Wie Unternehmen die Widerstandsfähigkeit ihrer Infrastruktur mit der Armis Asset Intelligence Plattform erhöhen

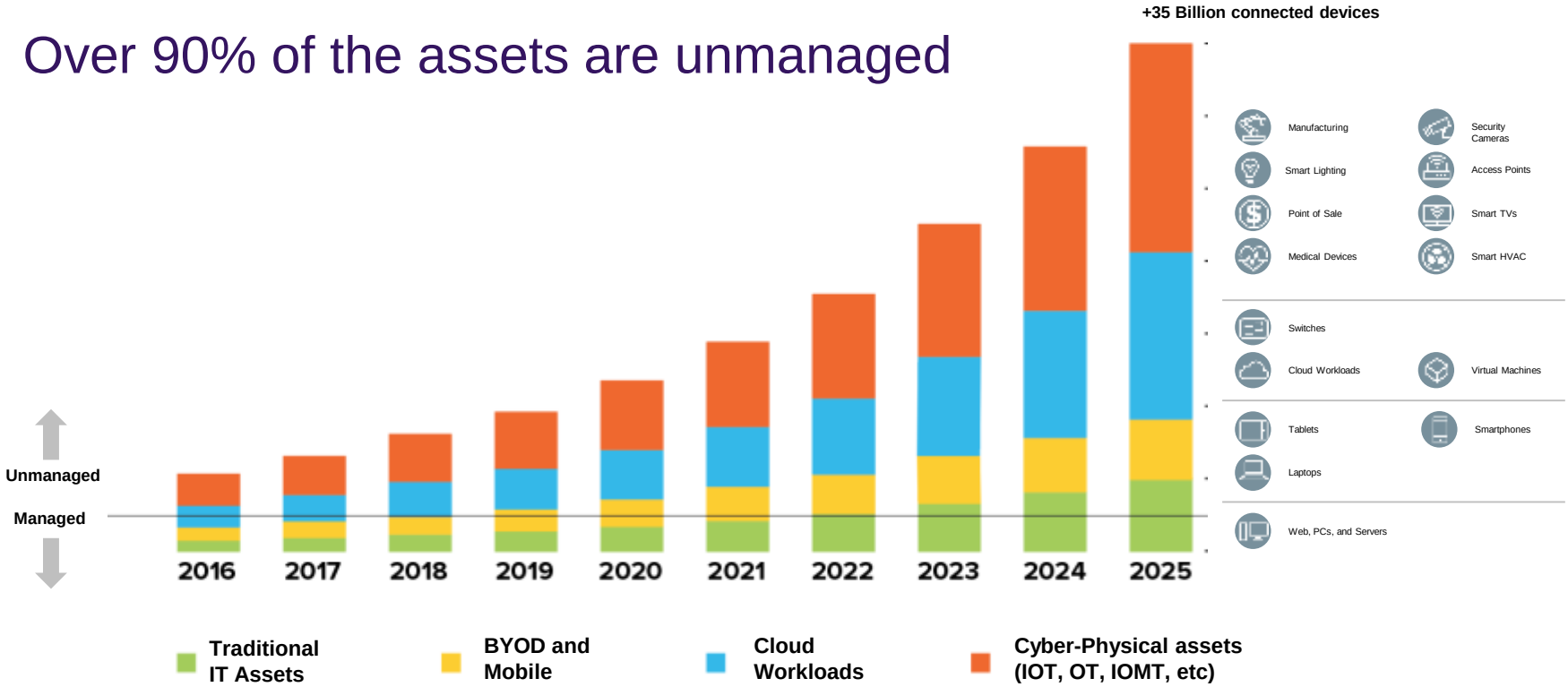
Mirko Bülles
Director TAM

it-sa

ARMIS.

Unprecedented Growth in Assets

Over 90% of the assets are unmanaged



Devices and Things Are Everywhere

- **No Perimeter.**
  Assets are everywhere (on the network, in the cloud, WFH)
- **No single source of truth**.
  Asset information is fragmented across tools.
- **No Control.**
  Policy management across too many tools means **no policy at all**.

ARMIS

Data-Driven Decisions in OT

Convergence is delivering competitive advantages

ARMIS

Critical Questions Companies should be able to answer

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

Is my CMDB data clean and accurate?

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

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

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

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

How many cloud or virtual assets do I have?

Do my devices have encryption hard drive enabled?

How to Remediate and Enforce Policies?

ARMIS

What does **Armis** do and what problems does it solve?

