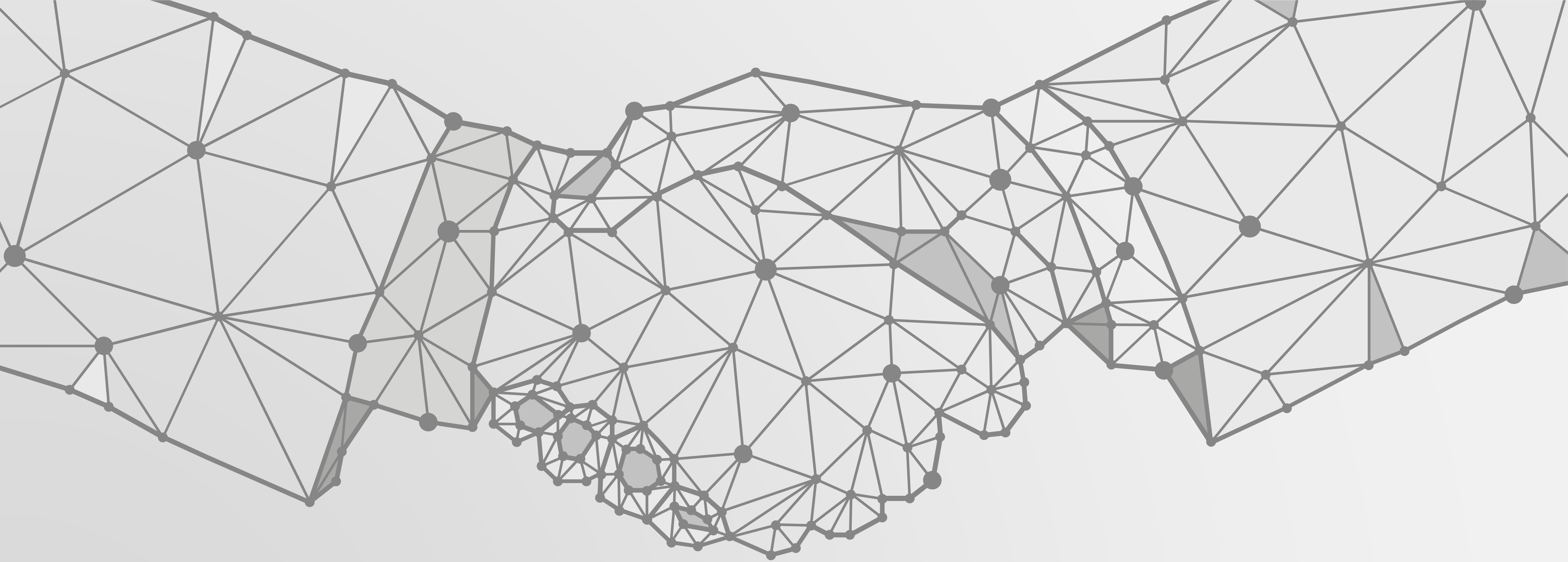


AGENTLESS DEVICE SECURITY

MAKING THE DIGITAL TRANSFORMATION SAFE FOR THE ENTERPRISE, ICT AND MEDICAL AREAS

Hotel Tatra, 9/6/22

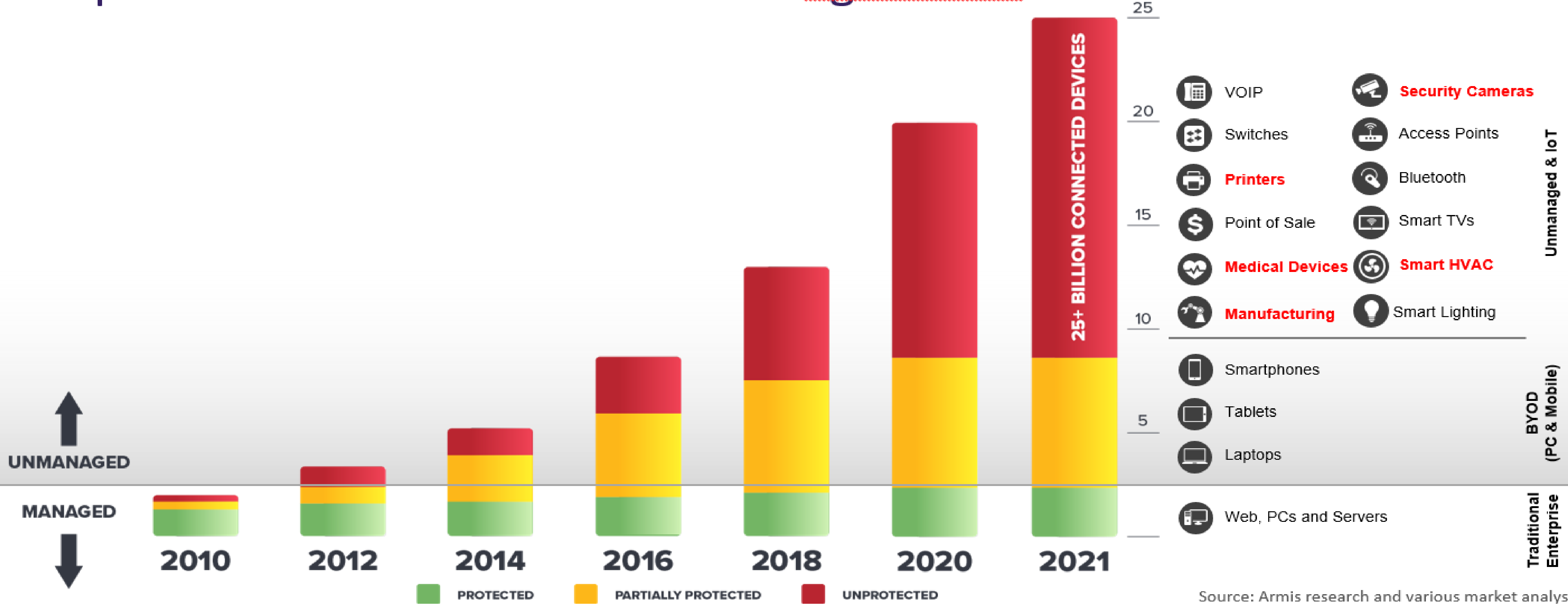
Ondrej, Sramek
Security Consultant

