Zero Trust Hardware Access

Use Case Portfolio

A practical guide for applying hardware-level trust across enterprise, branch, OT, healthcare, datacenter, and supply-chain environments.

Discover • Verify • Validate • Enforce

The hardware blind spot

Most security controls trust what a device says it is. Attackers exploit that assumption.

Declared identity

MAC, IP, hostname, agent status, certificate, serial number

Observed behavior

Traffic patterns, endpoint telemetry, logs, anomalies

Physical truth

Electrical / physical-layer evidence and device-level fingerprint

Sepio starts where software trust stops.

What Zero Trust Hardware Access means

A model for validating physical device identity before trust is granted.

Discover

Find every connected asset, including unknown, dormant, unmanaged, or misclassified devices.

Verify

Establish true identity using AssetDNA and physical-layer evidence, not declared identity.

Validate

Compare actual identity against expected role, location, ownership, and policy.

Enforce

Enable trust decisions, alerting, remediation guidance, and orchestration through existing tools.

Use case coverage map

The same hardware-trust foundation applies across multiple risk categories.

Supply chain

Counterfeit / tampered devices
OEM masquerade
Pre-installed hardware implants

Workforce & insider

Internal abusers
Unauthorized peripherals
Policy bypass

Network & branch

Rogue devices
Shadow IT
Unmanaged switches / bridges

Endpoint & USB

BadUSB / HID emulation
IP-KVM / remote access
Agentless devices

Critical environments

OT/ICS
Healthcare IoMT
ATM / POS / kiosks

Operations & governance

M&A inventory
Compliance evidence
Asset lifecycle validation

1. Hardware supply-chain attacks

Tampered device introduced before deployment • Golden image looks clean while hardware is compromised • Device passes procurement paperwork but fails physical trust

Threat pattern

- Tampered device introduced before deployment
- Golden image looks clean while hardware is compromised
- Device passes procurement paperwork but fails physical trust

Why conventional tools miss it

- EDR sees OS state, not hardware origin
- NAC often trusts MAC/OUI or certificates
- CMDB records can inherit supplier claims

How Sepio applies ZTHA

- Fingerprint device using AssetDNA
- Compare physical identity to approved baseline
- Flag mismatch before trust is granted

Business outcome

- Reduce counterfeit and implant risk
- Protect regulated procurement chains
- Create evidence for supplier assurance

2. Counterfeit or OEM-masquerading devices

Device claims a trusted brand or model • MAC address and certificates look legitimate • Hidden OEM lineage creates Section 889-style risk

Threat pattern

- Device claims a trusted brand or model
- MAC address and certificates look legitimate
- Hidden OEM lineage creates Section 889-style risk

Why conventional tools miss it

- Declared attributes can be cloned or spoofed
- Inventory tools normalize by vendor claims
- Traffic may appear normal

How Sepio applies ZTHA

- Validate physical identity independent of labels
- Expose device identity conflicts
- Correlate identity with policy and asset owner

Business outcome

- Find banned or risky equipment
- Reduce compliance exposure
- Avoid trust based on paperwork alone

3. Rogue network devices

Unauthorized device connected to live port • Small implant, access point, bridge, or mini switch added • Rogue device lives below the radar

Threat pattern

- Unauthorized device connected to live port
- Small implant, access point, bridge, or mini switch added
- Rogue device lives below the radar

Why conventional tools miss it

- No agent to detect
- May not generate suspicious traffic initially
- MAC/IP can be changed instantly

How Sepio applies ZTHA

- Discover at infrastructure edge
- Locate exact switch/AP/port context
- Alert on unknown or policy-violating hardware

Business outcome

- Accelerate containment
- Give IT the exact physical location
- Reduce dwell time for hardware attacks

4. Shadow IT and unmanaged assets

Teams add devices outside IT process • Lab equipment, printers, cameras, IoT, or test gear remains unmanaged • Inventory becomes incomplete and stale

Threat pattern

- Teams add devices outside IT process
- Lab equipment, printers, cameras, IoT, or test gear remains unmanaged
- Inventory becomes incomplete and stale

Why conventional tools miss it

- CMDB depends on manual onboarding
- EDR only covers supported endpoints
- Scanners miss dormant or segmented devices

How Sepio applies ZTHA

- Continuously discover connected hardware
- Classify and tag assets at scale
- Validate location, ownership, and expected behavior

Business outcome

- Build authoritative inventory
- Reduce audit gaps
- Bring unmanaged assets into governance

5. Internal abusers and policy bypass

Authorized user connects unauthorized hardware • Employee uses USB storage, rogue AP, or tethering device • Insider creates hidden path for exfiltration

Threat pattern

- Authorized user connects unauthorized hardware
- Employee uses USB storage, rogue AP, or tethering device
- Insider creates hidden path for exfiltration

Why conventional tools miss it

- User identity is trusted after login
- Peripheral events may lack context
- Intent may look like normal work

How Sepio applies ZTHA

- Validate hardware attached to trusted hosts or ports
- Detect deviations from allowed device classes
- Map user/workstation/location for response

Business outcome

- Reduce insider risk
- Enforce least privilege at device layer
- Support investigations with physical evidence

6. EDR/XDR coverage gaps

Devices exist without agents • Unsupported OS, guest device, IoT, printer, OT endpoint, or appliance • Attacker targets unmanaged assets

Threat pattern

- Devices exist without agents
- Unsupported OS, guest device, IoT, printer, OT endpoint, or appliance
- Attacker targets unmanaged assets

Why conventional tools miss it

- EDR protects only where the agent exists
- XDR correlates signals after telemetry exists
- Agent deployment status does not equal asset truth

How Sepio applies ZTHA

- Show every device without relying on agents
- Identify assets missing EDR coverage
- Feed findings into EDR/XDR and IT workflows

Business outcome

- Expand protection coverage
- Drive remediation and license expansion
- Prevent blind spots from becoming attack paths

7. NAC bypass and identity spoofing

Device spoofs MAC/OUI or borrows credentials • Endpoint profile matches allowed device type • Attacker abuses allowlists

Threat pattern

- Device spoofs MAC/OUI or borrows credentials
- Endpoint profile matches allowed device type
- Attacker abuses allowlists

Why conventional tools miss it

- NAC often relies on network identity and posture checks
- MAC and hostname are easy to spoof
- Credentials do not prove hardware authenticity

How Sepio applies ZTHA

- Add physical-layer identity verification to access decisions
- Detect device identity mismatch
- Trigger NAC/SOAR actions when trust fails

Business outcome

- Strengthen Zero Trust access
- Reduce spoofing risk
- Make NAC decisions hardware-aware

8. BadUSB / Rubber Ducky / HID emulation

Malicious USB acts like a keyboard or trusted peripheral • Payload executes through keystrokes • Device identity is intentionally deceptive

Threat pattern

- Malicious USB acts like a keyboard or trusted peripheral
- Payload executes through keystrokes
- Device identity is intentionally deceptive

Why conventional tools miss it

- HID devices are often permitted
- Software may see a normal keyboard
- Behavior may happen too fast for manual response

