



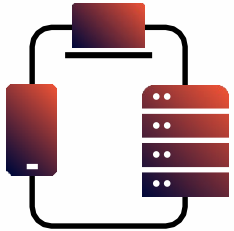
For Financial Services

Overview of Sepio's Asset Risk Management Platform

July 23



Hardware assets pose major security concerns



1

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

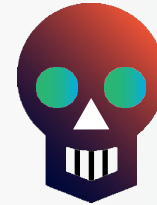
- Peripheral devices
- (MAC-less devices)
- Hardware BOM



2

Hardware Zero Trust

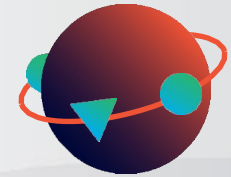
Control access to the enterprise through **granular policy enforcement & hardware identity validation**



3

Rogue Device Mitigation (RDM) of spoofed,

manipulated devices, and hidden implants



4

Detection of Hardware Manipulation

within the supply chain

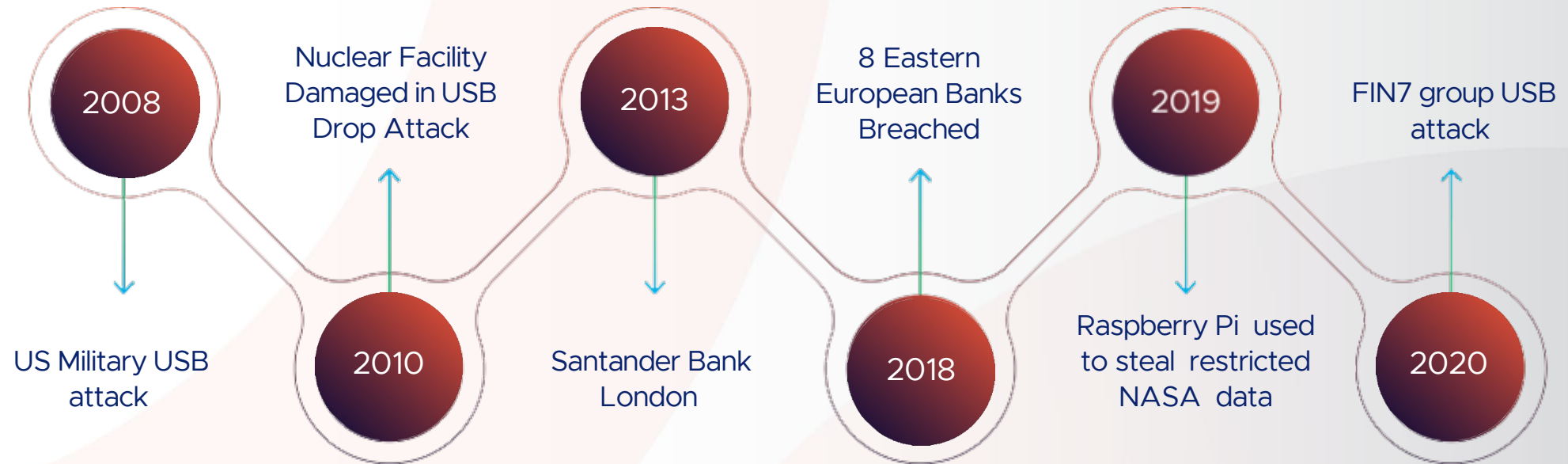
Hardware attack tools are gaining popularity

- 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 assets provide a permanent foothold for threat actors in the organization: MiTM, Data manipulation etc.



