# AGENTLESS DEVICE SECURITY

MAKING THE DIGITAL TRANSFORMATION SAFE FOR THE ENTERPRISE





ARMIS™

# Armis At-A-Glance

**20** FORTUNE 100 Companies (25% of Fortune 50)

**$2B** VALUATION — Brookfield, capitalG, INSIGHT PARTNERS

**165** Countries Covered

**360** Employees

**300** Deployments

**10** Patents Pending

**500M** Devices Tracked

Gartner Cool Vendor 2017

SC 2020 awards finalist — BEST THREAT DETECTION TECHNOLOGY

URGENT/11

Global coordinated security disclosure impacting 500M+ industrial, medical, and enterprise devices.

IoT Evolution Security Excellence 2019

The Channel Co. CRN IoT Internet of Things 50 2019

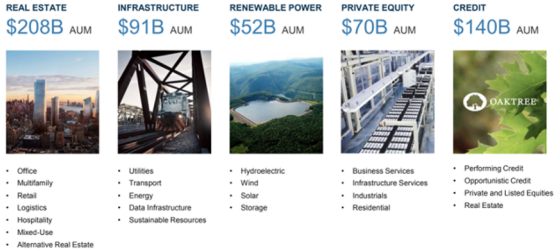
# Brookfield Asset Management Completes Strategic Growth Investment into Armis

*Brookfield Technology Partners' investment alongside Georgian increases funding to over $300M at a $2B valuation, supporting Armis' rapid growth across Real Estate, Power, Infrastructure and Healthcare verticals*

**Brookfield**

## Invested in long-term value

As an alternative asset manager with $600 billion in assets under management and a 120-year heritage as owners and operators, we are invested in long-life, high-quality assets and businesses in more than 30 countries around the world.





Search

Bloomberg

Technology

**Armis Raises Cash at $2 Billion Valuation in Brookfield Deal**

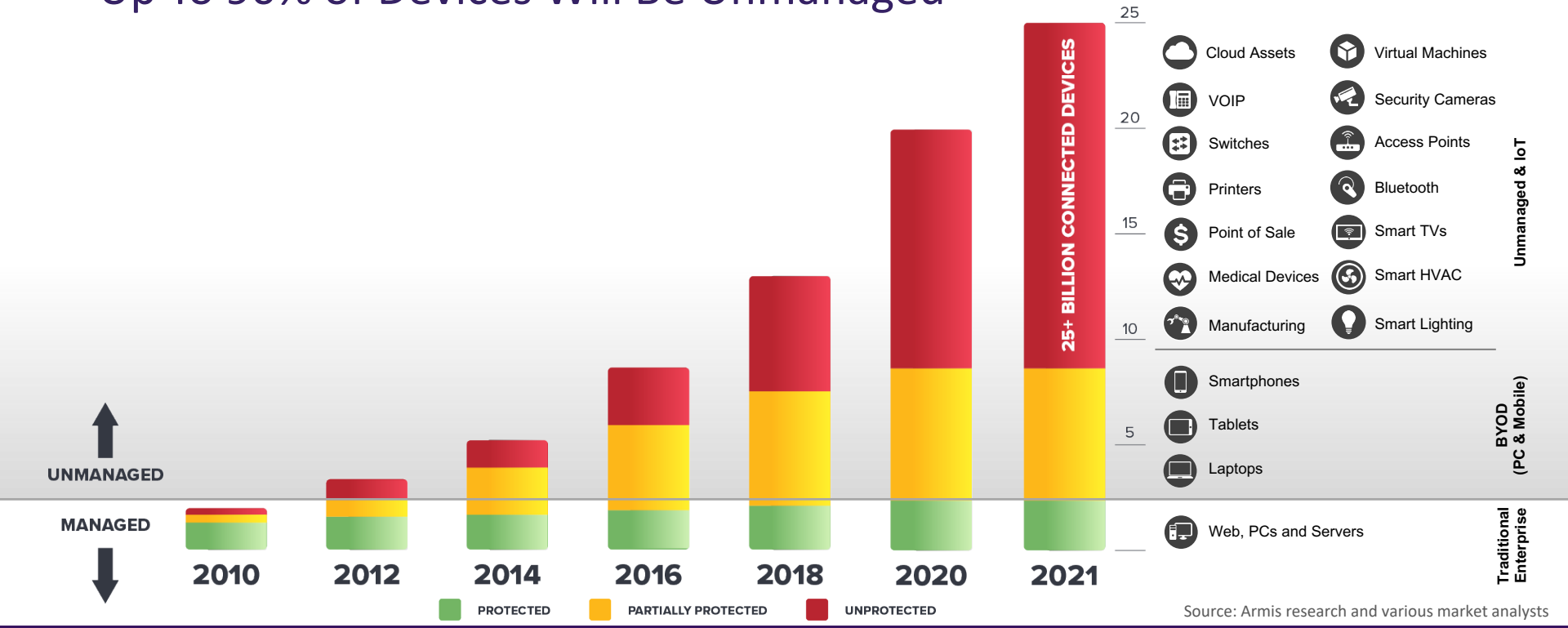
"Armis is an industry leader that offers the most comprehensive and effective security solutions for agentless devices," said Josh Raffaelli, Managing Partner, Brookfield Technology Partners. "Brookfield underwent a thorough yearlong industry evaluation, and it was clear that Armis was the only platform able to serve and scale globally across the vast industries in which we operate whether it be infrastructure, real estate, renewables, healthcare or telecom. We are very excited at the opportunity to partner with Armis at this juncture in their growth trajectory."



