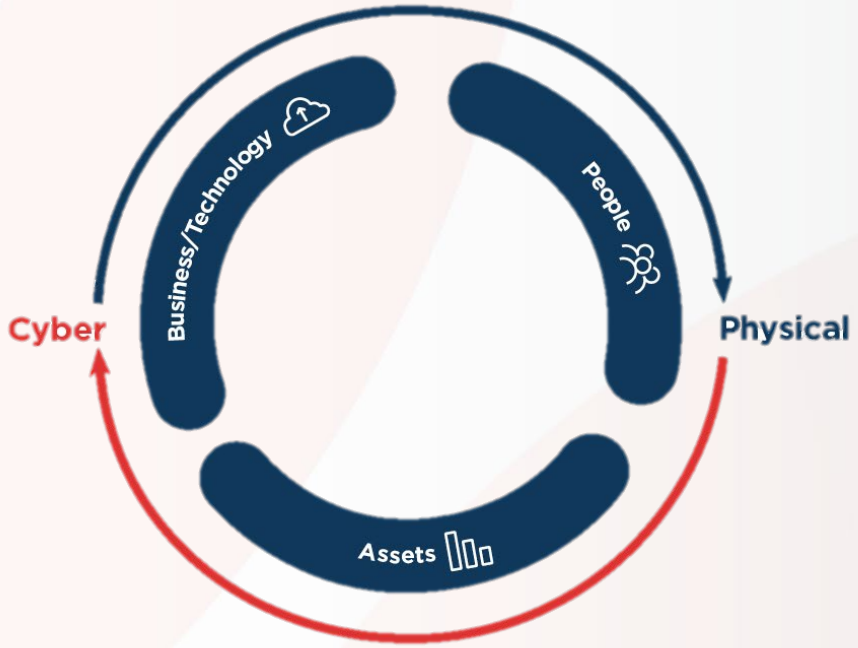
Mitigating Cyber Physical Systems Risks

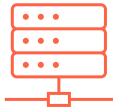
July 23

In a recent Gartner survey, security and risk leaders ranked IoT and cyber physical systems as their top concerns for the next three to five yearsd.



Source: Gartner®

CPS Popular attack vectors



Network

Removeable media

Supply chain

CPS Security challenges

Building a complete asset inventory

Enforcing granular security controls

Fulfilling regulatory compliance

Avoiding performance degradation

Questions our customers ask themselves

- Do I see all my assets?
- Are there any vulnerable assets?
- Are the assets, what they say they are?
- Is there something connected in the middle?
- Do I have regulatory compliance gaps?