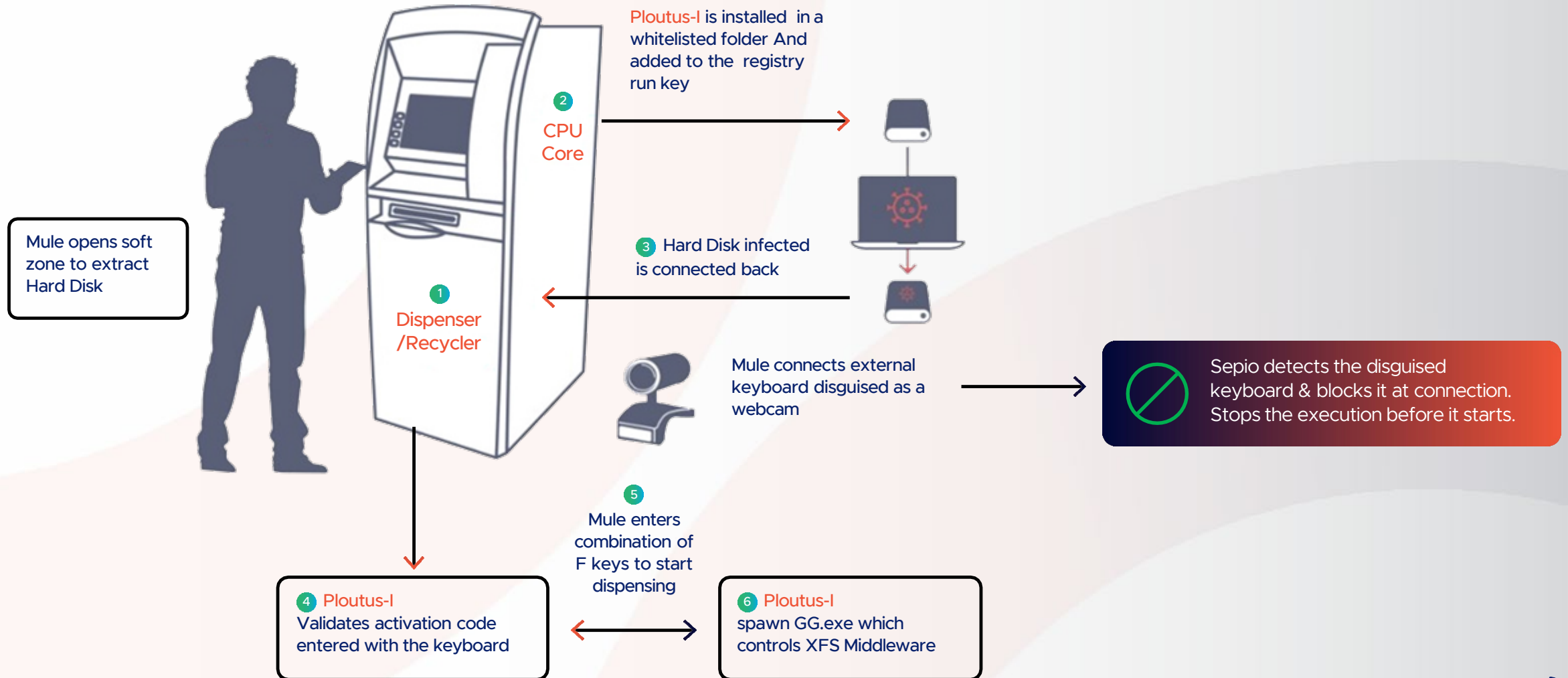
Is it really happening? **Yes!**

Why? Attackers are pursuing the path-of-least-resistance



Use cases

ATM use case: FiXS The new ATM malware in LATAM



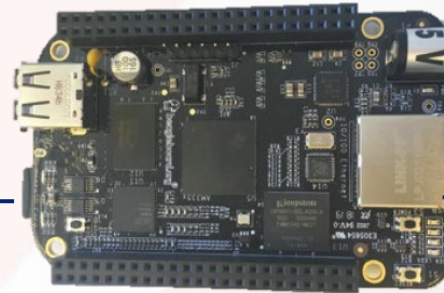
USB use case: Bypassing biometric security measures