ARMIS™

# An Unprecedented Growth In Devices

## Up To 90% of Devices Will Be Unmanaged




Source: Armis research and various market analysts





ARMIS

# This Broke Traditional Security Programs

| Asset Inventory | Network Segmentation | Vulnerability Management | Incident Response |
|---|---|---|---|
| *"I wish I knew what was really on my network. It's manual, timely, and still my IT asset inventory is never right."* | *"Network segmentation is too complicated. I don't have the skills, resources or tools to effectively design, build or maintain it."* | *"Lack of visibility is preventing me from understanding where I am exposed to security risks, let along prioritize or remediate. "* | *"Attackers avoid the controls and monitoring solutions I do have and are attacking things that I don't know how to monitor or protect."* |
| WHY IT BROKE | WHY IT BROKE | WHY IT BROKE | WHY IT BROKE |
| • Agents required<br>• Scanning is disruptive<br>• No visibility<br>• No control<br>• No reporting<br>• Compliance exposure | • Misses peer-to-peer protocols<br>• Infrastructure at risk<br>• Can't see behavior<br>• Can't manage without proper asset identification | • No clear asset inventory<br>• Can't scan<br>• Disrupts devices<br>• Tip over devices<br>• Impacts service or production | • Agents required<br>• No context<br>• No ability to investigate<br>• No automation<br>• No enforcement<br>• Manual & timely |

# Critical Questions

Is my CMDB data clean and accurate?

How many laptops do I have? How many unmanaged devices?

Which endpoints aren't running up-to-date EDR or EPP?


What applications and versions do I have installed across my entire environment?


What device had a specific IP address 2 months ago? Who owns that device?

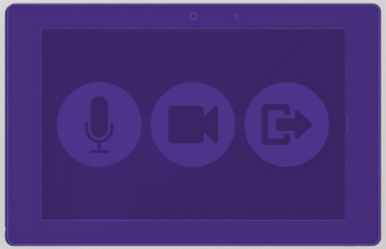
Which devices in my environment are affected by the new vulnerability or security advisory?

How many cloud or virtual assets do I have?

Am I compliant with CIS 1 thru CIS 6?

How many vulnerable assets do I have (by CVE, BU or location)?

