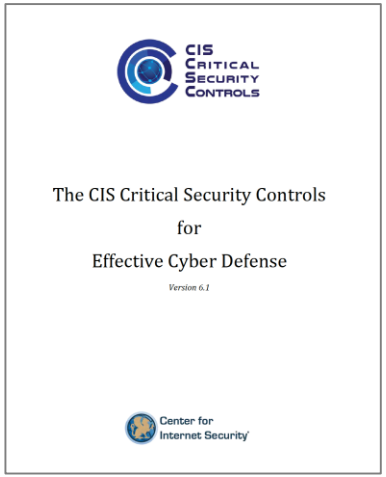
ARMIS SECURITY: “WE ARE THE” MAKE 85% OF YOUR EXISTING SECURITY TOOLS BETTER “COMPANY”

Critical Visibility

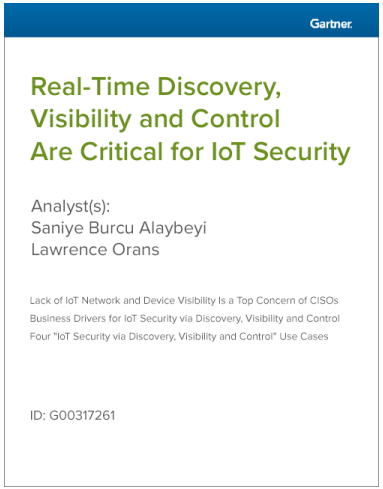
Joel Sible
joel@armis.com
630-803-1319

Discovery Is Critical



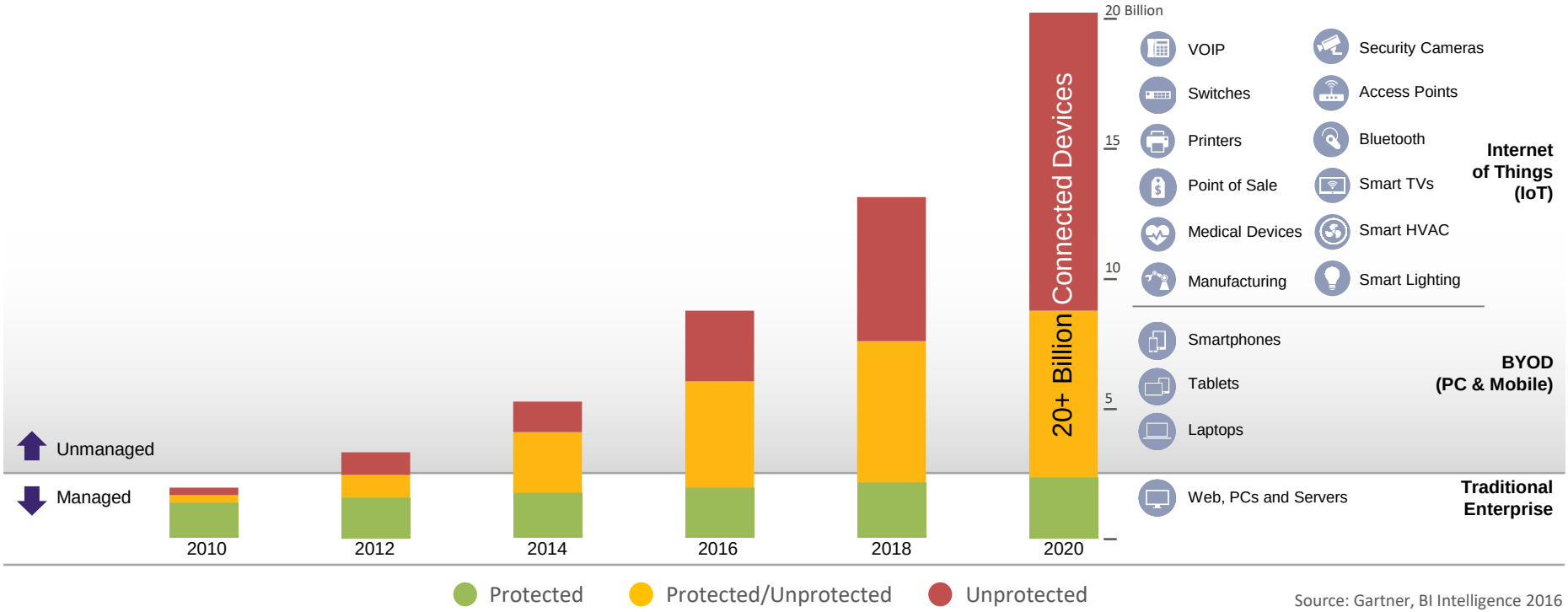
The #1 Recommendation

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



"**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."

