Find and Fix Unmanaged & IoT Devices Security Gaps

Florence Lau
Florence.Lau@armis.com
APJ Solution Architect - Channel

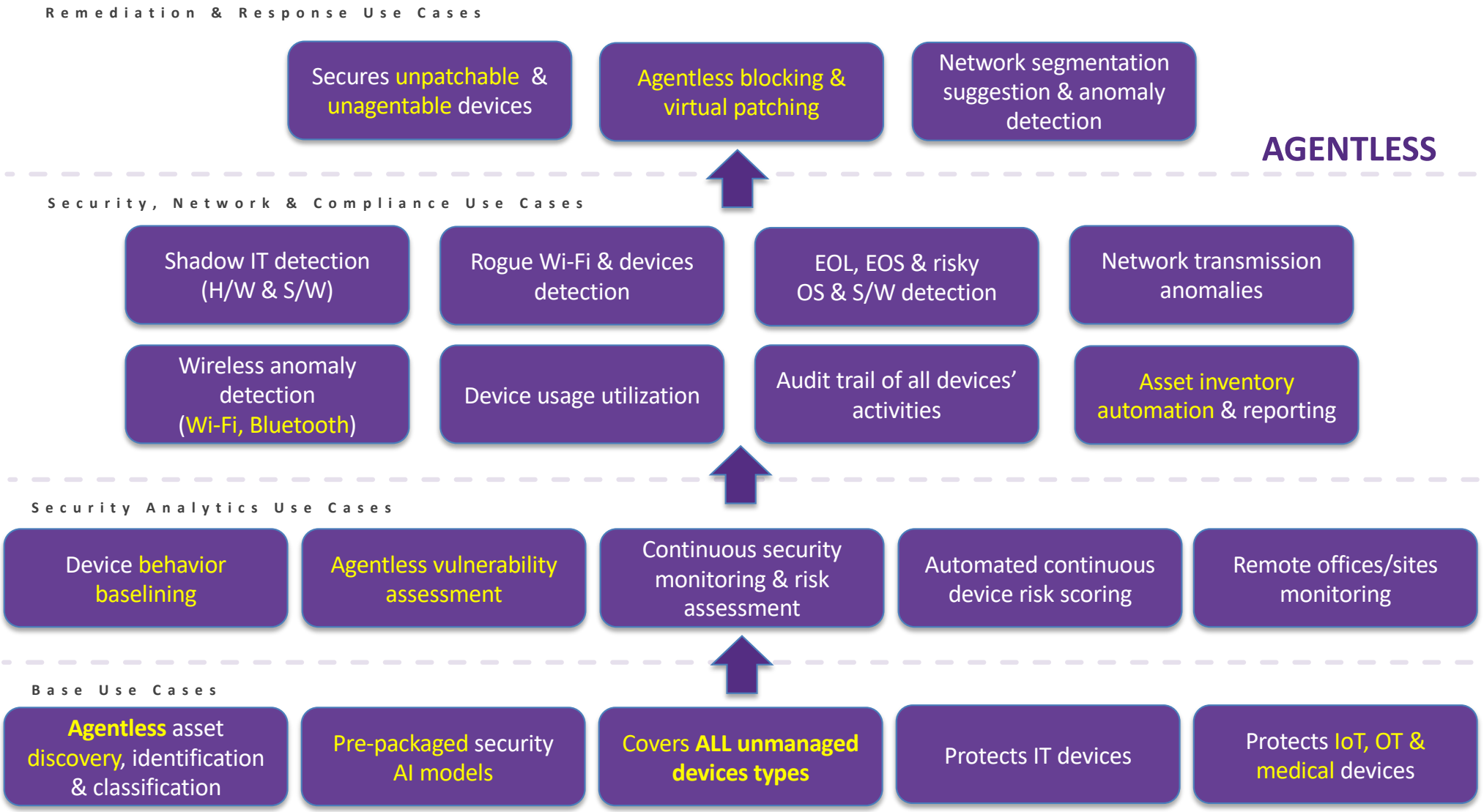
Henry Sin
Henry.Sin@armis.com
APJ Channel Director

Technology Partners

Armis addresses

Most popular questions Armis answers

Visibility	Give me a complete CMDB accuracy and gap analysis. CS2	How many laptops do I have? How many PLCs? How many MRI machines?	How many cloud or virtual assets do I have? Which aren't compliant with my policies?
Compliance	Am I compliant with CIS 1 thru CIS 6? Do I have rogue assets or shadow IT?	What EOL applications do I have across my entire environment?	Which endpoints aren't running my EDR or EPP? Which of them aren't up to date or not patched?
Risk & Security	Which devices in my environment are impacted by that new security advisory? CS3	What are the top most riskiest or non-compliant assets I have (by CVE, BU or location)?	What's the asset behind the IP address I'm investigating for an alert? Who is its owner and what's its location? CS1


Remediation & Response Use Cases
Secures unpatchable & unagentable devices
Agentless blocking & virtual patching
Network segmentation suggestion & anomaly detection
AGENTLESS
Security, Network & Compliance Use Cases
Shadow IT detection (H/W & S/W)
Rogue Wi-Fi & devices detection
EOL, EOS & risky OS & S/W detection
Network transmission anomalies
Wireless anomaly detection (Wi-Fi, Bluetooth)
Device usage utilization
Audit trail of all devices' activities
Asset inventory automation & reporting
Security Analytics Use Cases
Device behavior baselining
Agentless vulnerability assessment
Continuous security monitoring & risk assessment
Automated continuous device risk scoring
Remote offices/sites monitoring
Base Use Cases
Agentless asset discovery, identification & classification
Pre-packaged security AI models
Covers ALL unmanaged devices types
Protects IT devices
Protects IoT, OT & medical devices

Why Armis?

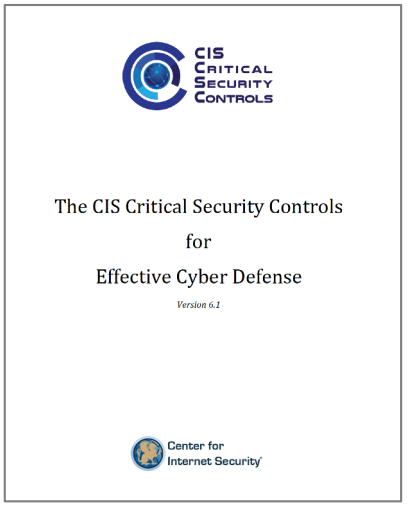
Business Outcomes

- Flexible licensing
- Low TCO
- 4 to 6 weeks completion time
- Reduced S/W, H/W wastage
- Convert PoV to production
- Covers unlimited devices
- Eliminate asset tracking pains
- Improved risk mgmt. with continuous device scoring

