Mitigating Cyber Physical Systems Risks

May 24

Questions our OT 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?

Are all my assets listed?

Sepio provides a complete asset inventory of whatever is connected – internal components HW BOM, USB peripherals, wired and wireless Ethernet connected devices.

Easily integrated with CMDB solutions (e.g., ServiceNow).

Where are my assets located?

Sepio provides asset location information based on their specific network switch, USB port location or slot within the endpoint.

Are there any vulnerable assets that put us at risk?

Sepio's embedded, regularly updated, known-to-be-vulnerable OSINT database provides an instant indication when an asset that might compromise the organization is connected.

Are my assets verified and can I trust them?

Sepio’s Zero Trust Hardware Access approach, where we validate the true identity of hardware assets before they can be trusted and granted access to the enterprise's resources, provides protection against spoofing or tapping devices.

Where are my regulatory compliance gaps?

Sepio's granular ruleset-based policies ensure that regulatory compliance gaps are easily detected and reported.

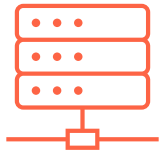
“Nearly three-quarters (73%) admit that they only have strong awareness of less than 80% of all assets”

Seeing half of the picture

is not enough!

Source: ESG ,April 2023

CPS Visibility Challenges



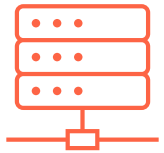
Active scanning → Potential impact on system responsiveness and availability.

Passive probing → Poor visibility (50%-80%) due to encrypted traffic.

Dormant assets→ Become “invisible” – MAC’less

Current Mean-Time-To-Value Challenges

Extensive use of human resources



Complexity due to additional sensors

Cumbersome network configuration

SEPIO

CPS Security challenges

Building a complete asset inventory

Enforcing granular security controls

Fulfilling regulatory compliance

Avoiding performance degradation

SEPIO

Friend or Foe?

Same MAC

00-1c-06-00-bc-37

00-1c-06-00-bc-37

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

Traffic Log - Network Threat Protection Logs

File Edit View Filter Action Help

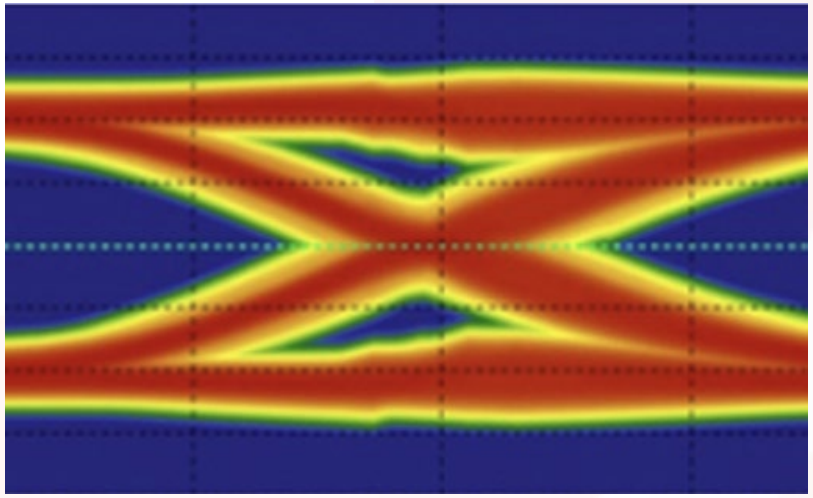
Date and...	Action	Severity	Direction	Protocol	Source Host	Source MAC	Source Port	Destination Host	Destination MAC	Destination Port	Applic
22/11/2013 8:07...	Allowed	5	Incoming	UDP	192.168.0.58	7C-05-07-91-D...	5353	224.0.0.251	01-00-5E-00-0...	5353	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52814	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-05-07-91-D...	1900	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.70	00-50-56-BE-7...	58498	192.168.0.117	00-0C-29-99-9...	443	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.56	00-0F-FE-F9-5...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.63	00-0F-FE-FD-8...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52815	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52816	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	62301	192.168.0.110	00-0C-29-2E-4...	8014	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52817	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52818	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.51	B4-B5-2F-7F-B...	50144	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	60848	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.58	7C-05-07-91-D...	HA	224.0.0.22	01-00-5E-00-0...	HA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-05-07-91-D...	51452	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52819	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52820	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52821	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52822	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	62303	192.168.0.110	00-0C-29-2E-4...	8014	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52824	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:09...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	62304	192.168.0.110	00-0C-29-2E-4...	8014	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52825	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52826	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:09...	Allowed	5	Incoming	IP	192.168.0.64	E0-69-95-FA-3...	HA	224.0.0.22	01-00-5E-00-0...	HA	
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	52124	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win

