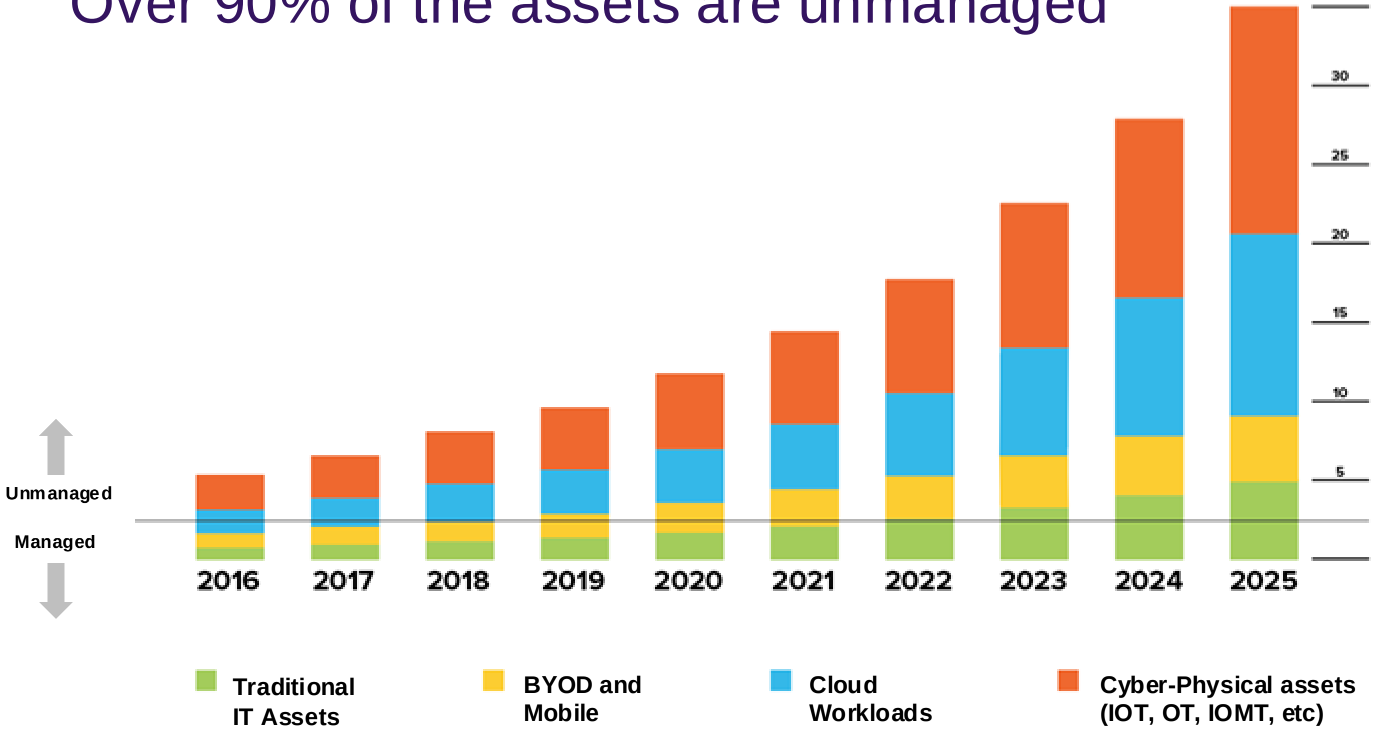
Out of Sight, Out of Control: Asset Intelligence