Operational Outcomes

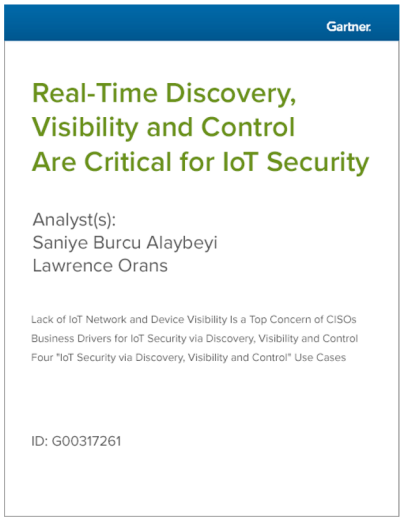
- 100% agentless & frictionless
- Single console for IT/IoT/OT/IoMT
- 1Billion device knowledgebase
- Prebuilt data models
- Covers Wi-Fi & LAN
- SaaS advantages
- Up-to-date security posturing

Discovery Is Critical



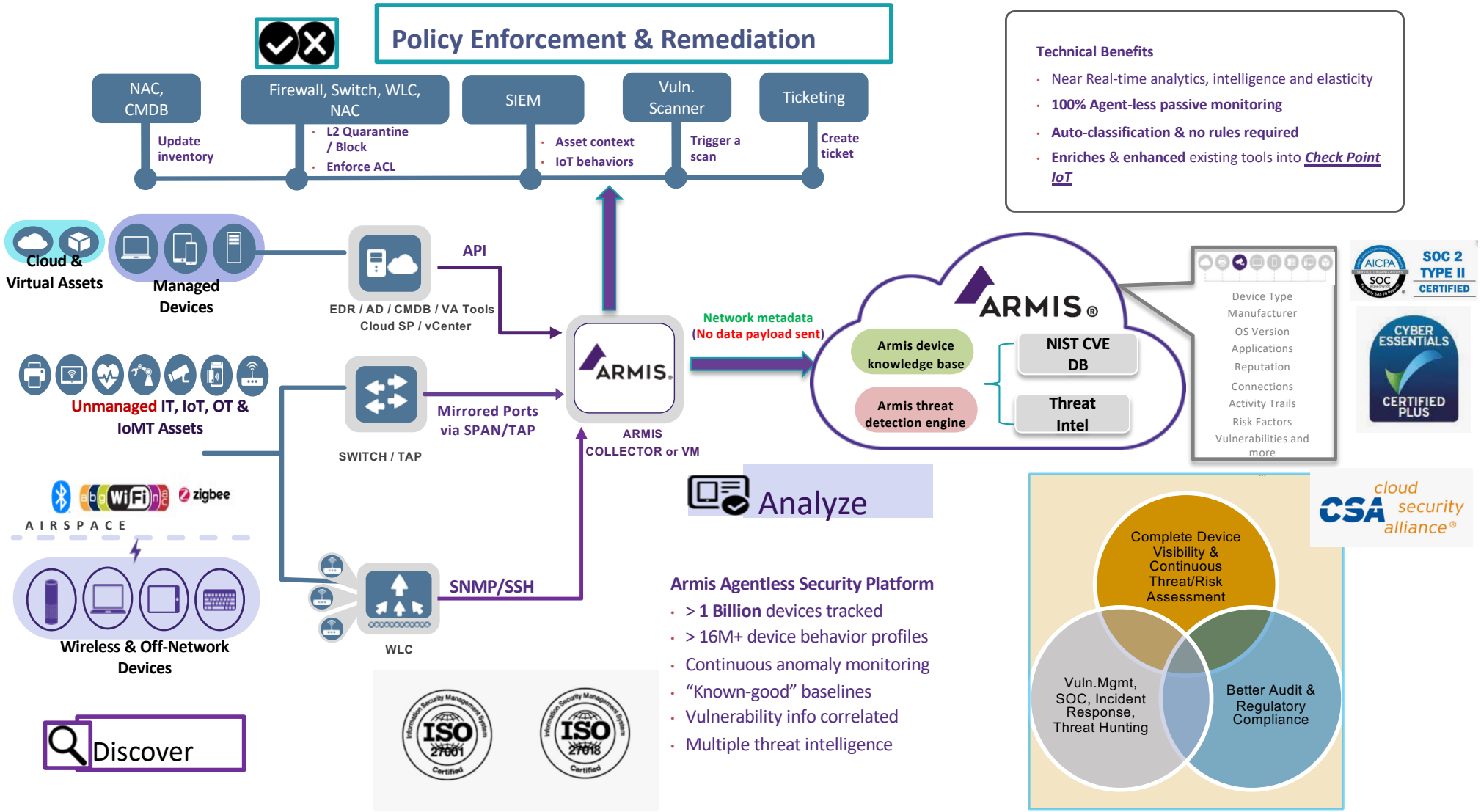
The #1 and #2 recommendations

CSC 1: **Inventory of authorized and unauthorized devices**
CSC 2: **Inventory of authorized and unauthorized software**