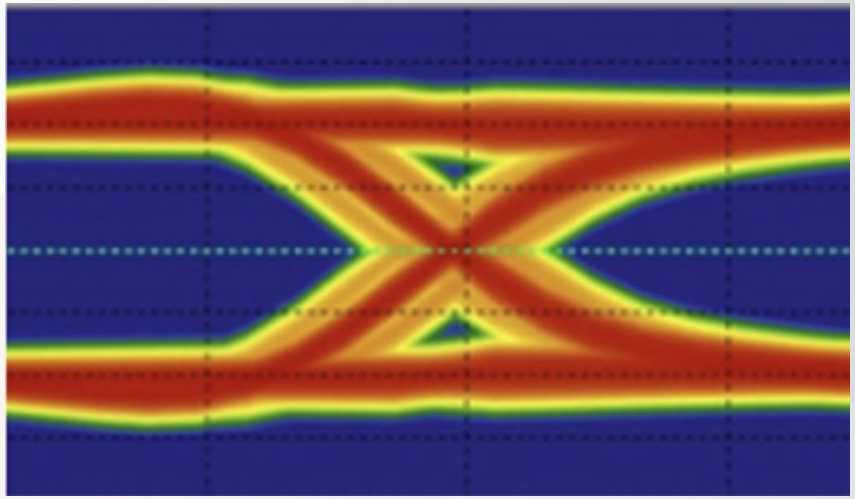
Traffic Log - Network Threat Protection Logs

File Edit View Filter Action Help

Date and...	Action	Severity	Direction	Protocol	Source Host	Source MAC	Source Port	Destination Host	Destination MAC	Destination Port	Applic
22/11/2013 8:07...	Allowed	5	Incoming	UDP	192.168.0.58	7C-05-07-91-D...	5353	224.0.0.251	01-00-5E-00-0...	5353	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52814	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-05-07-91-D...	1900	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.70	00-50-56-BE-7...	58498	192.168.0.117	00-0C-29-99-9...	443	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.56	00-0F-FE-F9-5...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.63	00-0F-FE-FD-8...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52815	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52816	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	62301	192.168.0.110	00-0C-29-2E-4...	8014	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52817	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52818	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.51	B4-B5-2F-7F-B...	50144	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.57	00-23-18-C3-F...	60848	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.58	7C-05-07-91-D...	HA	224.0.0.22	01-00-5E-00-0...	HA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-05-07-91-D...	51452	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52819	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52820	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52821	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52822	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	62303	192.168.0.110	00-0C-29-2E-4...	8014	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52824	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:09...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	62304	192.168.0.110	00-0C-29-2E-4...	8014	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52825	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52826	216.2.48.149	00-09-0F-09-0...	80	Dr\Pro
22/11/2013 8:09...	Allowed	5	Incoming	IP	192.168.0.64	E0-69-95-FA-3...	HA	224.0.0.22	01-00-5E-00-0...	HA	
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	52124	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	UDP	192.168.0.64	E0-69-95-FA-3...	137	192.168.0.127	FF-FF-FF-FF-F...	137	C:\Win

Different Asset DNA !