CLICO ARMIS

Security Networking Management

The Traditional Endpoint Security Challenge

Up To 90% of Devices Will Be “Un-agentable”



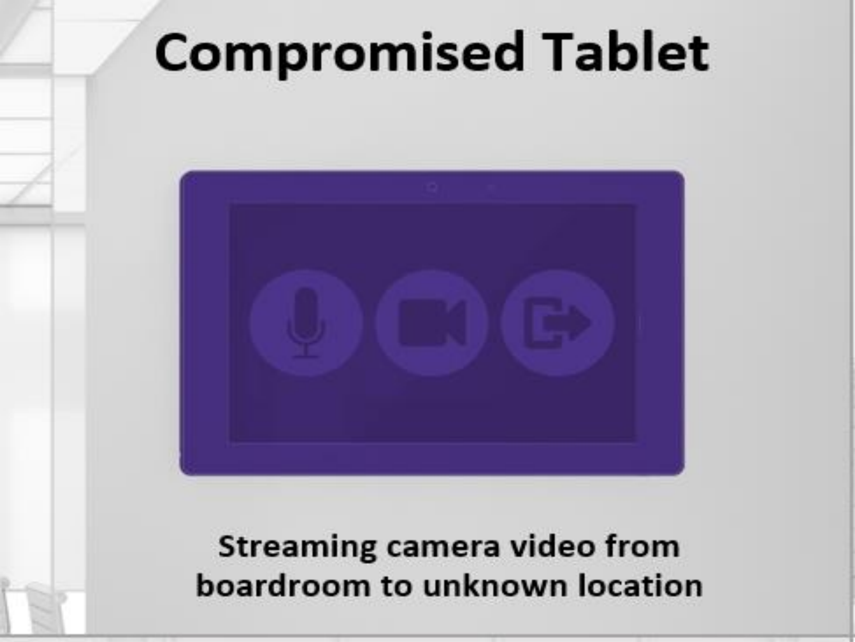
Source: Armis research and various market analysts