Use cases

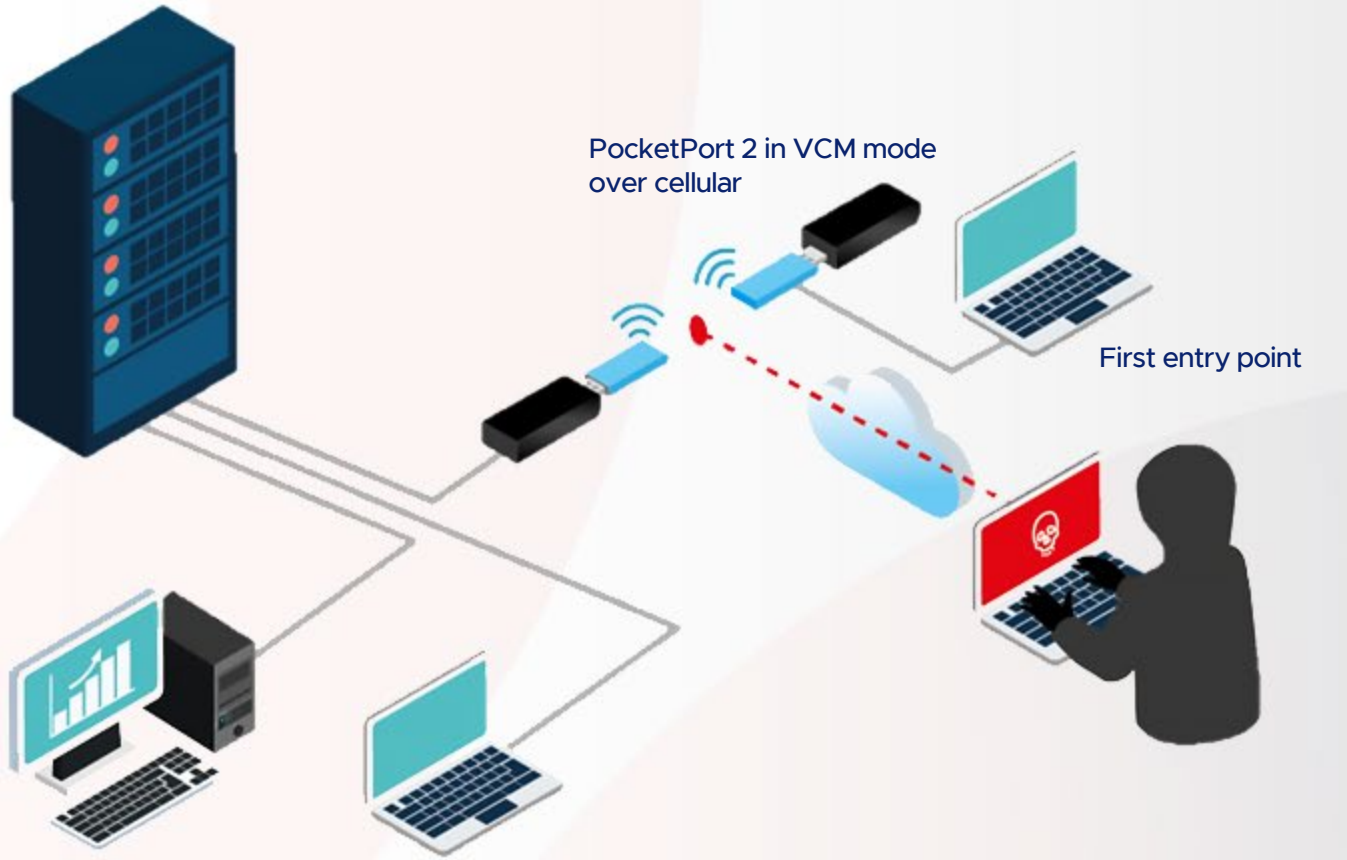
USB use case: Bypassing biometric security measures

Palm vein scanner
connected over USB

Beaglebone low-cost board
running USB Proxy MiTM.