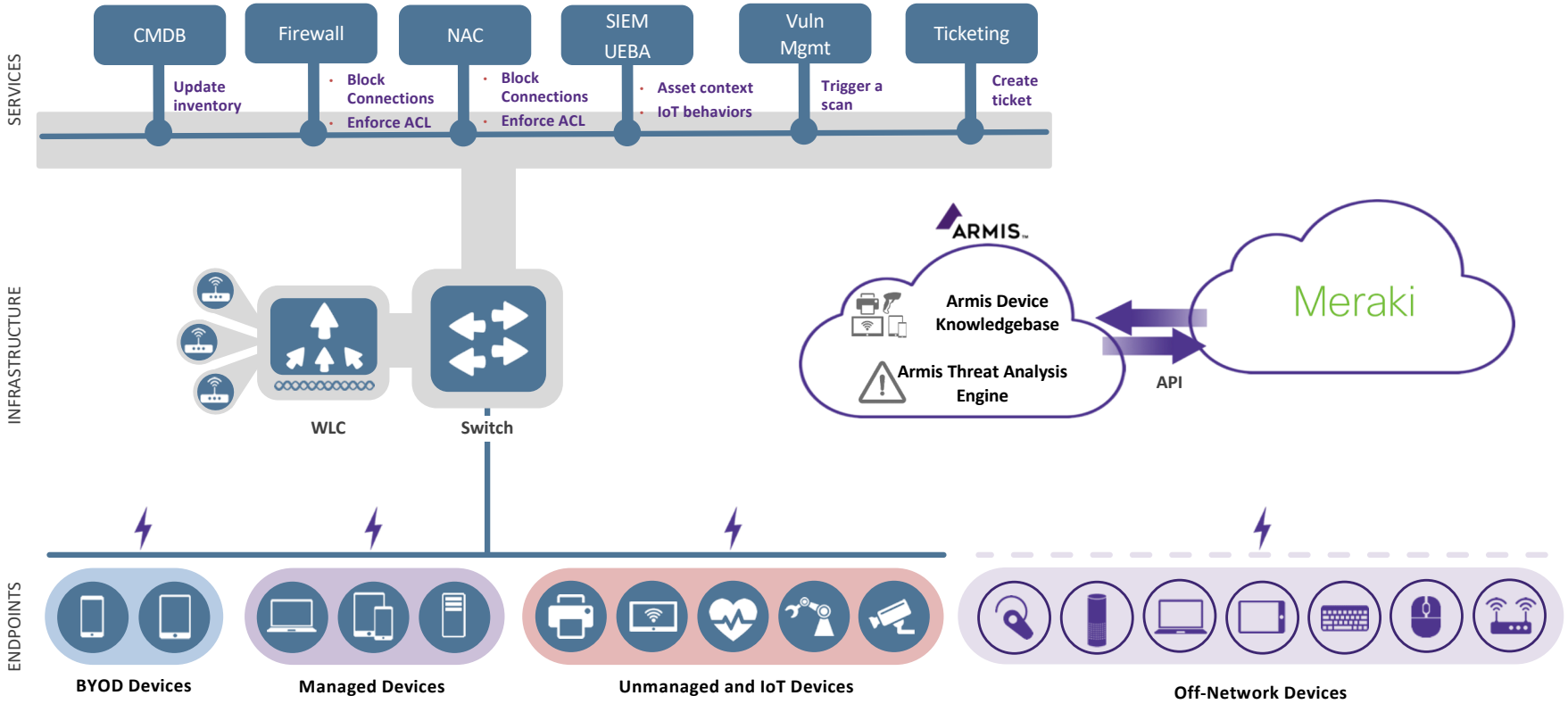


"**Discovery and visibility are critical prerequisites** to Internet of Things security. Security and risk management leaders in charge of IoT implementations will need to select an IoT network and device security strategy that will address specific visibility use-case requirements."

ARMIS


Policy Enforcement & Remediation
NAC, CMDB
Update inventory
Firewall, Switch, WLC, NAC
L2 Quarantine / Block
Enforce ACL
SIEM
Asset context
IoT behaviors
Vuln. Scanner
Trigger a scan
Ticketing
Create ticket
Technical Benefits
Near Real-time analytics, intelligence and elasticity
100% Agent-less passive monitoring
Auto-classification & no rules required
Enriches & enhanced existing tools into Check Point IoT
Cloud & Virtual Assets
Managed Devices
EDR / AD / CMDB / VA Tools
Cloud SP / vCenter
API
Unmanaged IT, IoT, OT & IoMT Assets
SWITCH / TAP
Mirrored Ports via SPAN/TAP
ARMIS
ARMIS COLLECTOR or VM
Network metadata
(No data payload sent)
ARMIS®
Armis device knowledge base
Armis threat detection engine
NIST CVE DB
Threat Intel
Device Type
Manufacturer
OS Version
Applications
Reputation
Connections
Activity Trails
Risk Factors
Vulnerabilities and more
SOC 2 TYPE II CERTIFIED
CYBER ESSENTIALS CERTIFIED PLUS
AIRSPACE
zigbee
Wireless & Off-Network Devices
WLC
SNMP/SSH
Analyze
Armis Agentless Security Platform
> 1 Billion devices tracked
> 16M+ device behavior profiles
Continuous anomaly monitoring
"Known-good" baselines
Vulnerability info correlated
Multiple threat intelligence
Discover
ISO 27001 Certified
ISO 27018 Certified
cloud security alliance®
Complete Device Visibility & Continuous Threat/Risk Assessment
Vuln.Mgmt, SOC, Incident Response, Threat Hunting
Better Audit & Regulatory Compliance

Cloud Integration with Cisco Meraki WLC



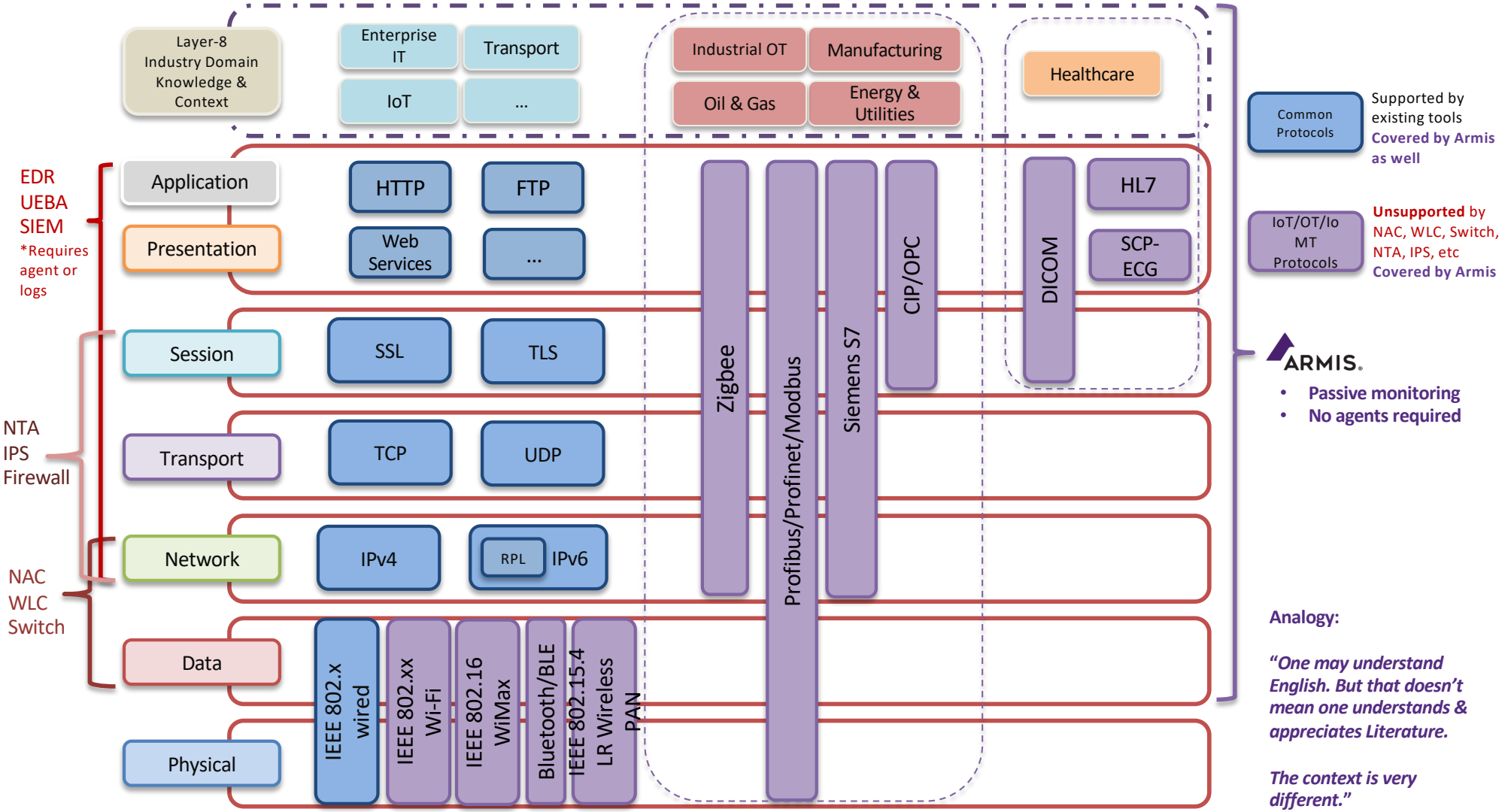
Armis Fills The Security Gap

Legacy security solutions are focused on managed devices, but not designed for unmanaged or IoT devices. Armis is purpose built for unmanaged devices, and yet provides an overlay protection for managed devices.

