SEPIO SYSTEMS

vetted dcode for federal

Gartner COOL VENDOR 2020

Hardware Access Control

Visibility, Control & Mitigation

Reducing The Risk of Unapproved and Rogue Devices

Jay Smilyk - CRO

Date: January 13, 2021

Agenda

> Introduction	10 Min.
> CMMC	5 Min.
> Sepio Tech	20 Min.
> Demo	15 Min.
> Q&A	15 Min.

About Us...

Founded in 2016

Founders are industry veterans with proven track record, working together for 29 years

Headquarters in Maryland

A solution for ultimate visibility and protection against rogue device attacks

US Proxy Board lead by market leaders and former government officials

Board and Advisory

Monique Shivanandan
CISO, HSBC
Chairwoman of the US Board

Kathleen Casey
Former Commissioner, SEC
US Board Member

Bonnie Stith
Former Director, CIA Cyber Intel
US Board Member

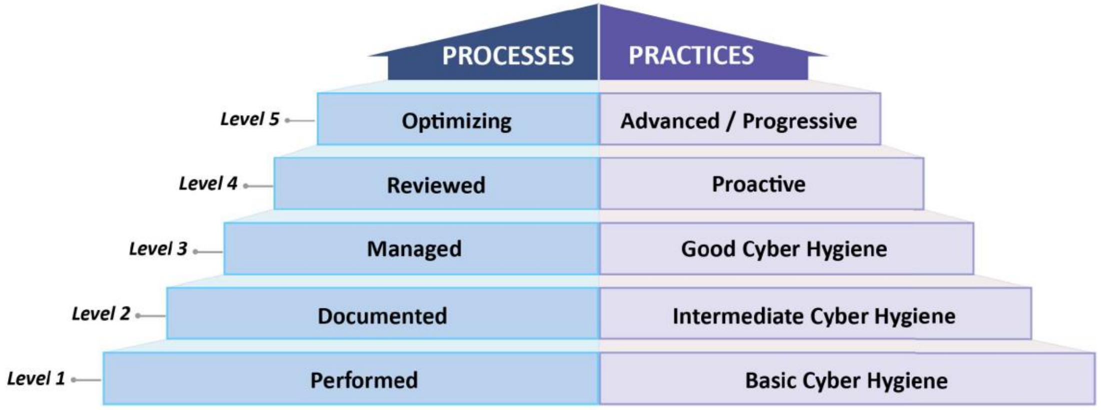
Lane Bess
Former CEO, Palo Alto
Senior Advisor

Robert Bigman
Former CISO, CIA
Senior Advisor

Suzan Zimmerman
Former SVP, SAIC and CACI
Senior Advisor

Dr. Edward Amoroso
Former CSO, AT&T
Senior Advisor

CMMC



PROCESSES | PRACTICES

Level 5 — Optimizing — Advanced / Progressive

Level 4 — Reviewed — Proactive

Level 3 — Managed — Good Cyber Hygiene

Level 2 — Documented — Intermediate Cyber Hygiene

Level 1 — Performed — Basic Cyber Hygiene

CMMC Level	Number of practices per domain that Sepio covers for CMMC levels	List of Practices that Sepio covers
1	9/17	AC.1.001, AC.1.003, IA.1.076, IA.1.077, PE.1.133, SC.1.175, SC.1.176, SI.1.210, SI.1.212
2	15/55	AC.2.006, AC.2.011, AU.2.041, AU.2.042, AU.2.044, CM.2.061, IR.2.092, MA.2.11, MP.2.121, PE.2.135, PS.2.128, RM.2.142, RM2.143, SI2.216, SI2.217
3	17/58	AU.3.045, AU.3.046, AU.3.048, AU.3.049, AU.3.050, AU.3.051, AU.3.052, CM.3.067, CM.3.068, IR.3.098, MP.3.123, PE.3.136, RM.3.144, RM.3.147, SA.3.169, SC.3.183, SC.3.186
4	10/26	AC.4.032, AM.4.226, AU4.054, IR4.100, RM4.149, RM.4.150, RM.4.151, SA.4.171, SC.4.197, SI.4.221
5	8/15	AC.5.024, AU.5.055, IR.5.102, IR.5.106, IR.5.108, SC.5.230, SI.5.222, SI.5.223
Total	59/171	