High privilege user
endpoint

Network use case: MiTM transparent attack



Peripheral asset attacks

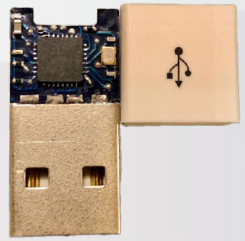
Way In

```
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

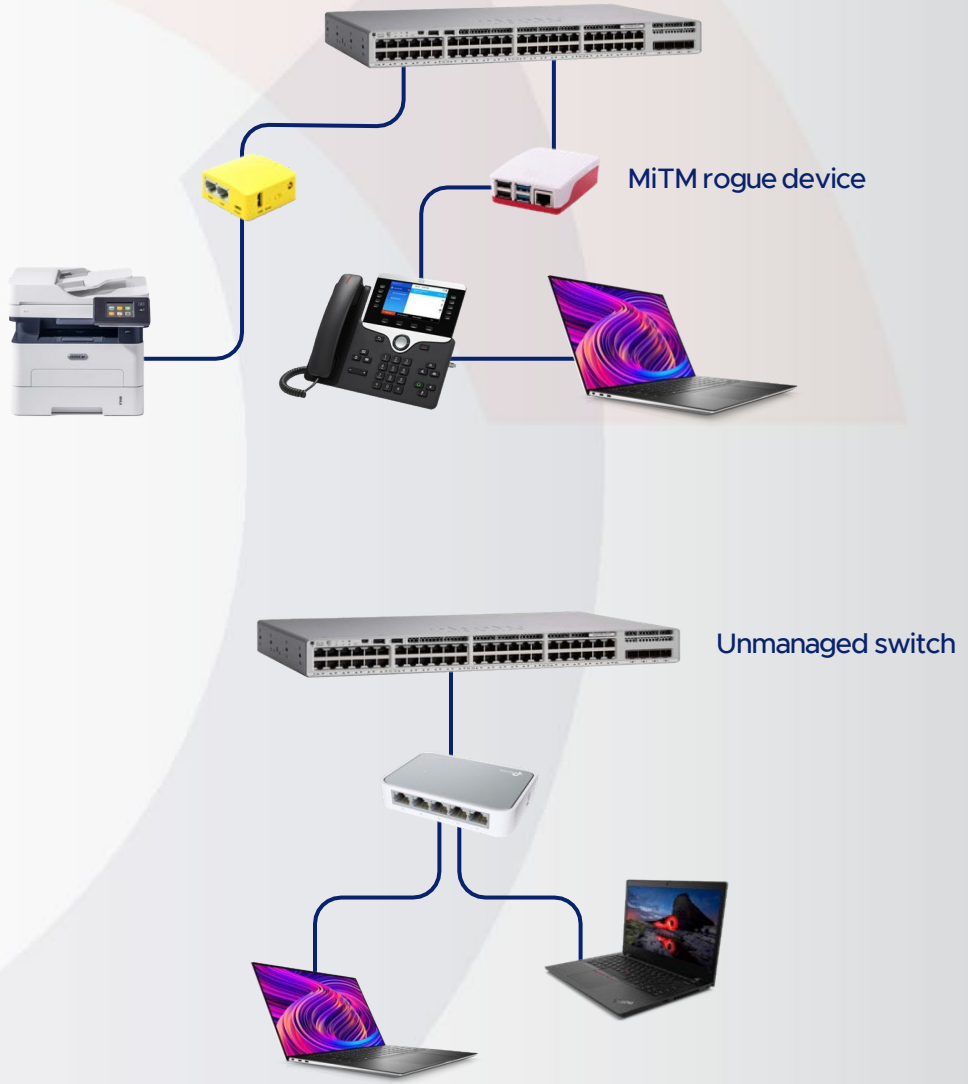


- Exfiltrate the data directly to the attack tool
- Use an integrated Wi-Fi to remotely extract
- Connect to the internet and exfiltrate the data "invisibly" – such as adding comments on youtube
- Use continuous and invisible remote shell into corporate PCs

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



Existing technologies blind spots

Friend or Foe?

Same MAC

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

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

Same Ports

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 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
```

Target: 192.168.10.46 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.10.46

Hosts Services

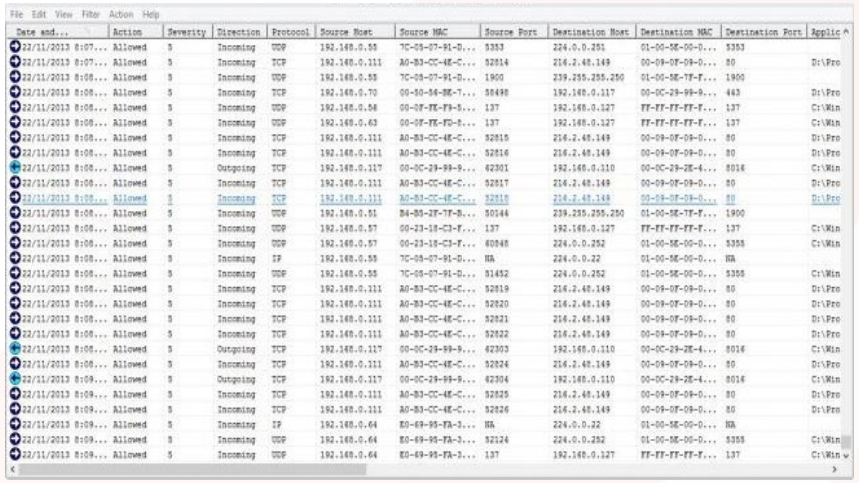
Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

