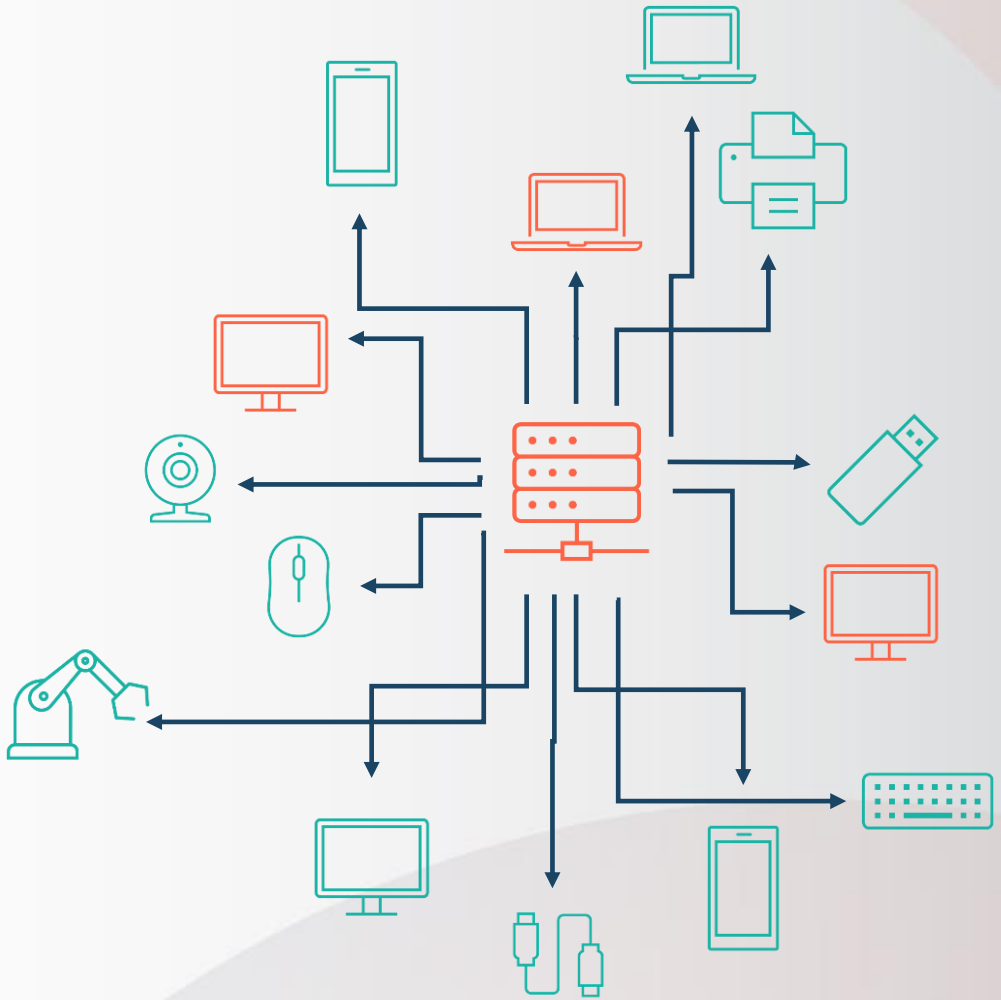
For Healthcare ITAM & Security Challenges

Innovative Hardware Asset Risk Management

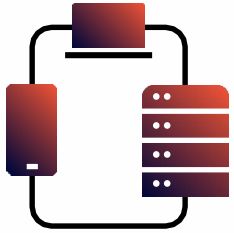


February 24

Questions our healthcare customers ask themselves

- Are all my assets listed?
- Where are my assets located?
- Are there any vulnerable assets that put us at risk?
- Are my assets verified and can I trust them?
- Where are my regulatory compliance gaps?

Hardware assets security concerns



1

Visibility and validation of **all Hardware Assets** including:

- Peripheral devices
- (MAC-less devices)
- Hardware BOM

2

Hardware Zero Trust
Control access to the enterprise through **granular policy enforcement & hardware identity validation**

3

Rogue Device Mitigation (RDM) of spoofed, manipulated devices, and hidden implants

4

Detection of Hardware Manipulation within the supply chain

Hardware attack tools are gaining popularity

- Every physical asset is an exposure
- Uncontrolled assets are an entry point for malware/ransomware payloads
- Uncontrolled assets are an exit door for sensitive data leakage
- Uncontrolled asset provide a permanent foothold for threat actors in the organization: MiTM, Data manipulation etc.