Sepio’s unique approach

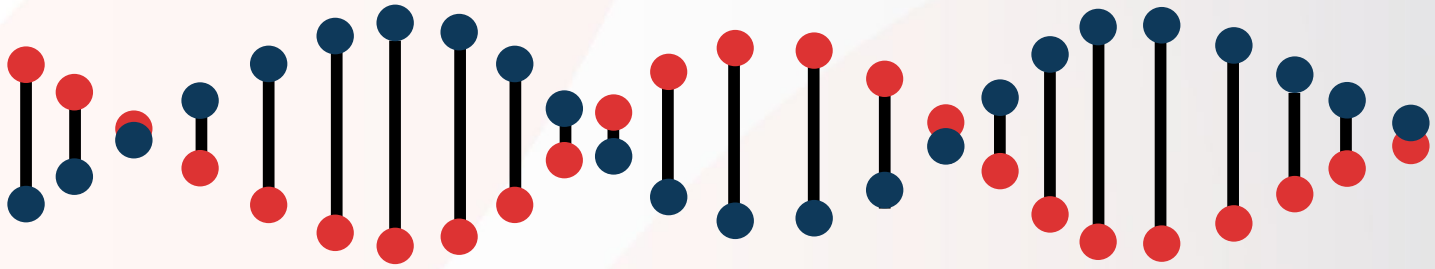
Harnessing new data source

getting to the true
source of asset risk
without traffic monitoring

- Create an Asset DNA
- Risk assessment
- Asset mapping

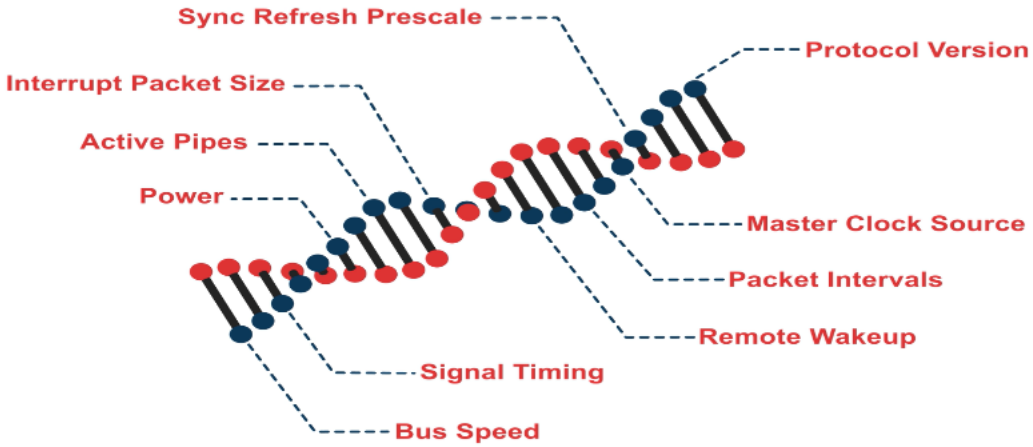
How do we do it?

