



Mitigating Cyber Physical Systems Risks

May 24



Questions our OT customers ask themselves -

- ① Are all my assets listed?
- ① Where are my assets located?
- ① Are there any vulnerable assets that put us at risk?
- ① Are my assets verified and can I trust them?
- ① Where are my regulatory compliance gaps?

② 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).

① Where are my assets located?

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

① 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.

① 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.

② 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!



CPS Visibility Challenges



Active scanning → Potential impact on system responsiveness and availability.



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

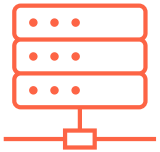


Dormant assets → Become “invisible” – MAC’less

Current Mean-Time-To-Value Challenges



Extensive use of human resources



Complexity due to additional sensors



Cumbersome network configuration

CPS Security challenges



Building a complete asset inventory



Enforcing granular security controls



Fulfilling regulatory compliance



Avoiding performance degradation

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] [Nmap Output] [Ports / Hosts] [Topology] [Host Details] [Scans]
OS Host
nmap -T4 -A -v 192.168.10.46
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 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] [Nmap Output] [Ports / Hosts] [Topology] [Host Details] [Scans]
OS Host
nmap -T4 -A -v 192.168.10.46
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 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
```

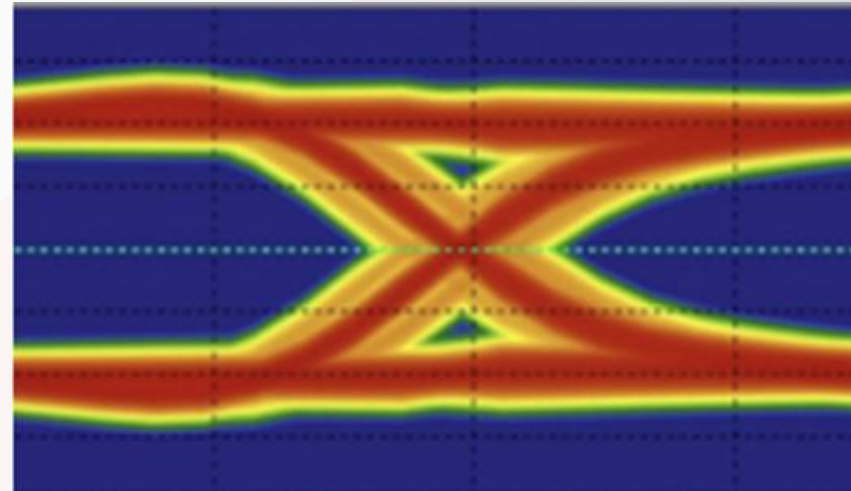
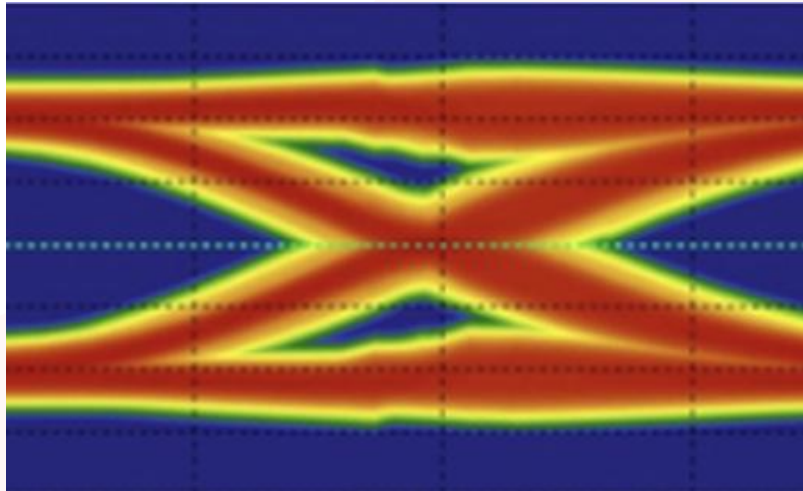
Same Traffic



Traffic Log - Network Threat Protection Logs											
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	TCP	192.168.0.58	7C-09-07-91-0...	3283	224.0.0.251	01-00-5E-00-0...	3283	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32814	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-09-07-91-0...	1900	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.70	00-50-54-9E-7...	58498	192.168.0.117	00-0C-29-99-9...	443	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.64	00-0F-FE-F3-5...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.63	00-0F-FE-F3-5...