CLICO

ARMIS

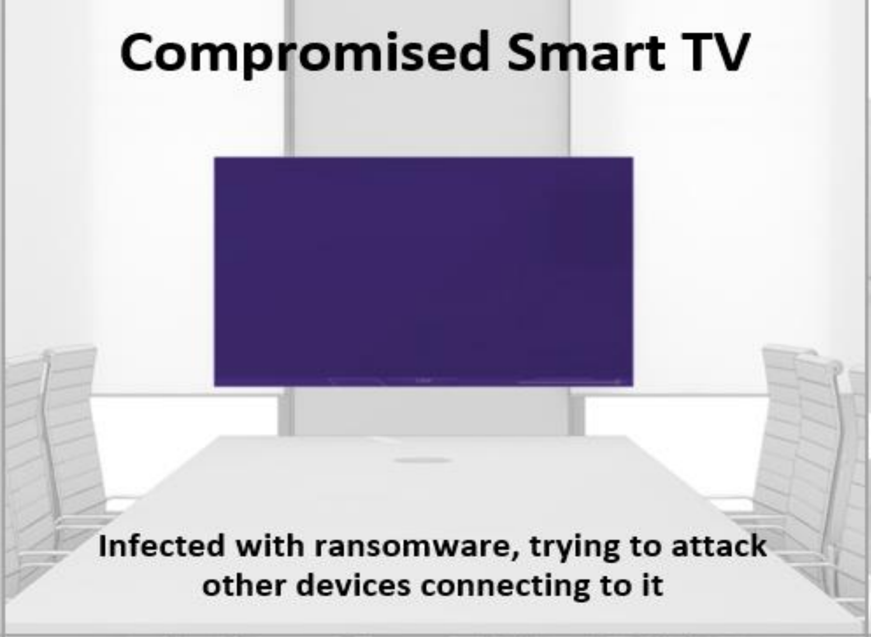
Security Networking Management

Compromised Tablet



Streaming camera video from boardroom to unknown location

Compromised Smart TV



Infected with ransomware, trying to attack other devices connecting to it

Security Camera Botnet

On the network and part of a botnet

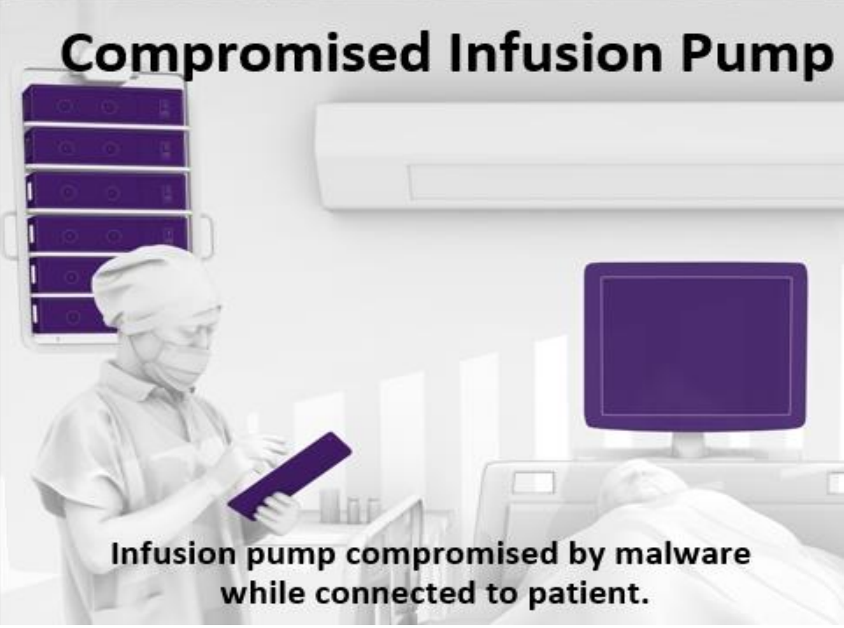
Manufacturing Plant

Production line HMI impacted by ransomware moving laterally through network

Wireless Printer Hotspot

Open hotspot that allows hackers to circumvent network access control

Compromised Infusion Pump



Infusion pump compromised by malware while connected to patient.