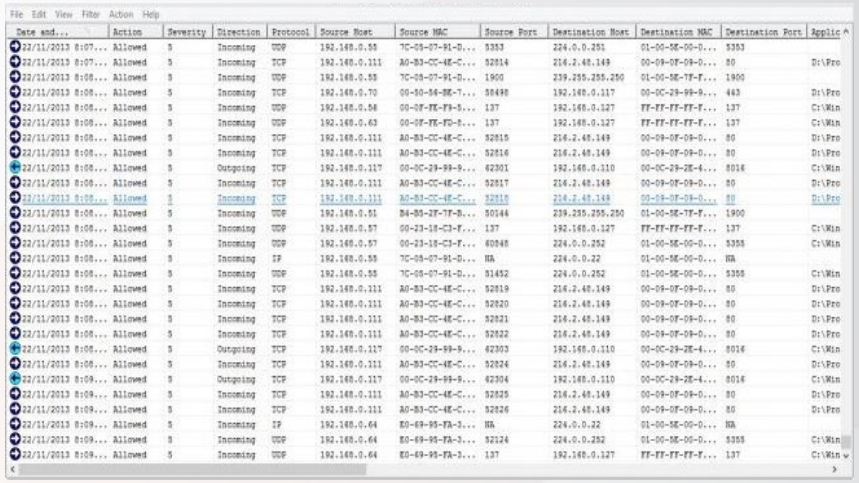
nmap -T4 -A -v 192.168.10.46 Details

```
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

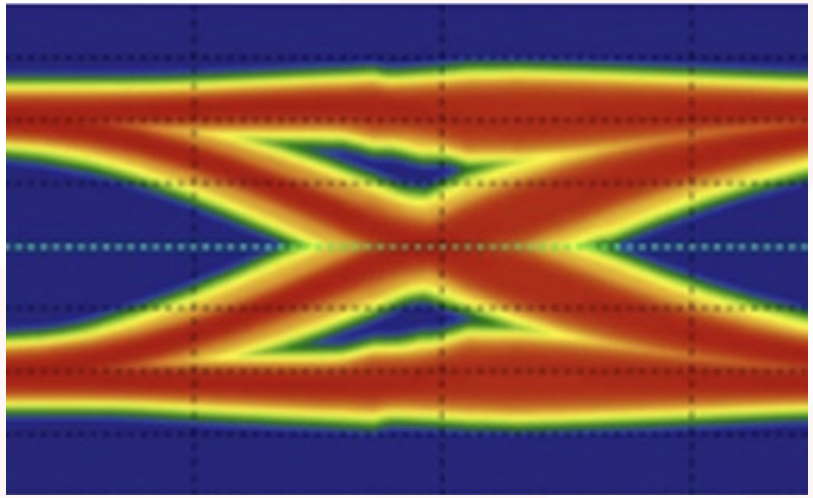


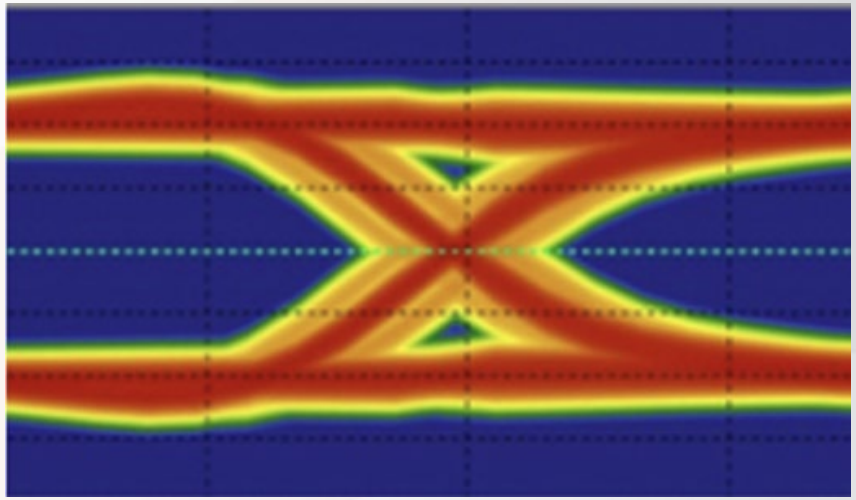
Date and...	Action	Severity	Direction	Protocol	Source Host	Source MAC	Source Port	Destination Host	Destination MAC	Destination Port	Applic
22/11/2013 8:07...	Allowed	5	Incoming	UDP	192.168.0.55	7C-05-07-91-D...	5353	224.0.0.251	01-00-5E-00-0...	5353	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52614	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.55	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	D:\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...	52615	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52616	216.2.48.149	00-09-0F-09-0...	80	D:\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...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52617	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52618	216.2.48.149	00-09-0F-09-0...	80	D:\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...	