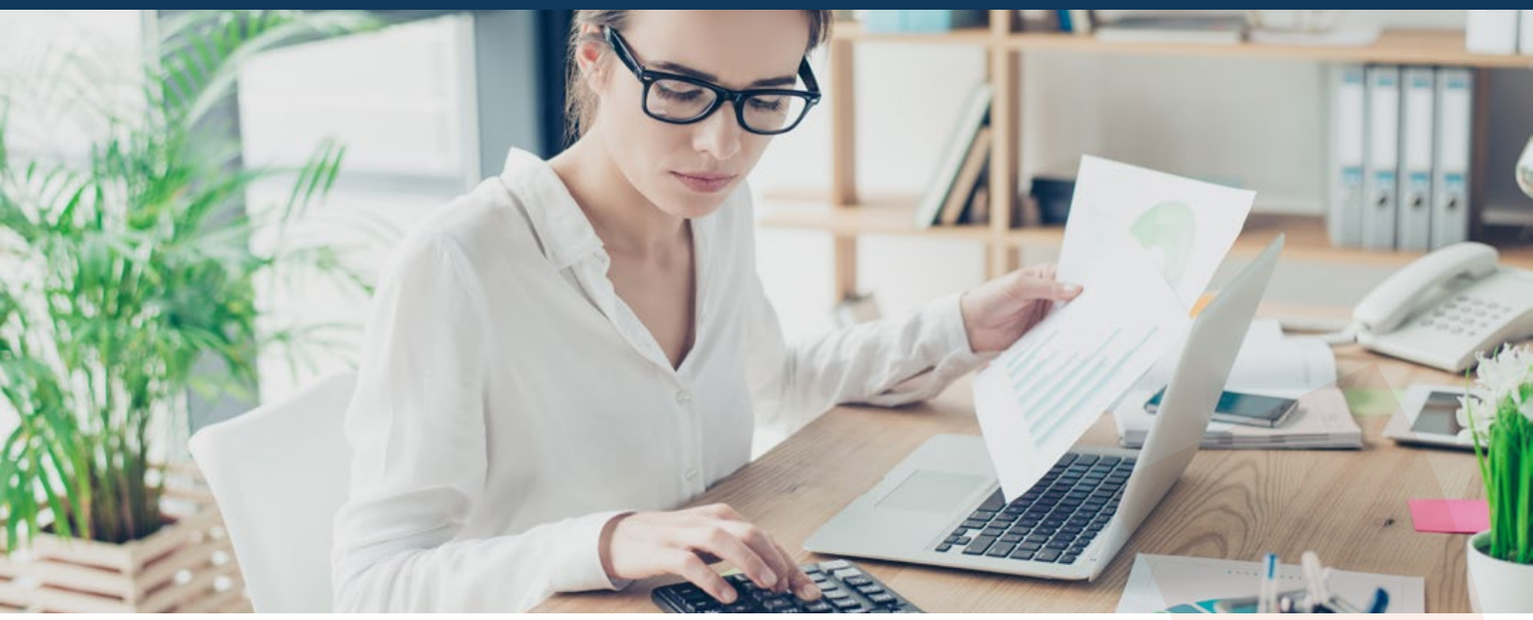
Datasheet

Sepio: Complete Hardware Assets Visibility and Control



Sepio's platform delivers comprehensive visibility and control over all hardware assets connected to enterprise endpoints and networks. Utilizing patented technology, Sepio provides discovery and control of all hardware assets, enabling unparalleled security and operational insights.

Key Benefits

Unified Hardware Assets Visibility and Risk Management:

- Discovers and inventories all connected hardware assets (USB, network, IT, OT, IoT, peripherals).
- Assesses and manages hardware-based risks, identifying potential vulnerabilities.
- Provides granular policy enforcement for mitigating malicious asset threats.

Real-time Threat Mitigation:

- Enables immediate blocking of risky assets upon connection via configurable policies or default settings.
- Offers granular USB port control for preventing unauthorized device access.

Phased Implementation Flexibility:

- Allows for staged deployment, starting with inventory visibility, progressing to risk assessment, and culminating in gradual policy enforcement.