Demonstrated value to IT operation

- Existing CMDB, CMMS and NAC performance boost
- Visibility across inventory, shadow and rogue assets
- Reduced hardware clutter and better budget spending
- Uninterrupted streamlined operations

Case study

BAPTIST HEALTH

Baptist deployment highlights

- More than 27,500 hosts and 544 network switches
- More than 635K connected assets
- Online – Sepio Cloud deployment
- Periodic reporting
- Attack surface reduction

CYBERSECURITY

CISO Michael Erickson Discusses Implementation of HAC-1 Solution

Michael Erickson, CISO of the Louisville, Ky.-based Baptist Health, sat down with Healthcare Innovation to discuss the implementation of the Rockville, Md.-based Sepio Systems' HAC-1 solution

Janette Wider

Can you discuss how the implementation of the HAC-1 solution went at Baptist Health?

Sepio's HAC-1 solution went very simply for Baptist, actually, and we were surprised by that. A lot of times when we work with technology companies, especially those that are more innovative, it can be quite an implementation challenge. In this case, we were pleasantly surprised that the system is very lightweight, very sophisticated, but installs rather easily along with our other threat detection types of tools.

What is the most challenging aspect of cybersecurity in hospitals today?

We're looking at the term zero trust quite closely right now, and I'm sure your readers are thinking about that strategy as well. For us, zero trust is difficult in an organization that serves the public. We want people to come and spend time in our organization to heal and be comforted. When we look at IT assets, we have to think about not just the activity of the devices that are coming into our organization, but the existence of those devices. So, working on visibility, working on understanding down to the peripheral level, the wireless level, and wired devices.

Understanding what's in our facilities at any given time is a is a big challenge and that's why we have invested in the Sepio product. It has given us a much more robust dataset than we've had previously with other vulnerability management tools.

SEPIO

Attack study

Peripheral asset attacks

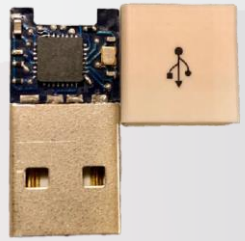
Way In

```
0x8A,0xC6,0x22,...
http://URL...
cmd /c netsh wlan show
profiles "+NetName+"...
```

Depending on attacker's "style" and prior knowledge of the target, they will either:

- Use HID emulation for binary payload
- "Send" the target PC to a pre-known/prepared web URL to download the payload
- Act as a Network Interface and inject the payload into the PC
- Use USB Proxy MiTM attacks