Palm vein scanner
connected over **USB**

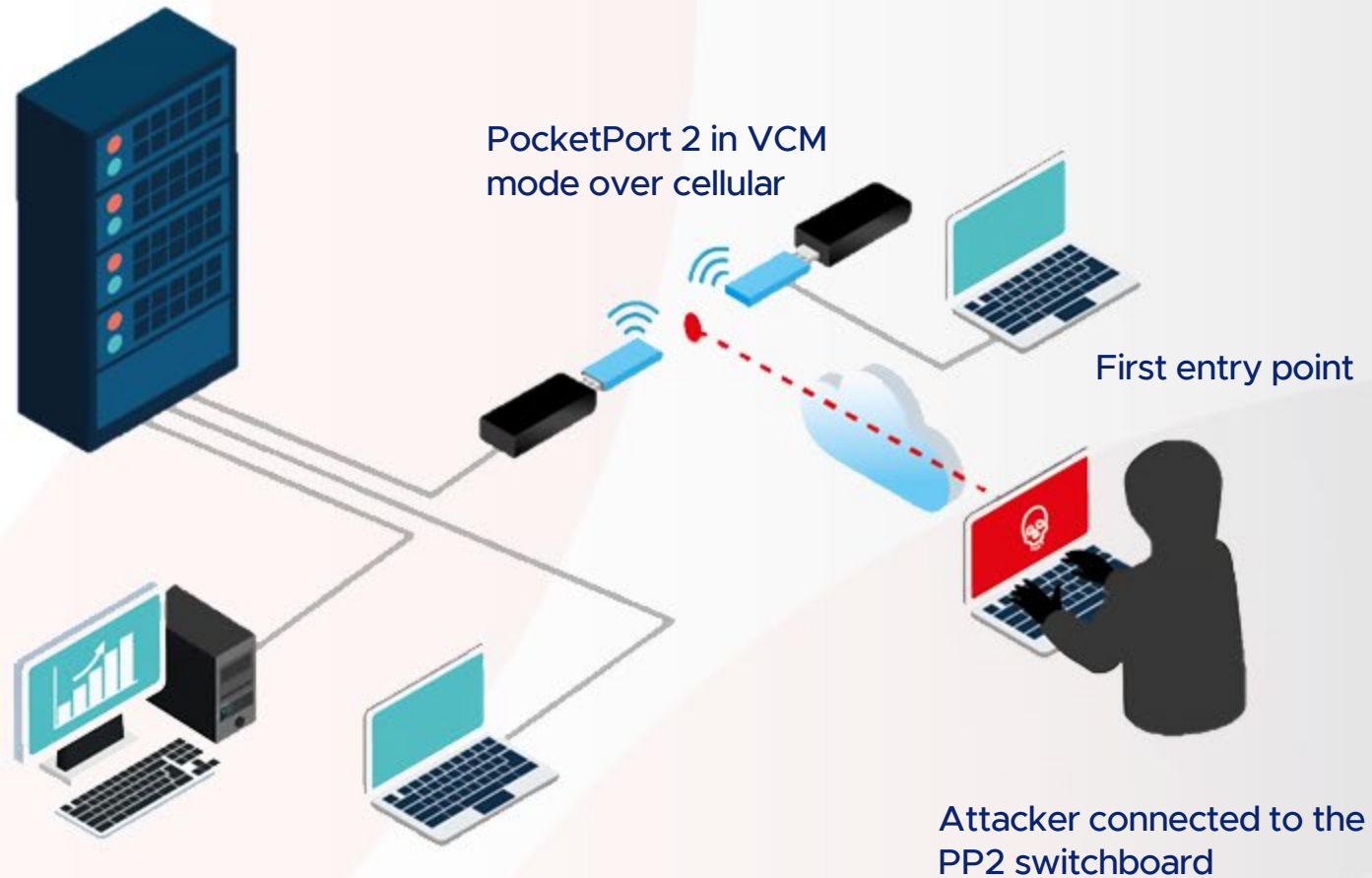


High privilege user
endpoint



Beaglebone low-cost board
running USB Proxy MiTM.