Challenges Enterprises Face Today

Gartner

75% of the enterprises do not know enough about their infrastructure and its vulnerabilities

Lack of hardware visibility invites attackers;
It is a risk unless visible

Lack of hardware control attracts attackers;
It is a vulnerability unless enforced

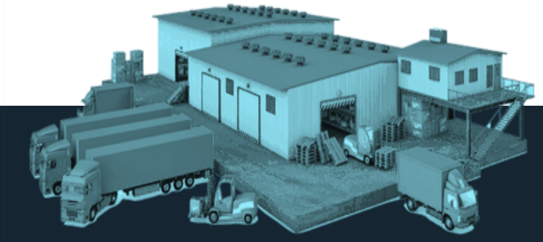
Sepio's Hardware Access Control (HAC)

Deployed in financial institutions, telecom, insurance, government, energy and health care...

1 Visibility of all Hardware Assets including peripherals, IT, OT and IOT (section 889)

2 Control of Hardware Access to the enterprise through policy enforcement

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



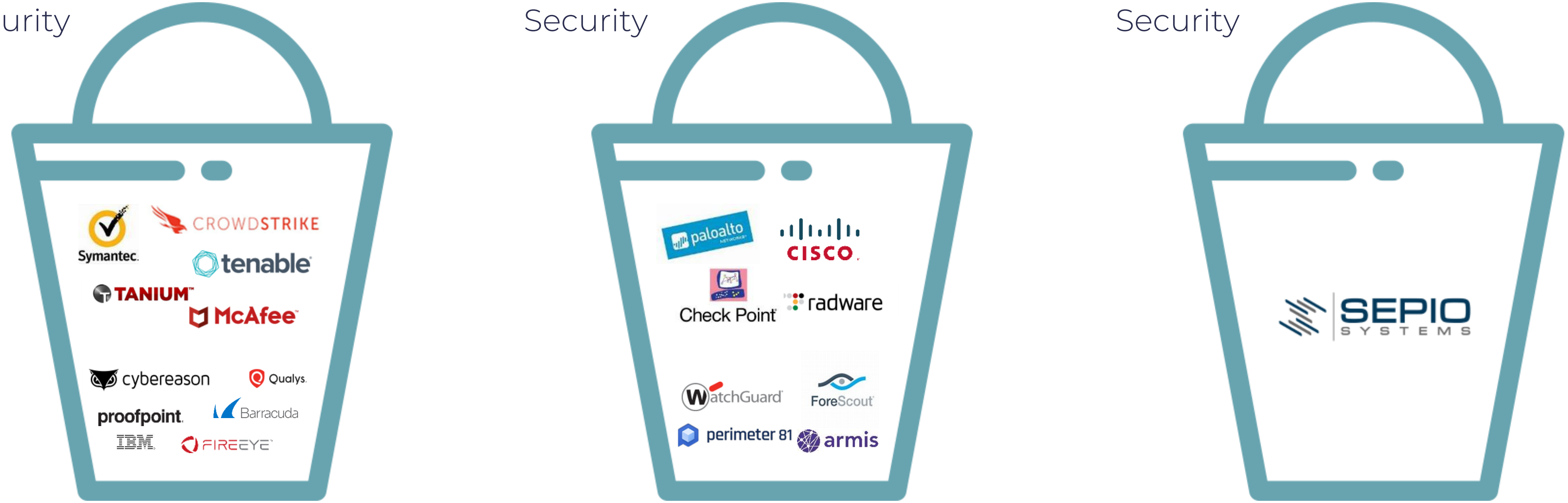
4 Detection of Hardware Manipulations within the supply chain

The 3 Buckets...