40848	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.55	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	192.168.0.55	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...	52619	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52620	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52621	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52622	216.2.48.149	00-09-0F-09-0...	80	D:\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...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52624	216.2.48.149	00-09-0F-09-0...	80	D:\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...	8016	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52625	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52626	216.2.48.149	00-09-0F-09-0...	80	D:\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

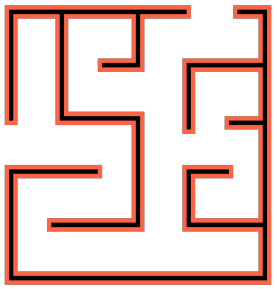


Date and...	Action	Severity	Direction	Protocol	Source Host	Source MAC	Source Port	Destination Host	Destination MAC	Destination Port	Applic
22/11/2013 8:07...	Allowed	5	Incoming	UDP	192.168.0.55	7C-05-07-91-D...	5353	224.0.0.251	01-00-5E-00-0...	5353	
22/11/2013 8:07...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52614	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	UDP	192.168.0.55	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	D:\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...	52615	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52616	216.2.48.149	00-09-0F-09-0...	80	D:\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...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52617	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52618	216.2.48.149	00-09-0F-09-0...	80	D:\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...	40848	224.0.0.252	01-00-5E-00-0...	5355	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	IP	192.168.0.55	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	192.168.0.55	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...	52619	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52620	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52621	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52622	216.2.48.149	00-09-0F-09-0...	80	D:\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...	8016	C:\Win