Way Out

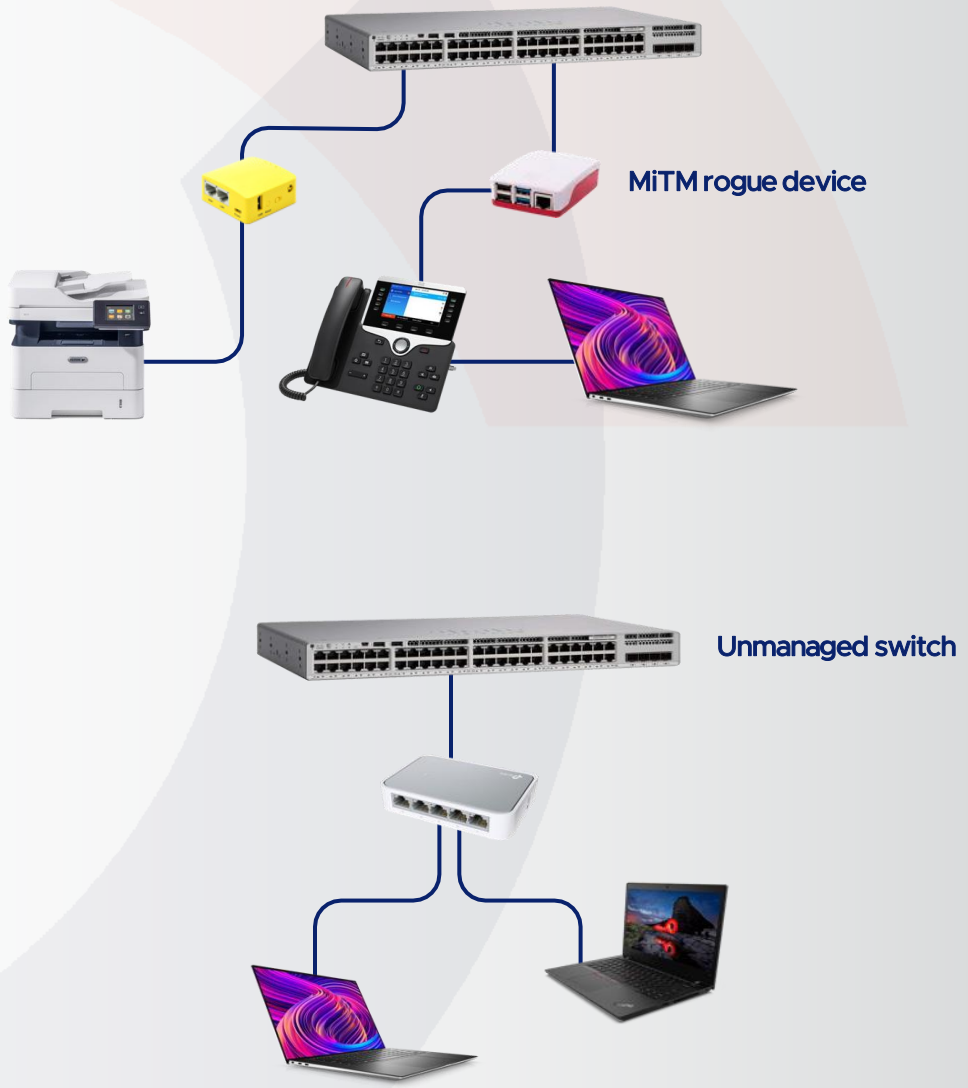


- Exfiltrate the data directly to the attack tool
- Use an integrated Wi-Fi to remotely extract
- Connect to the internet and exfiltrate the data "invisibly" – such as adding comments on youtube
- Use continuous and invisible remote shell into corporate PCs

SEPIO

Network asset - MiTM & 802.1x bypassing

- Unmanaged switch & uncontrolled (MiTM) hardware are completely invisible to **NAC** and **IDS/IPS**
- Any device that is connected poses a risk-
  - **Spoof to be a legitimate device** and send traffic into the network
  - **Intercept/manipulate** traffic between a legitimate asset and the network
  - **Invisibly infect/attack** a legitimate asset without being flagged
  - Create as **invisible and continuous** foothold in the infrastructure



Avoiding existing technologies blind spots

Friend or Foe?

Same MAC

MAC:00D085045802

MAC:00D085045802

Same Ports

Zenmap

Scan Tools Profile Help

Target: 192.168.10.46 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.10.46

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.10.46 Details

```
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-18 10:15 Jerusalem Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating ARP Ping Scan at 10:15
Scanning 192.168.10.46 [1 port]
Completed ARP Ping Scan at 10:15, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:15
Completed Parallel DNS resolution of 1 host. at 10:15, 0.07s elapsed
Initiating SYN Stealth Scan at 10:15
Scanning 192.168.10.46 [1000 ports]
Discovered open port 443/tcp on 192.168.10.46
Discovered open port 80/tcp on 192.168.10.46
Discovered open port 631/tcp on 192.168.10.46
Discovered open port 9100/tcp on 192.168.10.46
Discovered open port 515/tcp on 192.168.10.46
Completed SYN Stealth Scan at 10:15, 1.76s elapsed (1000 total ports)
Initiating Service scan at 10:15
```

Zenmap

Scan Tools Profile Help

Target: 192.168.10.46 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.10.46