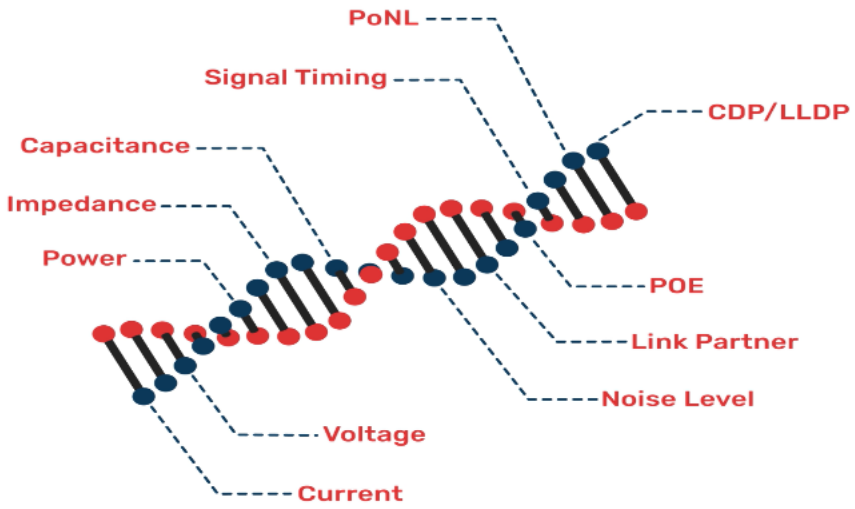
Asset DNA



Introducing Asset DNA

Host



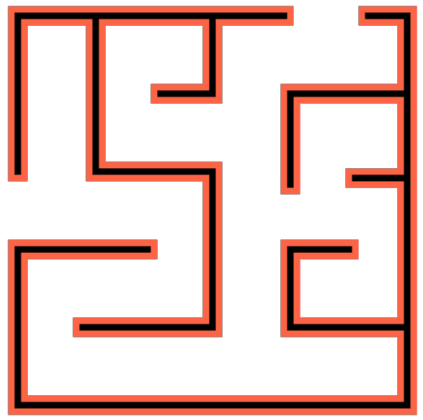


Network

SEPIO

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

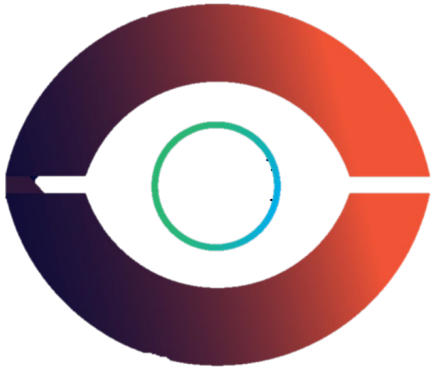
With our patented technology, we now harness a new data source – physical layer to accurately identify and classify your assets.



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

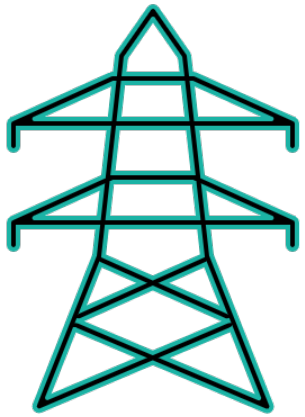
Go beyond legacy NAC solutions

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 proven value for CPS



Critical Infrastructure Business Benefits

"Sepio has an innovative and robust solution that identifies a type of threats that were difficult to identify otherwise"

R&D Engineer
Leading Global Energy and Utilities Provider

- Complete OT/IT/IoT asset visibility
- OT asset protection
- Maintaining operational continuity
- Easier risk management compliance
- Mitigate known threats