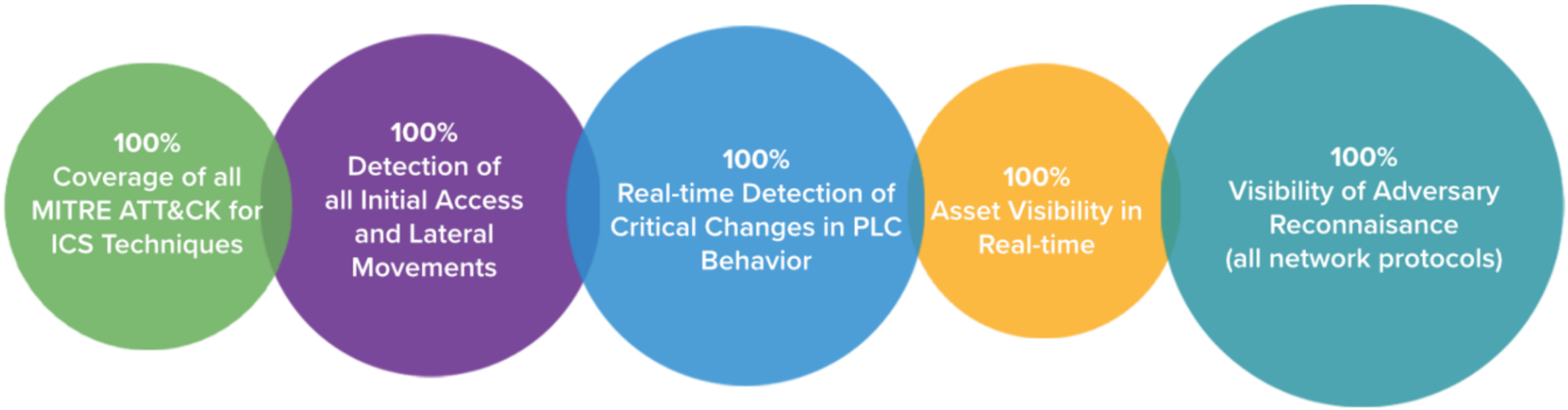
Security Function	Product Category	Managed Devices	BYOD	Unmanaged/IoT		Off-Network	
Hardware discovery	*NAC* (ForeScout)	●	●	◑	●	○	●
Software discovery	*Agent-based tools* (ForeScout)	●	○	○	●	○	●
	Network scanners (Qualys)	●	◑	○	●	○	●
Risk analysis	*Agent-based tools* (tripwire)	●	○	○	●	○	●
	Network scanners (Qualys)	●	◑	○	●	○	●
Threat analysis	*Agent-based tools* (Tanium)	●	○	○	●	○	●
	NTA (Darktrace)	●	●	◑	●	○	●
	UEBA (LogRhythm)	●	●	◔	●	○	●
Incident response	*NAC* (Cisco)	●	●	●	●	○	●