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32815	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32816	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42301	192.168.0.110	00-0C-29-2E-4...	8016	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32817	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32818	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.61	04-85-2F-7F-8...	30144	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.87	00-23-18-C3-F...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.87	00-23-18-C3-F...	80948	224.0.0.252	01-00-5E-00-0...	3288	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.58	7C-09-07-91-0...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-09-07-91-0...	51452	224.0.0.252	01-00-5E-00-0...	3288	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32819	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32820	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32821	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32822	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42303	192.168.0.110	00-0C-29-2E-4...	8016	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32824	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42304	192.168.0.110	00-0C-29-2E-4...	8016	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32825	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32826	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.64	80-69-95-7A-3...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.64	80-69-95-7A-3...	32124	224.0.0.252	01-00-5E-00-0...	3288	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.64	80-69-95-7A-3...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win

Traffic Log - Network Threat Protection Logs											
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-09-07-91-0...	3283	224.0.0.251	01-00-5E-00-0...	3283	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32814	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-09-07-91-0...	1900	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.70	00-50-54-9E-7...	58498	192.168.0.117	00-0C-29-99-9...	443	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.64	00-0F-FE-F3-5...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.63	00-0F-FE-F3-5...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32815	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32816	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42301	192.168.0.110	00-0C-29-2E-4...	8016	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32817	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32818	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.61	04-85-2F-7F-8...	30144	239.255.255.250	01-00-5E-7F-F...	1900	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.87	00-23-18-C3-F...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.87	00-23-18-C3-F...	80948	224.0.0.252	01-00-5E-00-0...	3288	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.58	7C-09-07-91-0...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.58	7C-09-07-91-0...	51452	224.0.0.252	01-00-5E-00-0...	3288	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32819	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32820	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32821	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32822	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42303	192.168.0.110	00-0C-29-2E-4...	8016	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32824	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Outgoing	TCP	192.168.0.117	00-0C-29-99-9...	