Software Security

Network Security

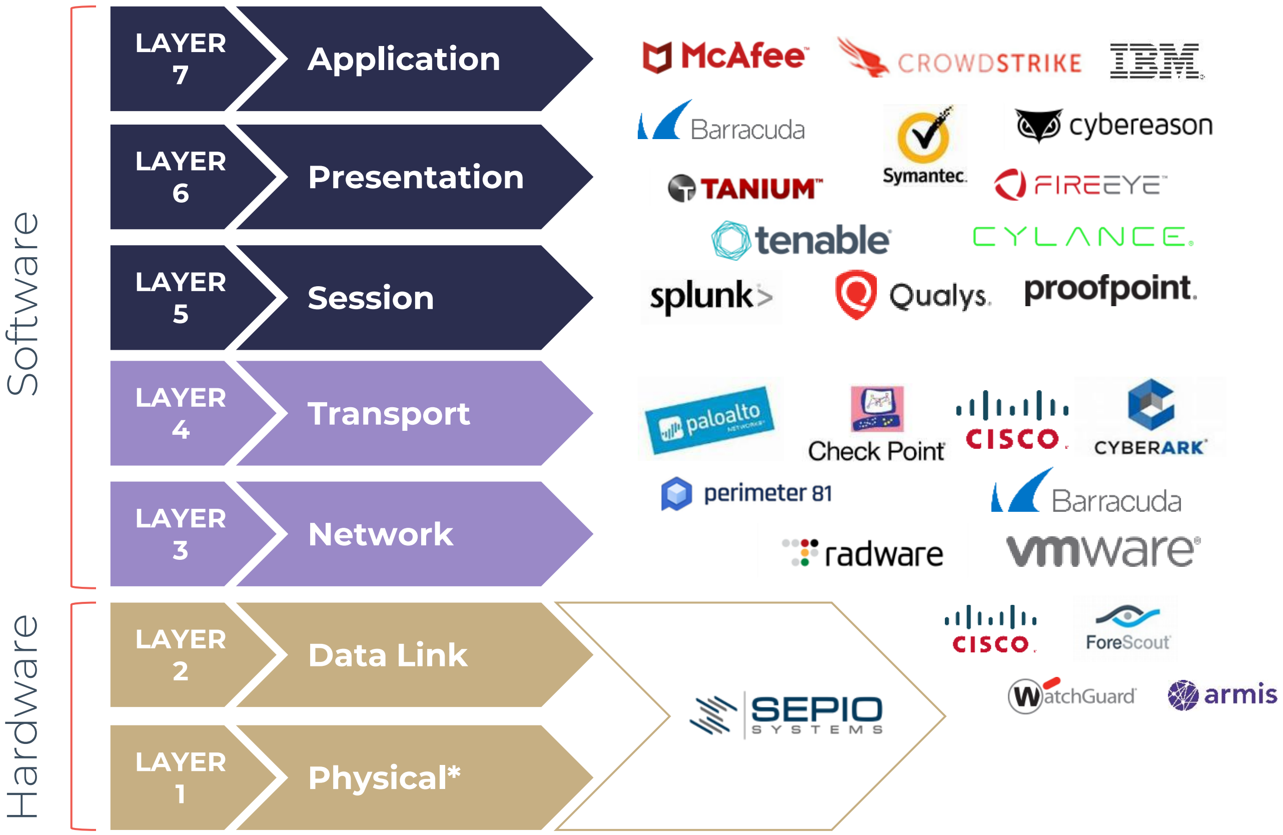
Hardware Security



While securing against threats from software and networks, you are still vulnerable to your Hardware assets.

It's ALL About The OSI Layers

- Discovery of ALL hardware assets requires a new approach
- Sepio's fingerprinting technology augmenting ALL hardware layers
- Detects ALL hidden devices which are invisible to ALL other tools