Centralized Management and Scalability:

- Simplifies security policy deployment and management across diverse device types.
- Ensures consistent and effective security across all endpoints and network segments.

Platform Modules:

Sepio offers two complementary modules, deployable individually or in combination, to address distinct hardware security challenges:

1. Endpoint Device Security:

- Provides real-time detection and monitoring of all USB-connected assets.
- Analyzes device capabilities and behavior for accurate risk assessment.
- Enables granular control through allow/block policies for specific assets and interfaces.
- Relies on a lightweight Sepio agent.

2. Network Device Securit:

- Continuously monitors the network for rogue, invisible, passive, idle hardware assets.
- Identifies devices operating without traditional network identifiers (IP, MAC).
- Detects unmanaged network switches and the devices that connected to them.
- Enables the exposure of shadow IT devices.

Sepio Agent: Endpoint Device Security

The Sepio Agent provides comprehensive hardware-based attack protection for enterprise endpoints, enabling granular control without hindering productivity.

Key Features:

Granular USB Device Control:

- Enables fine-grained policy enforcement for USB devices, allowing specific devices and interfaces while blocking others.

Rogue Peripheral Blocking and Remediation:

- Offers a comprehensive suite of protection modules to detect and rapidly block unauthorized peripherals.

Secure Removable Device Management:

- Allows for safe use of removable devices, eliminating the need for blanket USB port blocking.

Lightweight and Efficient Operation:

- Operates with a minimal memory footprint, ensuring comprehensive security without significant resource consumption.

Sepio Agent Operation Modes:

The Sepio Agent supports multiple operation modes, providing flexible control over USB device access:

Visibility (Free):

- Provides comprehensive inventory and visibility of connected USB devices.
- Reports device information to the Sepio Platform Management without enforcing blocking policies.

Armed (Block Unauthorized):

- Automatically blocks any USB device not explicitly designated as "Approved."
- Enforces strict security by default, preventing unauthorized device access.

Block Known Threats (BKT):

- Blocks known malicious USB devices based on a continuously updated threat intelligence database.
- Allows the use of other, non-threatening devices.

Block Mass Storage and Known Threats (BST):

- Blocks all mass storage devices (e.g., USB drives) and known malicious threats.
- Provides enhanced data loss prevention and threat mitigation.

Agent Minimum Requirements

- **OS** - Windows, MacOS, and Linux
- **CPU** - Dual core CPU / Core i3 or similar
- **Memory** - 4GB RAM
- **Free Disk Space** - 200 MB

Sepio Scan Engine: Network Device Security

The Sepio Scan Engine is a distributed component of the Sepio platform, designed for comprehensive discovery and identification of network infrastructure and connected devices. It gathers detailed asset data through interactions with network infrastructure equipment, providing crucial insights for security and risk management.

Key Features:

Distributed Architecture:

- Operates independently of the central management system, enabling scalable deployment across complex network environments.
- Supports both "Internal" (co-located with the management server) and "External" (deployed on separate systems) Scan Engines.
- Facilitates comprehensive network visibility in distributed and global network architectures.

Protocol-Based Data Collection:

- Utilizes SSH and other management protocols to connect to network devices.

Comprehensive Asset Intelligence:

- Asset Discovery: Identifies and locates all network assets.
- Asset DNA Collection: Gathers unique identifiers and characteristics for precise asset profiling.
- Classification: Categorizes assets based on role, type, and criticality.
- Asset Information Gathering: Collects additional relevant information available through network infrastructure.

Real-Time Risk Assessment:

- Relies on frequent and consistent scans for accurate asset inventory and vulnerability detection.
- Provides real-time risk alerts based on collected data.
- Requires established connections to network equipment for each scan.

Scan Engine Minimum Requirements

- **OS** - Windows and Linux Server
- **CPU** - Intel® Xeon® Processor E5-2690 or higher, 8 Cores, 2.6GHz
- **Memory** - 32GB RAM
- **System Disk** - 128GB
- **Storage** - 1TB
- **Network** - 2 x Gigabit Ethernet NICs