SEPIO

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

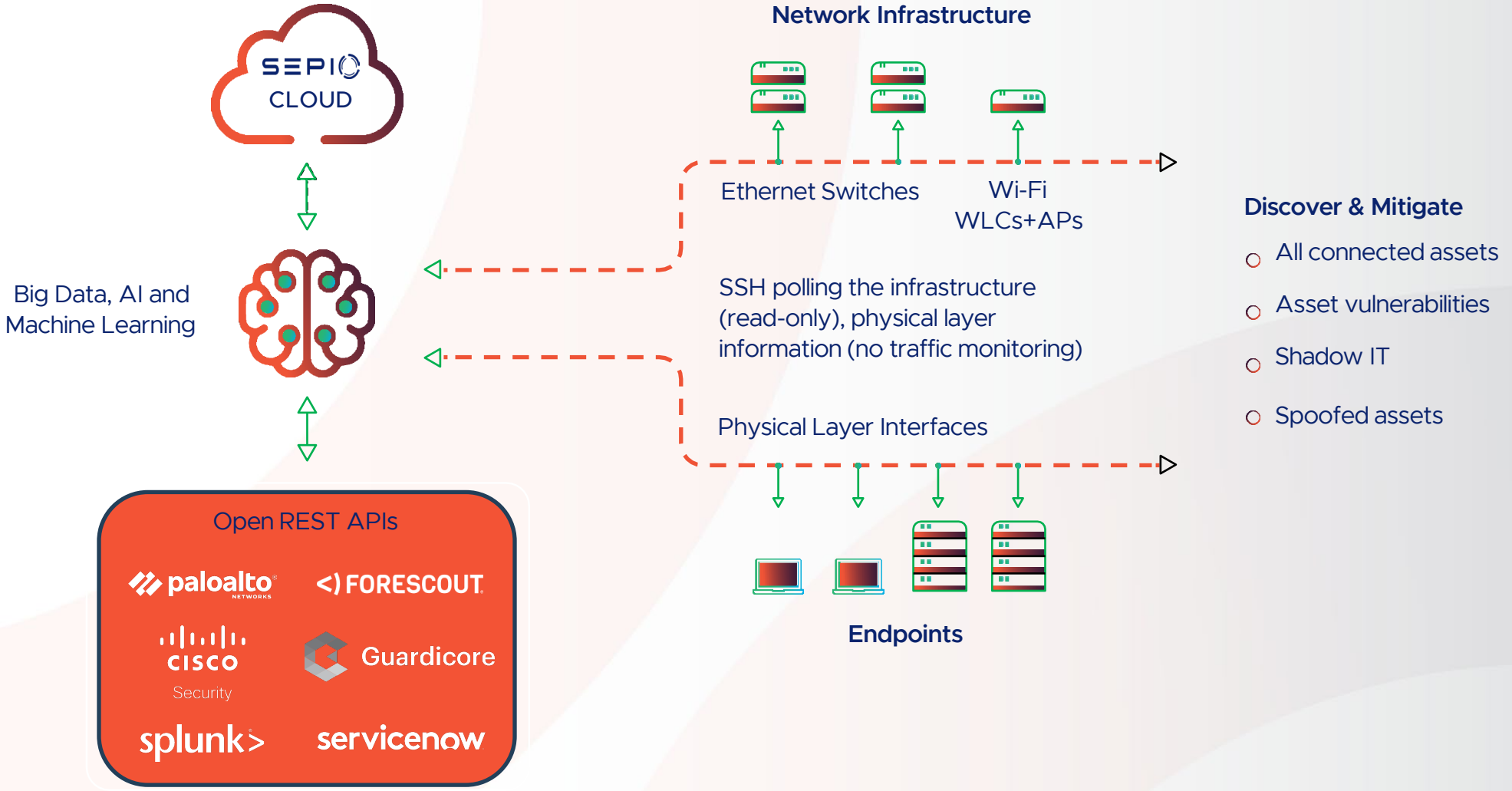
- Reduce complexity with a consolidated source of asset visibility across all environments
- Reduce hardware clutter
- Ensure operational efficiency of assets

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 (including VDI support)