October 4th, 2024

Michael A. Atkinson, SE Manager, SLED

Unprecedented Growth in Assets

Over 90% of the assets are unmanaged



+35 Billion connected IOT devices

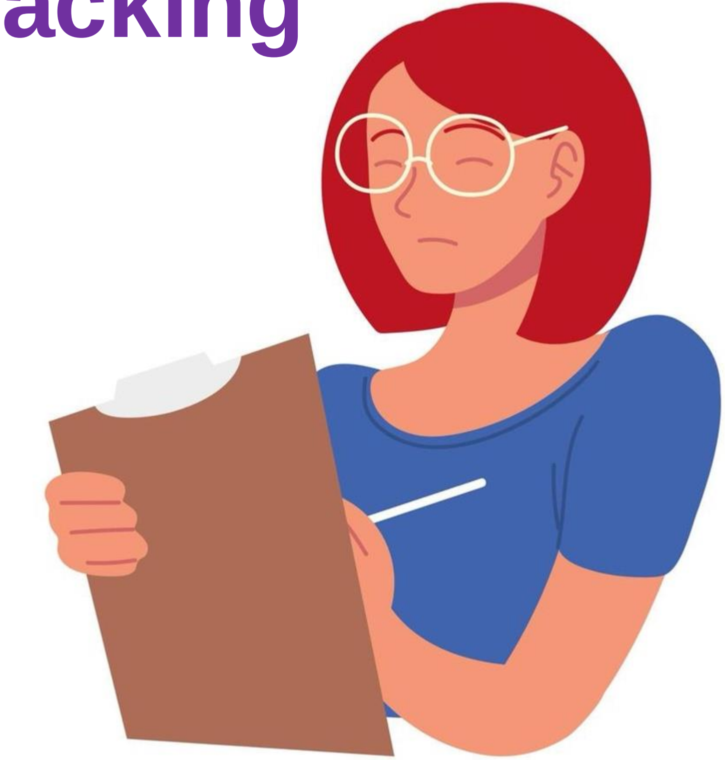
- Cloud Assets
- Virtual Machines
- VOIP
- Security Cameras
- Switches
- Access Points
- Point of Sale
- Smart TVs
- Medical Devices
- Smart HVAC
- Manufacturing
- Smart Lighting

- Smartphones
- Tablets
- Laptops

- Web, PCs, and Servers

Old School IT Asset Tracking

- In the past, a highly manual process
- Spreadsheets and stickers were primary tools
- Keeping this information up to date took a lot of human effort
- Hardware and software were tracked separately

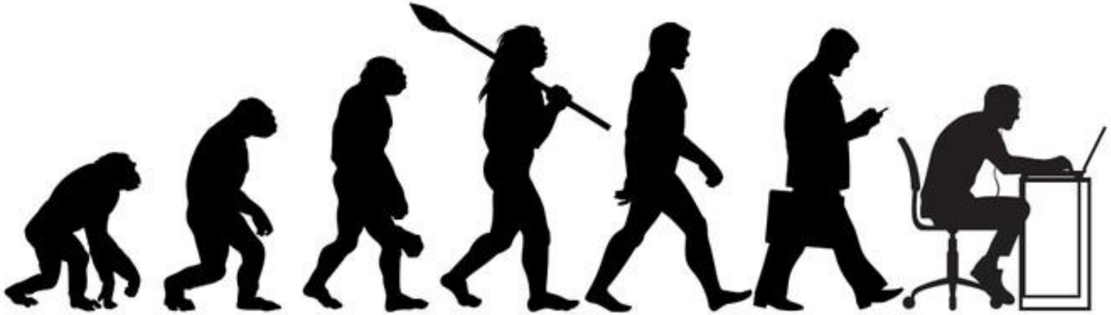


Why We Bothered

- Business managers needed to know where assets were
- Cost tracking, depreciation, finding unauthorized devices (“shadow IT”) were all important
- Software licensing drove these manual efforts to new heights

How It Evolved

- Software license tracking became its own industry
- Configuration Management Databases (“CMDBs”) were populated via multiple manual processes, often by the helpdesk team



Asset Visibility and Control is an **Unsolved** Challenge.

> “I wish I knew what was really used by my organization. I’ve got thousands of assets, on-prem and in the cloud, but my processes are still manual, my data is old, and my IT inventory is never right.”

CIO
Fortune 500 Tech Company

90%

of IT professionals say rapidly-changing environments make ITAM more difficult.