Unparalleled Enterprise Visibility



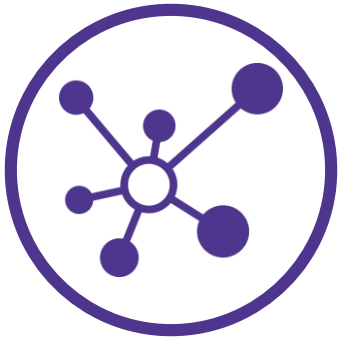
Source: Gartner, BI Intelligence 2016

Key Elements of Armis' Architecture

No Agent

Device Centric

Behavioral Insights



Integrated Solution

Sample – Fortune 1K Company (4K Employees)

1,212 Windows Machines	205 Unmanaged
578 Servers	
1117 Employee Phones	587 Unmanaged
370 Tablets	295 Unmanaged
213 Guest Phones	
60 Smart TVs	5 Previously Unknown
10 Telepresence Systems	
100 Printers	78 Open Hot Spots
500 VoIP Phones	2 Sending Data To Unauthorized IP

80 Switches	
110 APs	21 Unpatched Vulnerabilities
150 Security Cameras	10 Possible Botnet Infections
10 Gaming Consoles	
140 Smart Watches	17 Trying to Connect to other Devices
5 Digital Assistants	4 on Guest Network
25 Smart Thermostats	
20 HVAC Controllers	
2 WiFi Pineapples	Connecting to Multiple Corp Devices

Device Characteristics and Behavior Traits

Basic Device Information

- Device type
- 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

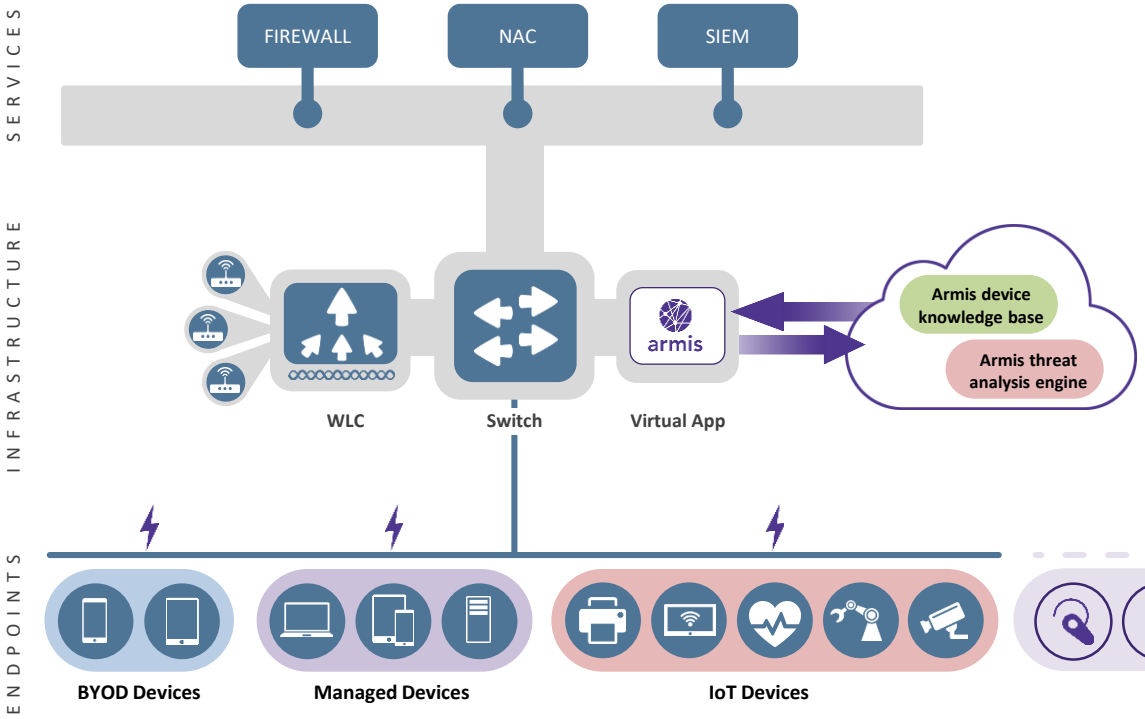
Switch Information

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

Wi-Fi Information

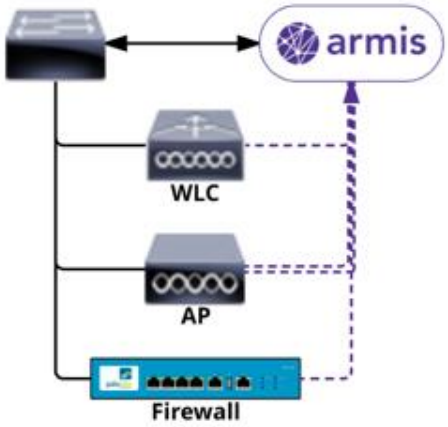
- AP name
- AP CPU utilization
- AP bandwidth utilization
- AP OS version
- AP BIOS version
- AP configuration
- Wi-Fi network name
- Wi-Fi channels used
- Wi-Fi power levels
- Signal levels
- Noise levels
- Jitter

