See-All to Secure-All

Complete unified asset visibility made simple

April 2022

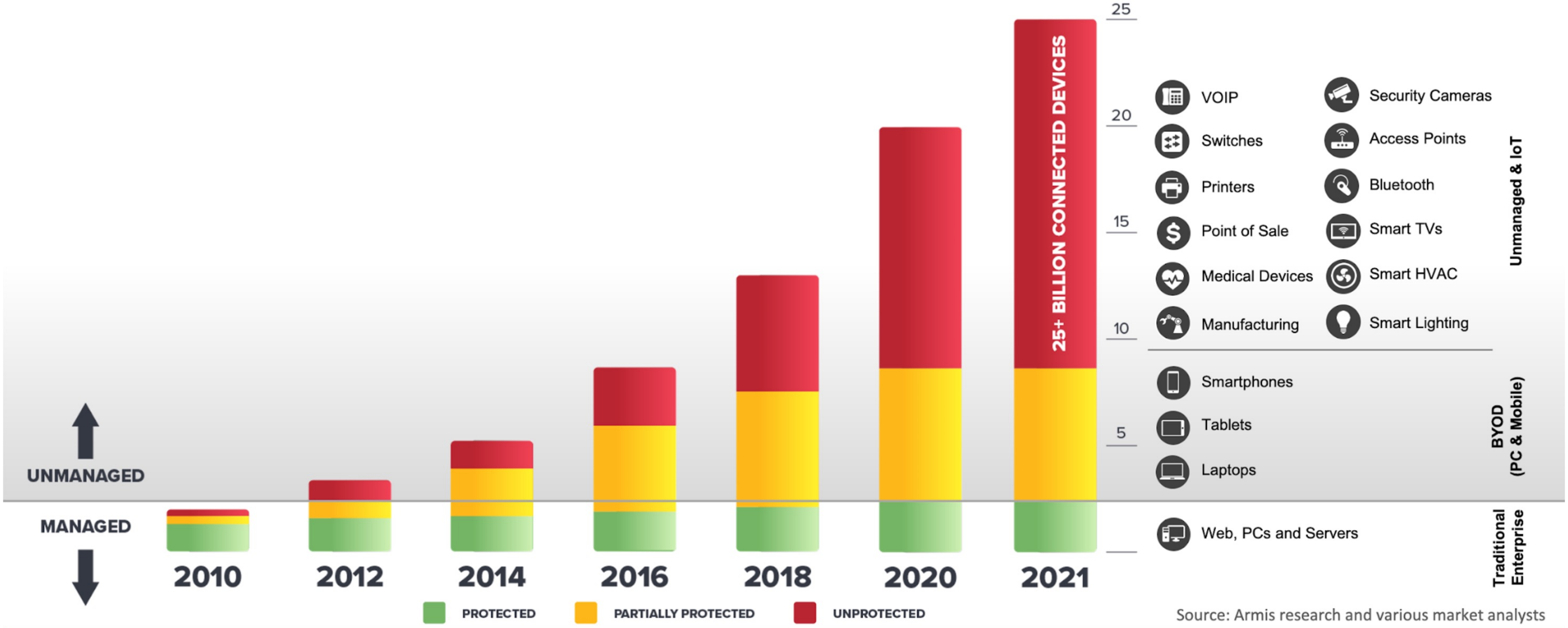
Agenda

- Armis’ Understanding of DoD’s Current Environment
- Current Trends & Their Likely Impact on DoD’s Environment Going Forward
- Thoughts on the Future
- Who is Armis?
- Armis Platform Discussion
- Armis Platform Demonstration
- Next Steps Discussion

Our Understanding of the Current DoD Situation

- **Huge, Complex, Global IT Environment**
- **Distributed & inconsistent visibility and control of IT assets within & across organizations**
- **Devices and users are and will still be a major and evolving attack vector**
- **Growing demand signal for advanced technologies (IOT, robotics, AI/ML, cloud, mobility, etc.)**
- **Historically siloed solutions, DoD staffing challenges, contractor expense**
  (ex. ACAS, C2C, HBSS, CSAAC, JRSS, Thunderdome, GSM-O, DES/4ENO, JWCC, etc.)
- **Evolving DCO C2 Authorities and Capabilities**

Explosive Growth …..