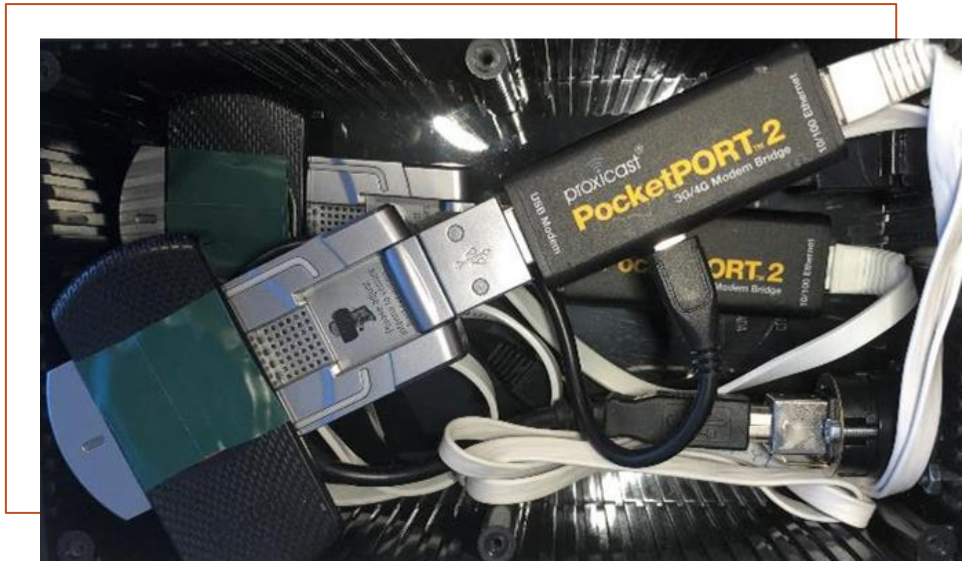


Use Case **Visibility**

Passive TAP devices connected to secured network running privileged customer data; MAC-less devices invisible to all other tools.

Commonly used, **unmanaged switch** brought in for adding more ports; became uncontrolled invisible threat.

Use Case **Insider Threat**

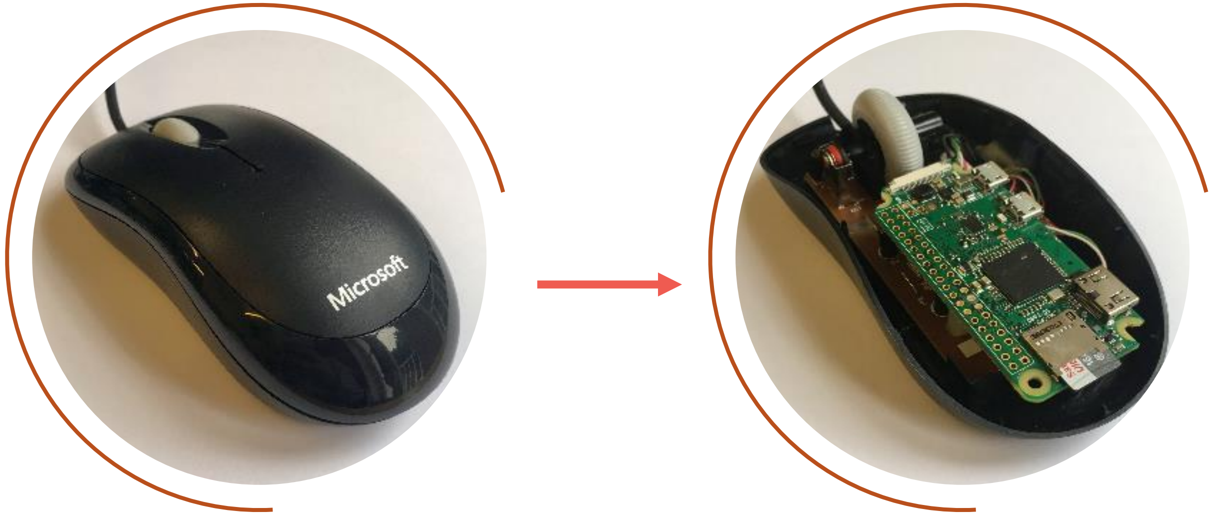


Tier 1 Bank Leaking Data; Attackers used Transparent Network Devices. Running out-of-band, undetected for months.

Use Case **Insider Threat**

In 2019 a US Federal Agency facility had been **hacked by a Raspberry Pi device** that was linked to the agency’s network without authorization claiming to be something else