How Armis Works



1. **Discover** and classify all devices – on network, off network, corporate, BYOD, IoT, rogue, Bluetooth, etc.
2. **Analyze** device behavior and compare to baseline for similar device types. Assess risk.
3. **Protect** by triggering WLC, NAC, switch, or firewall to block risky or attacking devices

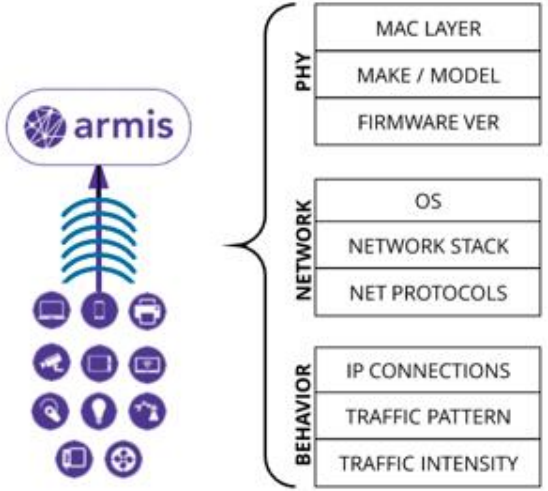
DATA SOURCES



DATA SOURCES:

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

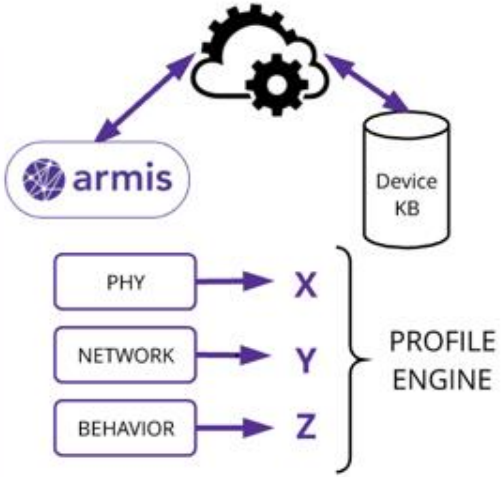
CAPTURE ATTRIBUTES



DEVICE ATTRIBUTES:

- Physical layer
- Network layer
- Connection and traffic behavior

PROFILING ENGINE



ID / MONITORING PROCESS:

- Classify by key attribute groups
- Determine match level
- Compare to class thresholds for ID result
- Continuous monitoring for anomaly detection

6.5 Million Plus Device Profiles

6	Automotive	Car System	Actia
7	Automotive	Car System	Ford Motor Company
8	Automotive	Car System	Harman/Becker Automotive Systems
9	Automotive	Car System	PeopleNet
10	Automotive	Car System	Street Storm
11	Automotive	DashCam	Paragon Technologies Inc.
12	Automotive	DashCam	Pittasoft
13	Automotive	DashCam	Shanghai Xiaoyi Technology
14	Automotive	DashCam	TrendVision Split
15	Automotive	DashCam	YICarCam
16	Automotive	Fleet Management	Rand McNally
17	Automotive	Fleet Management	Teltonika
18	Automotive	Fleet Management	Wistron Neweb Corporation
19	Automotive	GPS	Garmin
20	Automotive	GPS	TomTom
21	Automotive	GPS	Uniden
22	Communication	VOIP	Aastra Telecom
23	Communication	VOIP	ADTRAN
24	Communication	VOIP	Alcatel Internetworking
25	Communication	VOIP	Aruba Instant AP
26	Communication	VOIP	ASCOM

1079	Manufacturing	Robotics	ABB Robotics
1080	Manufacturing	Robotics	Kawasaki Robotics
1081	Manufacturing	Robotics	Omron
1082	Manufacturing	Robotics	Schunk
1083	Manufacturing	Robotics	TM Robotics
1084	Manufacturing	Robotics	YRG Robotics
1085	Medical	Diagnostic	Diazyme
1086	Medical	Diagnostic	Fujifilm
1087	Medical	Diagnostic	GH Healthcare
1088	Medical	Diagnostic	Haag-Streit Diagnostics
1089	Medical	Diagnostic	Siemens Healthineers
1090	Medical	Lab Equipment	Abbott
1091	Medical	Lab Equipment	Panasonic Healthcare
1092	Medical	Lab Equipment	Thermo Fisher Scientific
1093	Medical	Treatment	Insulet
1094	Medical	Treatment	Siemens Healthineers
1095	Medical	Treatment	Terumo
1096	Multimedia	Audio Headset	Adesso
1097	Multimedia	Audio Headset	Aluratek
1098	Multimedia	Audio Headset	Andrea Products
1099	Multimedia	Audio Headset	Apple Computer