ARMIS™

Agentless Device Security Platform

Asset Inventory

- Device identification & classification
- Managed, unmanaged, & IoT
- Populate vulnerability scanners and inventory tools
- Every device across every site (make, model, OS, & more)
- Across every environment and industry

Risk Management

- Passive, real-time continuous vulnerability assessment
- Extensive CVE & compliance databases
- Smart adaptive risk scoring
- Risk-based policies
- Auto-segmentation

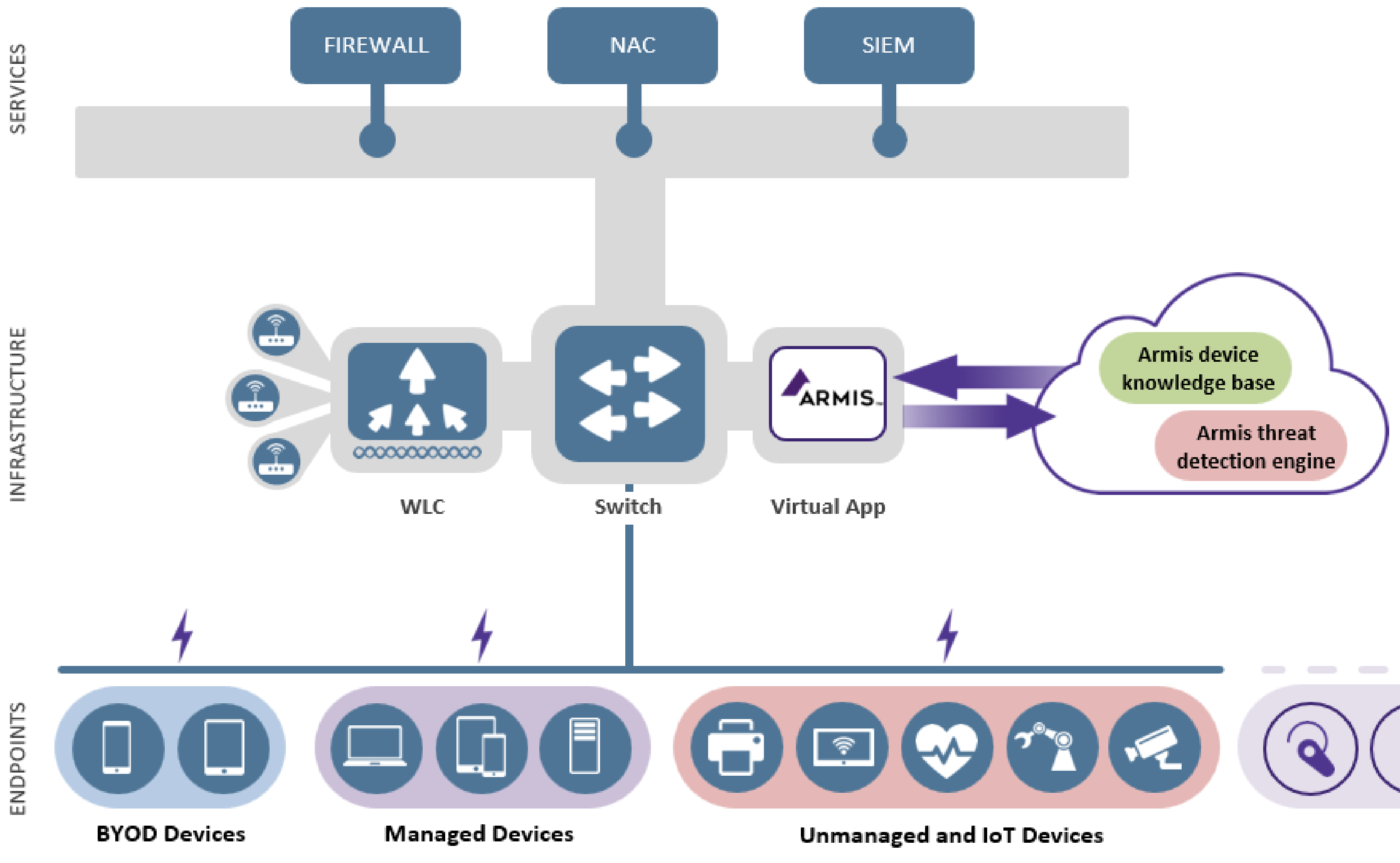
Detection & Response

- Device attribution of activities
- Anomalies based on Device KB
- Automatic policy-based response
- Ability to disconnect or quarantine
- Device context provided to every SOC tool & workflow (SIEM, Ticketing, Firewall, NAC, etc.)