Use Case **Supply Chain / WFH**

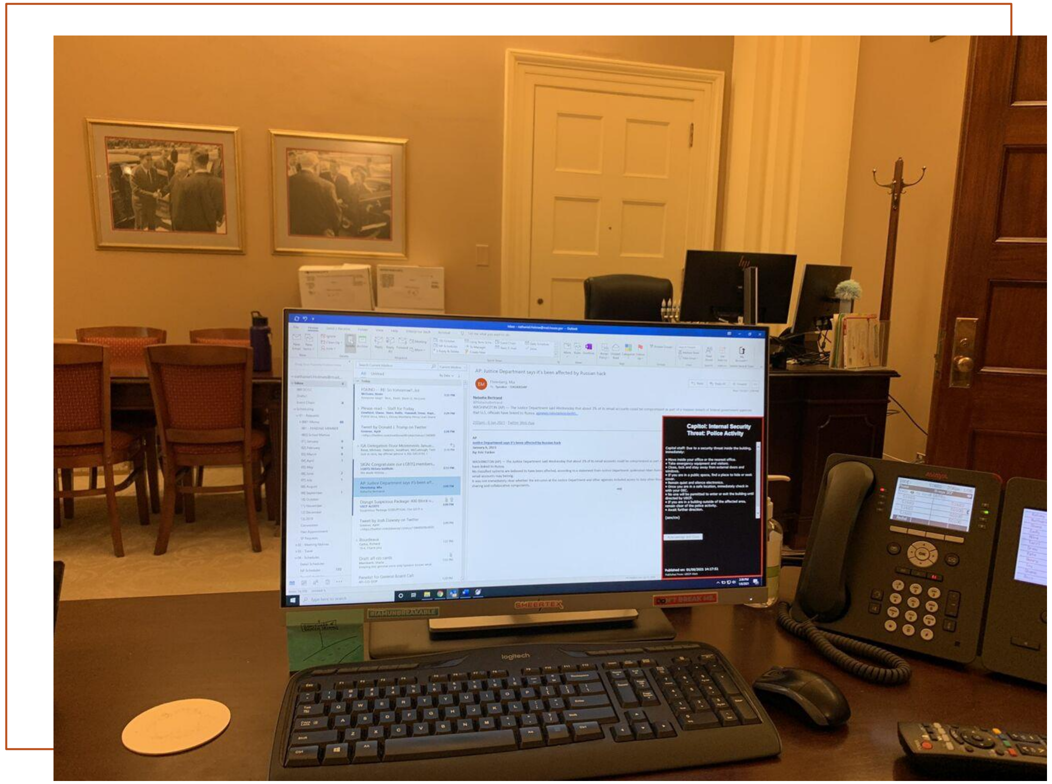


Hacking into air-gapped network **using a malicious peripheral device**; EDR/DLP reported a legitimate device.

Use Case **Section 889**

Section 889 of the 2019 **National Defense Authorization Act** prohibits the federal government, government contractors, and grant and loan recipients from procuring or using certain “covered telecommunication equipment or services” that are produced by Huawei, ZTE, Hytera, Hikvision, and Dahua and their subsidiaries as a “substantial or essential component of any system, or as critical technology as part of any system.”