8100 Different Attributes (Examples)

Domains

- Which domains it accessing (if public)?
- Are the DNS requests tunnel data?
- How often requests DNS servers?
- How many different private DNS servers requested?
- How many DNS requests without accessing IP after?
- How many public IPs accessed without DNS requests first?
- How many different public IPs accessed?
- How many different private IPs accessed? (What servers the device is contacting on the network?)
- Are there external IPs used for internal purposes?
- Which types of devices are called on private IPs?

Ports / Protocols

- Which ports are used?
- Which protocols are used per port?
- How much data is used per port?
- How many ephemeral ports are used?
- Which ports seem to be open?
- Existing / Used interfaces (WiFI, Bluetooth, etc)
- How frequently is each port used?
- How many different ports are used?

Time of activity

- Data histogram (average data sent per second/minute/hour/day/week/month)
- Activity times by activity type
- Data histogram per network

Headers

- User agents
- Type of encryption
- Cookies
- Extension (X-*) headers
- Method
- Server
- Path

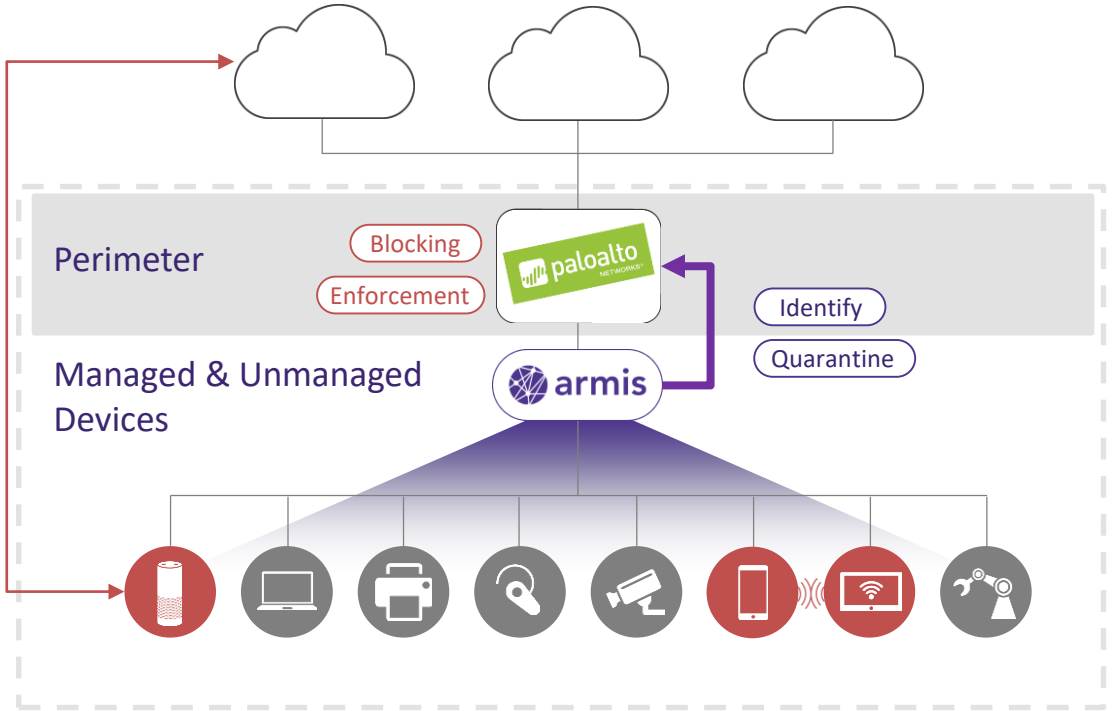
Top 9 Armis Use Cases:

Compromised Devices	Unmanaged Devices	Uncontrolled Networks
 Visibility and Root Cause Analysis	 SLA and performance Monitoring.	 Outside network is bridged to corporate LAN via corporate desktop
 IOT Protocol Discovery	 Enhanced security automation	 Corporate laptops connecting to rogue networks
 BYOD and Guest enablement	 Man in the Middle “MITM” attacks	 Tie in physical security.

Deeper, More Proactive Security

Armis tracks behavior for all devices
- Identifies the device
- Deep behavior profile and history
- Compares to other devices in the network and globally
- Wired and wirelessly

Dynamically enforces at the firewall
- Deny any anomalous behavior
- Feed context to threat engine



THANK YOU