ARMIS™ Extended Visibility/Security

ARMIS™ Core Visibility/Security

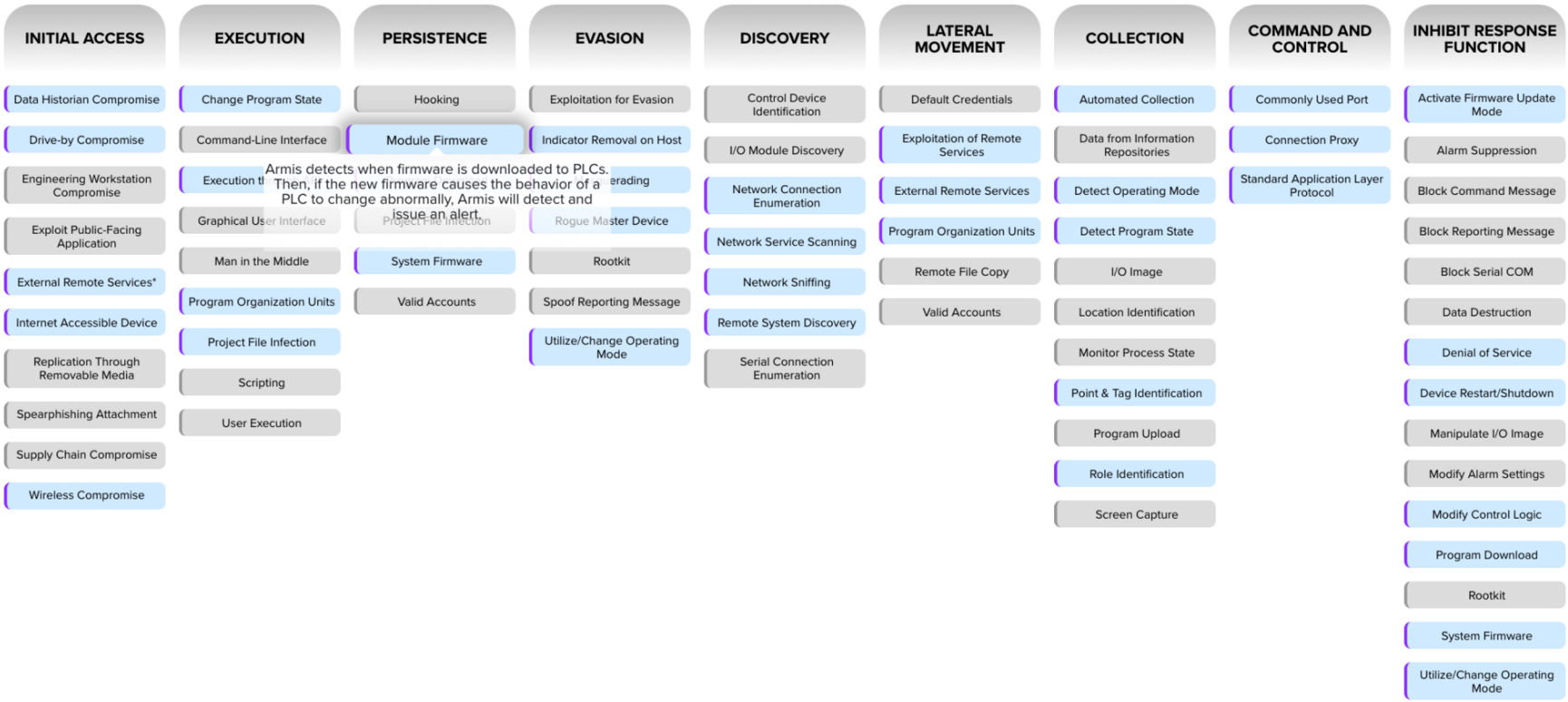

Layer-8
Industry Domain
Knowledge &
Context
Enterprise IT
Transport
IoT
...
Industrial OT
Manufacturing
Oil & Gas
Energy & Utilities
Healthcare
EDR
UEBA
SIEM
*Requires agent or logs
NTA
IPS
Firewall
NAC
WLC
Switch
Application
Presentation
Session
Transport
Network
Data
Physical
HTTP
FTP
Web Services
...
SSL
TLS
TCP
UDP
IPv4
RPL
IPv6
IEEE 802.x wired
IEEE 802.xx Wi-Fi
IEEE 802.16 WiMax
Bluetooth/BLE
IEEE 802.15.4 LR Wireless PAN
Zigbee
Profibus/Profinet/Modbus
Siemens S7
CIP/OPC
DICOM
HL7
SCP-ECG
Common Protocols
Supported by existing tools
Covered by Armis as well
IoT/OT/Io MT Protocols
Unsupported by NAC, WLC, Switch, NTA, IPS, etc
Covered by Armis
ARMIS.
• Passive monitoring
• No agents required
Analogy:
"One may understand English. But that doesn't mean one understands & appreciates Literature.
The context is very different."

The *only* solution that presents 100% visibility across IT, IoT and OT/ICS environments.



ARMIS.

MITRE ATT&CK for ICS



ARMIS.

DEVICE KNOWLEDGEBASE

Device Characteristics & Behavior Traits

Basic Device Information

- Device type, Category, Model
- Manufacturer
- IP address
- MAC address

Software Information

- Operating system type, version
- User name
- Applications

Connection Information

- Connection type (wired, WiFi, Bluetooth, etc.)
- Connection point (corp, guest, rogue, etc.)
- Physical location
- Traffic volume
- Traffic timing
- Traffic destination
- Open ports
- Internet domains accessed

Endpoint Behavior

- Stationary vs. moving
- Communication timing
- Communication volumes
- Cloud services accessed
- Tunnels utilized
- Encryption usage
- Data storage

Network Health

- Latency
- Packet loss
- Authentication errors

Switch Information

- Switch name
- Switch location
- Switch CPU utilization
- Switch configuration
- Internet domains accessed

Wi-Fi Information

- AP name
- AP CPU utilization
- AP bandwidth utilization
- AP OS version
- AP BIOS version
- AP configuration
- Wi-Fi network name
- Wi-Fi channels used
- Wi-Fi power levels
- Signal levels
- Noise levels
- Jitter

Inside Armis Knowledgebase

AC Drives
Access Point Interface
Access Points
Acute Cares
Alarms
Amplifiers
Analog Gateways
Anesthesia Machines
Angiography
Appliances
ATMs
Attendance Systems
Audio Headsets
AV Transmitters
Barcode Readers
Beacons
Biopsy Systems
Cabinets
Cable Managers
Cars
Carts
Central Stations
Chassis
Controllers
CR Systems
Credit Card Reader
CTs
Dash Cams
Defibrillators
Desktops
Diagnostics
Dialysis Machines
Digital Cameras
Driver Terminals
Drones
DSPs
DVRs
ECGs
EEGs
Electric Scooters
Elevator Panels
Emergency Response
Endoscopy
Engineering Stations
Engineering Workstations
Ereaders
Fillers
Firewalls
Fitness
Fluoroscopy
Frames
Game Consoles
Gaming
Gateways
General Imaging
Generic IO's
Generic OT's
Generic Rack Components
Historians
HMI
HMI Panels
Hotspots
Household Appliances
HVACs
Hypervisor
I/O
Imaging Workstations
Industrial Managed Switches
Industrial Robots
Infusion Pumps
Interactive Kiosks
Intercoms
Intrusion Prevention Systems
IOT Gateways
IP Cameras
Keyboards
Lab Equipment
Laptops
Laptops (by adapter)
Life Supports
Lightings
Malicious
Mammography
Material Transport
Measuring Instruments
Media Controllers
Media Players
Media Writers
Medication Dispensing Systems
Mobile Phones
Monitoring Equipment
Monitors
Motor Controllers
Mouses
MRIs
Nuclear Medicine
Nurse Call
Operator Workstations
Optometry Systems
PACSs
Panel PCs
Panels
Patch Panels
Patient Monitors
PDUs
Pentests
PFT Systems
PLCs
POC diagnostics
Points of Sale
Power Monitors
Printers
Product Scanners
Projectors
Radiology Injection
Radiology Systems
Remote IO's
Routers
SCADA Clients
SCADA Servers
Scanners
Security Equipment
Sensors
Servers
Servo Drives
Single-Board Computers
Smart Cameras
Smart Glasses
Smart Switches
Speakers
Storage and Transport
Storage Server
Switches
Tablets
Telehealth Systems
Terminal Servers
Therapeutics
Thermostats
Treatment Equipment
Triggers
Trucks
TVs
Ultrasounds
Unknown
UPS
VCs
Ventilators
Video Broadband Devices
Virtual Assistants
Virtual Machines
VLANs
VoIPs
VR Headsets
Vulnerability Scanners
WAN Optimizers
Watches
Weather Instruments
Wireless Equipment
WLCs
Workstations
X-Rays

Supported Protocols

AUTOMATION & PRODUCTION
- Siemens S7/S7-Plus
- CIP
- PCCC/CSPv4
- CCC
- Lantronix
- GE PAC8000
- GE-SRTP
- Mitsubishi Melsec/Melsoft SSL
- Sattbus
- OPC DA/AE/UA
- Profibus
- Profinet-DCP
- Modbus TCP
- Modbus Altivar
- Modbus Concept/Momentum
- Modbus RTU
- Modbus Schneider

BUILDING MANAGEMENT SYSTEMS
- Siemens P2
- BACnet IP
- BACnet MSTP serial: RS485
- LONWorks
- M-Bus
- 1-Wire
- CC-Link
- Eubac
- EnOcean
- DALI
- Dynet
- OpenTherm
- OpenWebNet
- MIDAC
- KNX
- VSCP

DISTRIBUTED CONTROL SYSTEMS
- Honeywell Experion
- FTE (Honeywell)
- Emerson Ovation DCS protocols
- Emerson DeltaV DCS protocols
- Yokogawa ProSafe H1
- GE Mark6e (SDI)

MEDICAL
- ASTM
- DICOM
- HL7
- HL7 aECG BKV
- SCP-ECG Medical
- Smiths Medical
- Welch Allyn Medical
- X12