Hosts Services

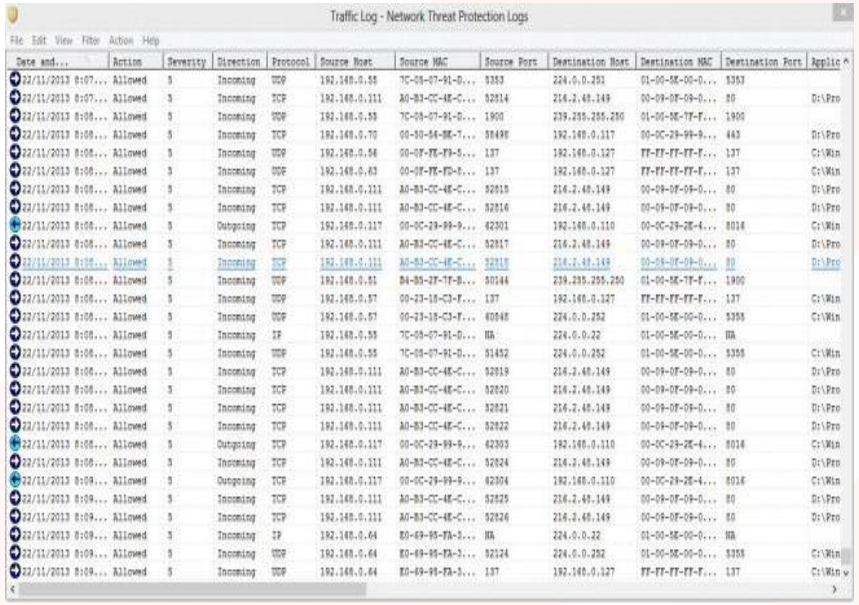
OS Host

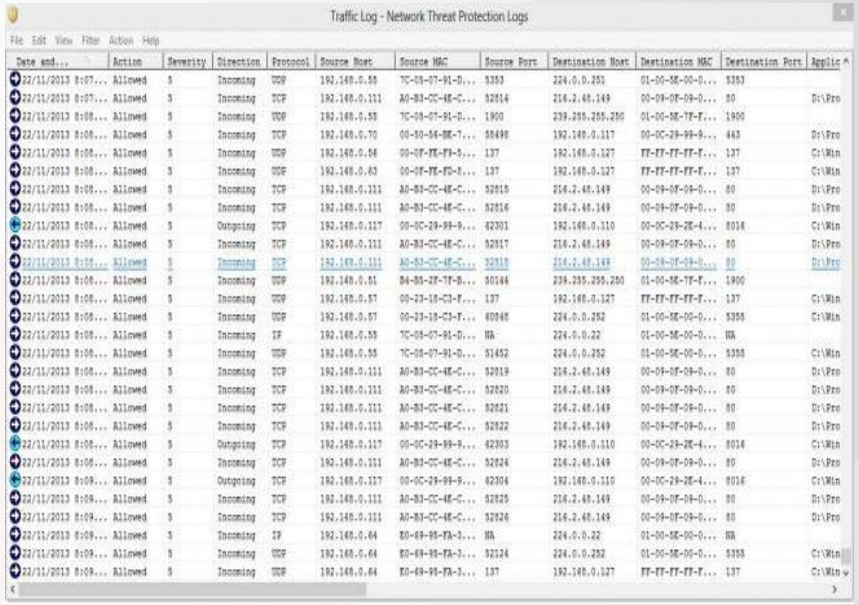
Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.10.46 Details

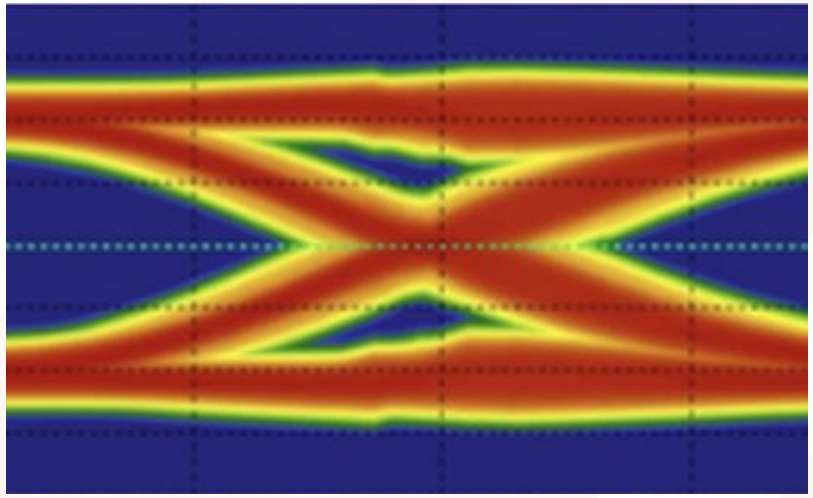
```
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-18 10:15 Jerusalem Daylight Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating ARP Ping Scan at 10:15
Scanning 192.168.10.46 [1 port]
Completed ARP Ping Scan at 10:15, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:15
Completed Parallel DNS resolution of 1 host. at 10:15, 0.07s elapsed
Initiating SYN Stealth Scan at 10:15
Scanning 192.168.10.46 [1000 ports]
Discovered open port 443/tcp on 192.168.10.46
Discovered open port 80/tcp on 192.168.10.46
Discovered open port 631/tcp on 192.168.10.46
Discovered open port 9100/tcp on 192.168.10.46
Discovered open port 515/tcp on 192.168.10.46
Completed SYN Stealth Scan at 10:15, 1.76s elapsed (1000 total ports)
Initiating Service scan at 10:15
```