42304	192.168.0.110	00-0C-29-2E-4...	8016	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32825	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-83-CC-4E-C...	32826	216.2.48.149	00-09-0F-09-0...	80	Di/Pre
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.64	80-69-95-7A-3...	NA	224.0.0.22	01-00-5E-00-0...	NA	
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.64	80-69-95-7A-3...	32124	224.0.0.252	01-00-5E-00-0...	3288	Ct/Win
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.64	80-69-95-7A-3...	137	192.168.0.127	FF-F7-F7-F7-F...	137	Ct/Win

Different Asset DNA !

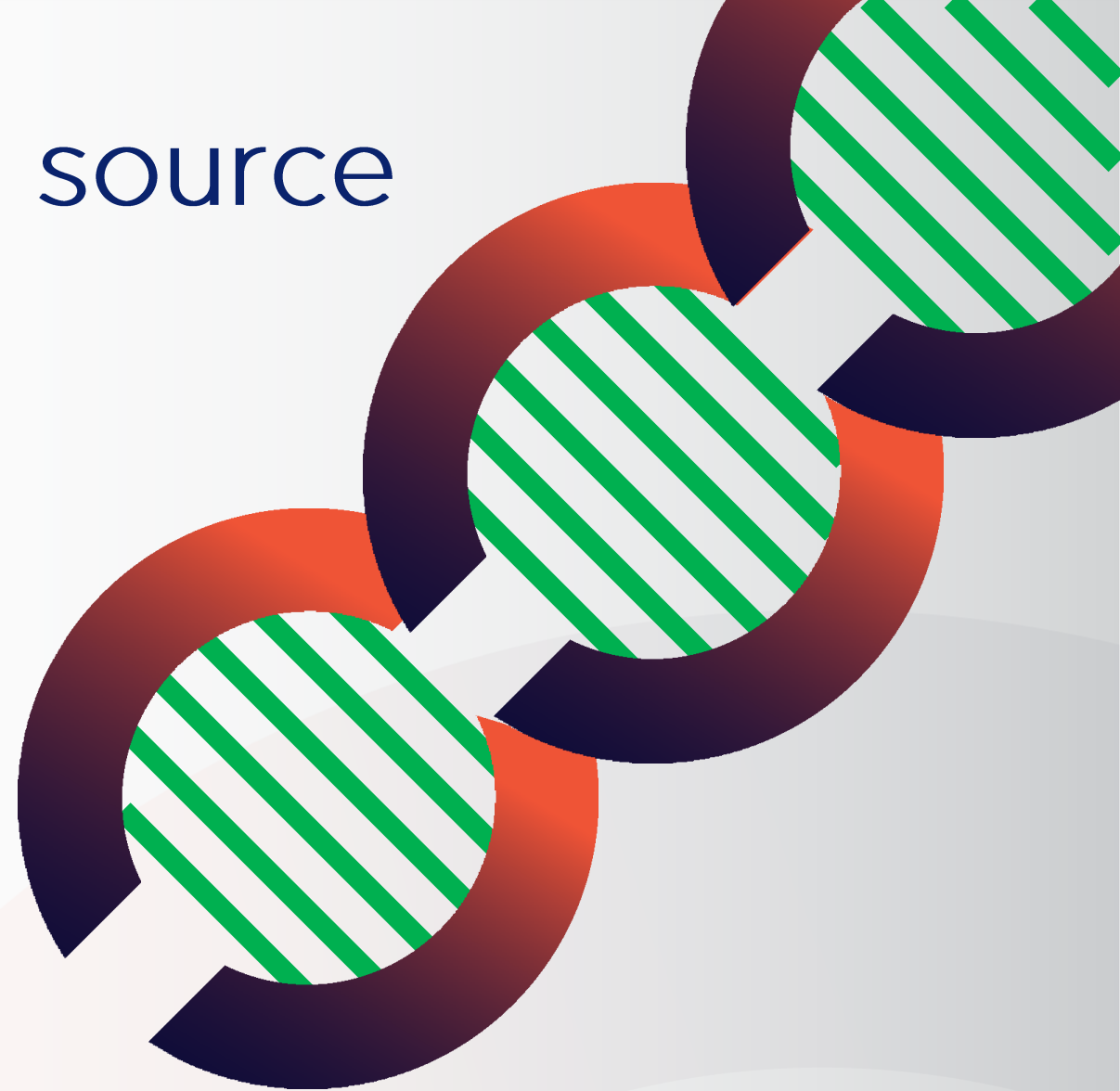


Sepio's unique approach

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

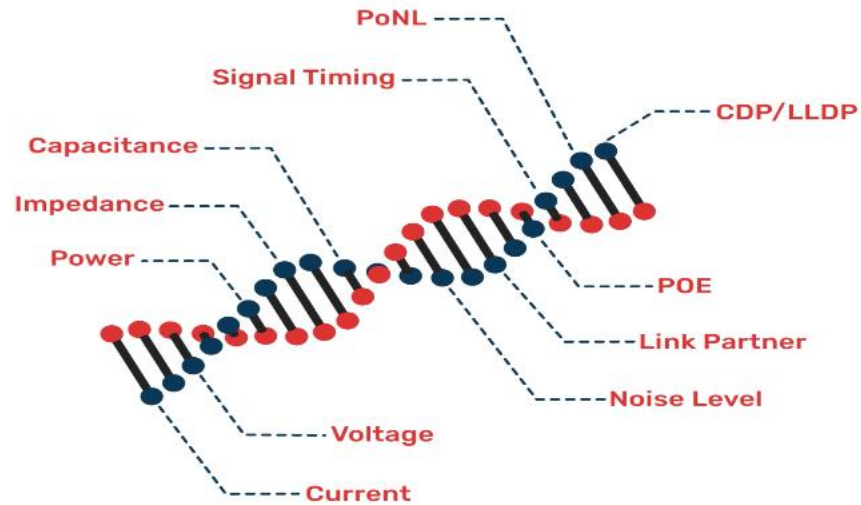
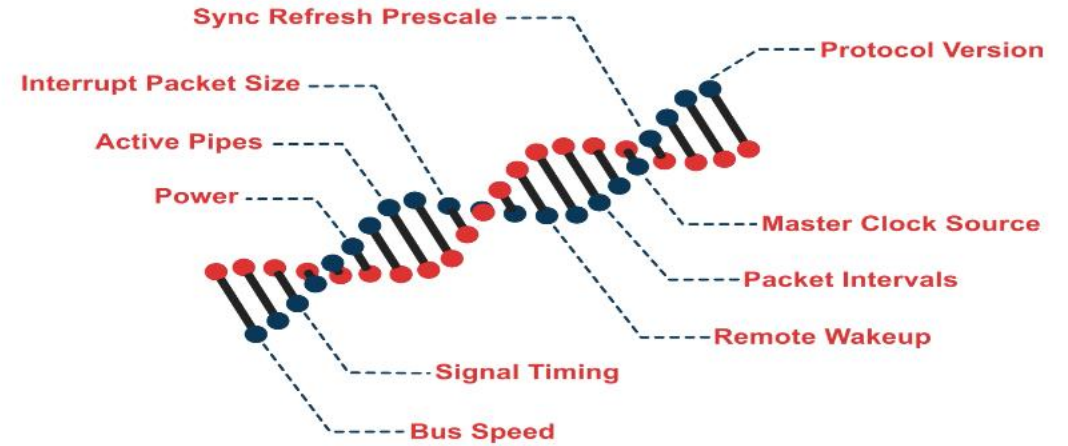


Asset DNA provides a single source of truth,
focusing on **EXISTENCE** – rather than
ACTIVITY.

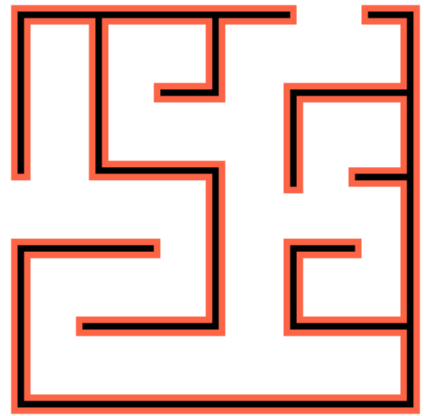
With our patented technology, we now
harness a new data source – **physical layer**
to accurately identify and classify your
assets.

Introducing Asset DNA

Host

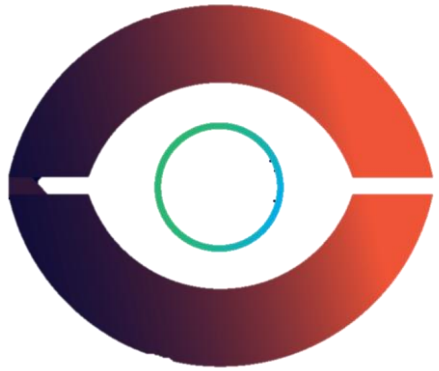