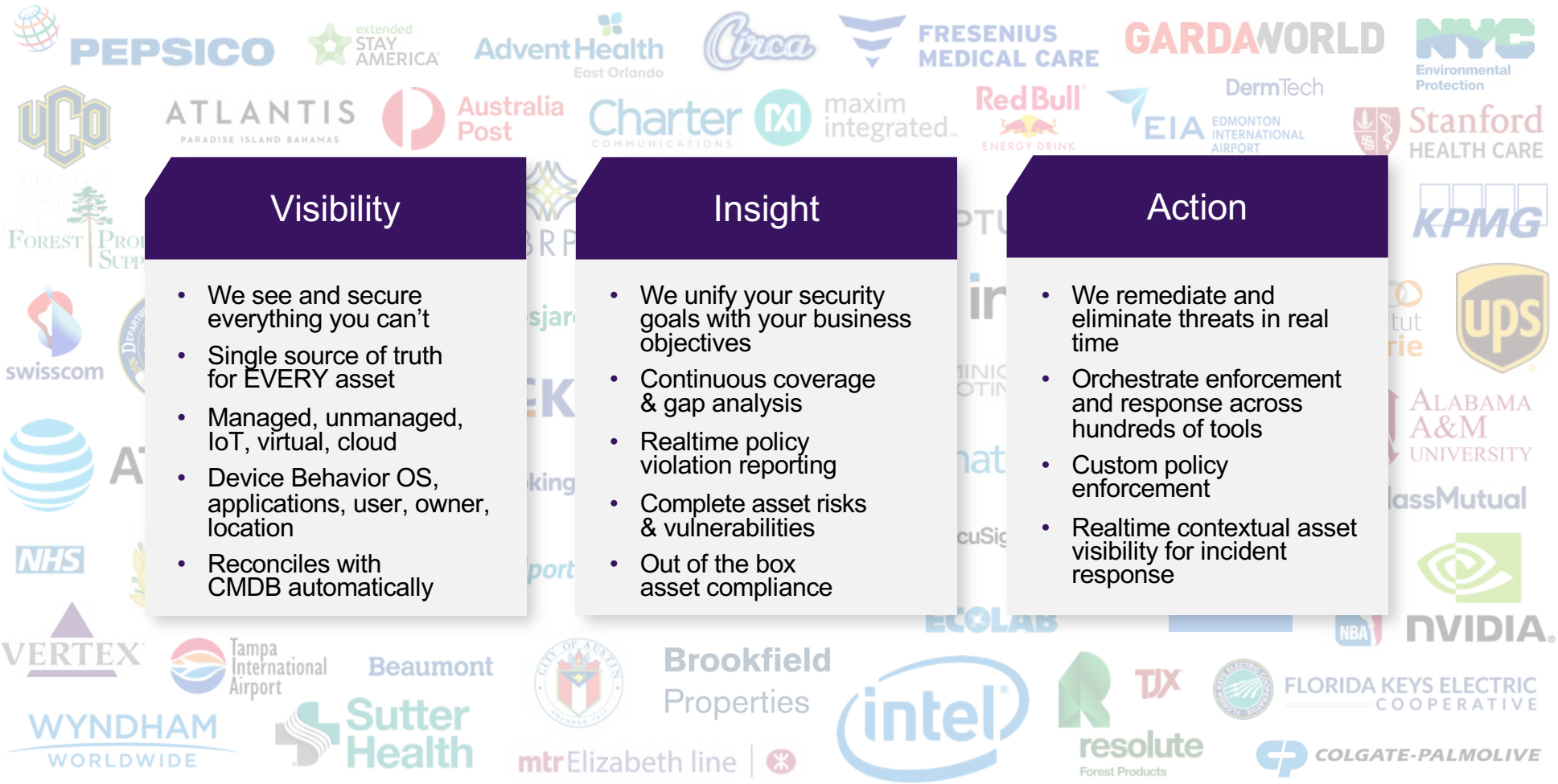
OIL & GAS
- VNC Emerson ROC
- ABB TotalFlow

SAFETY
- Triconex
- Yokogawa VNet/IP

ELECTRIC & DISTRIBUTION
- ABB 800xA DCS protocols
- MMS
- ICCP TASE.2
- IEC104/101
- DNP3
- GOOSE
- Schweitzer
- Bently Nevada

ADDITIONAL IT & ENTERPRISE PROTOCOLS
- ARP
- ATSVC
- BLE
- Bluetooth
- CDP
- CTI
- DCE/RPC
- DHCP V4/V6
- DNS
- Ethernet/IP
- GIOP
- GRE
- JEP-0047
- FTP
- HTTP/HTTPS
- ICMP
- IGMP
- IPv4/IPv6
- LLDP
- NetBios
- NTP
- NTLMSSP
- PCT1-A
- RDP
- SMB/CIFS
- SNMP
- SSDP
- SSH
- SSL
- TCP/IP
- Telnet
- TFTP
- Wi-Fi EtherNet/IP
- Wi-MAX
- Zigbee

Why Armis?



Visibility

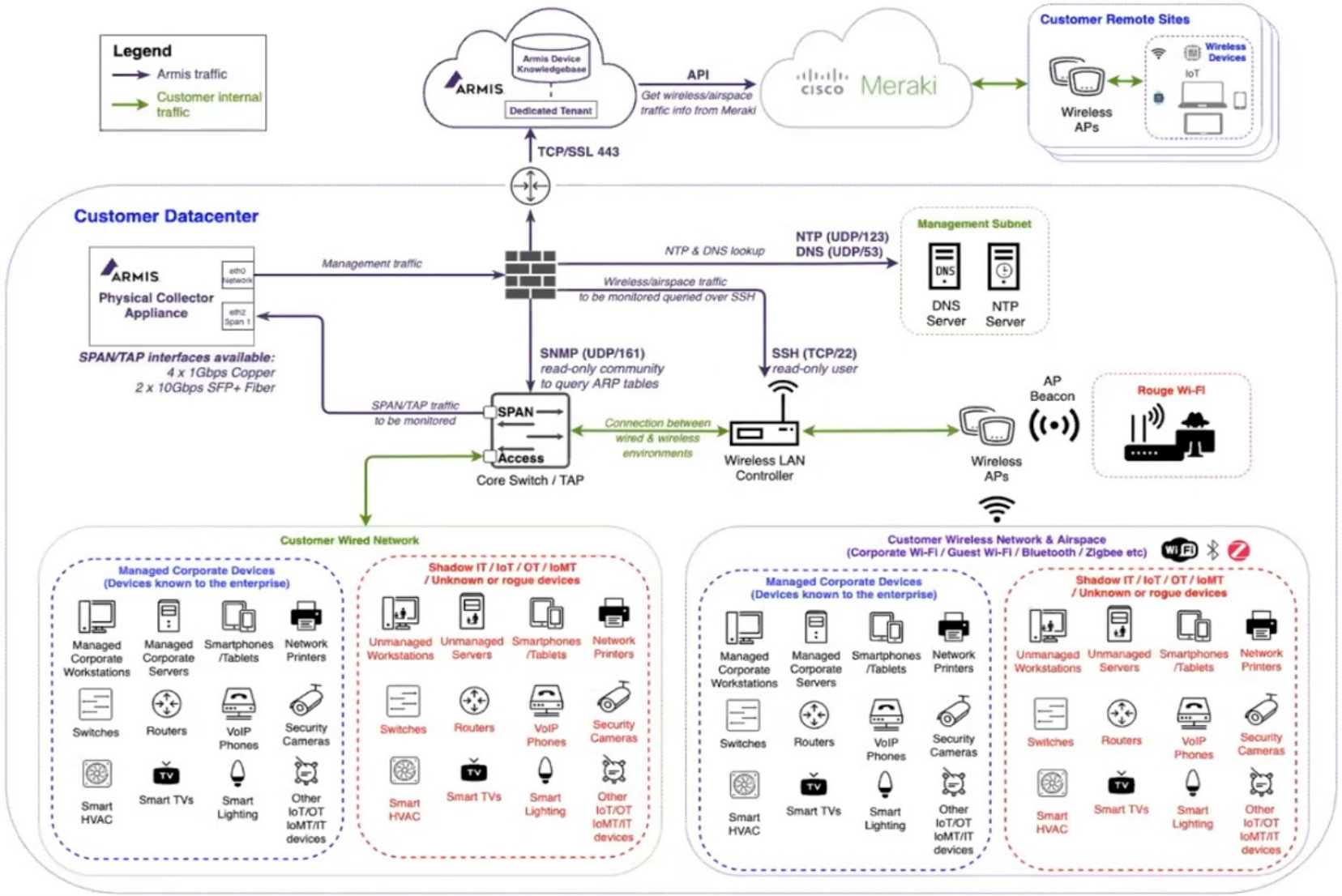
- We see and secure everything you can't
- Single source of truth for EVERY asset
- Managed, unmanaged, IoT, virtual, cloud
- Device Behavior OS, applications, user, owner, location
- Reconciles with CMDB automatically