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**

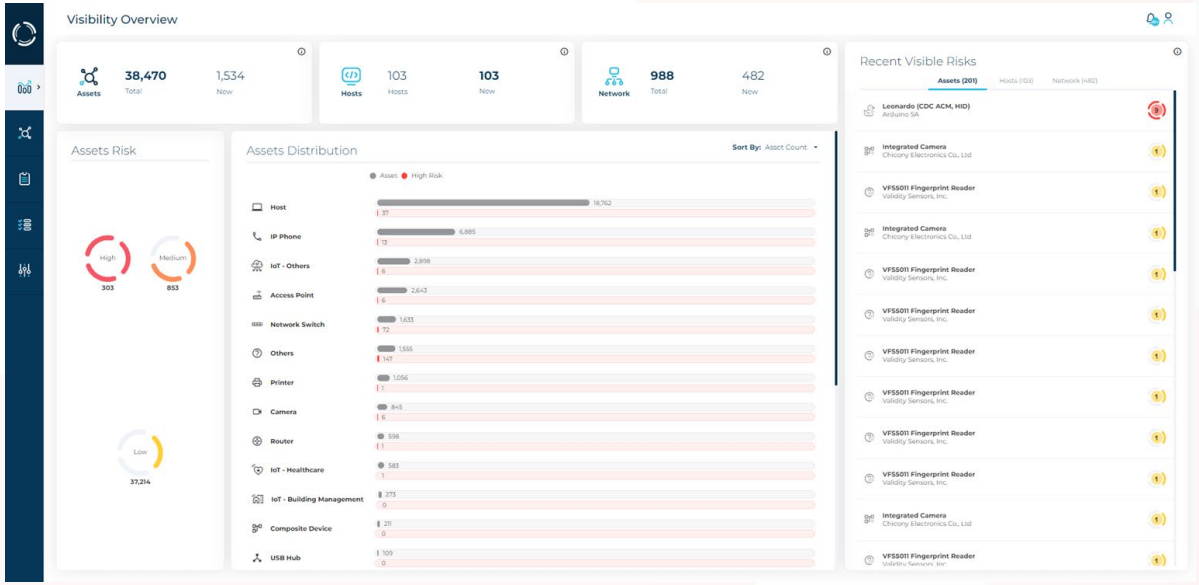
   Can be done manually by providing IP-SSH username – SSH password
   Can be done by importing CSV file