Source: Armis research and various market analysts

Improving the Current DoD Situation Will Require

- **Passive and agentless total asset discovery for…**
  all IT, IOT, ICS; on-prem & cloud; managed & unmanaged assets; wired & wireless networks

- **Continuous asset identification, behavioral mapping, & operational risk assessment**
  Leveraging cloud/AI

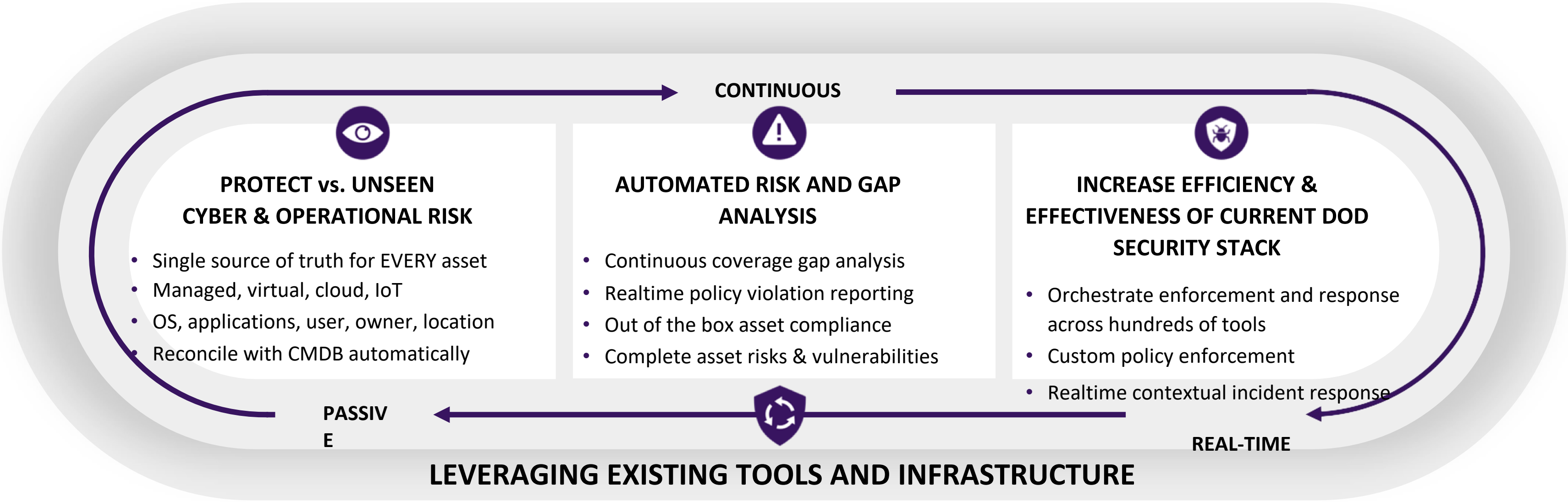
- **Integration w/DoD current security stack for automated CAO enforcement/response**
  (C2C, SIEM 2.0, ACAS, ESS, Zero Trust, etc.)

- **Complete, universal, role-based Cyber Situational Awareness across all echelons**
  Organizational, Geographic, Asset Category, User, etc

Who is Armis?

- Founded in 2015
- Mission: Help enterprises protect themselves against unseen cyber and operational risk from: *unmanaged devices, under-managed devices, IT, IOT, ICS, on-premise & cloud, wired & wireless*
- A US owned and operated entity, headquartered in Palo Alto, California
- In use by over 40% of Fortune 100 companies
- Unique consumption & pricing model: NOT # of devices, rather number of employees or sites
- Armis Federal LLC created in 2021
- Available via Federal BIC GWACs such as GSA Schedule, NASA SEWP, CDM APL
- Sponsored and enroute to FedRAMP Moderate and DoD IL4 certification in 2022

ARMIS



CONTINUOUS

PROTECT vs. UNSEEN CYBER & OPERATIONAL RISK

- Single source of truth for EVERY asset
- Managed, virtual, cloud, IoT
- OS, applications, user, owner, location
- Reconcile with CMDB automatically

AUTOMATED RISK AND GAP ANALYSIS

- Continuous coverage gap analysis
- Realtime policy violation reporting
- Out of the box asset compliance
- Complete asset risks & vulnerabilities