## 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

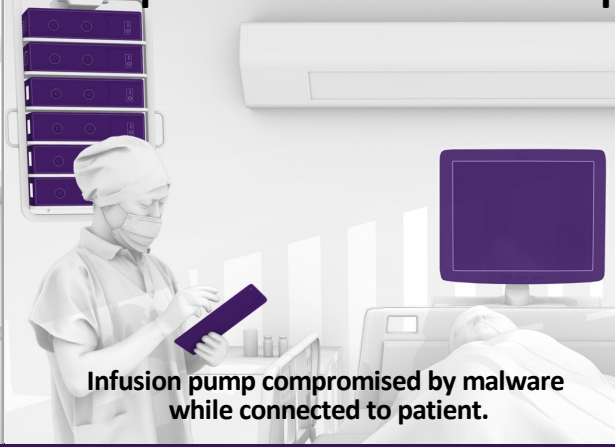
## Manufacturing Plant

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

# What We Have Found – Threats


Human machine interface (HMI) devices were infected with WannaCry.

Vulnerable industrial control devices exposed to the Internet.

Third-party devices opened reverse tunnels, breaching network segmentation.

Employee downloaded manufacturing plans and data to their laptop.

Connection of personal employee devices to the manufacturing network.

# What We Have Found

MRI machine (and others) communicating with Command & Control in Russia.

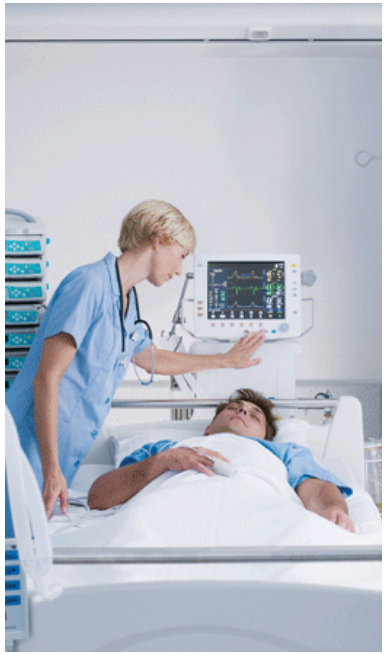
Many WannaCry infected medical devices spreading across a flat open network.

Infusion pump compromised by malware while connected to patient.

Medical crash carts being used to access Facebook, have accessed phishing websites.

X-Ray machines and others sending patient information and diagnosis unencrypted over the internet.