22/11/2013 8:08...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52624	216.2.48.149	00-09-0F-09-0...	80	D:\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...	8016	C:\Win
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52625	216.2.48.149	00-09-0F-09-0...	80	D:\Pro
22/11/2013 8:09...	Allowed	5	Incoming	TCP	192.168.0.111	A0-B3-CC-4E-C...	52626	216.2.48.149	00-09-0F-09-0...	80	D:\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!

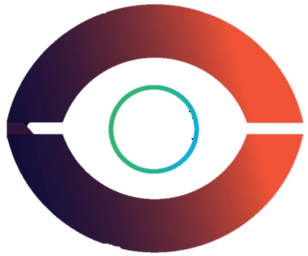






Passive network probing is an IT/OT nightmare

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.

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’s unique approach

Sepio's approach:
Identify and validate

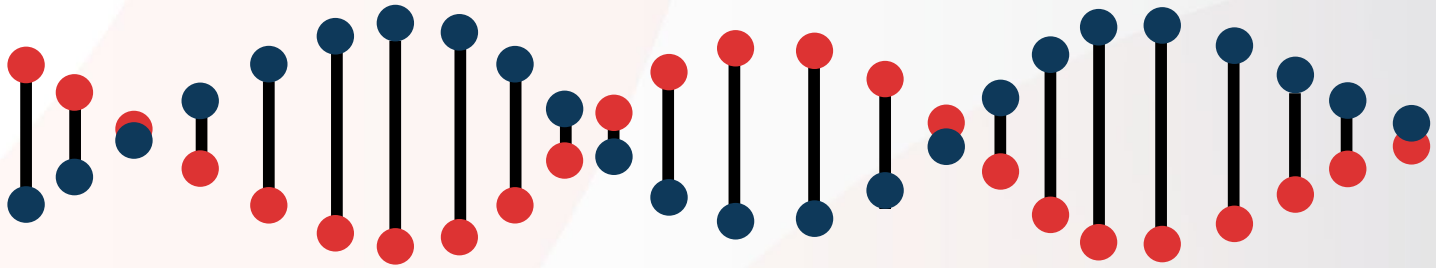
- Visibility and identity gaps
- Business value

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.

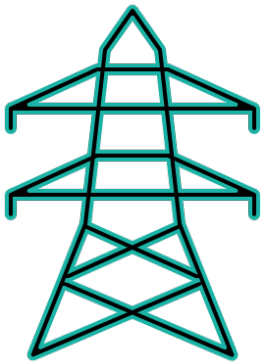
Introducing Asset DNA

Host

Network