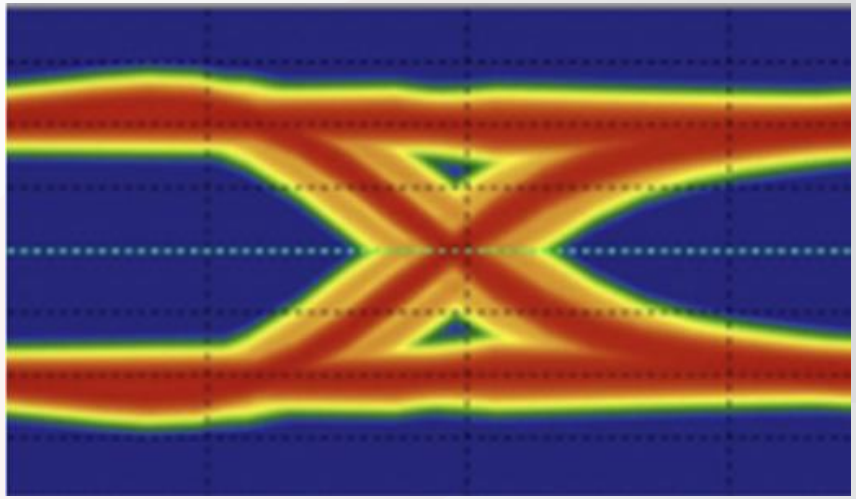
Same Traffic

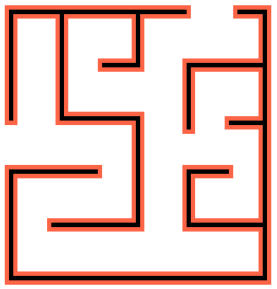




Different Asset DNA!



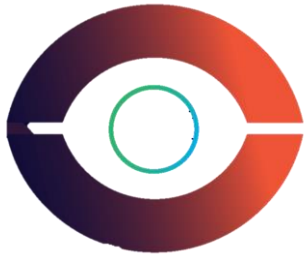




Passive network probing is an IT/OT nightmare

Sepio's trafficless solution avoids cumbersome deployments and privacy issues, vertical, type and protocol indifferent, at any scale, without effecting the network performance.

SEPIO



XDR/EDR device control still has blind spots

Sepio's enhanced visibility provides unmatched rogue device mitigation, while supporting USB entitlement at scale.

SEPIO

Go beyond legacy NAC solutions

Embrace Sepio's Zero Trust Hardware Access (ZTHA) to augment your ZTNA initiatives across all your assets (IT/IoT/OT).

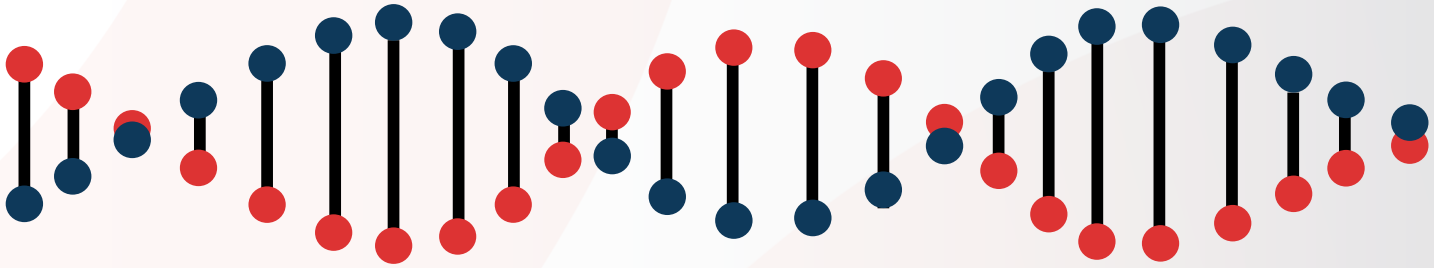
Establish trust validate assets, enforce regulatory compliance with a single low TCO solution.

SEPIO

Sepio’s unique approach

How do we do it?

Asset DNA



Asset DNA provides a single source of truth, focusing on EXISTENCE – rather than ACTIVITY.

With our patented technology, we now harness a new data source – physical layer to accurately identify and classify your assets.

Introducing Asset DNA

Host

Network

Sepio’s proven value for healthcare

Who benefits from our data?

SIEM/SOAR

- Instant alerts when unwanted or rogue devices are connected, eliminating unnecessary noise
- Contextual information, i.e., asset location, expedites response time to prevent crises
- Publicly recognized asset vulnerability module (OSINT and proprietary) for an immediate mitigation

Security team

- Understand what needs attention with actionable data
- Enforce organization policies and establish trust at the asset level
- Greater ROI by radically improving the efficacy of existing tools