Source: Deloitte Global ITAM Survey, 2021

Visibility and Control Challenges

Accurate and Complete Asset Inventory

Promote IT Hygiene and Remove Technical Debt

Control and Reduce the Asset Attack Surface

Manage Asset Vulnerabilities and Prioritize by Risk

Detect & Mitigate Assets Impacted by Threats

Compliance w/ Internal Policies and Industry Standards

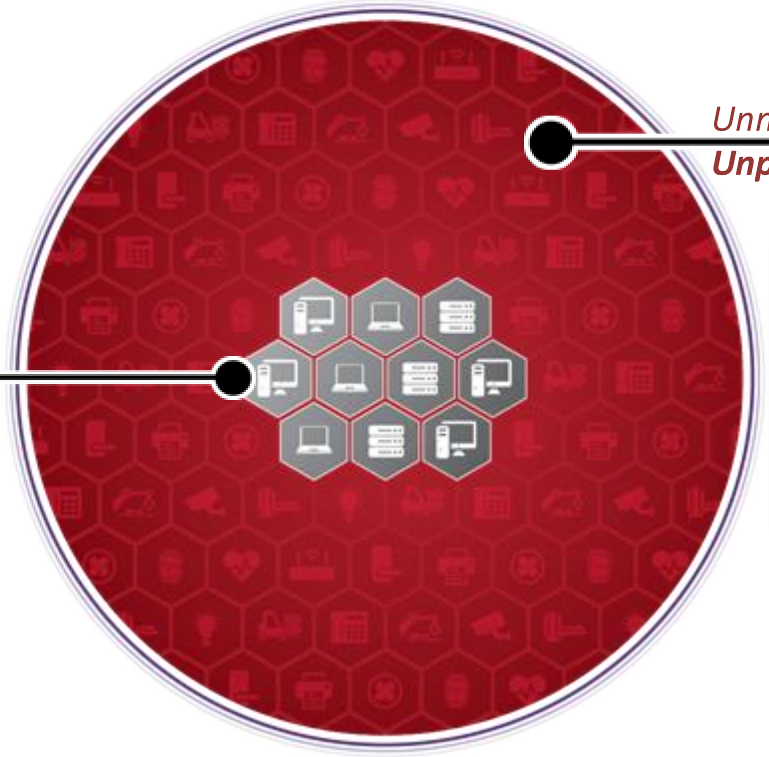
Risk Exposure Without Asset Intelligence

🟩 PROTECTED 🟨 PARTIALLY PROTECTED 🟥 UNPROTECTED

TANIUM · CISCO Meraki · Qualys.

FORTINET · CISCO · Gigamon

paloalto · Check Point · vmware



Managed devices
Protected by traditional security

Unmanaged & un-agentable devices
Unprotected

Traditional Enterprise

- PCs & Servers
- Tablets
- Smartphones
- Laptops

Unmanaged & IoT

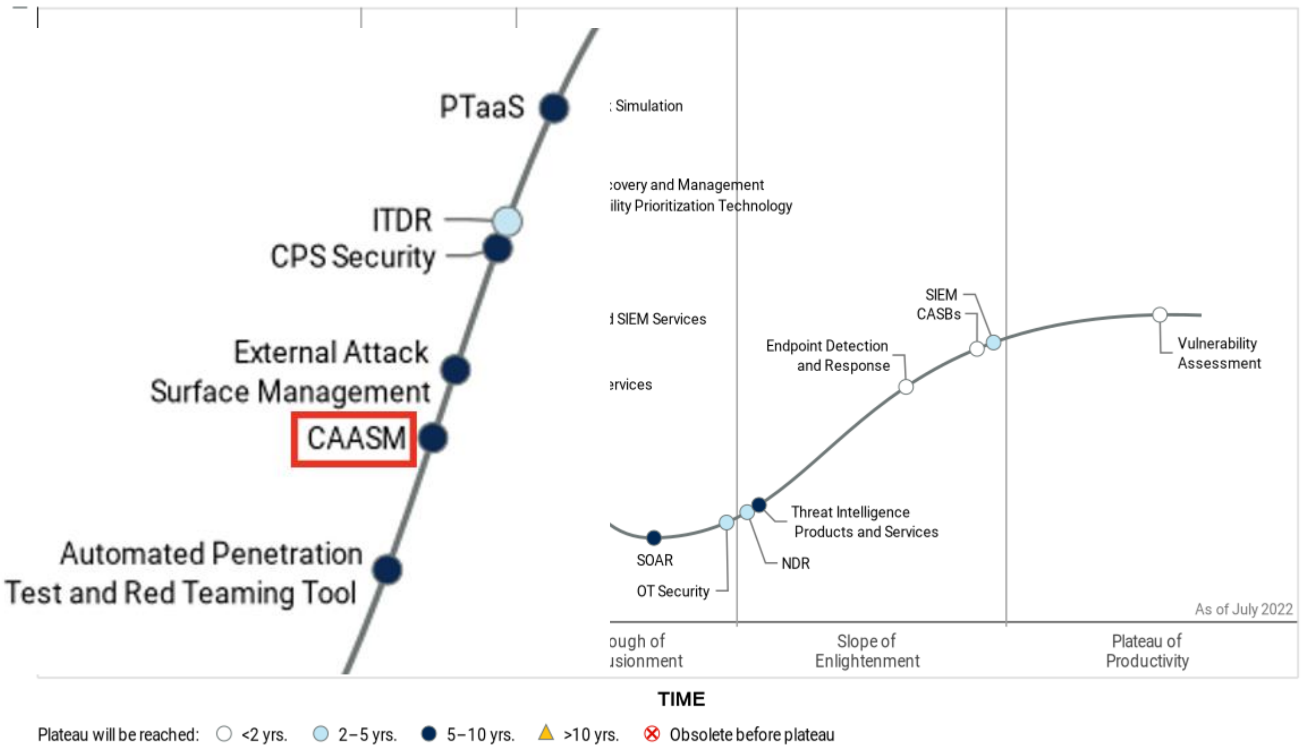
- VOIP
- Security Cameras
- Switches
- Access Points
- Printers
- Bluetooth
- Point of Sale
- Smart TVs
- Medical Devices
- Smart HVAC
- Manufacturing
- Smart Lighting