# Healthcare Organization Concerns

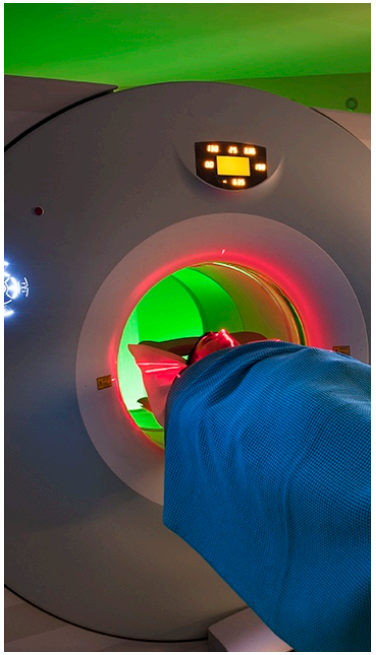


**Patient Safety**
Medical Device Behavior


**Disruption**
Ransomware


**Data Breach**
Personal Health Info


**Inventory**
Locating Medical Devices



**Utilization**
Maximizing Efficiency

# 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

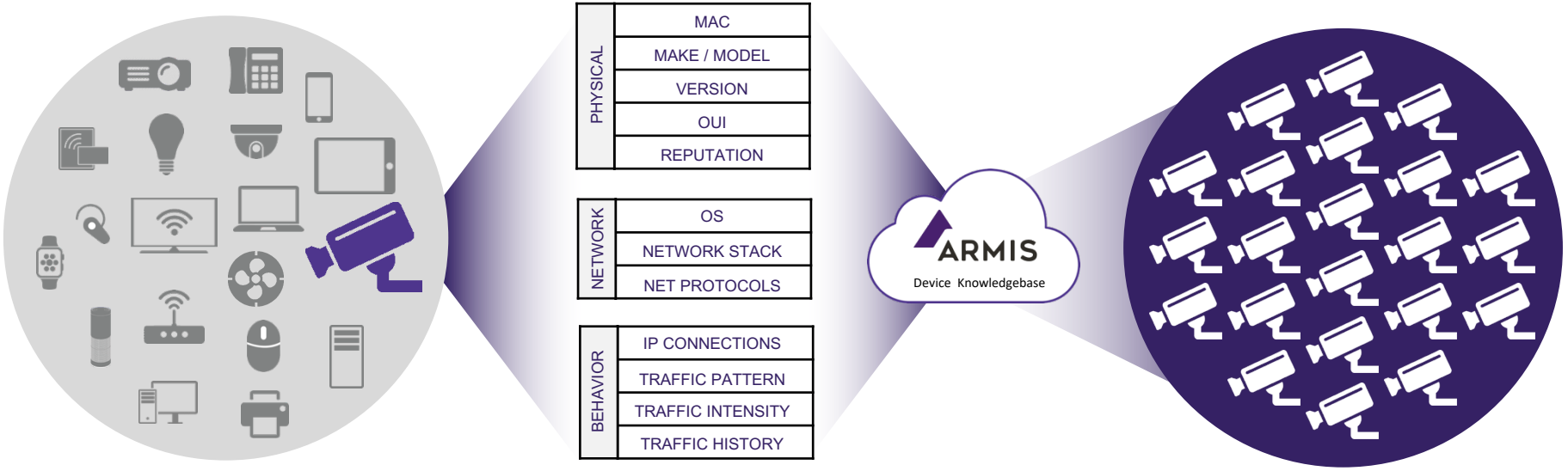
## Detection & Response

- 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

# Agentless Device Identification & Tracking




## 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)

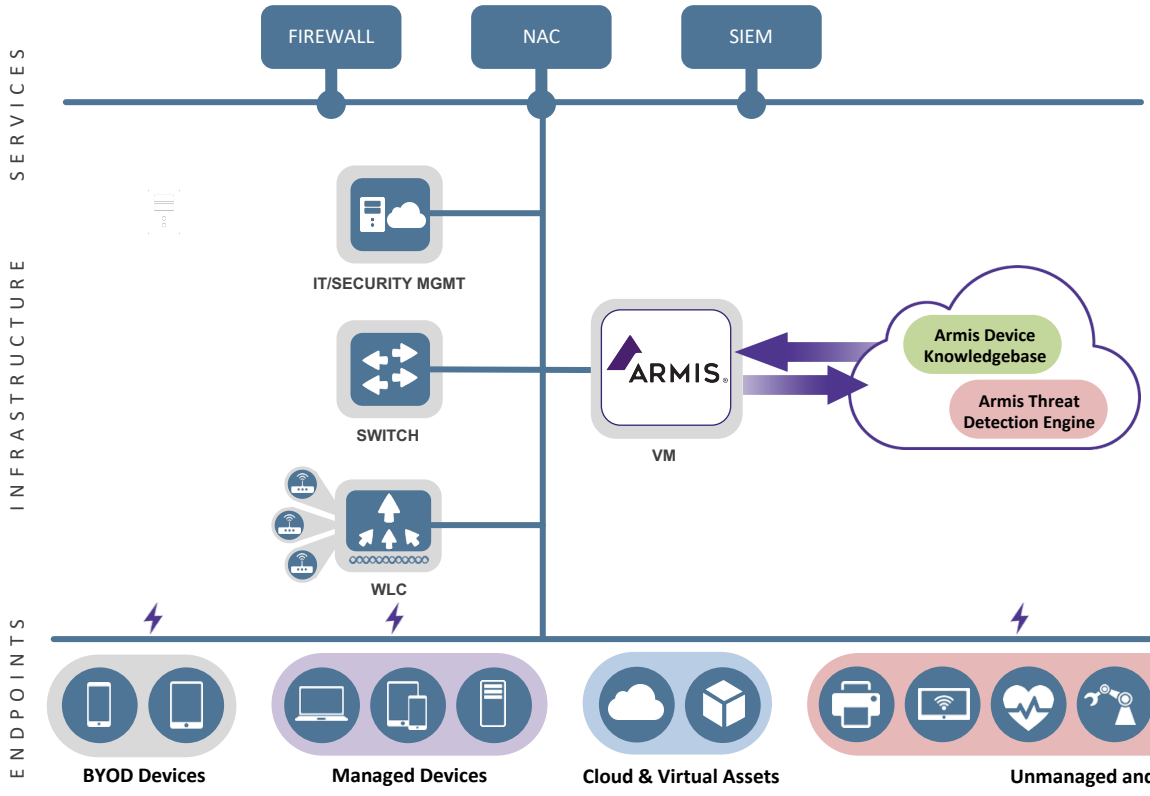
## Behavioral Attributes

- Physical
- Network
- Behavioral

## Analyze & Protect

- Tracking 500M devices with 15M device profiles
- Compare to class thresholds for ID result
- Enrich with threat intelligence for device risk assessment
- Continuous monitoring for behavioral anomaly detection