How Sepio applies ZTHA

- Classify USB peripherals by hardware identity
- Detect unexpected peripheral classes
- Support policies per user, host, location, and device type

Business outcome

- Reduce USB attack surface
- Prevent trusted-interface abuse
- Improve endpoint peripheral governance

9. IP-KVM and remote-control hardware

External remote-access hardware is attached to a server or workstation • Device emulates keyboard/mouse/video path • Bypasses software remote-access controls

Threat pattern

- External remote-access hardware is attached to a server or workstation
- Device emulates keyboard/mouse/video path
- Bypasses software remote-access controls

Why conventional tools miss it

- EDR may see legitimate keyboard/mouse input
- Network tools may see a generic device
- Physical presence is the attack channel

How Sepio applies ZTHA

- Discover and classify connected remote-access hardware
- Validate whether such devices are authorized
- Locate where they are connected for removal

Business outcome

- Prevent hidden remote-access paths
- Protect admin workstations and servers
- Strengthen privileged access assurance

10. Unmanaged switches, bridges, and rogue APs

Mini switch or wireless bridge creates an unauthorized segment • Multiple devices hide behind one approved connection • Network topology becomes inaccurate

Threat pattern

- Mini switch or wireless bridge creates an unauthorized segment
- Multiple devices hide behind one approved connection
- Network topology becomes inaccurate

Why conventional tools miss it

- Traffic tools see aggregated or indirect activity
- CMDB has no record of physical topology change
- Basic NAC sees a known upstream device

How Sepio applies ZTHA

- Detect physical topology and infrastructure changes
- Surface unexpected downstream devices
- Map edge-port location and device relationships

Business outcome

- Eliminate hidden network paths
- Restore accurate topology
- Reduce lateral movement opportunities

11. ATM, POS, kiosk, and branch protection

Black-box device added to ATM/POS network • Peripheral tampering or rogue connectivity in branch environment • Remote site has limited technical staff

Threat pattern

- Black-box device added to ATM/POS network
- Peripheral tampering or rogue connectivity in branch environment
- Remote site has limited technical staff

Why conventional tools miss it

- Branch devices are distributed and heterogeneous
- Traffic inspection is hard and costly at scale
- Local response may be slow

How Sepio applies ZTHA

- Provide trafficless hardware discovery
- Locate device to exact branch/port context
- Enable centralized policy and response workflows

Business outcome

- Reduce fraud and jackpotting exposure
- Improve branch security operations
- Protect revenue-generating endpoints

12. OT/ICS and manufacturing environments

Unapproved engineering workstation, converter, PLC accessory, or IIoT device • Legacy OS and fragile operations cannot tolerate scanning • Unauthorized hardware disrupts safety and uptime

Threat pattern

- Unapproved engineering workstation, converter, PLC accessory, or IIoT device
- Legacy OS and fragile operations cannot tolerate scanning
- Unauthorized hardware disrupts safety and uptime

Why conventional tools miss it

- Active scans can be risky
- Agents are often impossible
- Traffic visibility alone does not validate hardware identity

How Sepio applies ZTHA

- Discover without traffic inspection or active endpoint scanning
- Classify assets across IT/OT boundaries
- Validate device role and location against policy

Business outcome

- Improve OT visibility without operational disruption
- Support segmentation and incident response
- Reduce unauthorized hardware risk

13. Healthcare IoMT and clinical device sprawl

Medical devices, carts, cameras, and peripherals proliferate • Shared clinical spaces introduce unmanaged assets • Patient safety and privacy depend on accurate inventory

Threat pattern

- Medical devices, carts, cameras, and peripherals proliferate
- Shared clinical spaces introduce unmanaged assets
- Patient safety and privacy depend on accurate inventory

Why conventional tools miss it

- Agents rarely supported on IoMT
- Clinical devices move locations
- Traditional scans can create operational concerns

How Sepio applies ZTHA

- Continuously identify and locate hardware assets
- Maintain context even when devices move
- Separate trusted clinical assets from unknown hardware

Business outcome

- Improve IoMT governance
- Support compliance and incident readiness
- Reduce risk without disrupting care

14. Datacenter and cloud-edge infrastructure

Unauthorized console, management, network, or test device appears in a high-value environment • Misplaced hardware creates hidden access path • Scale makes manual audits impractical

Threat pattern

- Unauthorized console, management, network, or test device appears in a high-value environment
- Misplaced hardware creates hidden access path
- Scale makes manual audits impractical

Why conventional tools miss it

- Datacenter inventory often lags physical reality
- Management ports and peripherals are overlooked
- Telemetry depends on installed tools

How Sepio applies ZTHA

- Create hardware-level inventory across racks, switches, and hosts
- Detect anomalous connections at the physical edge
- Integrate with CMDB/SIEM/SOAR for workflows

Business outcome

- Protect crown-jewel infrastructure
- Accelerate audits and change validation
- Reduce unauthorized access paths

15. Site consolidation, and unknown environments

Consolidated networks contain unknown devices and legacy assets • Security teams inherit unmanaged hardware risk • Integration creates fast-moving blind spots

Threat pattern

- Consolidated networks contain unknown devices and legacy assets
- Security teams inherit unmanaged hardware risk
- Integration creates fast-moving blind spots

Why conventional tools miss it

- CMDBs are incomplete or incompatible
- Agents take time to deploy
- Discovery projects are manual and fragmented