Real-time & Continuous

ORACLE® Mondelēz International Allergan Sysco PerkinElmer MATTRESSFIRM

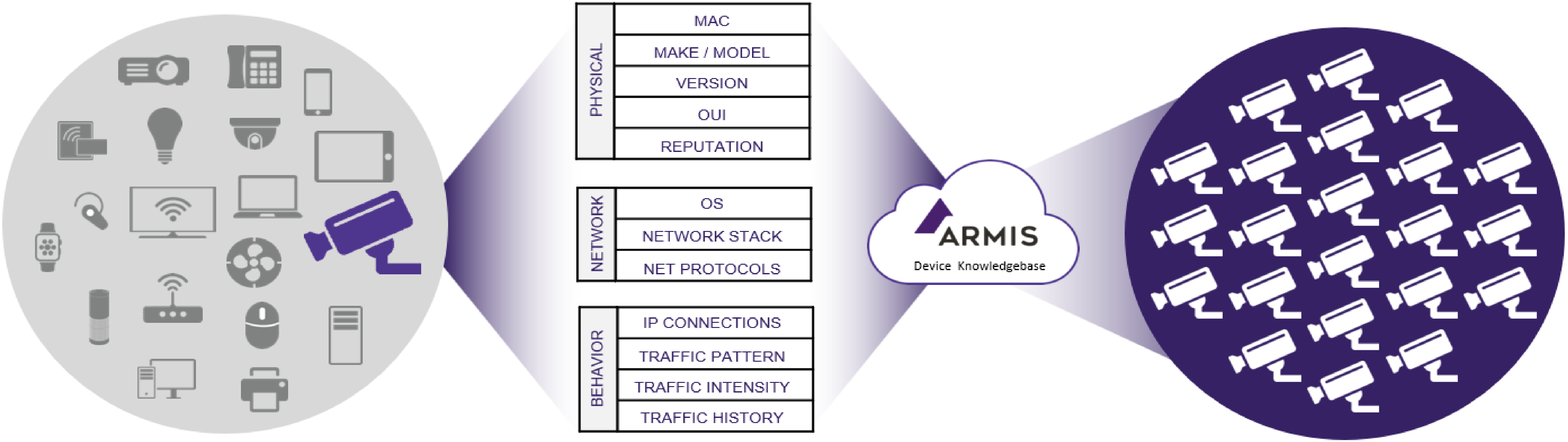
How Armis Works



Frictionless to Deploy

- No agents
- Deploys in minutes to hours
- Integrates into existing security solutions
- No network impact

Agentless Device Identification & Tracking



PHYSICAL

MAC

MAKE / MODEL

VERSION

OUI

REPUTATION

NETWORK

OS

NETWORK STACK

NET PROTOCOLS

BEHAVIOR

IP CONNECTIONS

TRAFFIC PATTERN

TRAFFIC INTENSITY

TRAFFIC HISTORY

Deep Device Visibility

- WLC – Device metadata, connection states, etc.
- AP – Packet traffic, RF signal data
- Switch – Span port or packet capture system (ex: Gigamon)
- Other – Network / security infrastructure (ex: firewall for SYSLOG, rule sets)