ITAM & CMDB

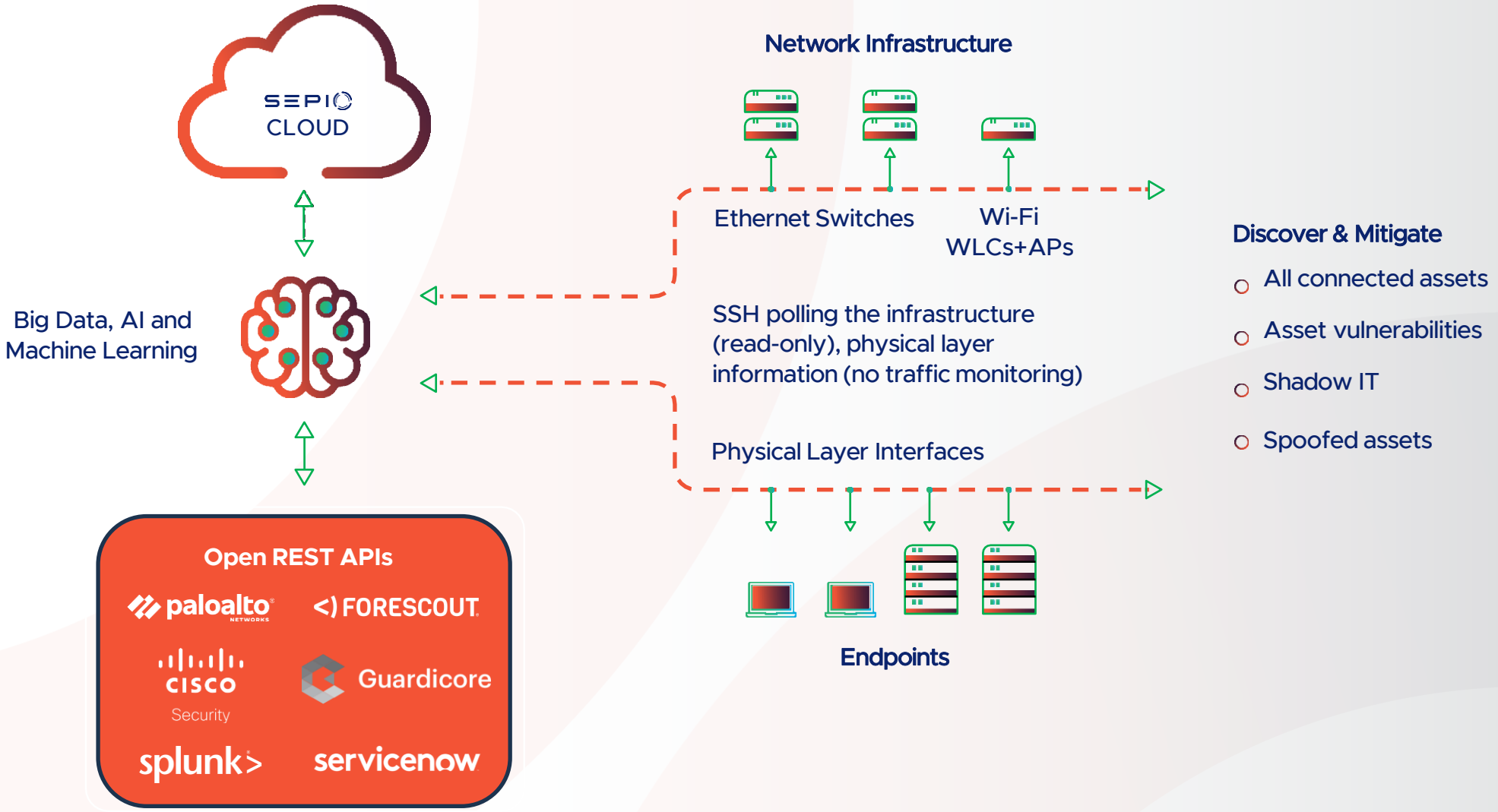
- Reduce complexity with a consolidated source of asset visibility across all environments
- Reduce hardware clutter
- Ensure operational efficiency of assets

CAASM

- Augment existing data sources
- Validate security controls
- Remediate issues

SEPIO

Architecture and Deployment aspects


SEPIO CLOUD
Big Data, AI and Machine Learning
Open REST APIs
paloalto NETWORKS
FORESCOUT
cisco Security
Guardicore
splunk>
servicenow
Network Infrastructure
Ethernet Switches
Wi-Fi WLCs+APs
SSH polling the infrastructure (read-only), physical layer information (no traffic monitoring)
Physical Layer Interfaces
Endpoints
Discover & Mitigate
All connected assets
Asset vulnerabilities
Shadow IT
Spoofed assets