How Sepio applies ZTHA

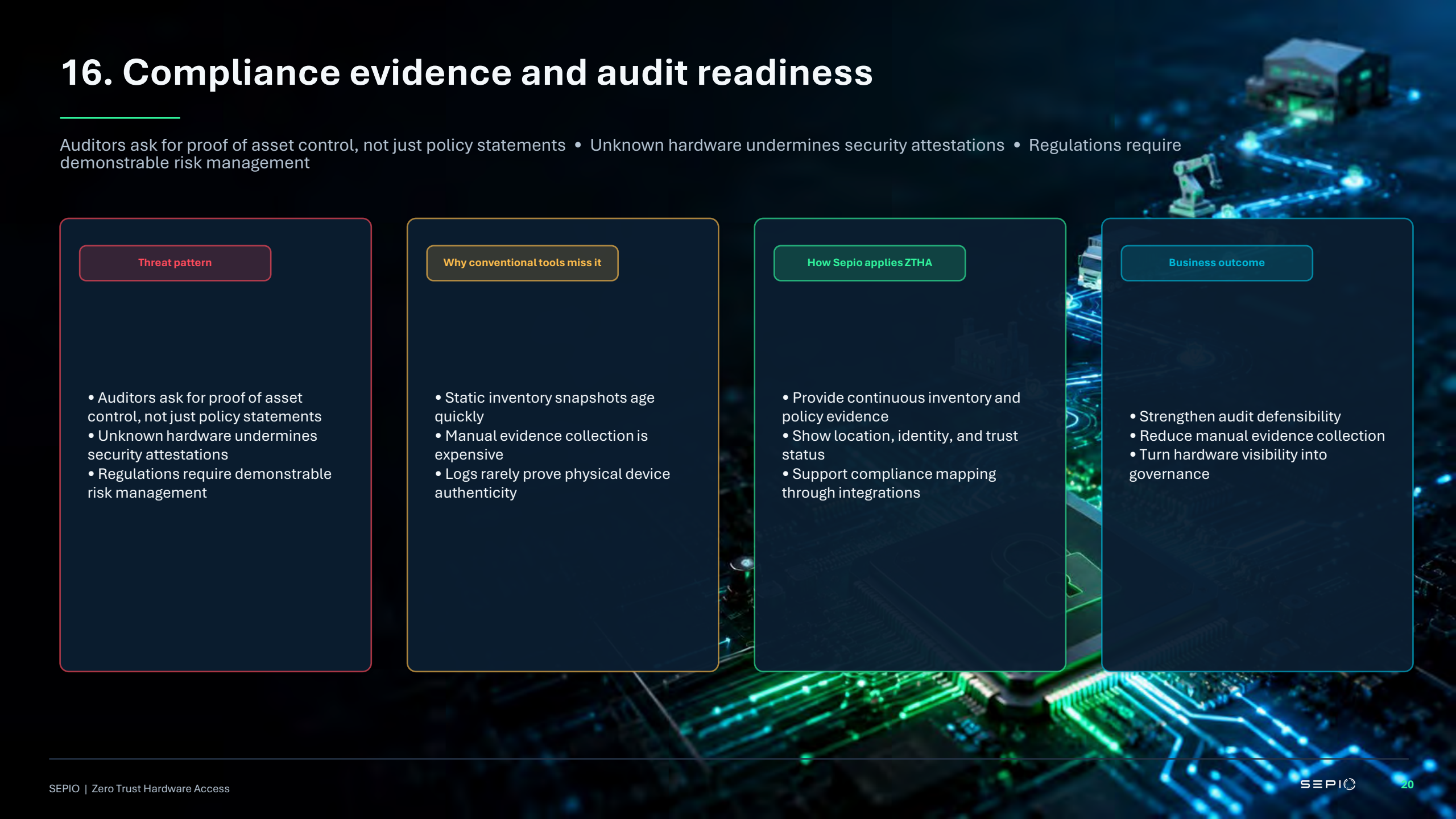
- Rapidly establish baseline hardware inventory
- Identify unmanaged, risky, or policy-violating devices
- Prioritize remediation by location and device class

Business outcome

- Compress due-diligence timelines
- Reduce integration risk
- Create a single hardware truth layer

16. Compliance evidence and audit readiness

Auditors ask for proof of asset control, not just policy statements • Unknown hardware undermines security attestations • Regulations require demonstrable risk management



Threat pattern

- Auditors ask for proof of asset control, not just policy statements
- Unknown hardware undermines security attestations
- Regulations require demonstrable risk management

Why conventional tools miss it

- Static inventory snapshots age quickly
- Manual evidence collection is expensive
- Logs rarely prove physical device authenticity

How Sepio applies ZTHA

- Provide continuous inventory and policy evidence
- Show location, identity, and trust status
- Support compliance mapping through integrations

Business outcome

- Strengthen audit defensibility
- Reduce manual evidence collection
- Turn hardware visibility into governance

From detection to action

ZTHA turns hardware identity into an operational workflow.

1

Detect

Unknown or mismatched device appears

2

Locate

Exact switch/AP/USB/host context

3

Validate

Compare to role, owner, location and policy

4

Respond

Alert, ticket, isolate port, invoke SOAR/NAC

5

Learn

Update baseline and policy for future enforcement

Operational principle: do not grant trust because a device looks familiar — grant trust because its hardware identity is verified and policy-valid.

Use case prioritization matrix

Where Sepio typically creates fastest value.

High urgency / high visibility	Rogue devices, EDR gaps, NAC bypass, USB/HID, IP-KVM
High compliance exposure	Supply chain, counterfeit/OEM masquerade, Section 889-style risks, audit evidence
High operational scale	Shadow IT, Consolidated inventory, datacenter, branch/POS/ATM
High safety / continuity sensitivity	OT/ICS, healthcare IoMT, critical infrastructure

Value by stakeholder

The same platform speaks to different priorities.

CISO / Risk

Close hardware blind spots
Extend Zero Trust to device identity
Demonstrate governance

SecOps

Prioritize unknown devices
Locate assets quickly
Trigger SIEM/SOAR workflows

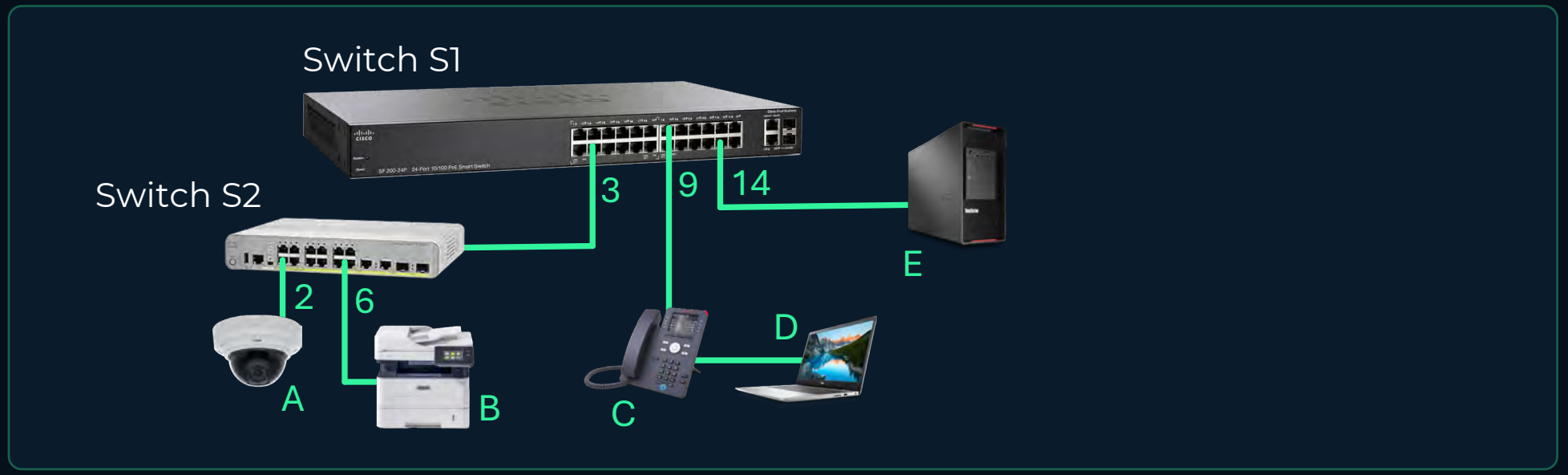
IT / Network Ops

Authoritative inventory
Less manual discovery
No taps/probes/traffic inspection

Compliance / Audit

Continuous evidence
Traceable policy exceptions
Reduced audit scramble

Security – AssetDNA (Fingerprint) Background



- MAC Addresses seen on a switch port represents all the devices that are connected through that port
  (but suffers from the effects of cascading… aging… etc.)
- Port Fingerprints represents only the “first” device that is physically connected to the port