BYOD (PC & Mobile)

- Smartphones
- Laptops
- Tablets
- Wearables

Gartner Hype Cycle

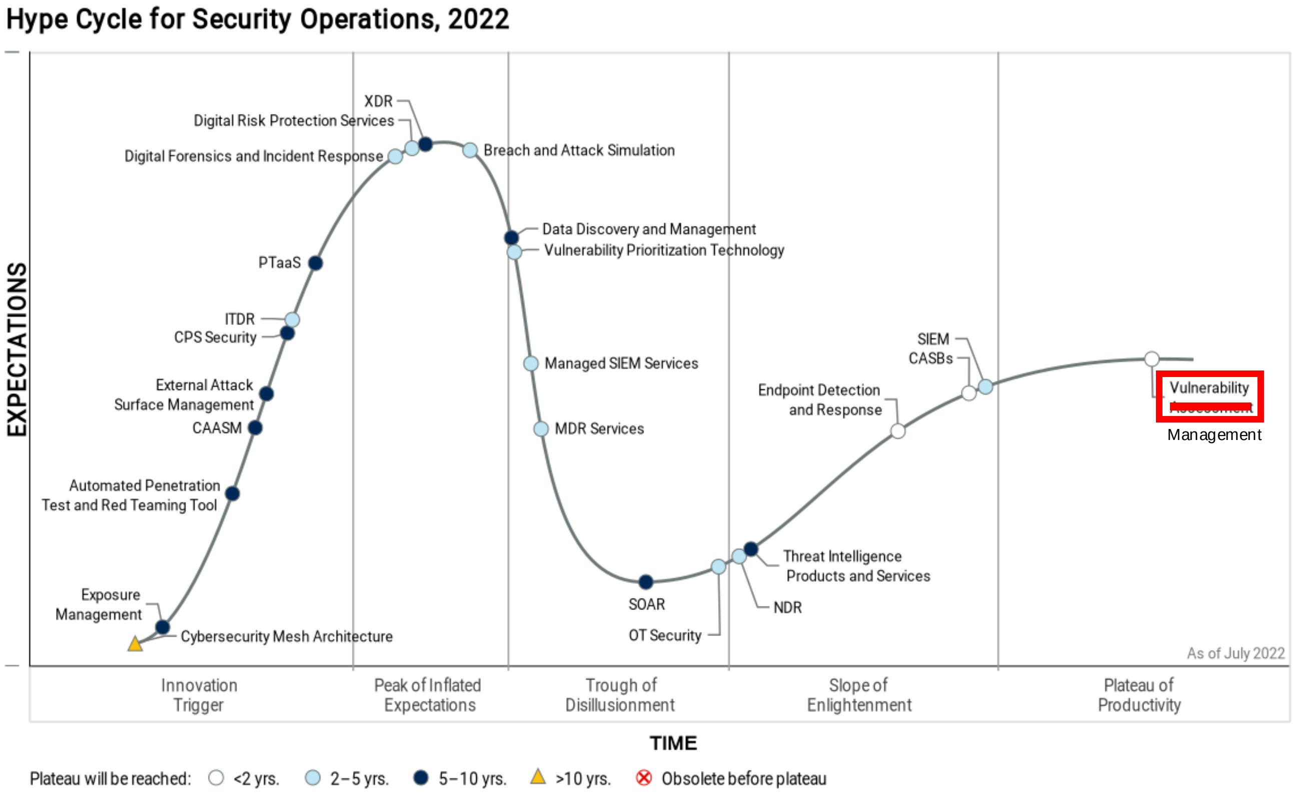
Hype Cycle for Security Operations, 2022



CAASM

- Cyber Asset Attack Surface Management
- Gartner defines CAASM as "…an emerging technology aimed at empowering security teams to solve persistent cybersecurity asset visibility and vulnerability challenges…"
- Gartner's definition includes remediation and alludes to automation
- Gartner further defines CAASM as working solely through API integrations with existing tools