Network use case: MiTM transparent attack



Peripheral asset attacks

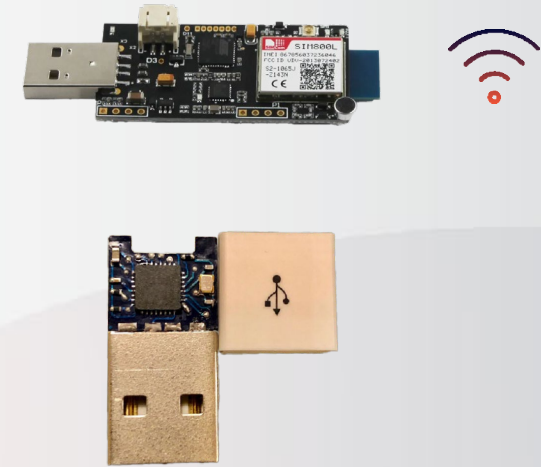
Way In



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

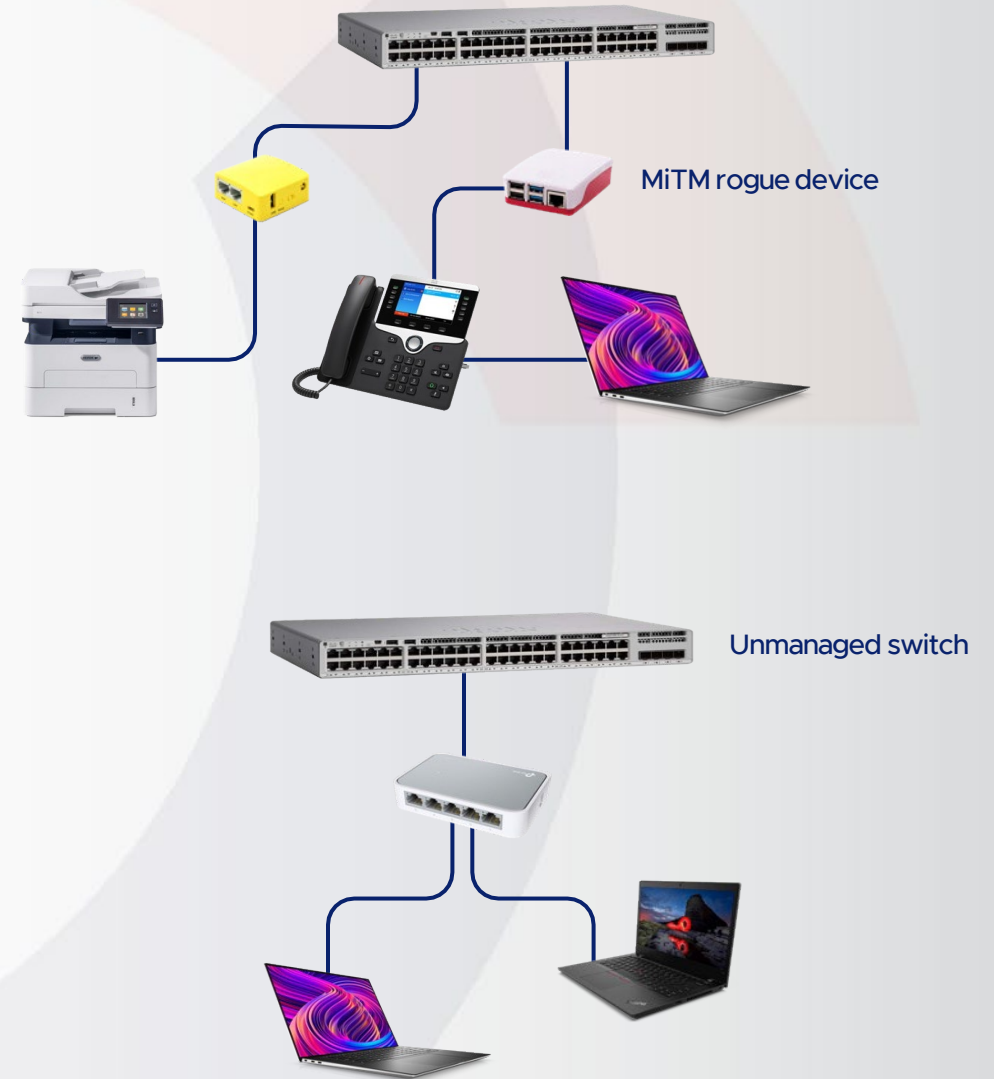
Way Out



- 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

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



Questions our customers ask themselves

- ① **Do I see all my assets?**
- ① **Are there any vulnerable assets?**
- ① **Are the assets, what they say they are?**
- ① **Is there something connected in the middle?**
- ① **Do I have regulatory compliance gaps?**

Existing technologies blind spots

Friend or Foe?



Same MAC



MAC:00D085045802



MAC:00D085045802

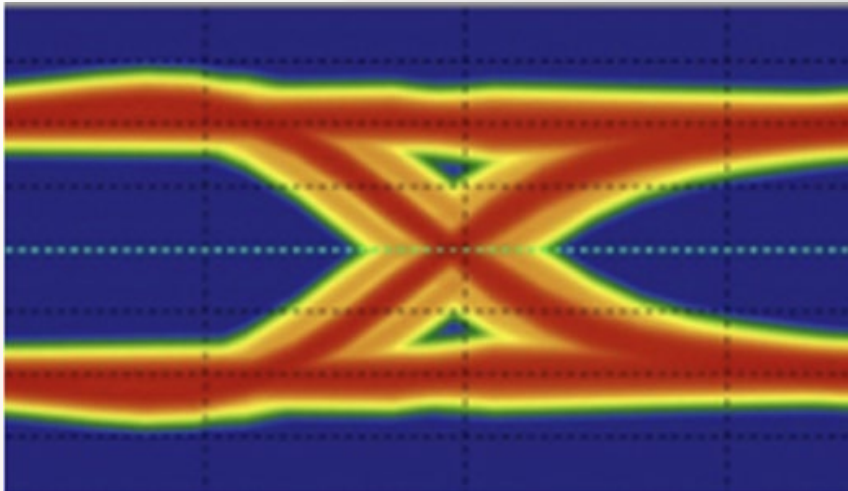
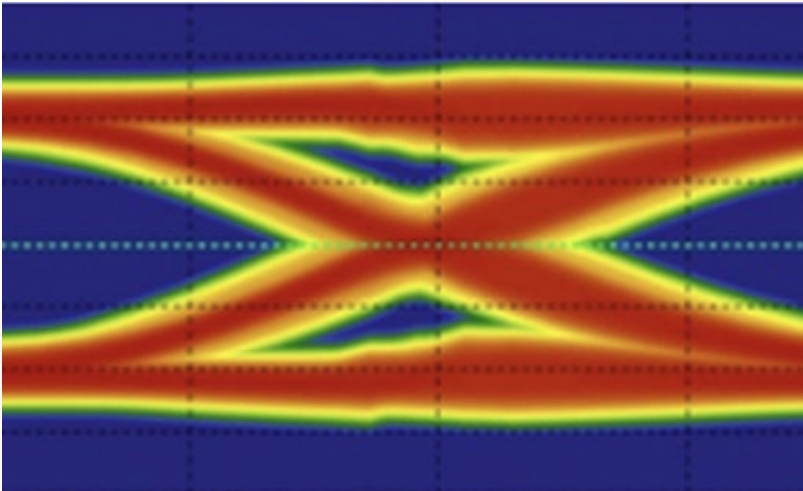
Same Ports

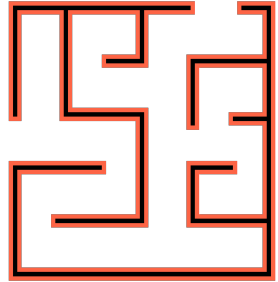


```
Target: 192.168.10.46 Profile: Intense scan [Scan] [Cancel]
Command: nmap -T4 -A -v 192.168.10.46
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v 192.168.10.46 [Details]
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-18 10:15 Jerusalem Daylight Time
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
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
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
```

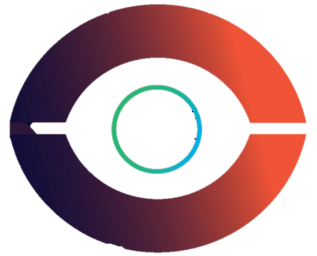

Different Asset DNA!