Behavioral Attributes

- Physical
- Network
- Behavioral

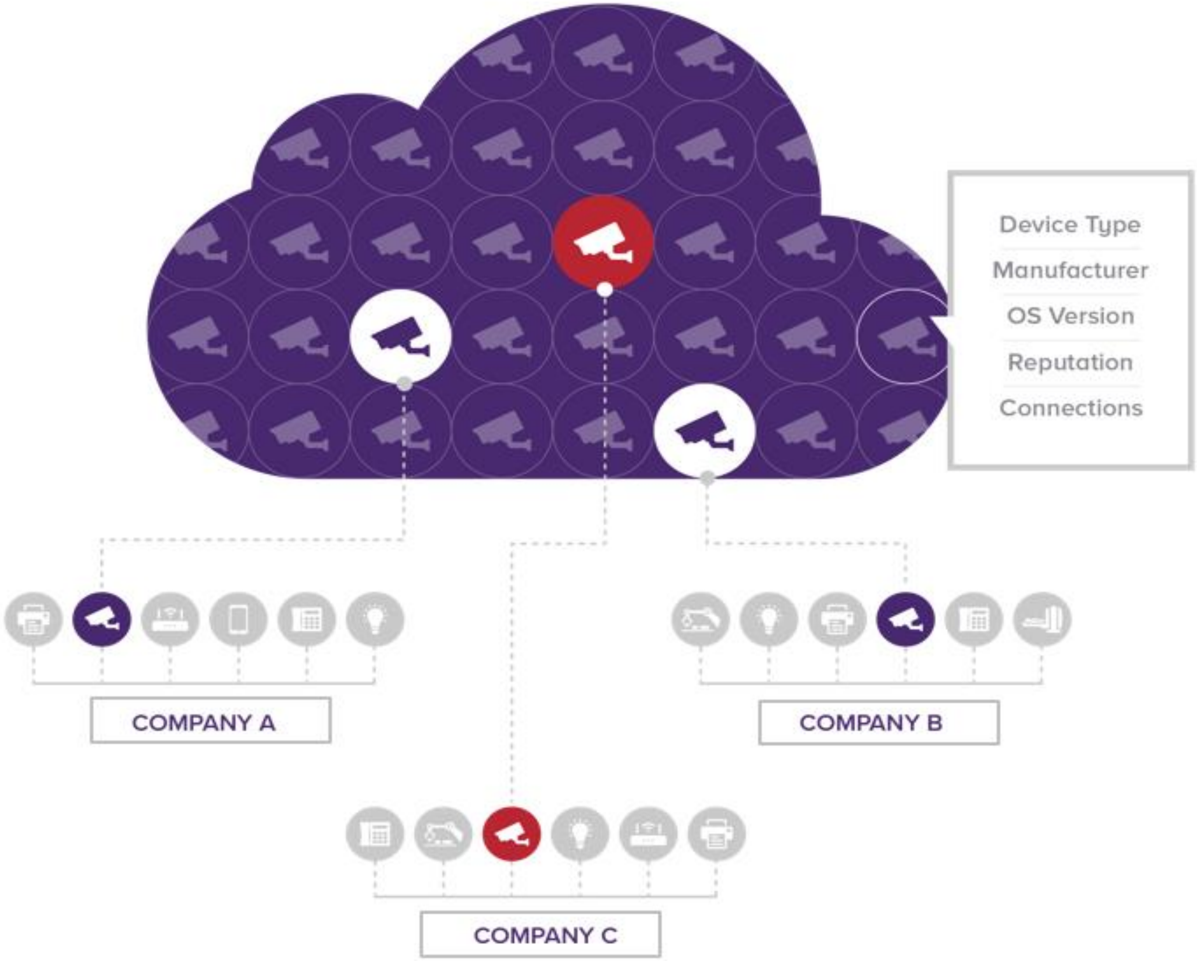
Analyze & Protect

- Tracking 1 500M devices with 35M device profiles
- Compare to class thresholds for ID result
- Enrich with threat intelligence for device risk assessment
- Continuous monitoring for behavioral anomaly detection