Back To The Gartner Hype Cycle

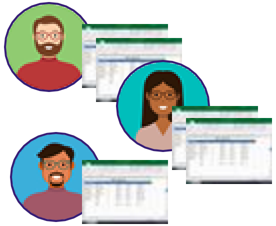


Hype Cycle for Security Operations, 2022

Vulnerability Management Challenges

Sheer volume of vulnerabilities with no business risk prioritization

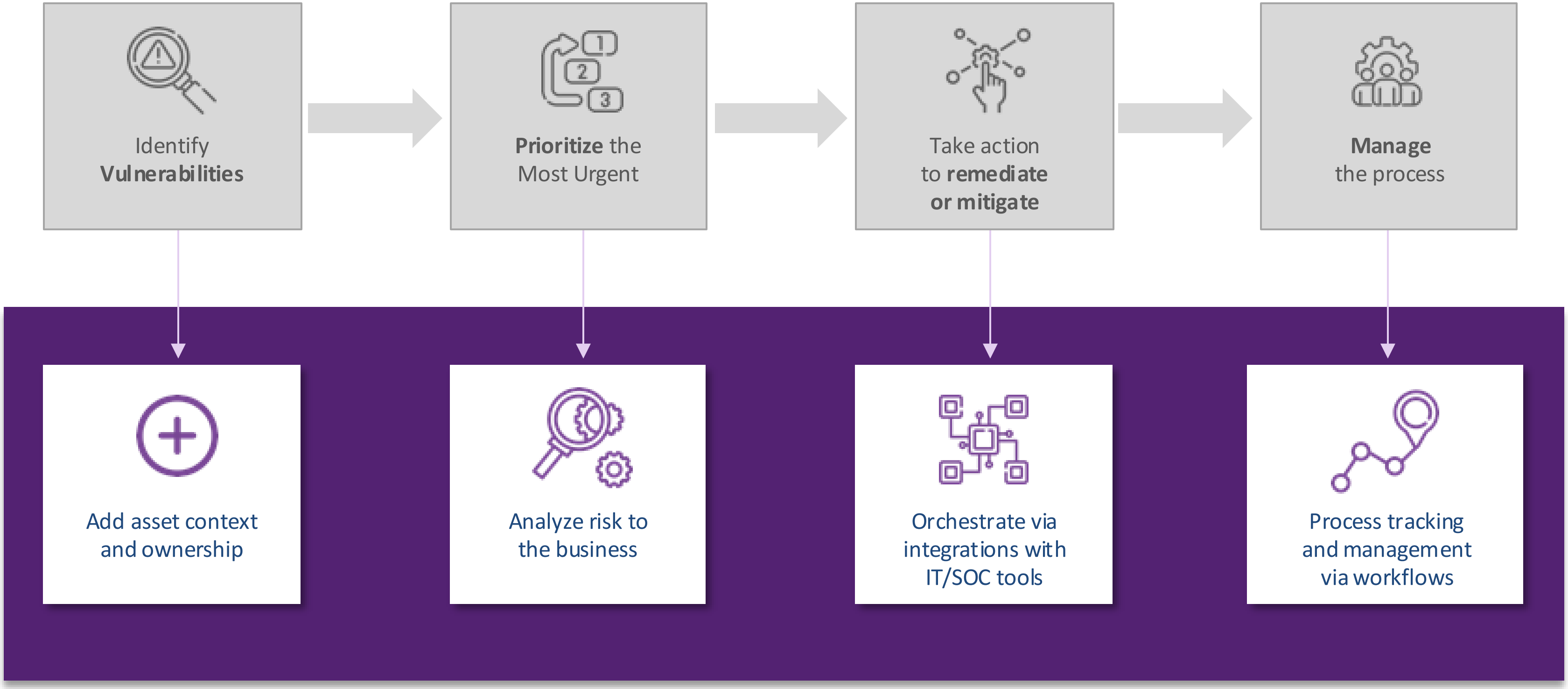
Incomplete and unreliable vulnerabilities data