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.



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

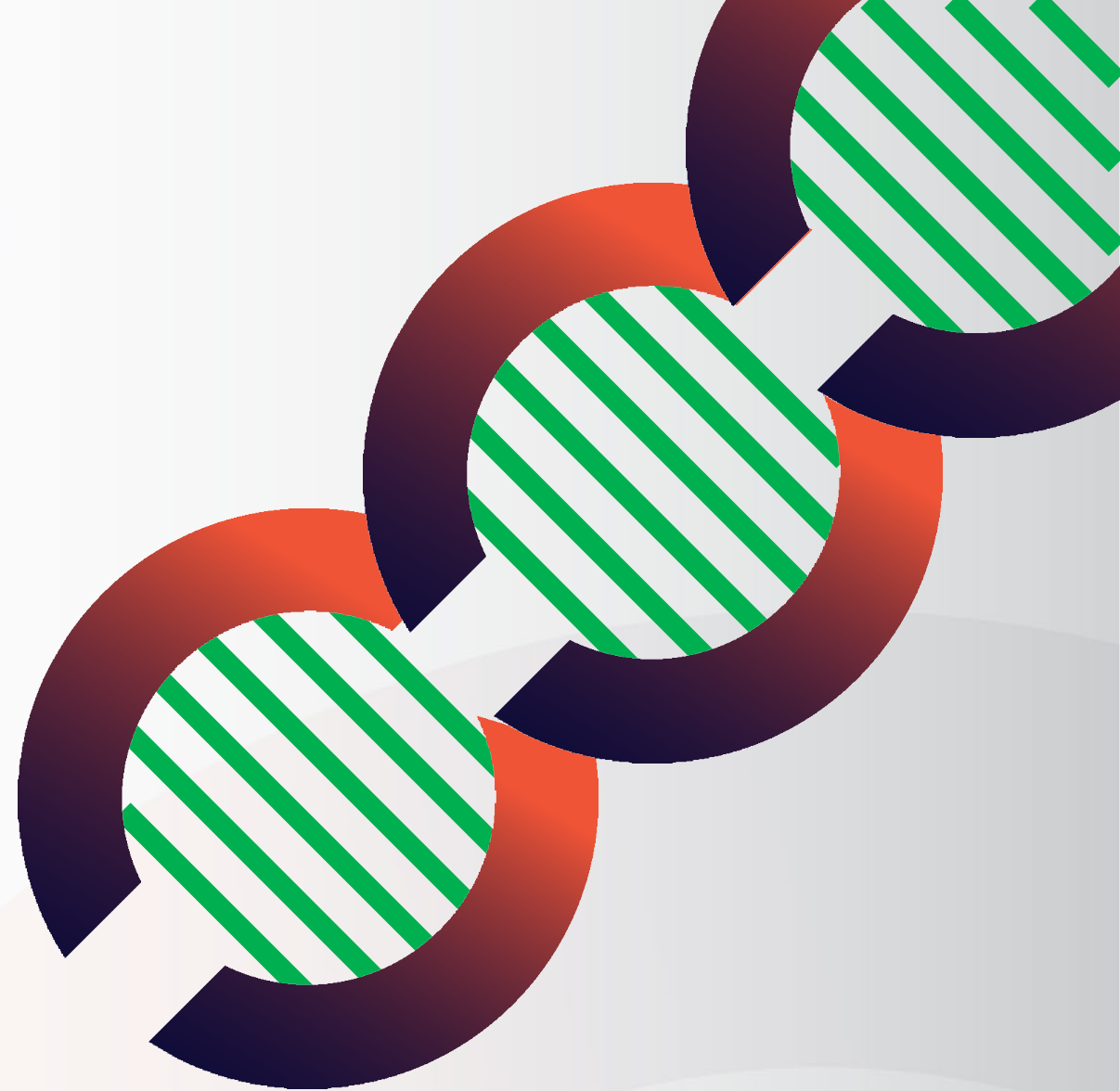
Sepio's approach: Identify and validate

- Visibility and identity gaps
- Business value



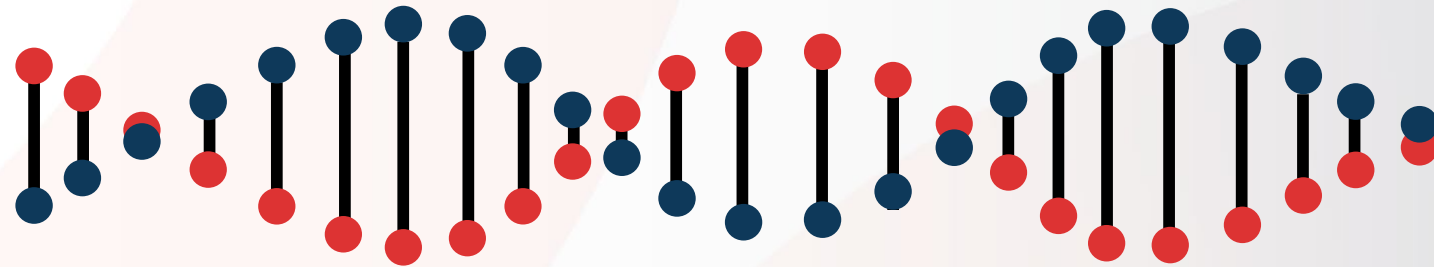
Harnessing new data source.
Getting to the **true** source of
asset risk without traffic
monitoring

- Create an Asset DNA
- Risk assessment
- Asset mapping



How do we do it?

Asset DNA

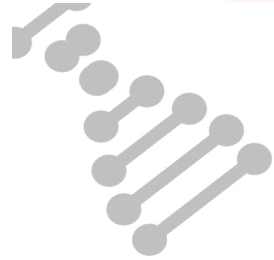


Asset DNA provides a single source of truth, focusing on **EXISTENCE** – rather than **ACTIVITY**.

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

Introducing Asset DNA

Host 

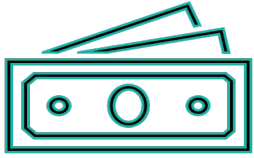


 Network

ARF – Risk Assessing



Sepio's proven value for FIS



Finance Business Benefits



Sepio sheds light on items I couldn't identify and now I can make better decisions; I can contextualize what a device is where I wouldn't have had visibility otherwise.



Director of Network Architecture and Engineering,
Tier 1 Financial Institution

- Complete asset visibility
- Mitigate rogue devices and supply chain risks.
- Close NAC gaps and fortify micro segmentation
- Support regulatory compliance
- Budget and resource planning
- Apply assets usage policy entitlement, at scale.