INCREASE EFFICIENCY & EFFECTIVENESS OF CURRENT DOD SECURITY STACK

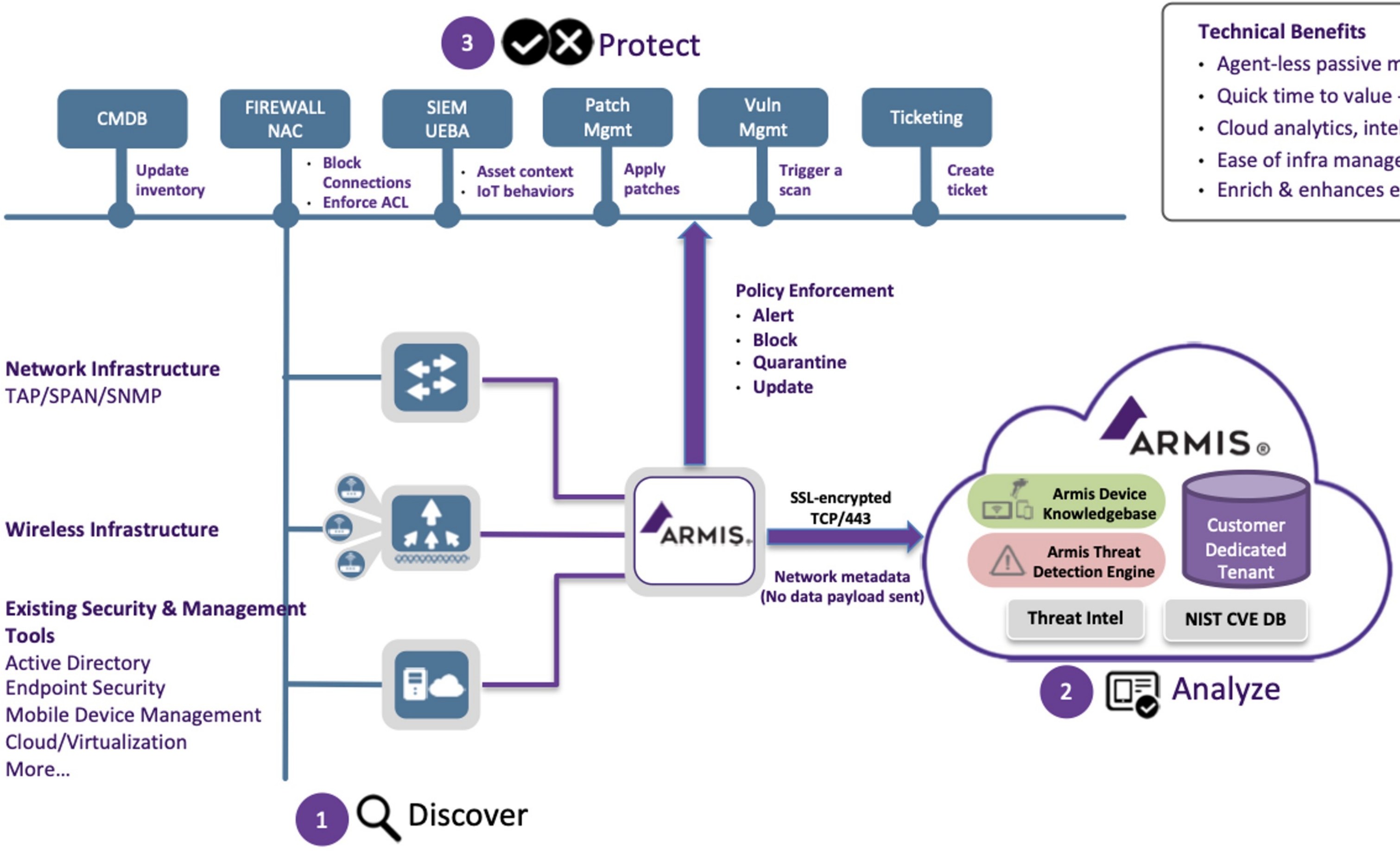
- Orchestrate enforcement and response across hundreds of tools
- Custom policy enforcement
- Realtime contextual incident response

PASSIVE

REAL-TIME

LEVERAGING EXISTING TOOLS AND INFRASTRUCTURE

ORACLE DocuSign Mondelēz International flex Allergan Sysco THE HOME DEPOT CLEARENT INTELLIGENT PROCESSING PerkinElmer MATTRESSFIRM