Security – AssetDNA (Fingerprint) Background

Port Fingerprint composition and behavior • Determined at link establishment • Influenced by switch chipset complexity

Port Fingerprint factors

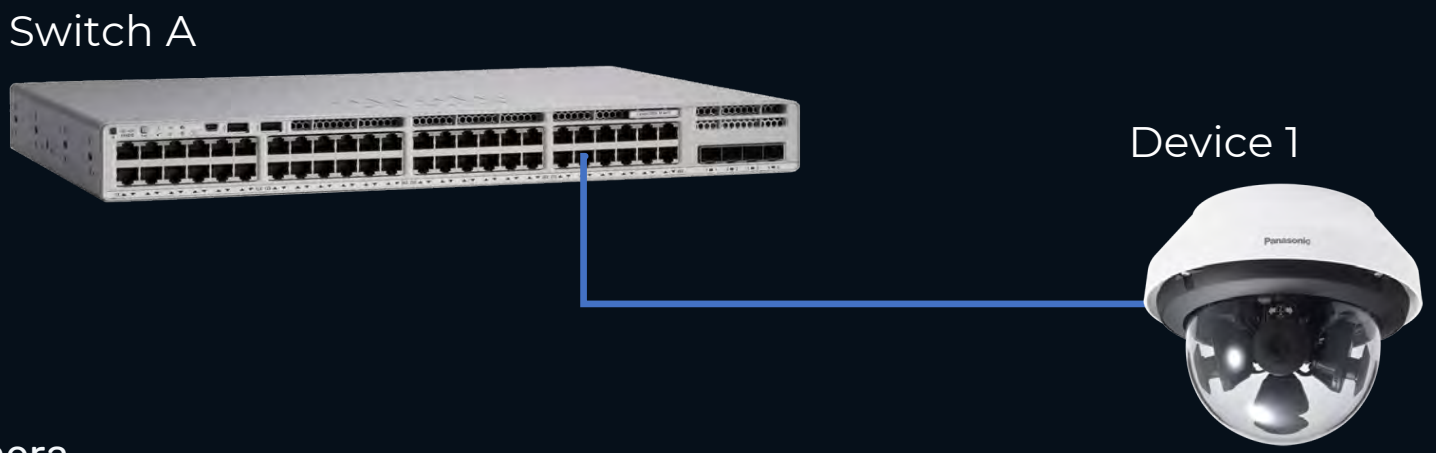
- The end device (physically connected on the port)
- The switch chipset (“behind” the switch port)
- The switch model
- The negotiated link speed (due to port config, in some cases manual/forced)
- Determined during link establishment — will not change until link goes down
- More advanced chipsets produce richer fingerprint data and more variants

FpData examples

```
"FpData":"1140796dae02501101e14de100650000--------00012300000085140000----"
"FpData":"1140796dae02501101e14de100650000--------00010300000085140000----"
"FpData":"1000796D002062D00DE14DE100052001----3000----0300----8517----0617"
"FpData":"1000796D002062D00DE14DE100052005----3000----0300----8557----0617"
"FpData":"1000796D002062D00DE14DE100052009----3000----0300----8597----0617"
"FpData":"210079CD03625D7300010000006400000000300040012300000005040000021E"
"FpData":"210079CD03625D730001000000640000000030004001230000000504000000CB"
"FpData":"210079CD03625D73000100000064000000003000400123000000050400000213"
```

Security – AssetDNA (Fingerprint) Background

Most simple example – one Asset connected directly to the Supervised Switch:



MAC Address:

- Panasonic Camera

Fingerprint:

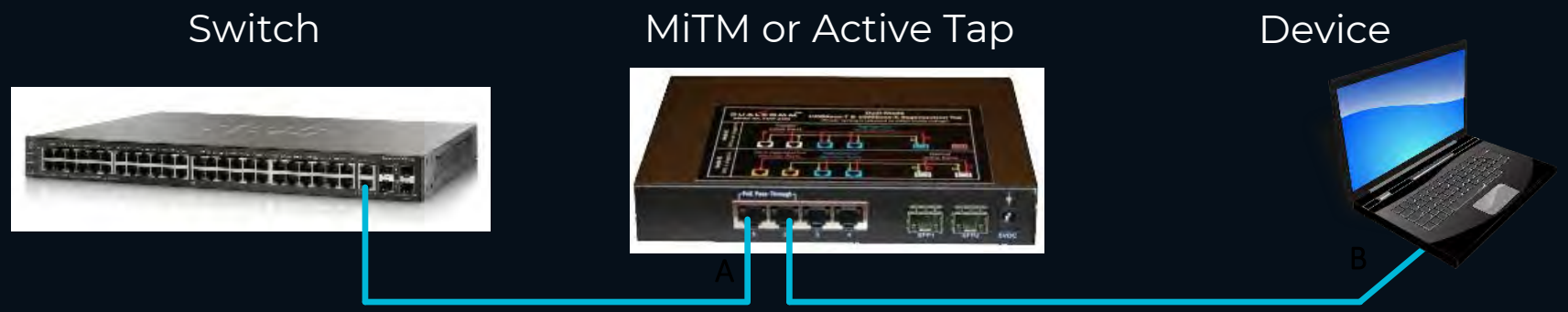
- Panasonic Camera (also function of the specific Chipset switch A)

PoE:

- Potentially, if both the Camera supports (and configured to use) and Switch supports (and enabled) Port Fingerprints represents only the “first” device that is physically connected to the port

Security – AssetDNA (Fingerprint) Background

Using L1 Asset DNA to detect an attack:



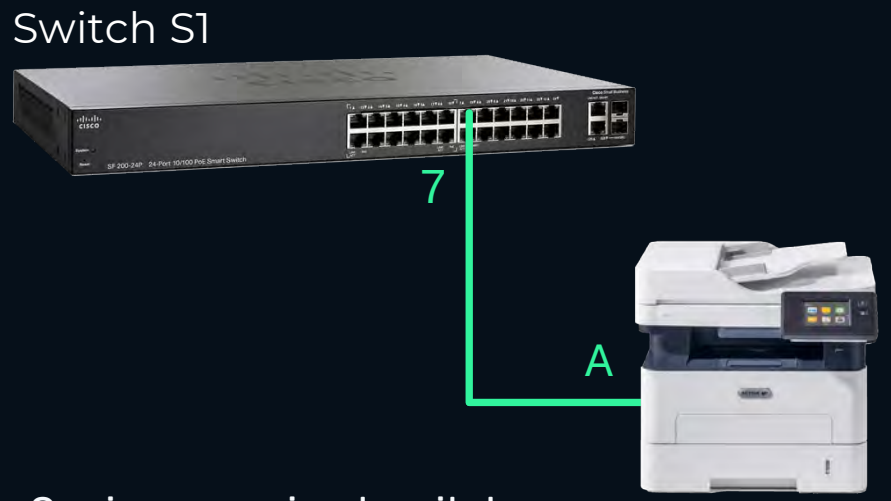
From the switch point of view: Physical fingerprint of point A Logical entity of point B

And being able to detect:

- MiTM devices
- Spoofed devices
- “Partisan” unmanaged switches, WiFi bridges
- “Shadow IT”

Security – Attack Type 1 (Spoofing A)

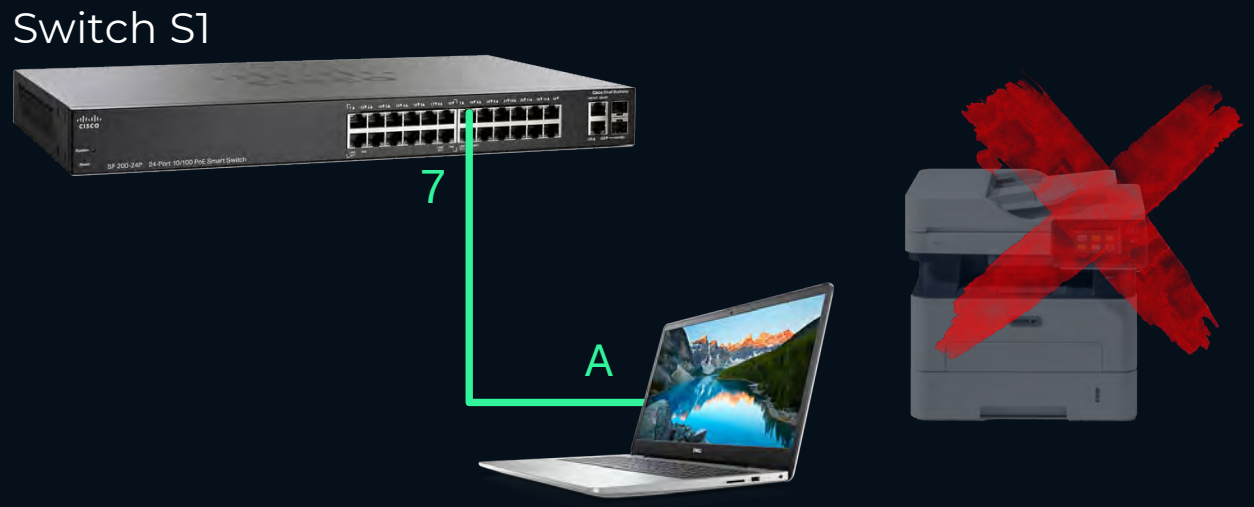
Normal Situation:



- A legitimate HP printer is connected to a port of a Sepio supervised switch.
- Sepio sees MAC address and other logical parameters of the HP printer
- Sepio sees the expected DNA of the HP printer
- Sepio reports no risk

Security – Attack Type 1 (Spoofing A)

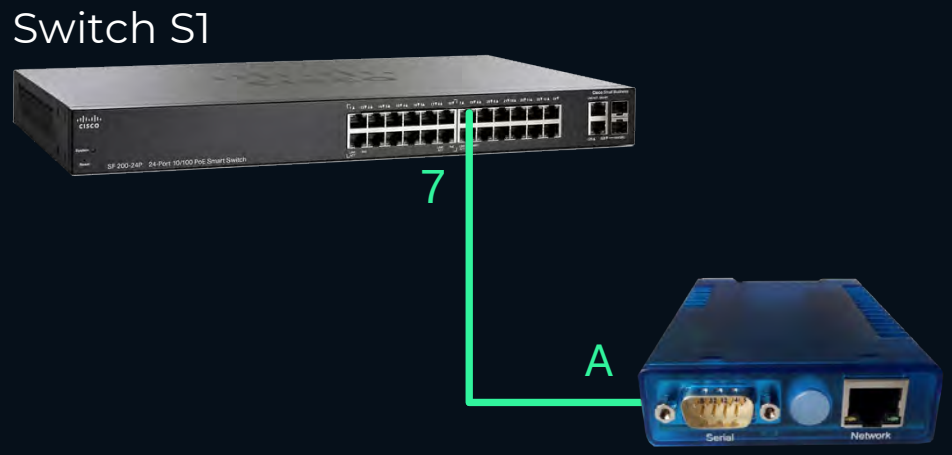
Attack Situation



- The HP printer is disconnected
- A Dell Laptop is spoofing to be the HP printer (so uses a MAC address similar to the HP printer)
- Sepio sees MAC address and other logical parameters of the HP printer
- Sepio sees the Dell Laptop DNA that is different than the expected DNA of the HP printer
- Sepio reports a DNA Anomaly risk

Security – Attack Type 1 (Spoofing A) Rare

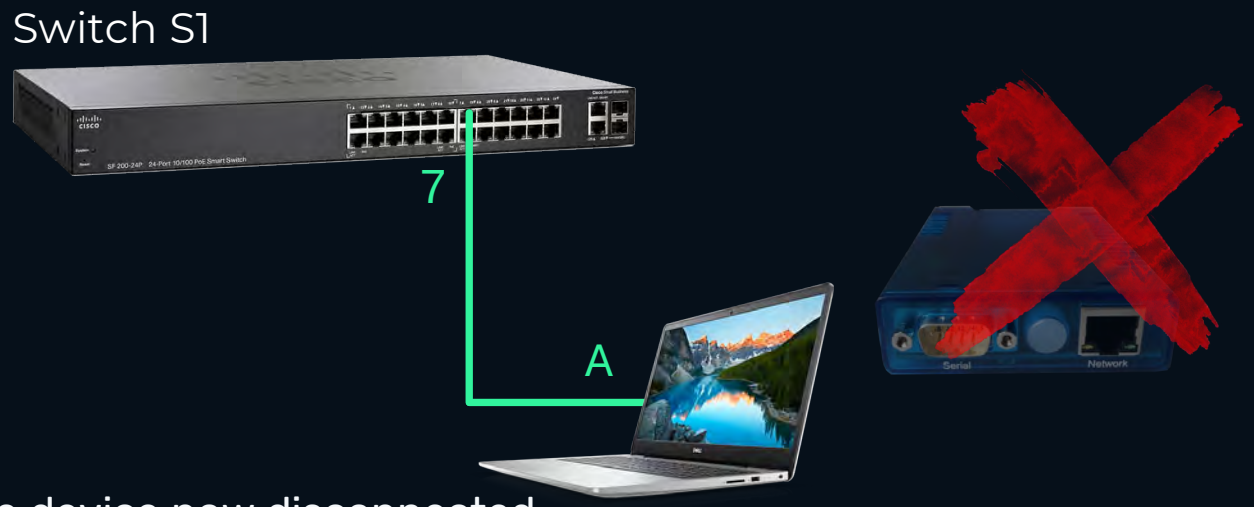
Normal Situation:



- A legitimate device that is unknown to Sepio (or seen only once) is connected to a port of a Sepio supervised switch
- Sepio sees MAC address and other logical parameters of that never seen before device
- Sepio sees the DNA of the never seen before device
- Sepio reports “Rare device” risk.