ARF – Risk Assessing

Sepio’s proven value for CPS



Critical Infrastructure Business Benefits

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

"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

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

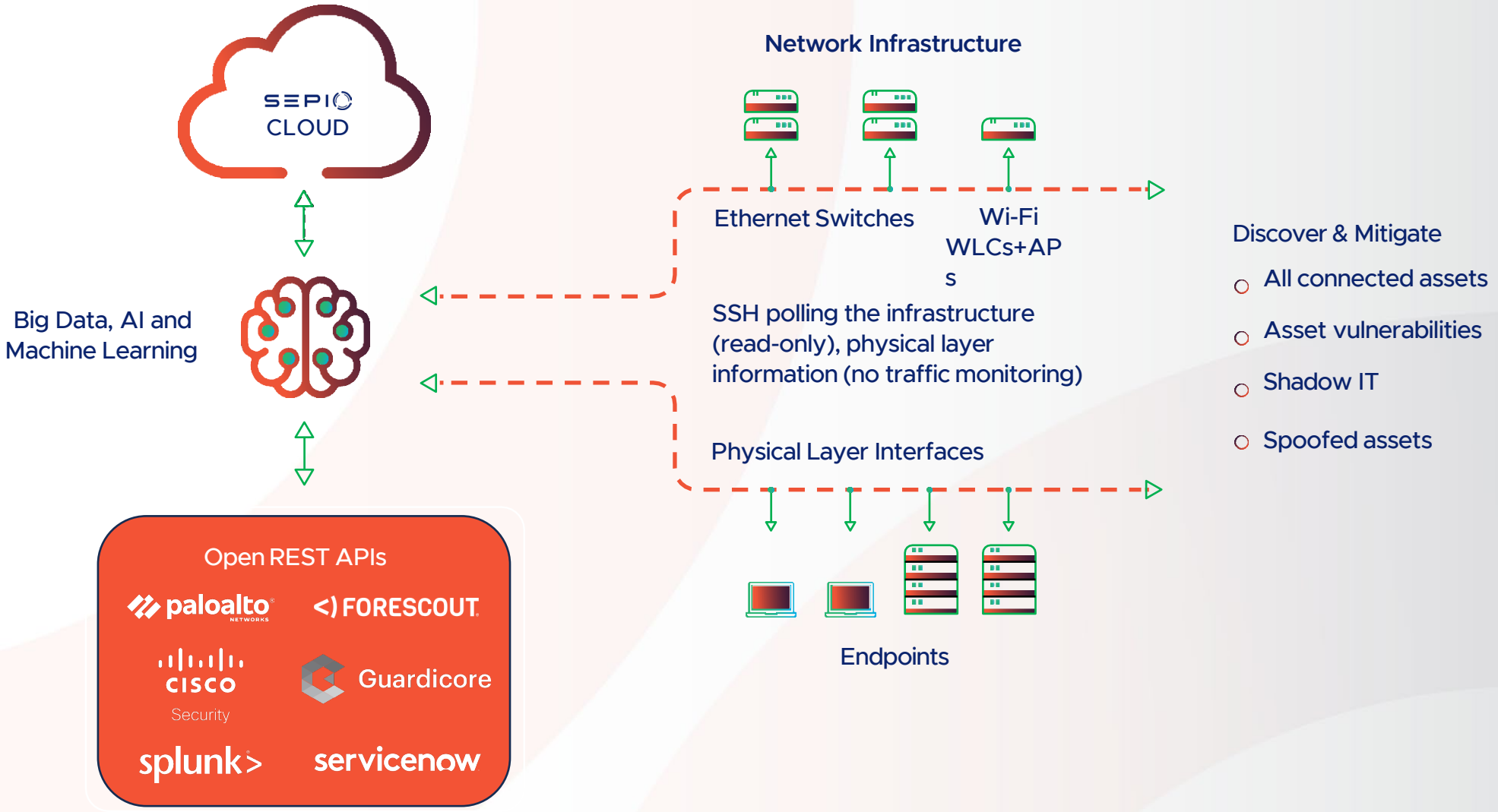
- Reduce complexity with a consolidated source of asset visibility across all environments
- Reduce hardware clutter
- Ensure operational efficiency of assets

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

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

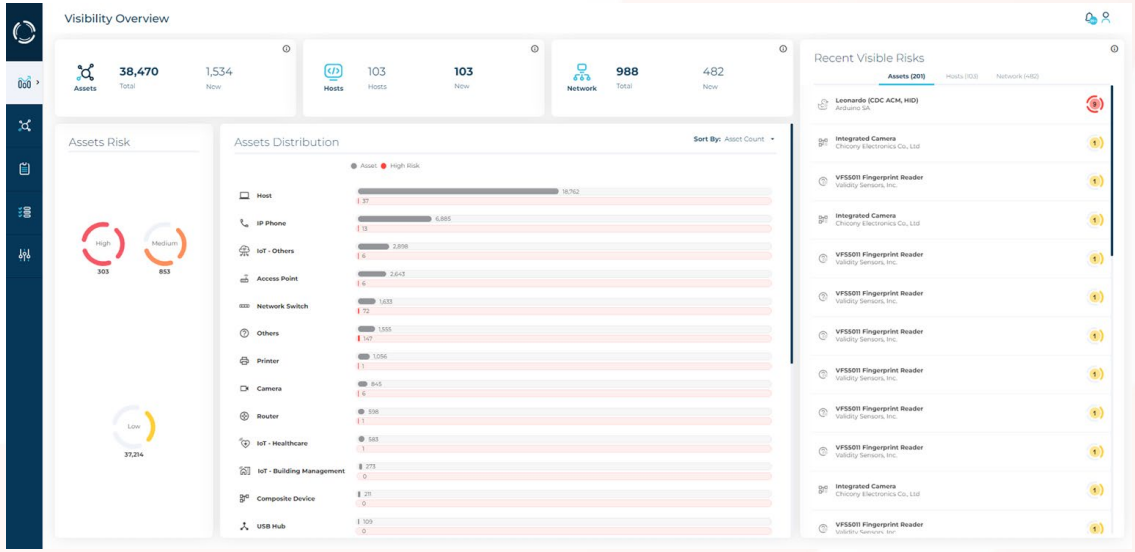
3. Import switches/WLC to Sepio

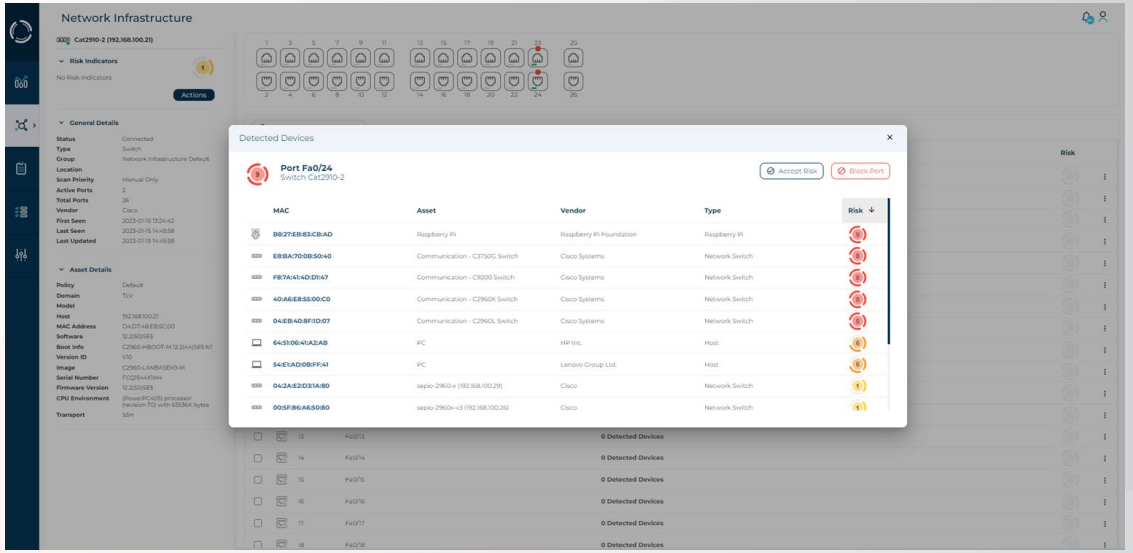
   Can be done manually by providing IP-SSH username – SSH password
   Can be done by importing CSV file

4. Deploy Sepio agents

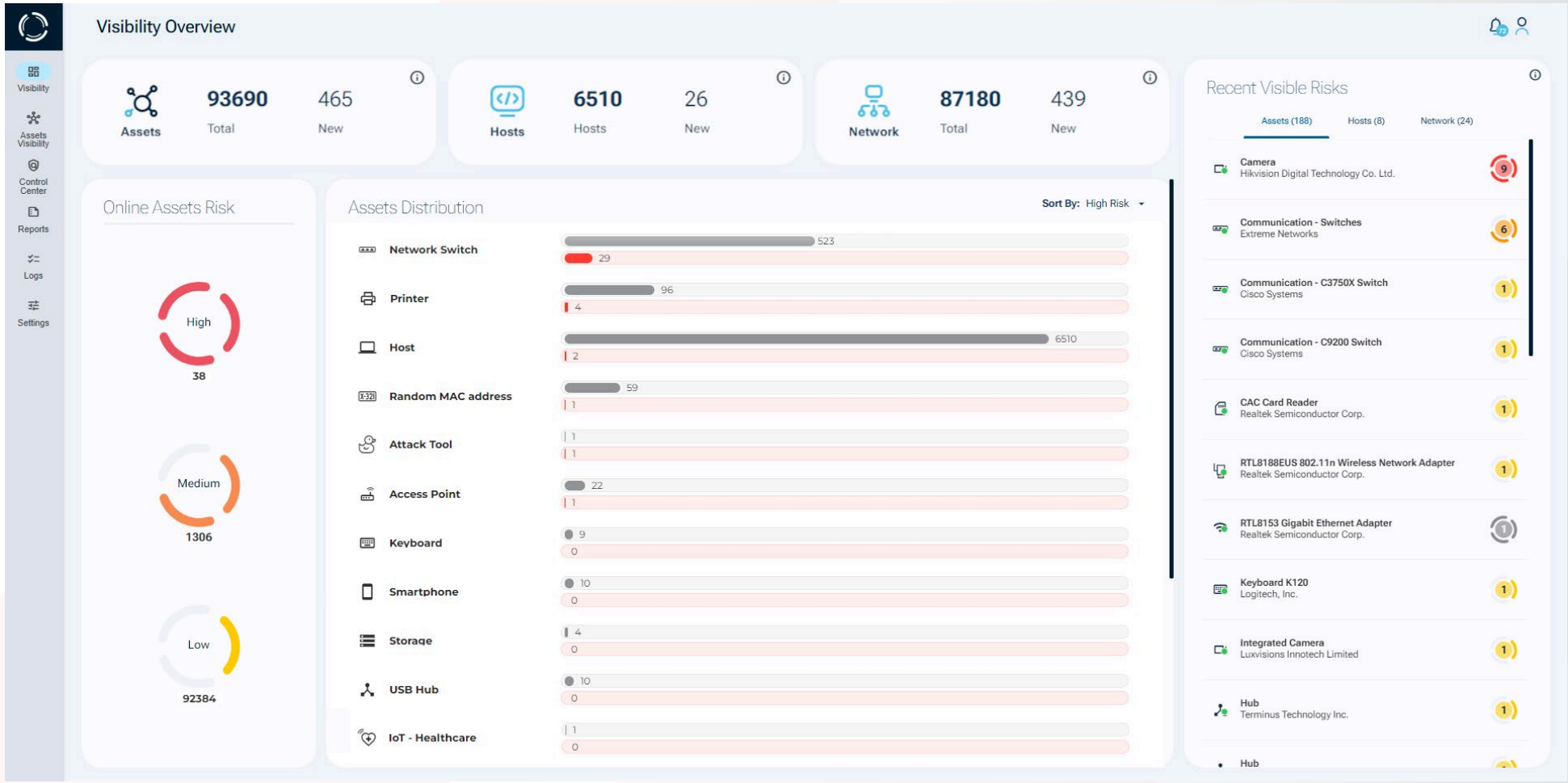
   Supports Windows/RHEL/Debian
   Can be installed manually or using a distribution tool

5. Complete integration in upstream systems





Sepio's Asset Risk Management solution



SEPIO

See what you've been missing.