There are **three key areas** which answer these questions.

Agentless Device Security Platform

Discover All Assets

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

Agentless Device Security Platform

Discover All Assets

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

Identify Risks/Gaps

- Risks & vulnerability identification
- Extensive CVE & compliance databases
- Smart adaptive risk scoring
- Risk-based policy violations
- Configuration errors
- Compromised credentials

ARMIS®

Agentless Device Security Platform

Discover All Assets

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

Identify Risks/Gaps

- Risks & vulnerability identification
- Extensive CVE & compliance databases
- Smart adaptive risk scoring
- Risk-based policy violations
- Configuration errors
- Compromised credentials

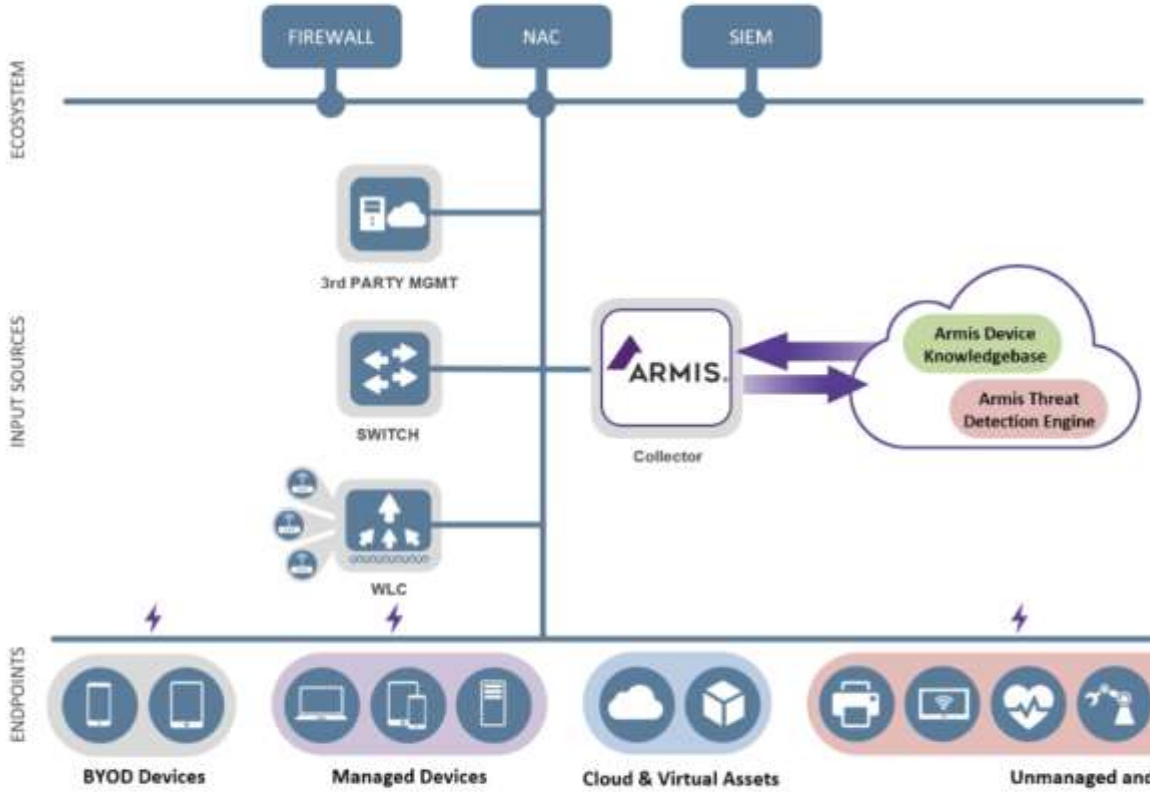
Automate Enforcement

- Active threat & remediation
- Device behaivior anomalies
- Malware, ransomware or exploits
- Security policy violations
- Anomalous communications
- Decive context provided to every SOC tool & workflow (SIEM, Ticketing, Firewall, NAC, etc.)

Passive • Real-time • Continous

ARMIS

How **Armis** Works



Deploys in Minutes

- VM
- SaaS Cloud Backend

Extensible Visibility:

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

Packets on the wire

Packets over the air

Anything that is third-party related

The real value of **Armis** is amplified by taking that information and making it **available to the rest of your technology stack enhancing their capabilities.**

VIELEN DANK

Mirko Bülles
Director TAM

https://www.linkedin.com/in/mirkobulles/