Sepio agent deployment options

Fixed agent

Session based

Dissolvable agent

Typical Customer Journey

Workshop with extended team

Identify key use cases – endpoint or network

PoV – installs in hours; standard duration up to 2 weeks

Develop deployment and integration plan

Present business case for approval

Deployment process

1. **Install the software only Sepio Platform using preferred method**

   Cloud, virtual, on-prem or via Azure marketplace

2. **Using the browser UI, import a license**

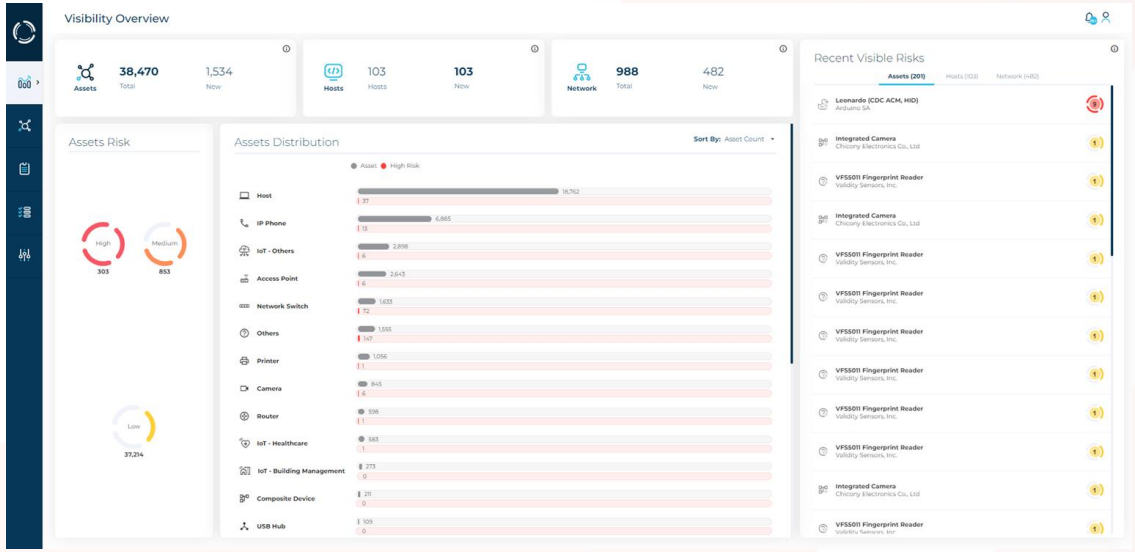
3. **Import switches/WLC to Sepio**

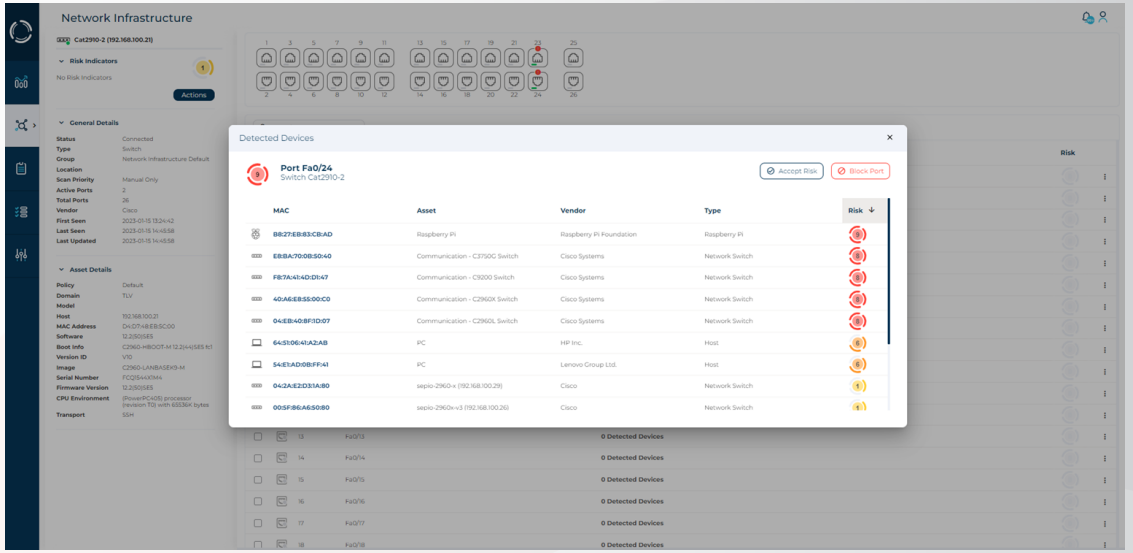
   Can be done manually by providing IP-SSH username – SSH password
   Can be done by importing CSV file