CLICO ARMIS

Security Networking Management

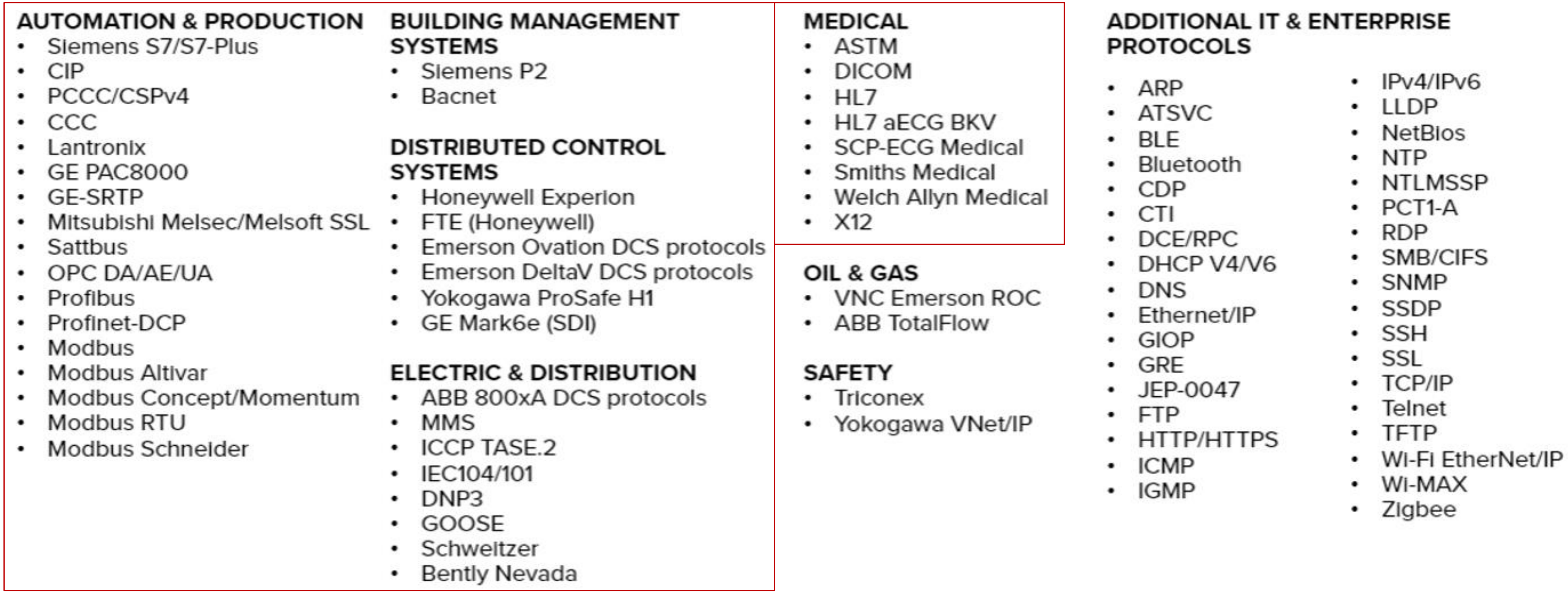
Armis Device Knowledgebase



Context Matters

- ✓ 1 500M+ Devices Tracked (and growing)
- ✓ 35M Device Profiles
- ✓ Largest Cloud-based, crowd sourced, device knowledgebase
- ✓ Compares real-time device behavior to "known-good" baselines
- ✓ Identifies policy violations, misconfigurations, or abnormal behavior
- ✓ Rapid deployment & operationalization

Protocols Supported by Armis



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
- Modbus Altivar
- Modbus Concept/Momentum
- Modbus RTU
- Modbus Schneider