Insight

- We unify your security goals with your business objectives
- Continuous coverage & gap analysis
- Realtime policy violation reporting
- Complete asset risks & vulnerabilities
- Out of the box asset compliance

Action

- We remediate and eliminate threats in real time
- Orchestrate enforcement and response across hundreds of tools
- Custom policy enforcement
- Realtime contextual asset visibility for incident response

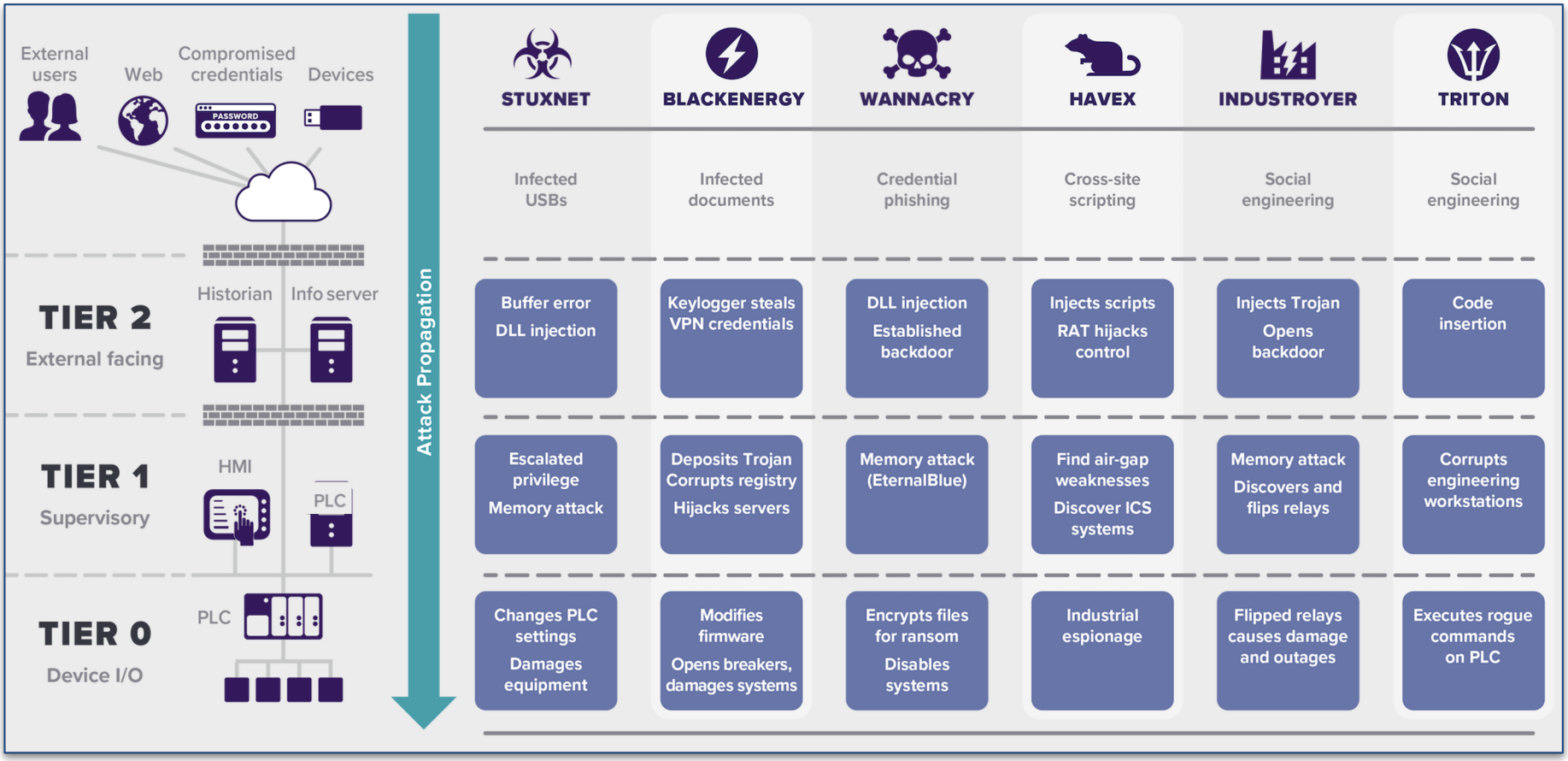

Legend
Armis traffic
Customer internal traffic
ARMIS
Armis Device Knowledgebase
Dedicated Tenant
API
Get wireless/airspace traffic info from Meraki
cisco Meraki
Customer Remote Sites
Wireless APs
Wireless Devices
IoT
TCP/SSL 443
Customer Datacenter
ARMIS
Physical Collector Appliance
eth0 Network
eth2 Span 1
SPAN/TAP interfaces available:
4 x 1Gbps Copper
2 x 10Gbps SFP+ Fiber
Management traffic
NTP & DNS lookup
NTP (UDP/123)
DNS (UDP/53)
Management Subnet
DNS
DNS Server
NTP Server
Wireless/airspace traffic to be monitored queried over SSH
SNMP (UDP/161)
read-only community
to query ARP tables
SSH (TCP/22)
read-only user
SPAN/TAP traffic to be monitored
SPAN
Access
Core Switch / TAP
Connection between wired & wireless environments
Wireless LAN Controller
AP Beacon
Wireless APs
Rouge Wi-Fi
Customer Wired Network
Managed Corporate Devices (Devices known to the enterprise)
Managed Corporate Workstations
Managed Corporate Servers
Smartphones /Tablets
Network Printers
Switches
Routers
VoIP Phones
Security Cameras
Smart HVAC
Smart TVs
Smart Lighting
Other IoT/OT IoMT/IT devices
Shadow IT / IoT / OT / IoMT / Unknown or rogue devices
Unmanaged Workstations
Unmanaged Servers
Smartphones /Tablets
Network Printers
Switches
Routers
VoIP Phones
Security Cameras
Smart HVAC
Smart TVs
Smart Lighting
Other IoT/OT IoMT/IT devices