4. **Deploy Sepio agents**

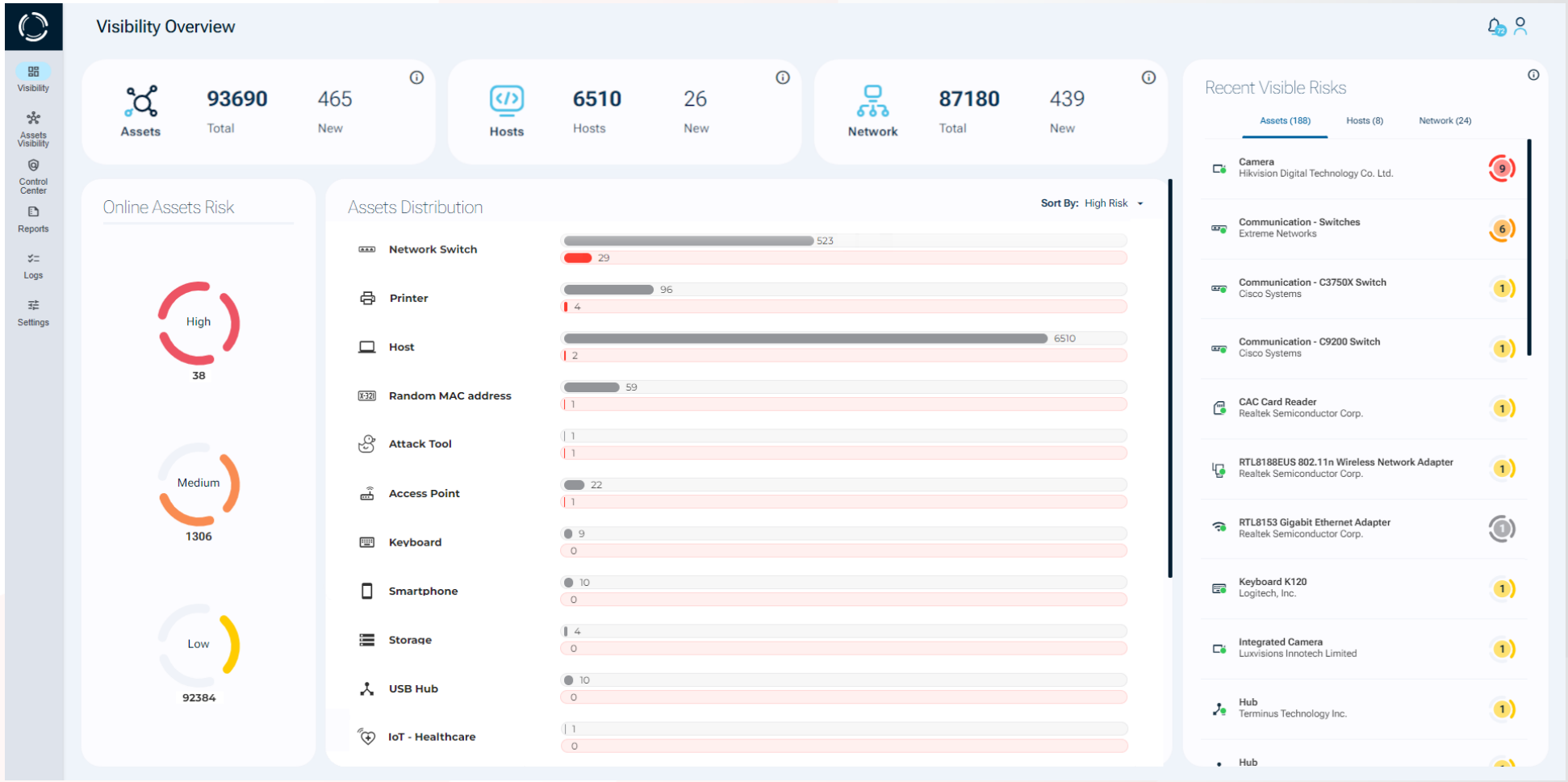
   Supports Windows/RHEL/Debian
   Can be installed manually or using a distribution tool

5. **Complete integration in upstream systems**





Sepio's Asset Risk Management solution



Additional video resources

- https://www.youtube.com/watch?v=kv8_YzFQ4OY&list=PLIhAGMBWwGmex8Fk5w4PbbFNZH7O0nE0q&index=5
- https://www.youtube.com/watch?v=CCiUqsyf-H8&list=PLIhAGMBWwGmfe-wUejNyOzTpiadr715m6
- https://www.youtube.com/watch?v=bJPfINfYumc
- https://www.youtube.com/watch?v=A3Lf16GfGGE&list=PLIhAGMBWwGmdIt7aRfTc0C07N_1kA49p4&index=7

SEPIO

See what you've been missing