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

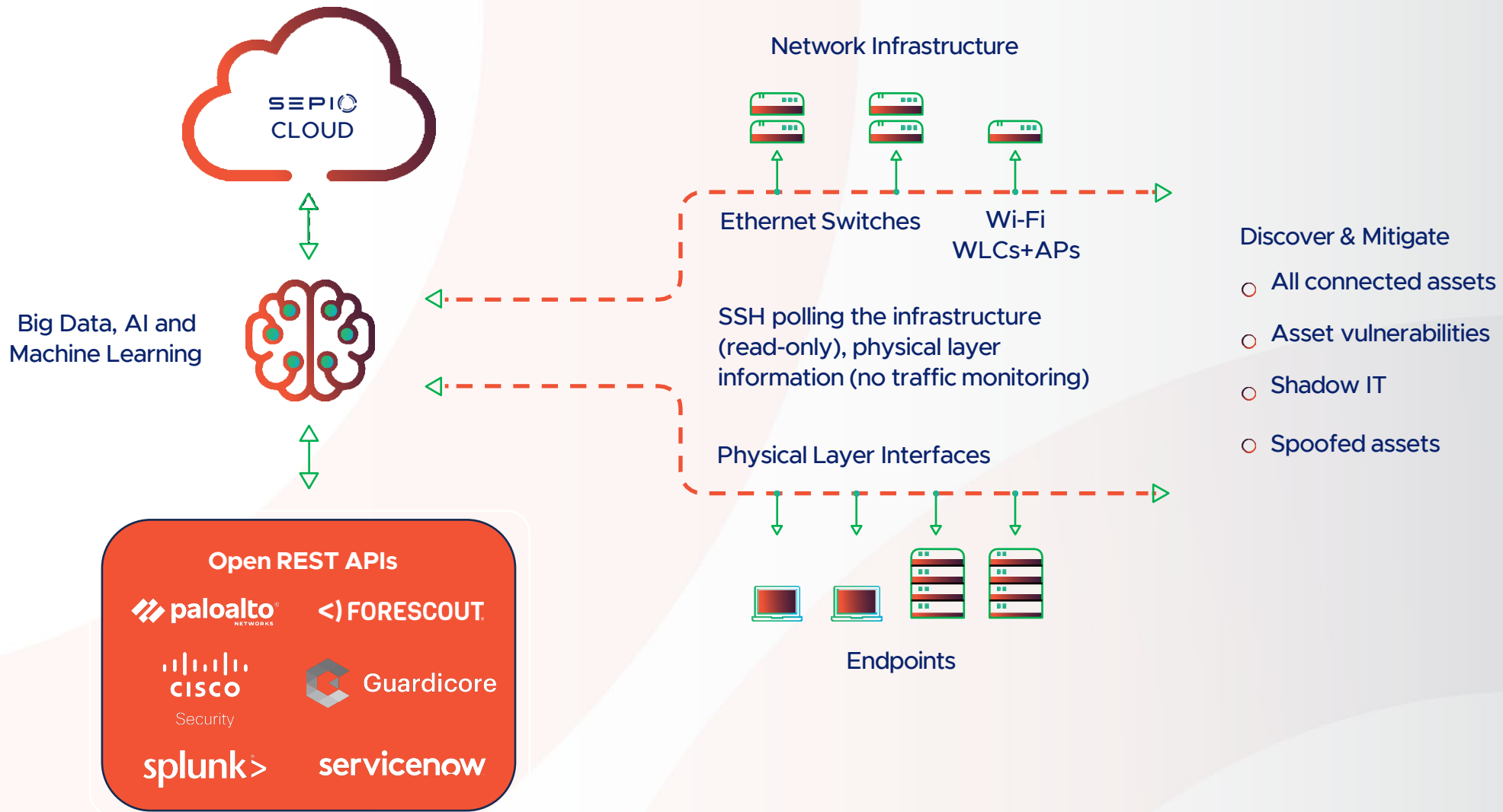
ITAM & CMDB

- 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