Lack of process management and automated workflows

Missing vulnerabilities from unscannable assets

Vulnerability Management Requirements



Identify **Vulnerabilities**

Prioritize the Most Urgent

Take action to **remediate or mitigate**

Manage the process

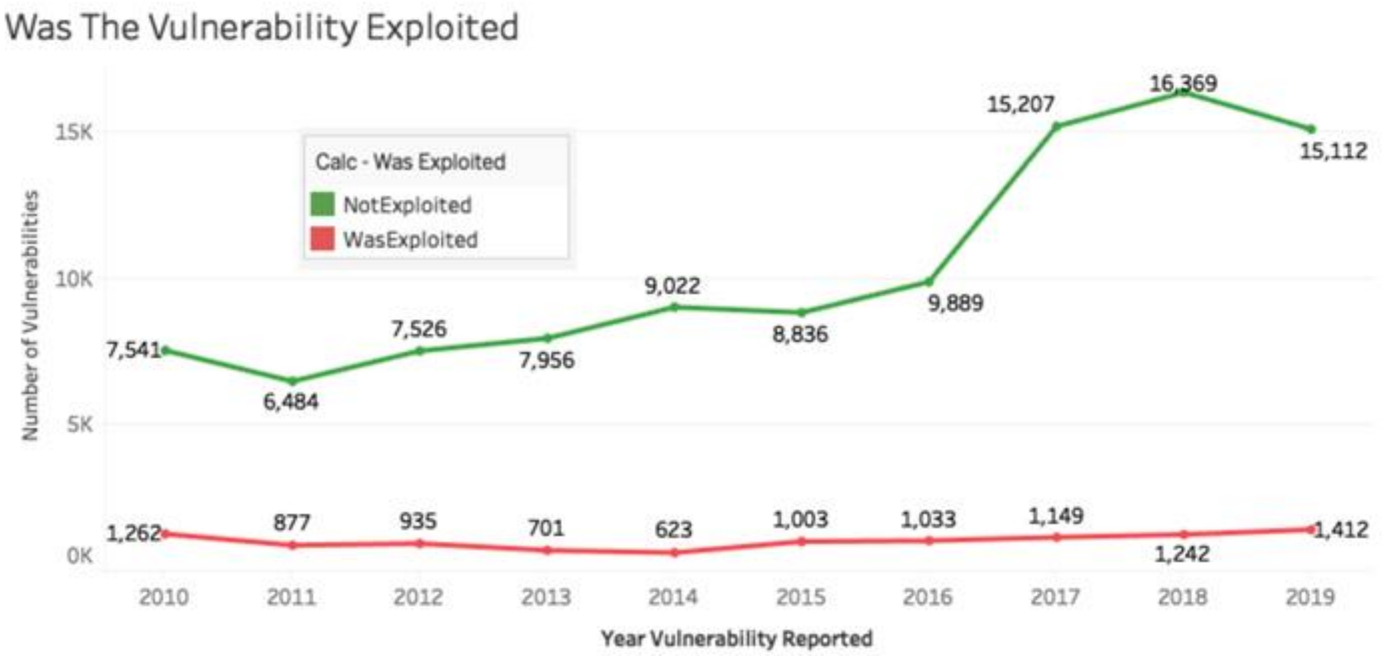
Add asset context and ownership

Analyze risk to the business

Orchestrate via integrations with IT/SOC tools

Process tracking and management via workflows

Not all CVEs are Attractive for Attackers

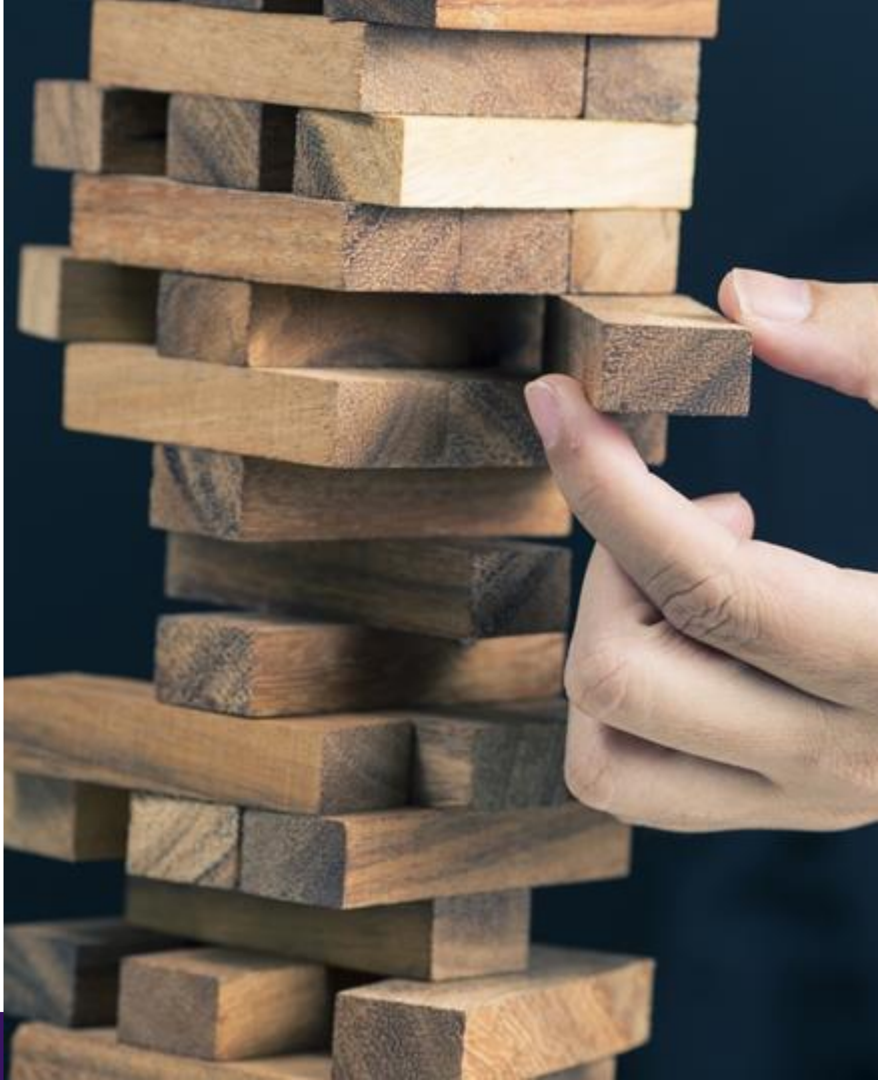


Lower chance that attackers will seek those CVEs

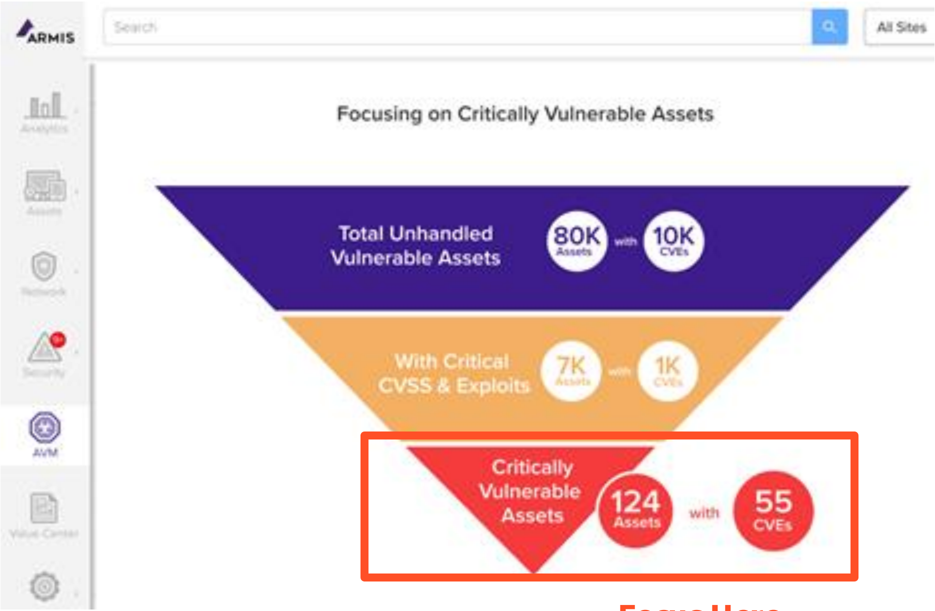
Higher chance that attackers will seek those CVEs