Use Case **Hardware vulnerability**



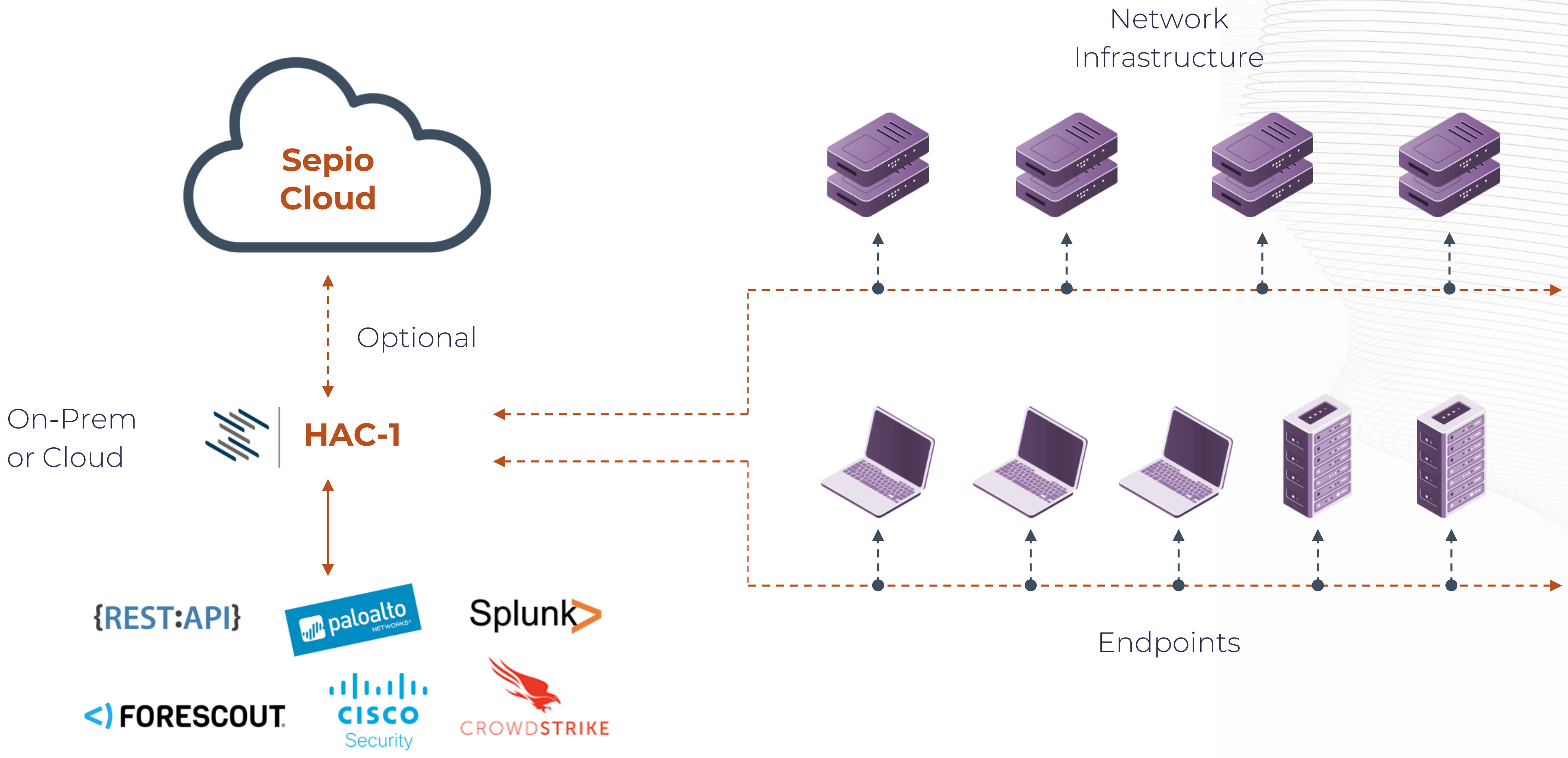
Logitech wireless keyboard and mouse with 10 different risks:

- Force pairing
- Keystroke injection
- Fake mouse
- HID packet injection
- Unencrypted keystroke injection
- Unencrypted keystroke injection fix bypass
- Encrypted keystroke injection
- Malicious macro programming

Use Case **Pen-Testing Tools**

Off-the-shelf pen-testing tools used for demonstrating vulnerabilities; running below radar of all EDR/EDP, NACs...