Customer Wireless Network & Airspace (Corporate Wi-Fi / Guest Wi-Fi / Bluetooth / Zigbee etc)
Managed Corporate Devices (Devices known to the enterprise)
Managed Corporate Workstations
Managed Corporate Servers
Smartphones /Tablets
Network Printers
Switches
Routers
VoIP Phones
Security Cameras
Smart HVAC
Smart TVs
Smart Lighting
Other IoT/OT IoMT/IT devices
Shadow IT / IoT / OT / IoMT / Unknown or rogue devices
Unmanaged Workstations
Unmanaged Servers
Smartphones /Tablets
Network Printers
Switches
Routers
VoIP Phones
Security Cameras
Smart HVAC
Smart TVs
Smart Lighting
Other IoT/OT IoMT/IT devices

SELLING POINT & POV

Strategy Move	Value to Customer
SaaS Model	Quick time to value and fast deployment
Agentless & Passive	No interruption to network
Minimal configuration	Able to identify and auto-classification all device brands, characteristics – enriched the context
Airspace protocols recognition	WI-FI, **Bluetooth and Zigbee
IoMT awareness	Rich protocols and awareness based on Medical Equipment such as • HIS (Hospital Information System) • LIS (Laboratory Information System) • Radiology Information System (RIS)

OT PURDUE LEVEL

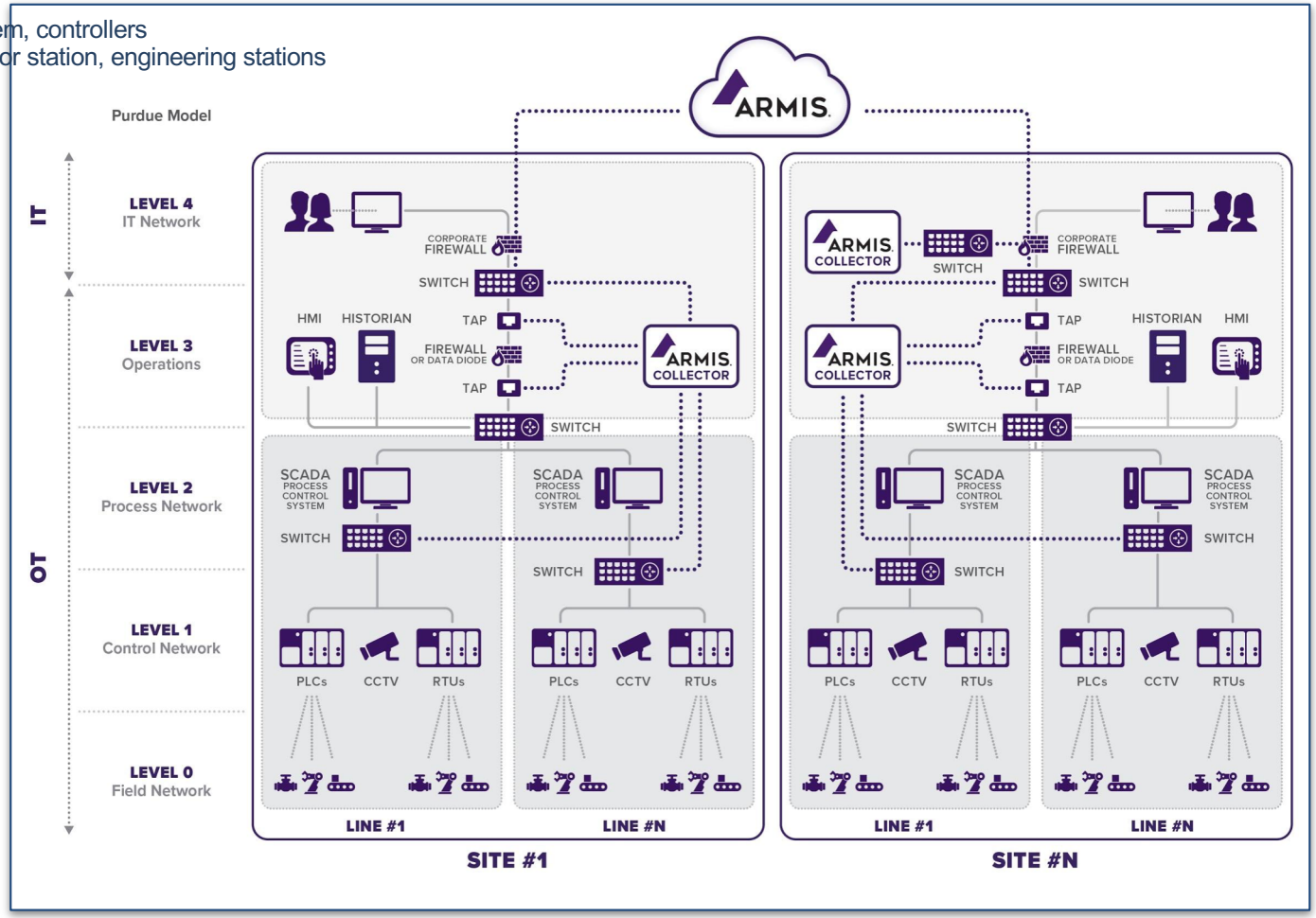
Attacks, Vectors, and their Effects on Industrial Control Systems



Armis maps these threats against Mitre's *ATT&CK Framework for ICS*

Level 0 – Field: Sensors, actuators, motors
Level 1 – Process: Automation Devices, safety system, controllers
Level 2 – Supervision: SCADA stations, DCS operator station, engineering stations
Level 3 – manufacturing operations: MES, LIMS
Level 4 and 5 – IT (Office, PC, messaging, intranet)

- **Passive** ☑
- **Agentless** ☑
- **Continuous** ☑
- **Real-Time** ☑
- **Anomaly Detections** ☑
- **Vulnerability Management** ☑
- **Purdue Model Compliant** ☑



ARMIS

Safely Deploy Cloud-based Solutions

Armis Purdue Levels