The Risk to the Business **Depends on the Asset** that Holds the Vulnerability

- What is the asset **functionality**?
- Who are the asset **owners**?
- Does it contain sensitive **data**?
- What is the **cost** of the asset?



Prioritize Critically Vulnerable Assets



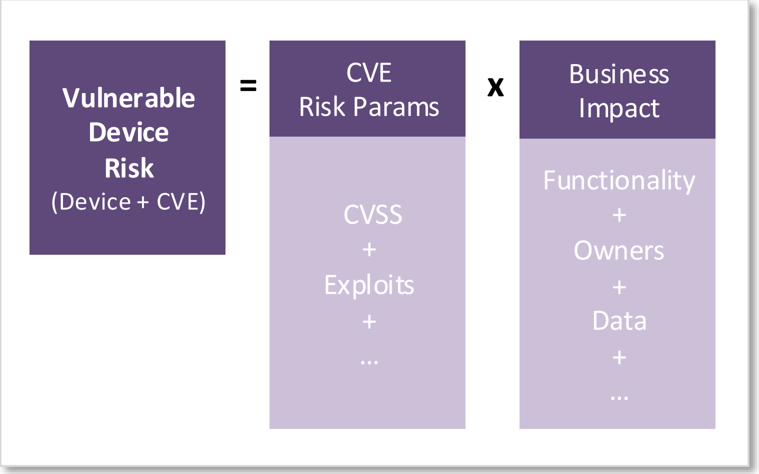
Focusing on Critically Vulnerable Assets

Total Unhandled Vulnerable Assets 80K Assets with 10K CVEs

With Critical CVSS & Exploits 7K Assets with 1K CVEs

Critically Vulnerable Assets 124 Assets with 55 CVEs

Focus Here



Vulnerable Device Risk (Device + CVE) = CVE Risk Params × Business Impact

Vulnerable Device Risk (Device + CVE)	=	CVE Risk Params	x	Business Impact
		CVSS + Exploits + ...		Functionality + Owners + Data + ...