Network



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.



XDR/EDR

device control

still has blind spots

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

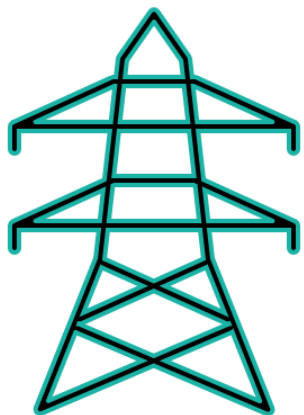


Go beyond legacy NAC solutions

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'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

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

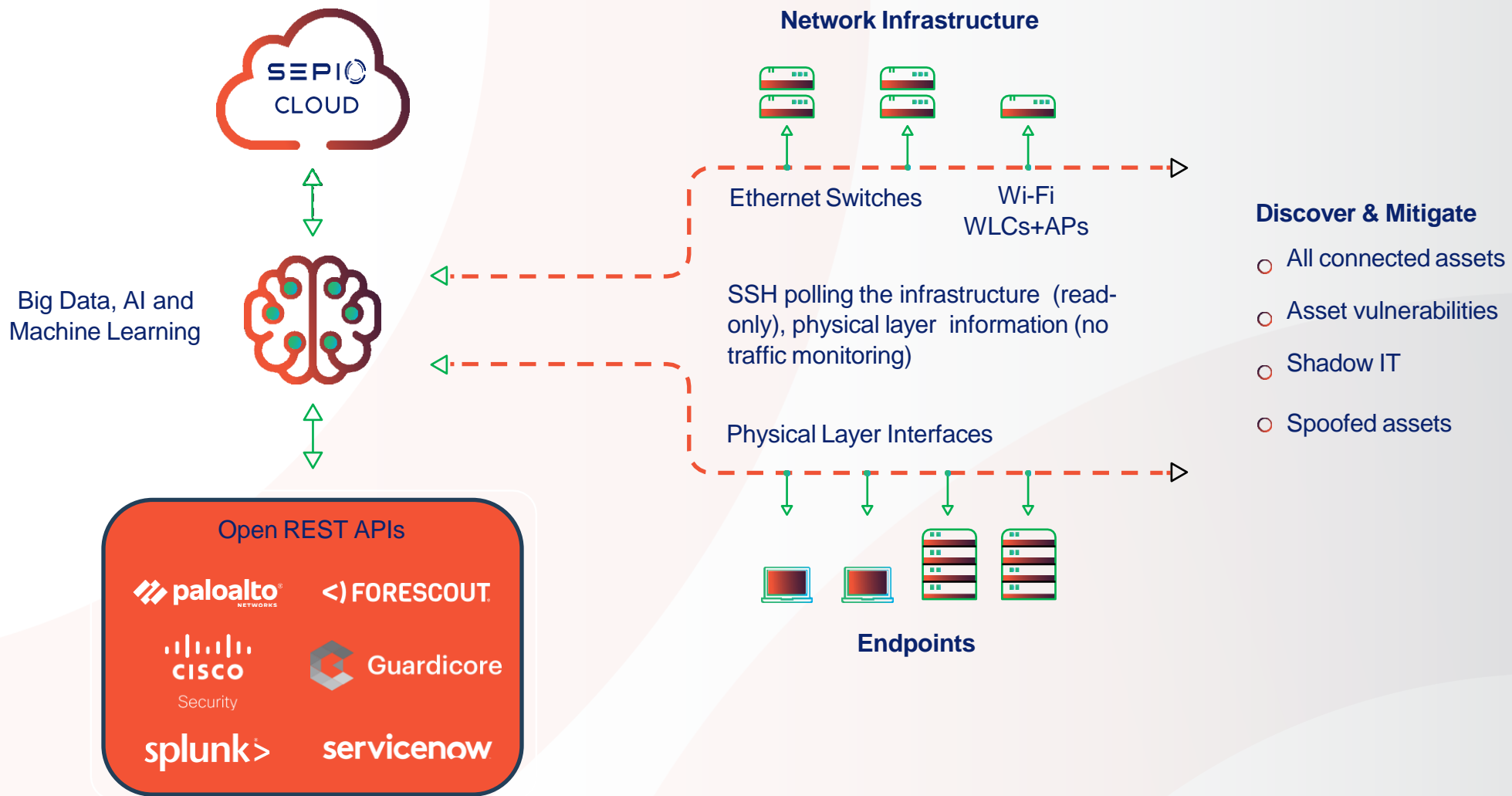
ITAM & CMDB

- 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

Architecture and Deployment aspects



Sepio agent deployment options



Fixed agent



Session based

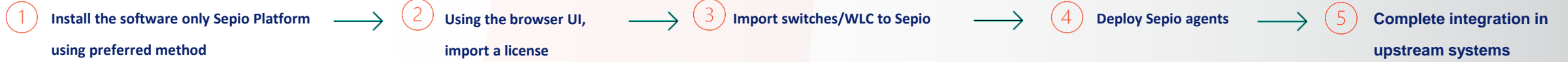


Dissolvable agent

Typical Customer Journey



Deployment process

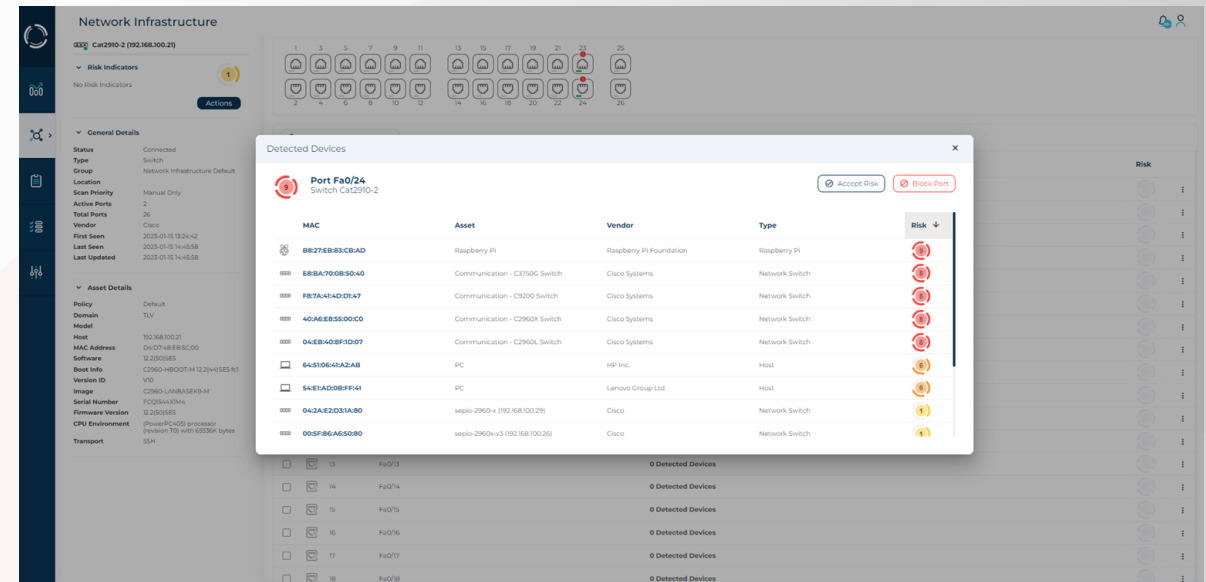
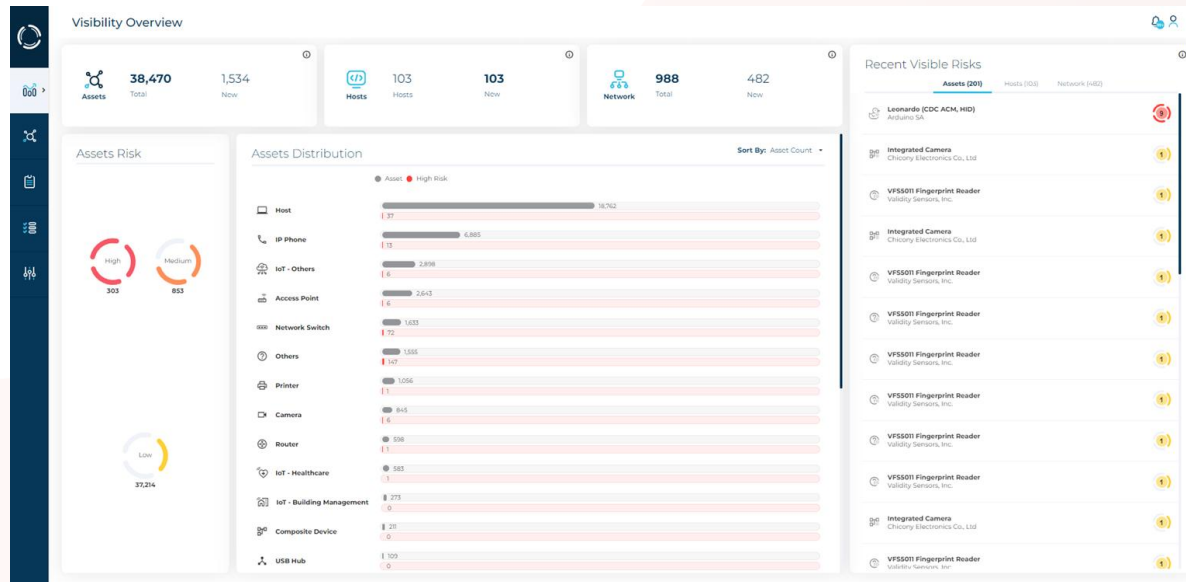


Cloud, virtual, on-prem or via Azure marketplace

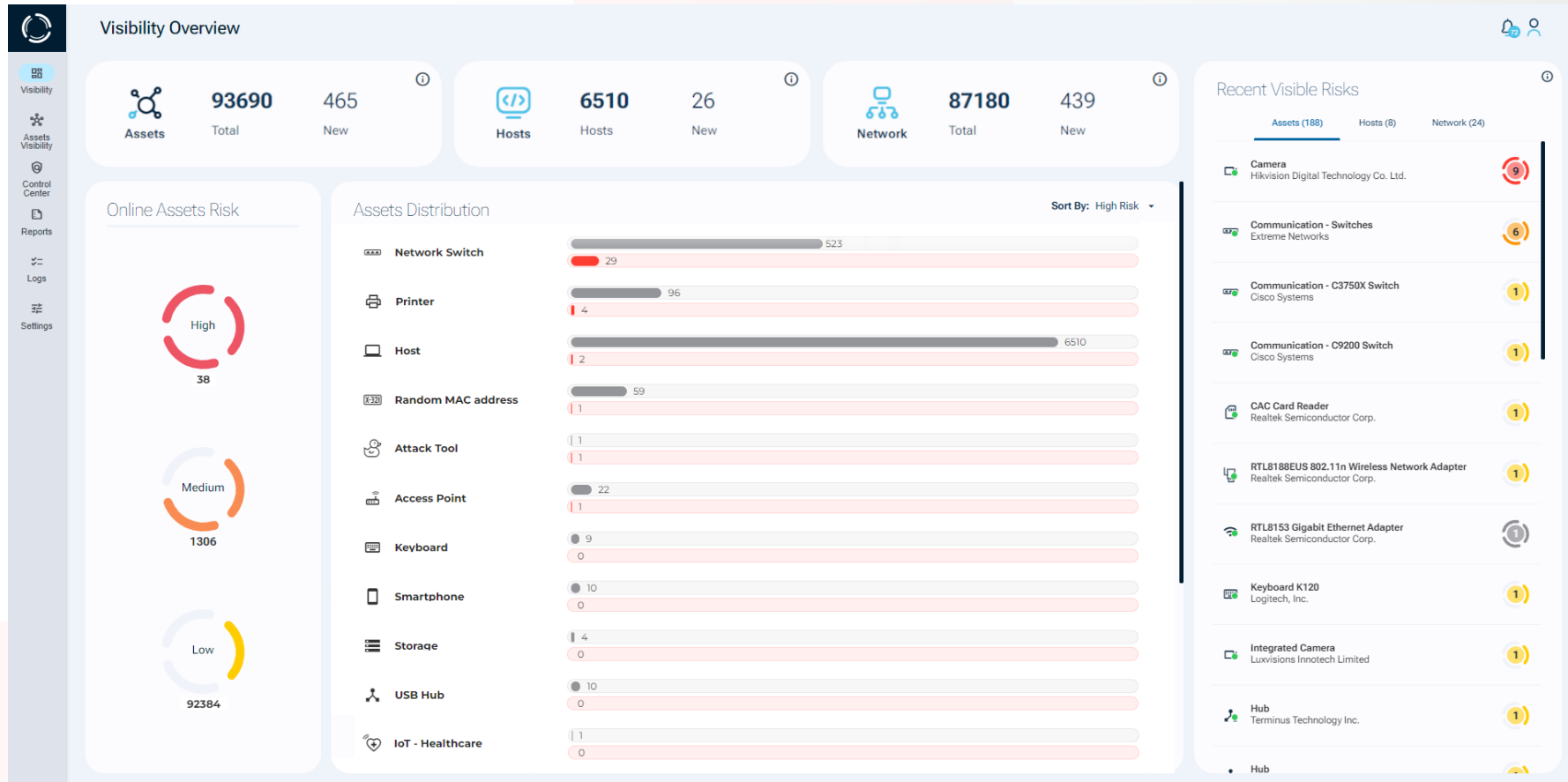
Can be done manually by providing IP-SSH username – SSH password
Can be done by importing CSV file

Supports Windows/RHEL/Debian

Can be installed manually or using a distribution tool



Sepio's Asset Risk Management solution





See what you've been
missing.