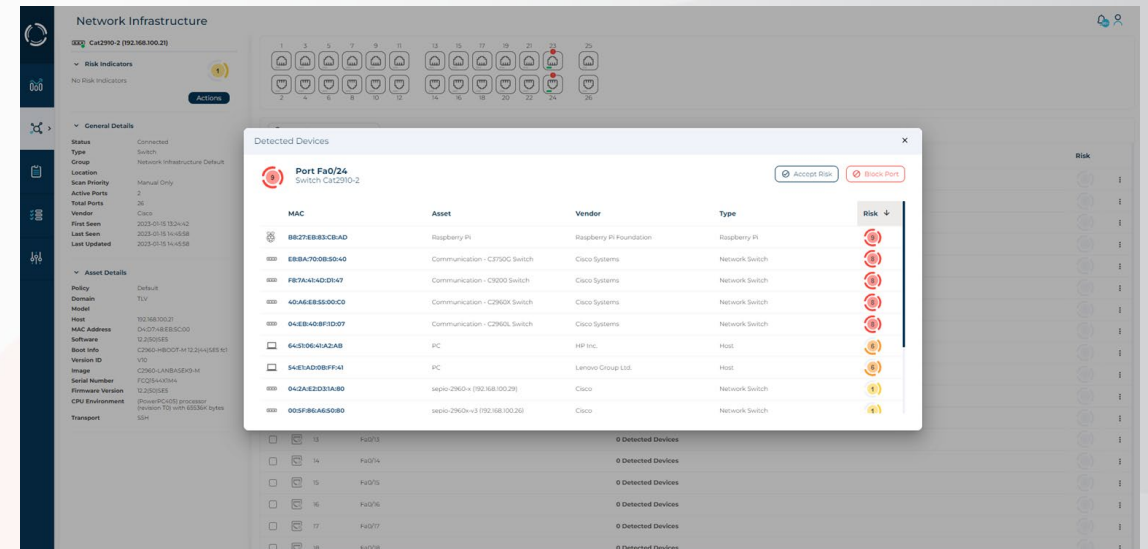
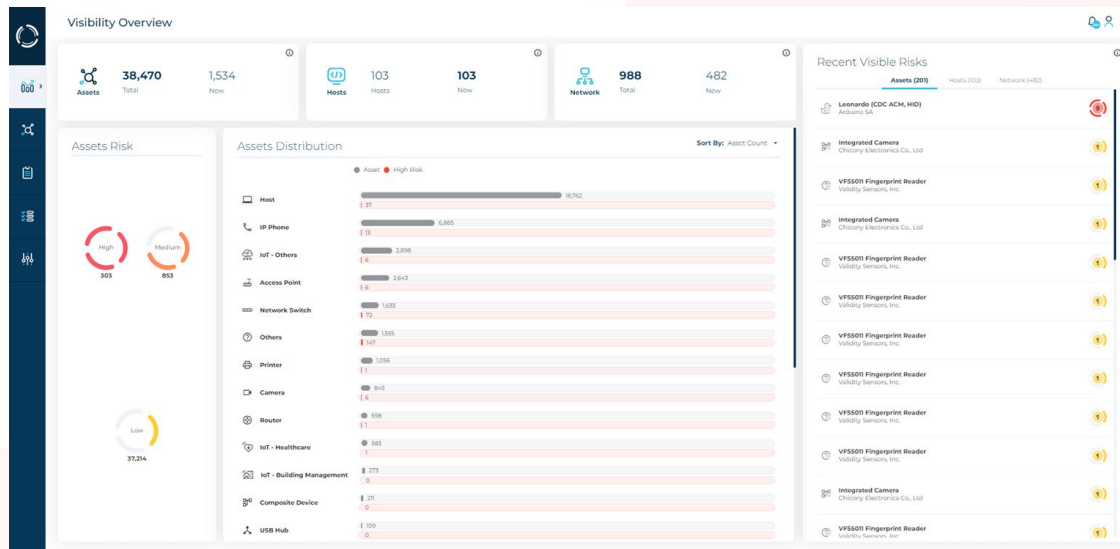
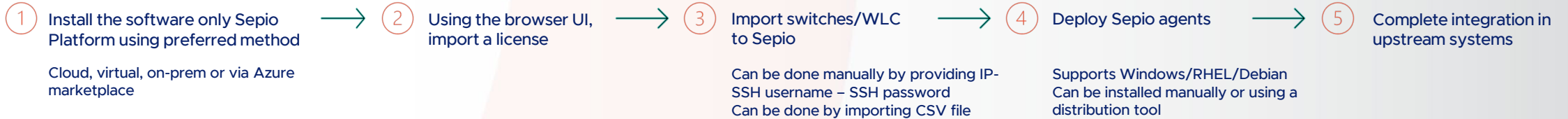