System Architecture



Network Infrastructure

Sepio Cloud

Optional

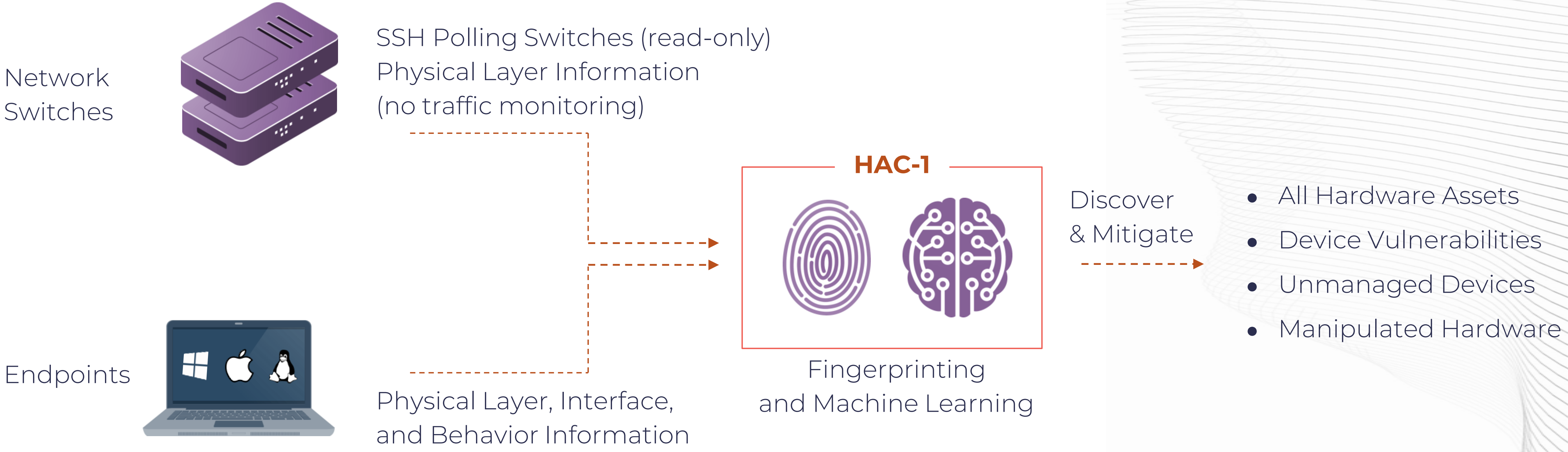
On-Prem or Cloud

HAC-1

Endpoints

How It Works

SEPIO SYSTEMS



Network Switches

SSH Polling Switches (read-only)
Physical Layer Information
(no traffic monitoring)

Endpoints

Physical Layer, Interface,
and Behavior Information

HAC-1

Fingerprinting
and Machine Learning

Discover
& Mitigate

- All Hardware Assets
- Device Vulnerabilities
- Unmanaged Devices
- Manipulated Hardware

Security & Compliance

Approved by the CDM Program

Made in the USA

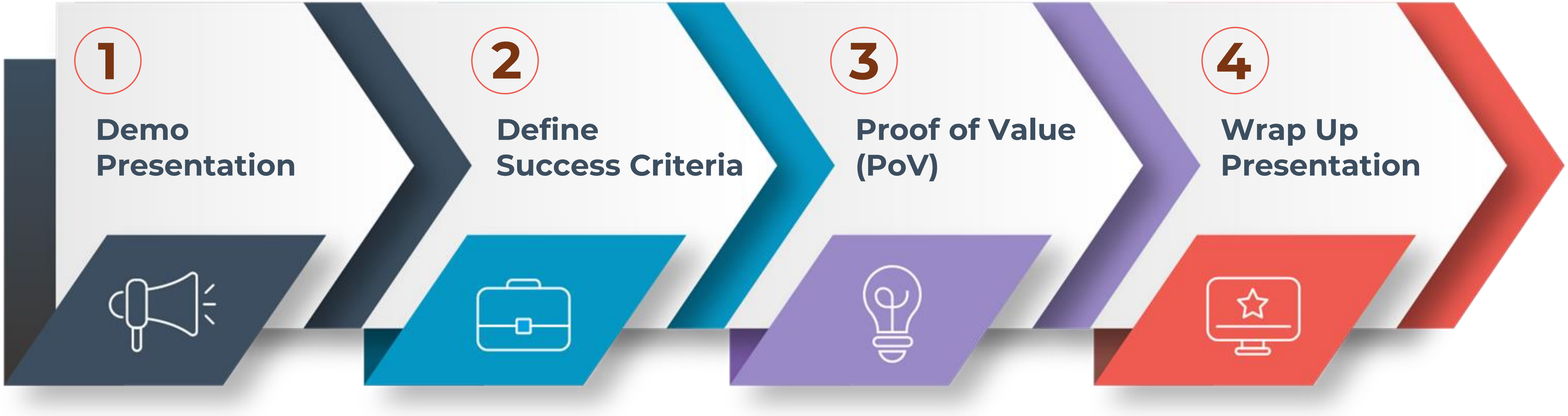
FIPS 140-2 Compliant

Full Transparency Program

NIST 800-53

Next Steps...

Sepio brings visibility, control and mitigation to zero trust, insider threat, WFH, BYOD, IT, OT and IoT security programs...



1 **Demo Presentation**

2 **Define Success Criteria**

3 **Proof of Value (PoV)**

4 **Wrap Up Presentation**

GSA Schedule 70

SEWP V

NAICS CODES : 511210 541519 541690 541512 541618 541511 518210 541330 541611

THANK YOU!

www.sepio.systems