Asset Intelligence

- Visibility
- Insight
- Action

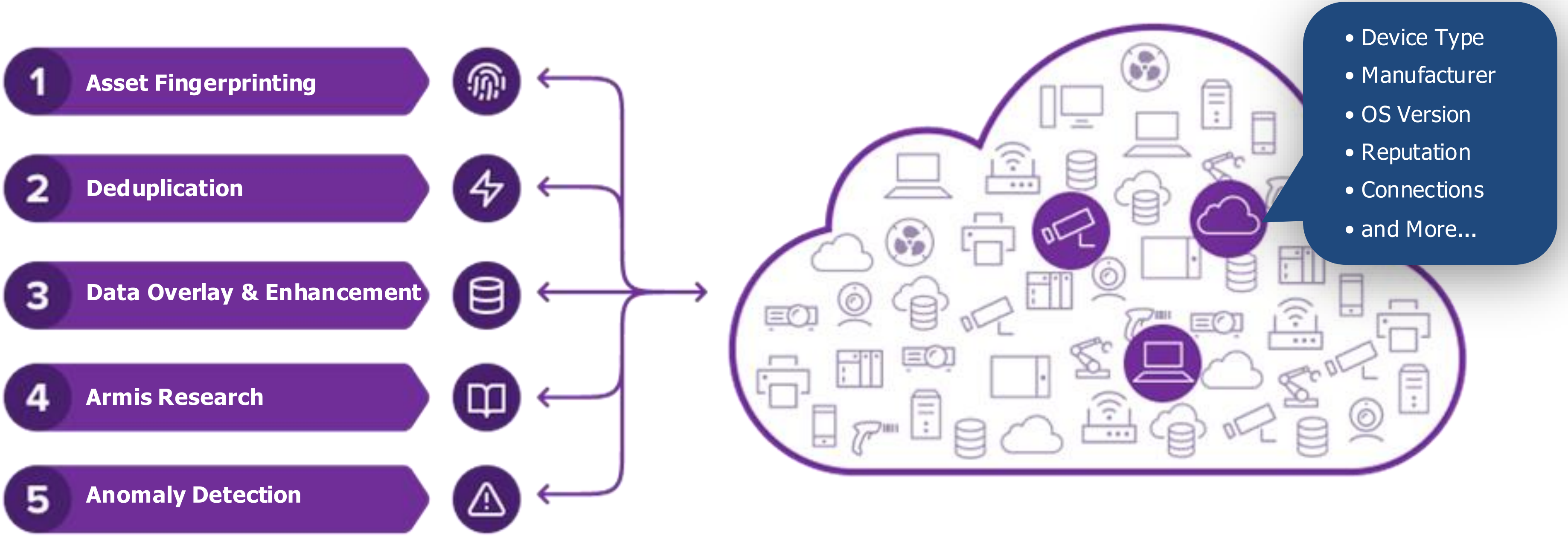
What About Other Technologies?

	Asset Intelligence	NAC and Other Network Security Tools	UEBA
Device visibility and classification	Wired, WiFi, Bluetooth, BLE, Zigbee, Wimax, others	Wired and WiFi only Very limited accuracy	None
Anomalous behavior and threat detection	Detects anomalies based on learned behavior and peer groups Generates risk score based on many different characteristics	Limited or no understanding of behavior	Misses IoT devices that don’t generate traditional logs Unaware of asset peer group behavior. No knowledge base
Topology awareness	Topology-aware, detects bridges over any protocol, catches device-to-device connections across boundaries	Enforces only traditional network segmentation	Understands user roles, but not network topology
Content awareness	Content and encryption aware	None	None
Traffic monitoring	Troubleshoot wired and wireless network problems Alert on anomalous connections	No asset knowledgebase, only very limited anomaly detection	None

Armis Asset Intelligence

Almost 5 Billion assets tracked and monitored

Tens of millions of unique device profiles



1. Asset Fingerprinting
2. Deduplication
3. Data Overlay & Enhancement
4. Armis Research
5. Anomaly Detection

- Device Type
- Manufacturer
- OS Version
- Reputation
- Connections
- and More...

What would you see if you had Asset Intelligence?

THANK YOU