Dissolvable agent

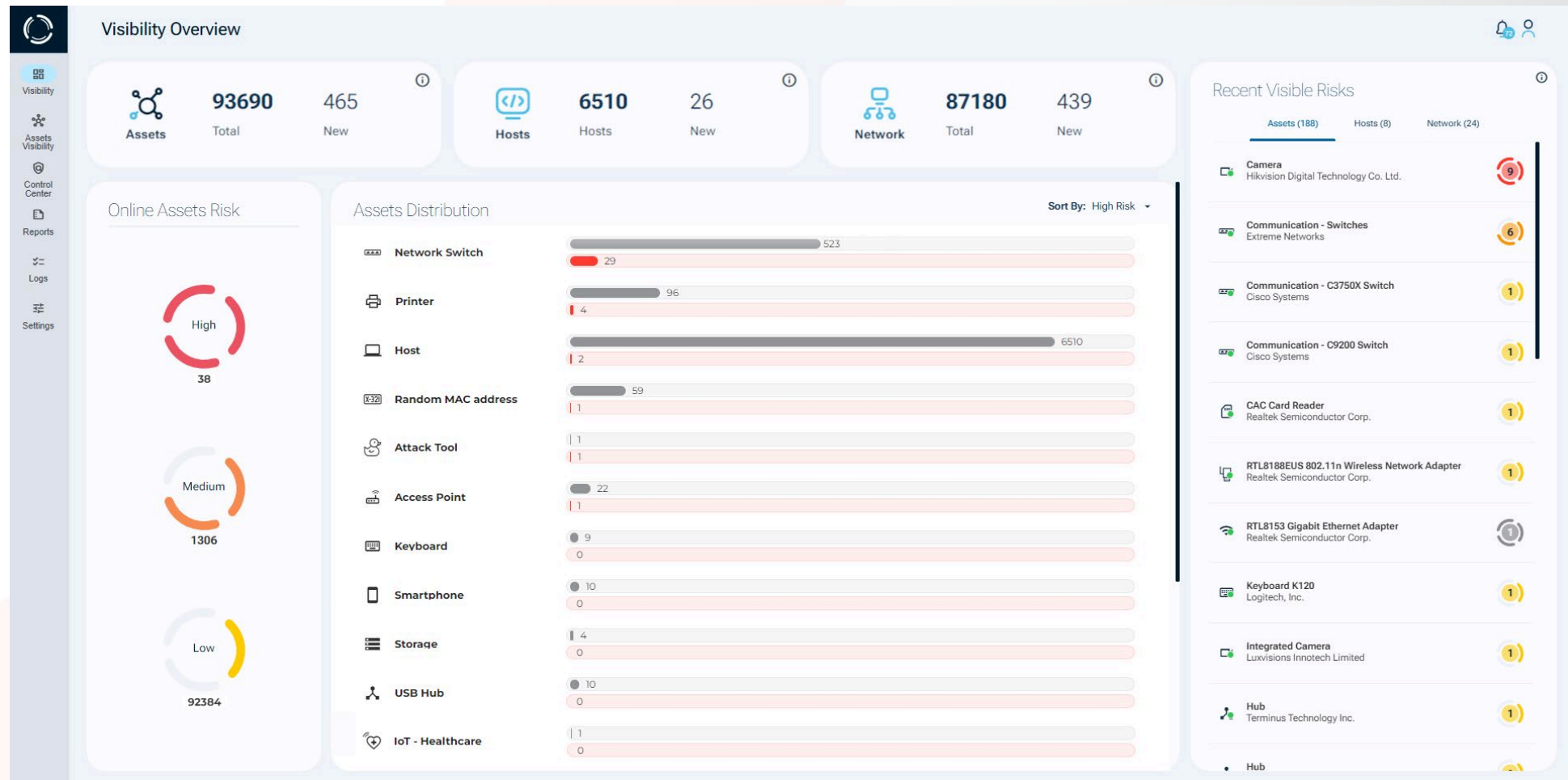
Typical Customer Journey



Deployment process



Sepio's Asset Risk Management solution



SEPIO
See what you've been missing