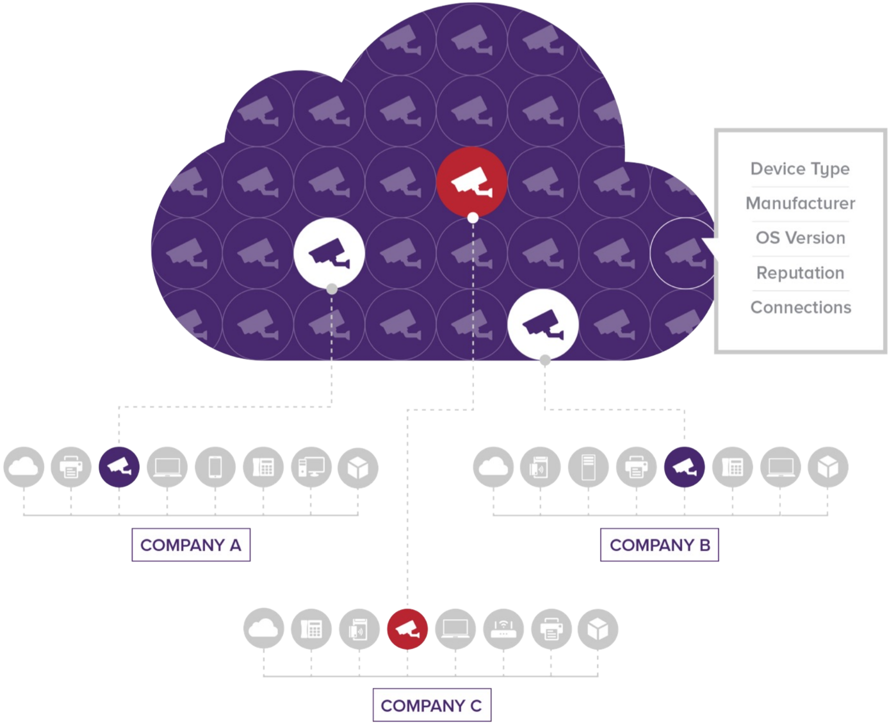
Technical Benefits

- Agent-less passive monitoring
- Quick time to value - deploys in minutes
- Cloud analytics, intelligence and elasticity
- Ease of infra management
- Enrich & enhances existing tools

Armis Cloud

- > 2B devices tracked
- > 16M device behavior profiles
- Continuous anomaly monitoring
- Known-good baselines
- CVE info correlated
- Multiple threat intelligence
- > 100 protocols supported

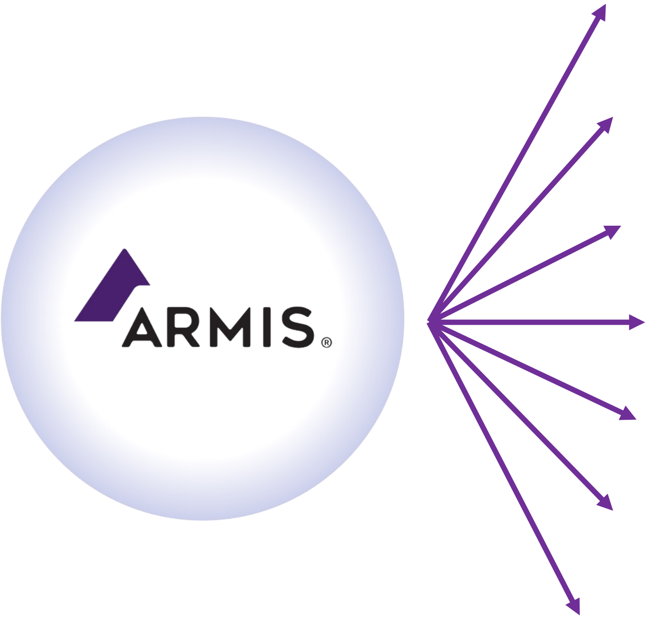
Asset Intelligence and Context



Armis Asset Knowledgebase

- ✓ 2B+ devices tracked in all clients combined (and growing)
- ✓ Largest cloud-based, crowd sourced, asset intelligence
- ✓ Enriches the asset insights with even more sources of intelligence and risk data
- ✓ Automatically identifies policy violations, misconfigurations, vulnerabilities, abnormal behavior
- ✓ One console - configure once, connect everywhere
- ✓ Armis asset intelligence is much more than the sum of its data sources

Actions & Orchestrations



Alert	Internal Armis alerts, or integration with SIEM, email, Splunk, QRadar, and others
Create Ticket	ServiceNow, Jira, Remedy, etc.
Trigger Scan	Such as tenable.io, Qualys
Push Asset Info	CMDBs, SIEM and SOAR tools
Enforce Devices	Block/allow using NACs, firewalls, EDLs, switch, ACLs
Tag Devices	Label devices for multi-dimensional logical segmentation
Patch Devices	Integration with patch management systems

Next Steps for Consideration

- Deeper technical demonstration (one hour)

  Armis’ Support for C2C; Support for ZTN; Support for Thunderdome

- Hands-on Test Drive, virtual or in-person (four hours)

- No-cost proof of concept in DoD environment (one day to 3 weeks)

THANK YOU

Tom Conway
Director, Business Development - FSIs
(M) 703.801.0752
tom.conway@armis.com

Case Studies

Case Study – Global Health Care Provider, 10,000+ sites

*“CMDB was worthless and there was **no way to gain complete visibility** to the entire distributed environment of over **10,000 sites**, let alone discover rogue devices or non-compliant assets.*

***Other solutions required appliances, agents, or a costly years long deployment** across this challenging environment.”*

ARMIS

- **Deployed within an hour**
- **See every asset** in every location
- **CMDB** is now up to date

- **Prioritize risks**
- Set **compliance actions** with a click
- **Automate responses** for millions of assets

Case Study – Large US retailer, 2,000+ stores

MISSED

*“Our **vulnerability scanner would miss around 40% of scannable assets** in every weekly scan… And these are just the assets we know about.*

*The **vendor asked us to install agents for continuous vulnerability scanning**, which is costly and impractical for many devices and environments.”*

ARMIS

- Automated **smart scanning for devices** as they join the network
- Increased vulnerability **scanner coverage to 95%**
- **Reducing manual operations** immeasurably