BUILDING MANAGEMENT SYSTEMS

- Siemens P2
- Bacnet

DISTRIBUTED CONTROL SYSTEMS

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

ELECTRIC & DISTRIBUTION

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

MEDICAL

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

OIL & GAS

- VNC Emerson ROC
- ABB TotalFlow

SAFETY

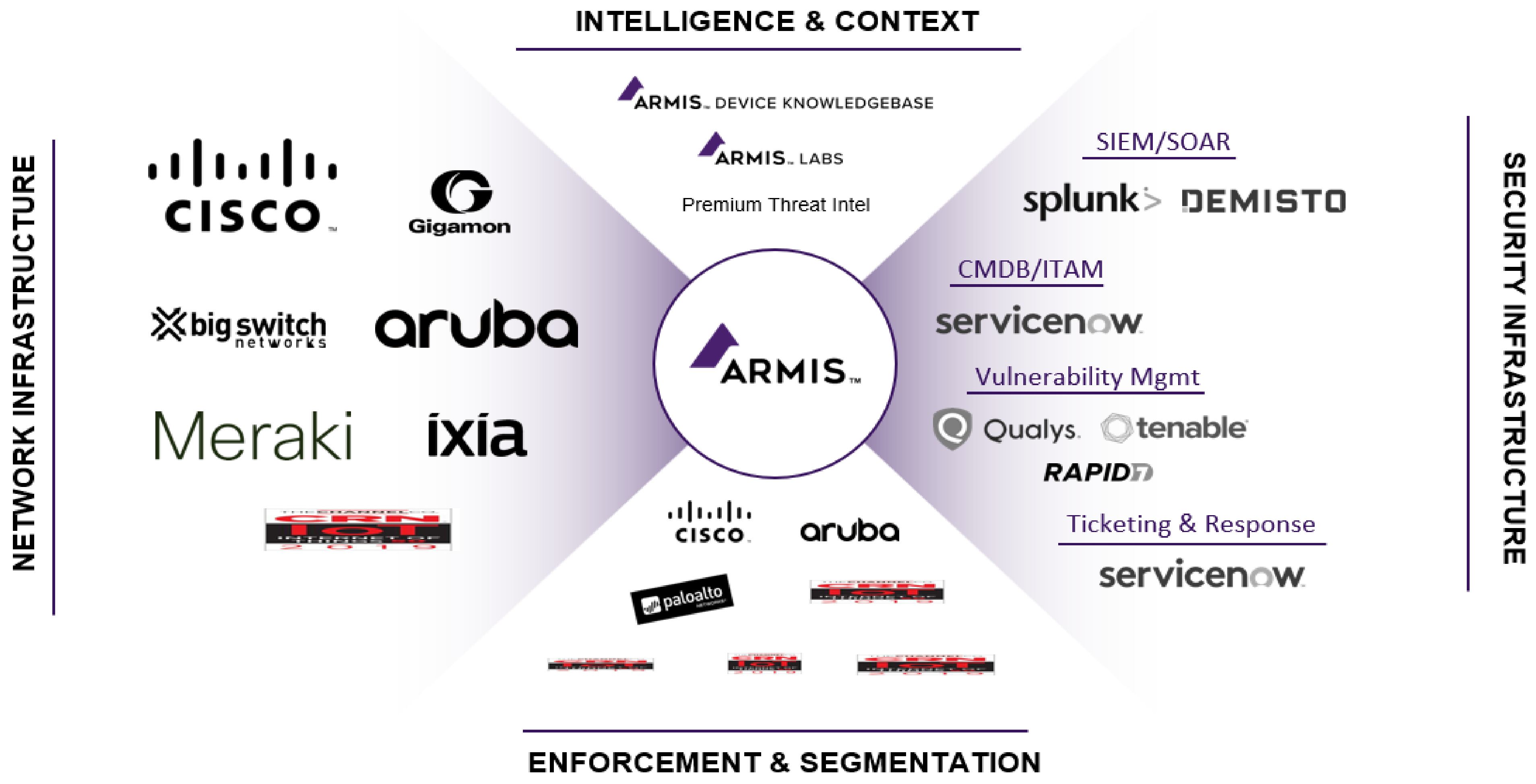
- Triconex
- Yokogawa VNet/IP

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

Security Networking Management

Simple & Easy Integration



INTELLIGENCE & CONTEXT

ARMIS DEVICE KNOWLEDGEBASE

ARMIS LABS

Premium Threat Intel

NETWORK INFRASTRUCTURE

cisco

Gigamon

big switch networks

aruba

Meraki

ixia

ARMIS

SECURITY INFRASTRUCTURE

SIEM/SOAR

splunk>

DEMISTO

CMDB/ITAM

servicenow

Vulnerability Mgmt

Qualys.

tenable

RAPID7

Ticketing & Response

servicenow

cisco

aruba

paloalto NETWORKS

ENFORCEMENT & SEGMENTATION

CLICO

ARMIS

Security Networking Management

DEMONSTRATION

CONTACT
Name: Ondrej Sramek
Mobile: +420 603 227 456
E-mail: ondrej.sramek@clico.cz

www.clico.eu

CLICO ARMIS

Security Networking Management