Security – Attack Type 1 (Spoofing A)

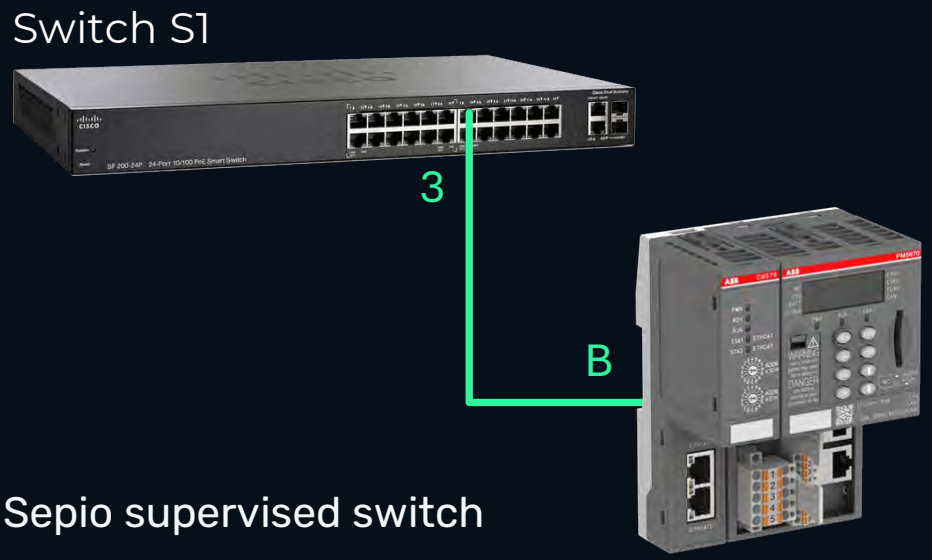
Attack Situation:



- A trusted rule has been created for the legitimate device now disconnected
- A Dell Laptop is spoofing to be the disconnected device (so uses a similar MAC address)
- Sepio sees MAC address and other logical parameters of the device printer
- Sepio sees Dell Laptop DNA conflict with a trusted rule.
- Sepio reports a DNA Anomaly risk

Security – Attack Type 2 (Spoofing B)

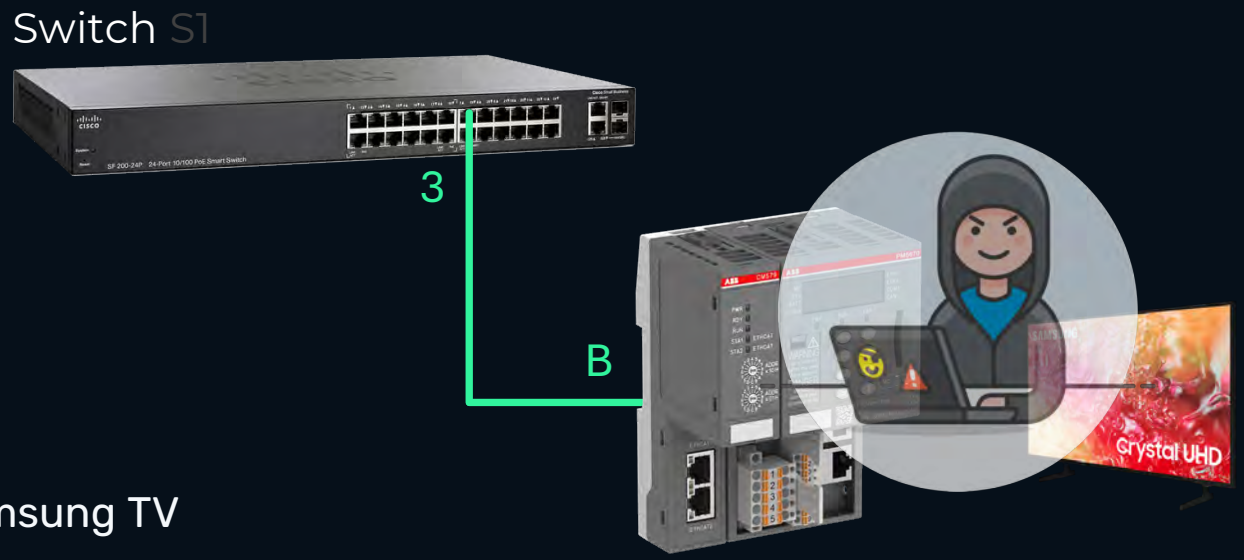
Normal Situation:



- A legitimate ABB PLC is connected to a port of a Sepio supervised switch
- Sepio sees MAC address and other logical parameters of the ABB PLC printer
- Sepio sees the expected DNA of the ABB PLC printer
- Sepio reports no risk

Security – Attack Type 2 (Spoofing B)

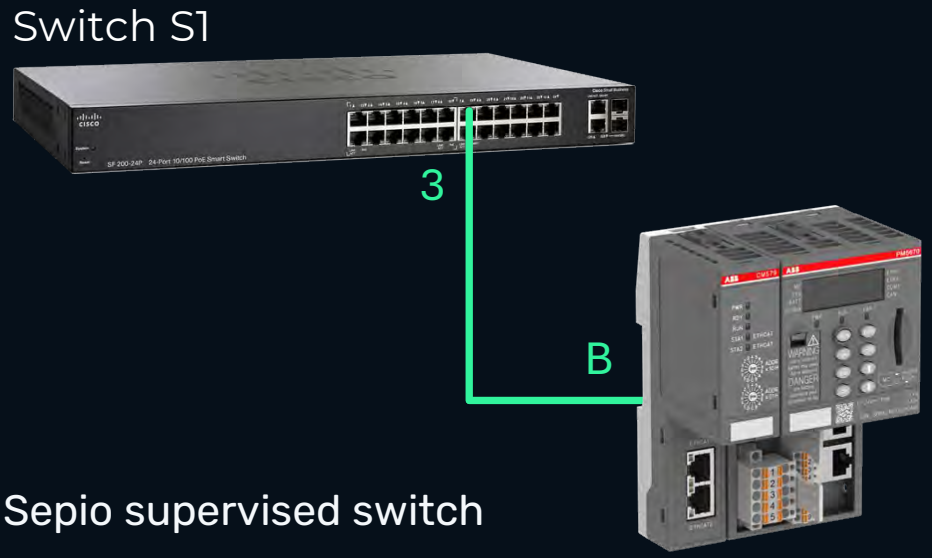
Attack Situation:



- The ABB PLC is manipulated to spoof to be a Samsung TV
- Sepio sees MAC address and other logical parameters of the Samsung TV
- Sepio sees the ABB PLC DNA that is different than the expected DNA of the Samsung TV
- Sepio shows the Asset as a Samsung TV
- Sepio reports a DNA Anomaly risk