# How Armis Deploys



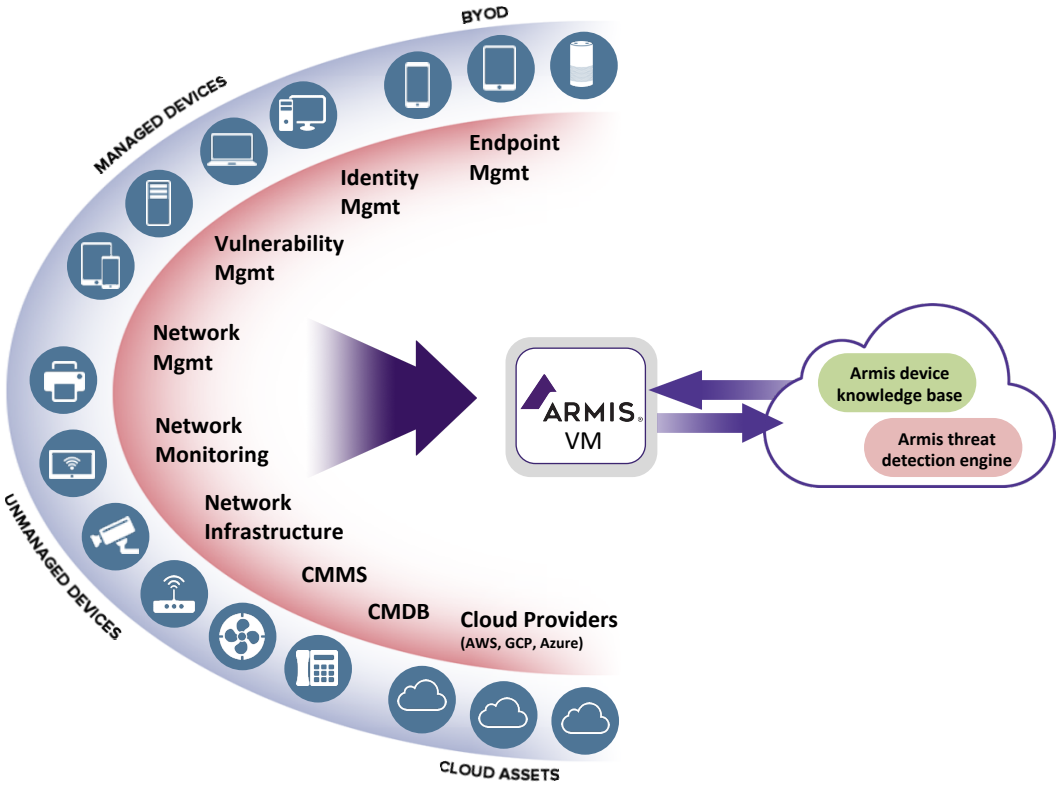

**Deploys in Minutes**

- VM
- SaaS Cloud Backend

**Extensible Visibility:**

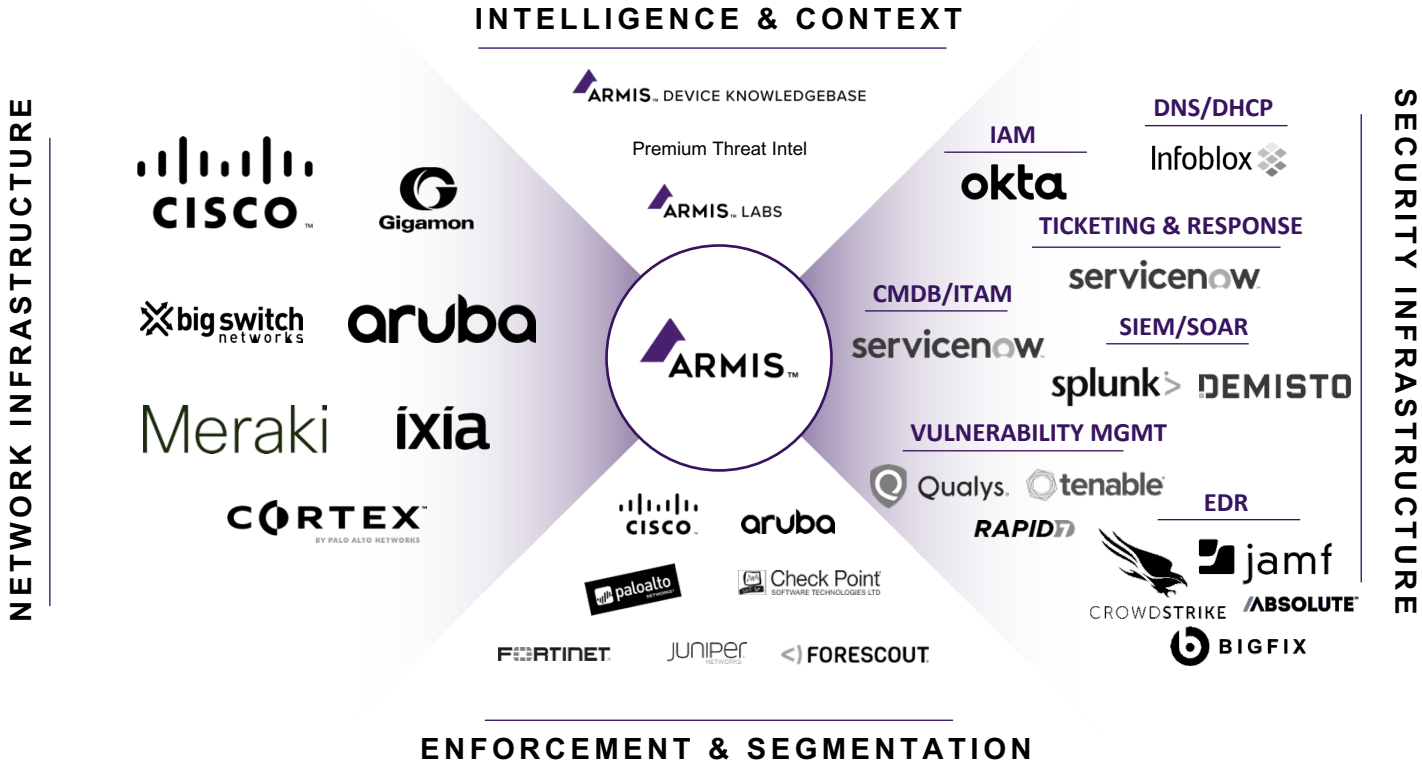
- Connect to IT Management Tools
- Connect to Security Tools
- Connect to Network Infrastructure

# How Armis Does It




1. **Discover** devices via hundreds of different security and network tools to extract data, no agents, no appliances.
2. **Identify** and classify every device, on-prem and off-prem, on network and cloud, along with risk, vulnerabilities and behavior.
3. **Automate** through orchestration, automation, and policy across the entire global environment from one place.

# Simple & Easy Integration



# THANK YOU