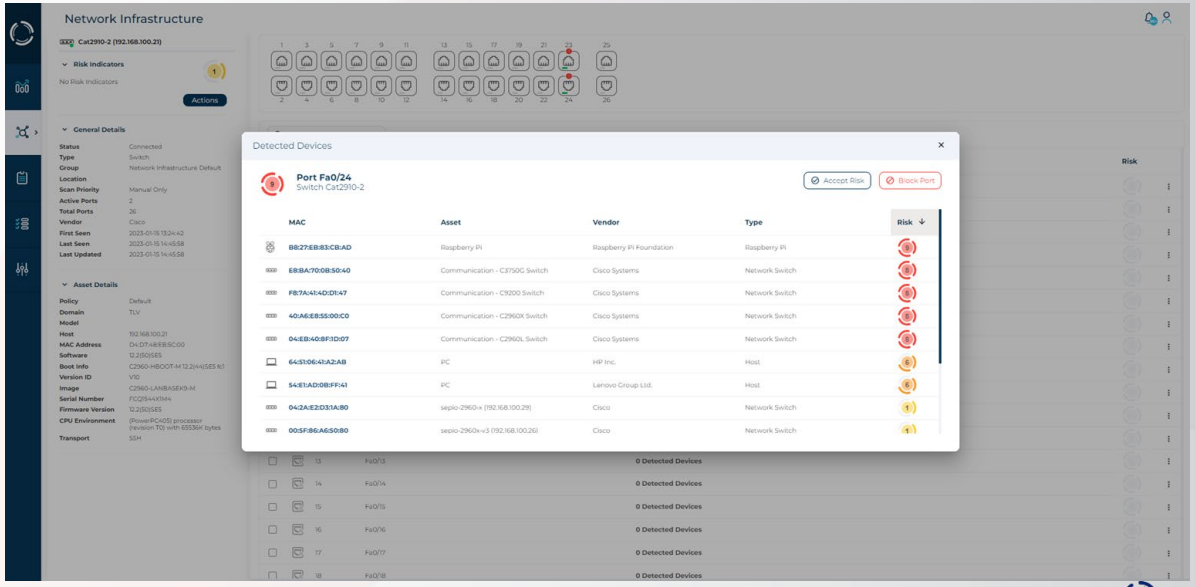
4. **Deploy Sepio agents**

   Supports Windows/RHEL/Debian

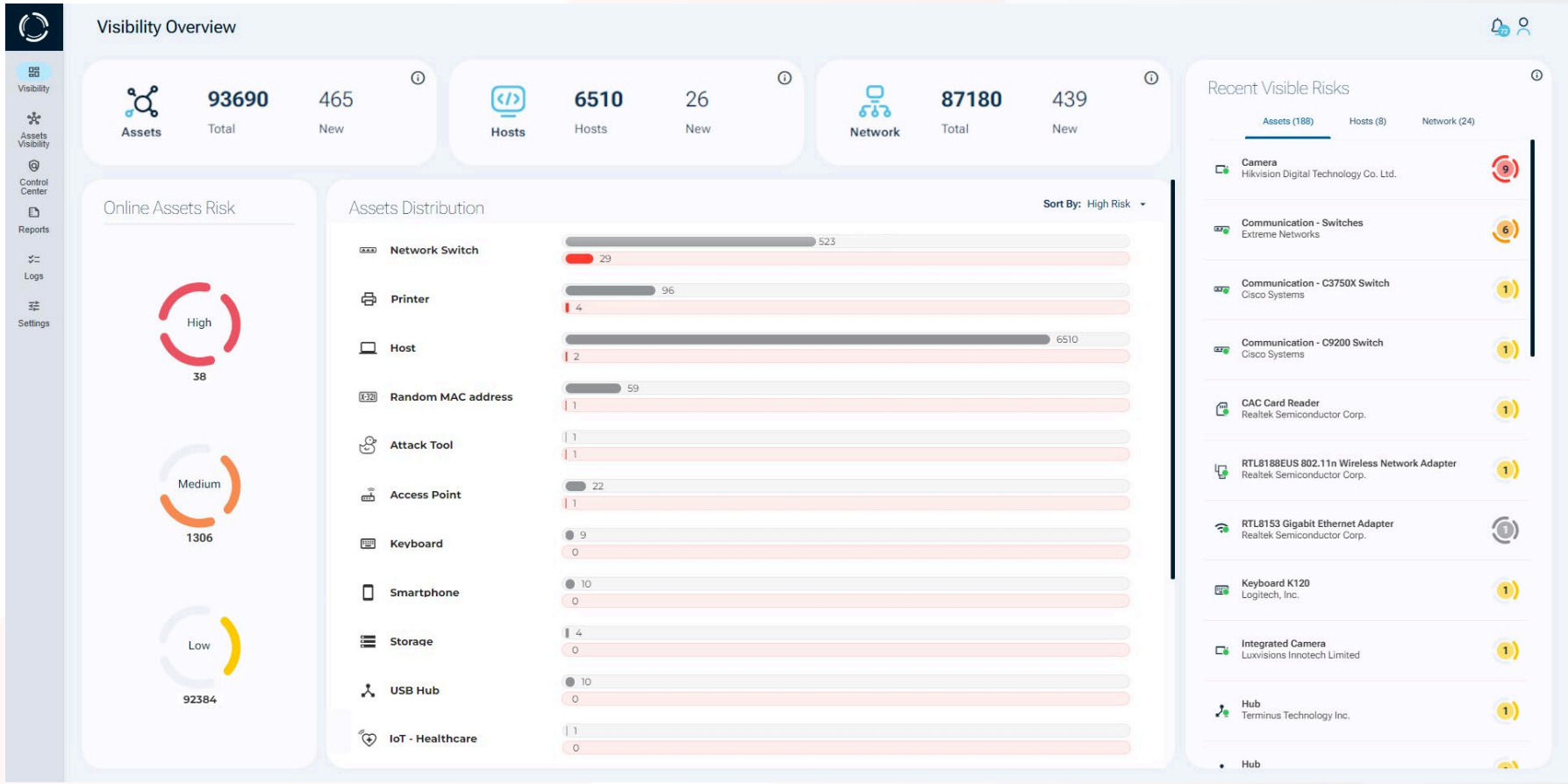
   Can be installed manually or using a distribution tool

5. **Complete integration in upstream systems**





Sepio's Asset Risk Management solution



SEPIO

See what you've been missing