Security – Attack Type 2 (Spoofing B) Limitation

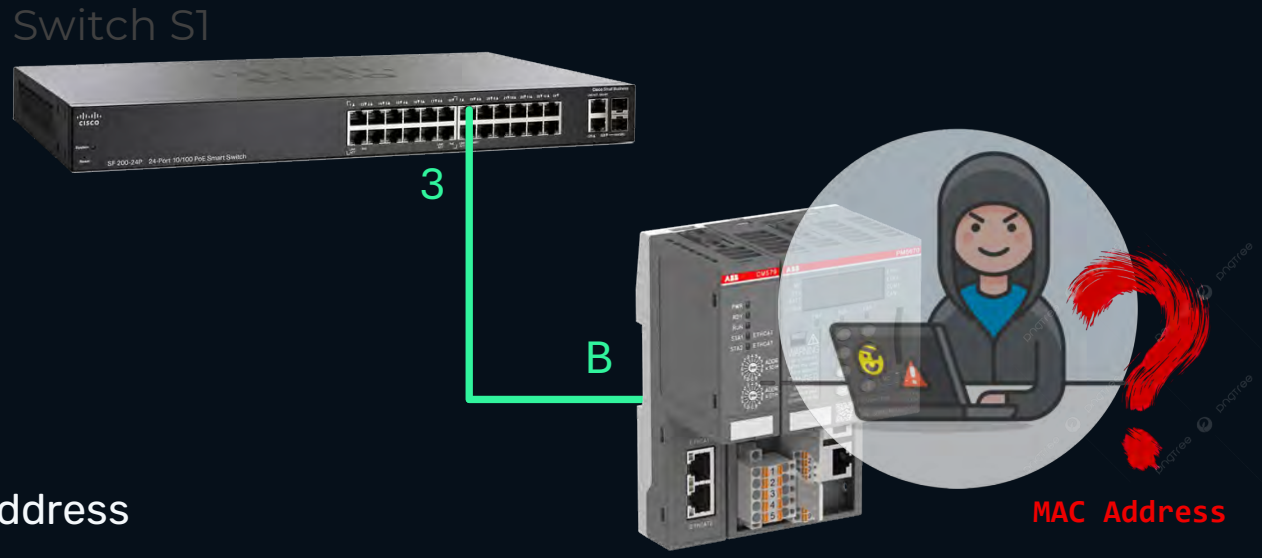
Normal Situation:



- A legitimate ABB PLC is connected to a port of a Sepio supervised switch
- Sepio sees MAC address and other logical parameters of the ABB PLC printer
- Sepio sees the expected DNA of the ABB PLC printer
- Sepio reports no risk

Security – Attack Type 2 (Spoofing B) Limitation

Attack Situation:



- The ABB PLC is manipulated an unknown MAC Address
- Sepio sees MAC address and other logical parameters of an unknown device
- Sepio shows the MAC Address that is in use, and shows the asset as “Other” and vendor as “Other”
- Sepio sees the DNA of the “Other” device but has while analyzing has no trusted base for comparison
- Sepio does not reports a DNA Anomaly risk

  * Rare Asset risk indicator

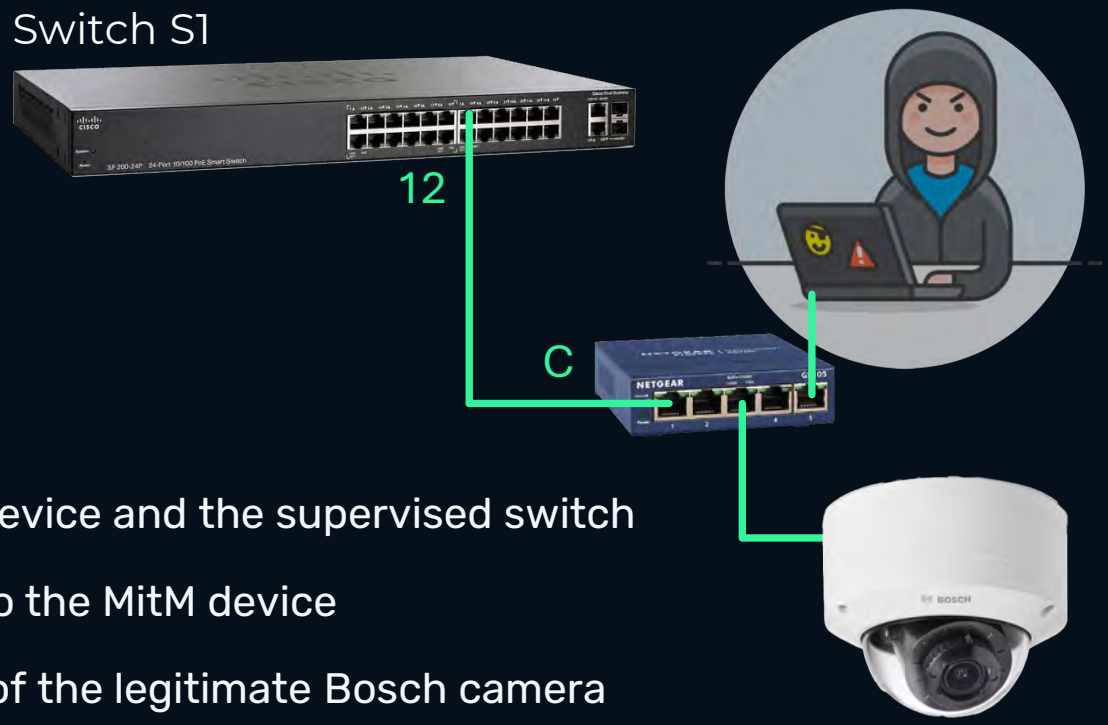
Security – Attack Type 3 (MitM)

Normal Situation:

- A legitimate Bosch camera is connected to a port of a Sepio supervised switch
- Sepio sees MAC address and other logical parameters of the Bosch camera
- Sepio sees the expected DNA of the Bosch camera
- Sepio reports no risk

Security – Attack Type 3 (MitM)

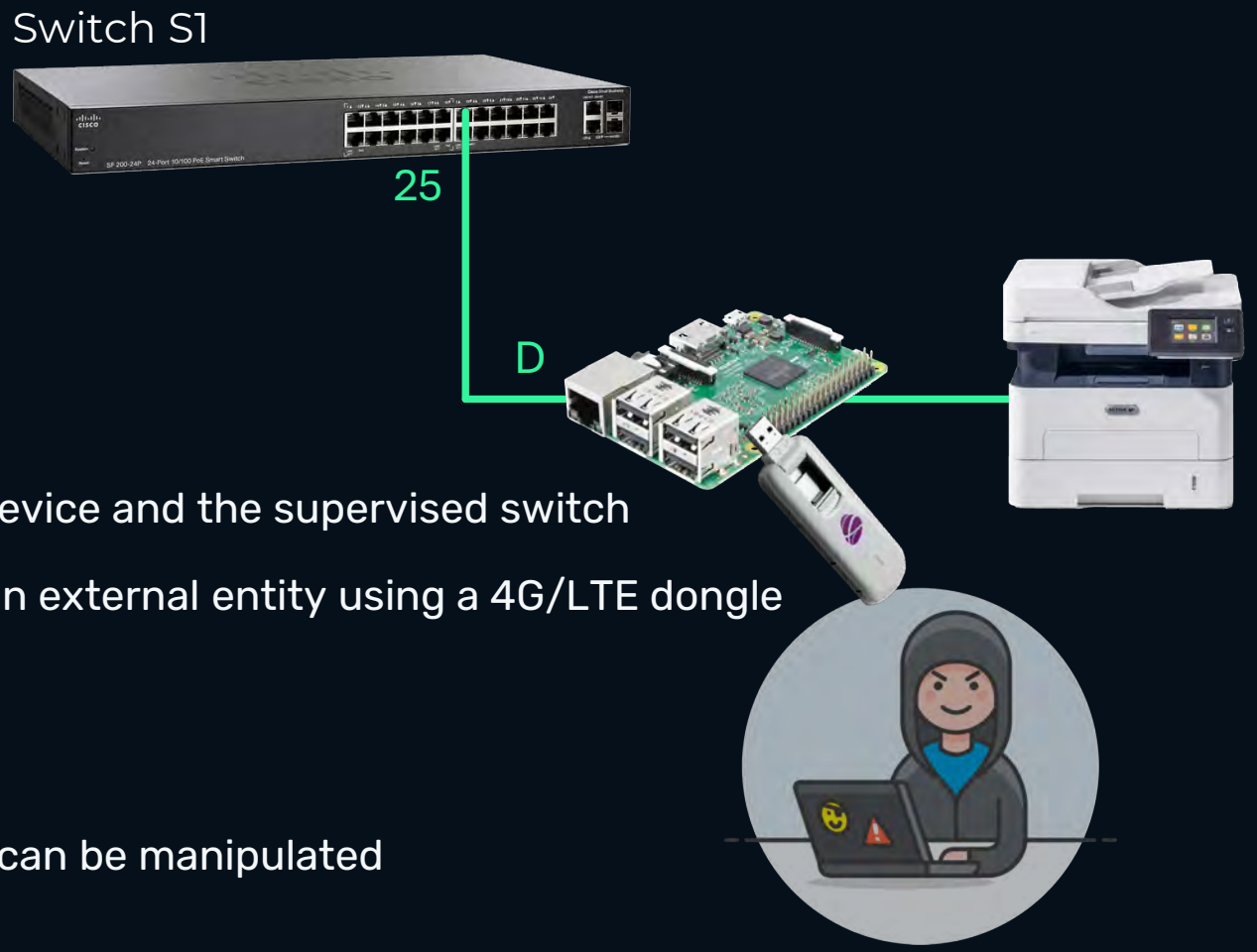
Attack Situation:



- A MitM device is added between the legitimate device and the supervised switch
- A laptop (that is in receive only mode) is added to the MitM device
- Using the laptop they can see the MAC address of the legitimate Bosch camera
- The laptop will spoof the MAC address of the Bosch camera
- The laptop can now send data to the network as if it came from the legitimate device

Security – Attack Type 3 (MitM)

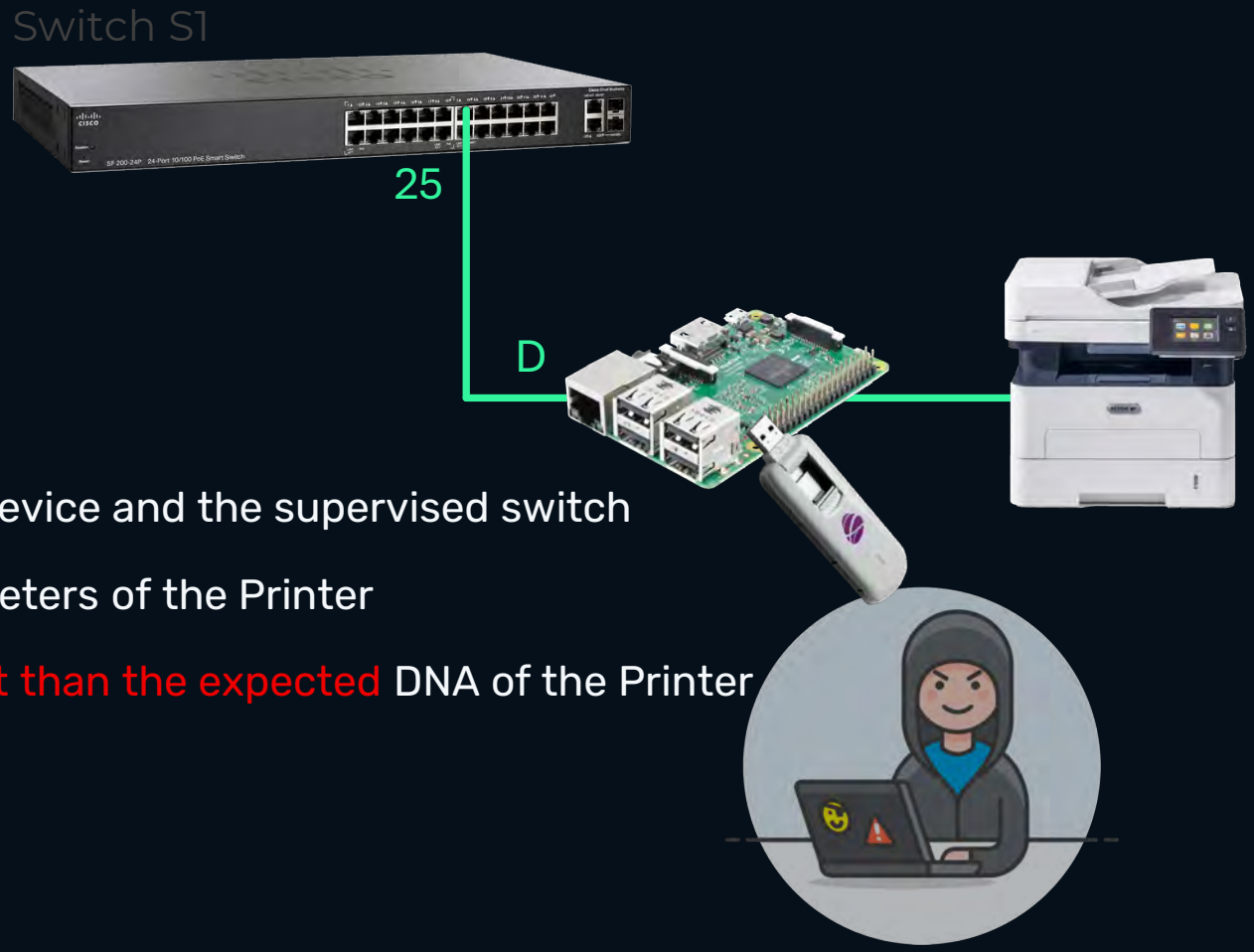
Attack Situation:



- A MitM device is added between the legitimate device and the supervised switch
- The MitM device is passing all the data through an external entity using a 4G/LTE dongle
- The traffic can be 100% intercepted
- Credentials and cookies can be stolen
- The traffic (and printed documents in this case) can be manipulated

Security – Attack Type 3 (MitM)

Attack Detection:



- A MitM device is added between the legitimate device and the supervised switch
- Sepio sees MAC address and other logical parameters of the Printer
- Sepio sees the Raspberry Pi DNA that is different than the expected DNA of the Printer
- Sepio shows the Asset as the printer
- Sepio reports a DNA Anomaly risk

See What You've Been Missing.

Sepio helps organizations discover, verify, validate, and enforce trust at the hardware layer — before unknown devices become business risk.

Zero Trust Hardware Access