IoTSecure™

Solving Modern IT Asset Inventory and Vulnerability Detection Challenges

Introduction – Why Device Profiling Matters

As modern networks face a growing Internet of Things footprint (e.g. IoT, OT, IIoT, ICS, IoMT), organizations face a daunting task: managing their ever-growing device inventories for both compliance and to update security measures.

Traditional approaches fall short on profiling xIoT devices, leaving networks vulnerable to unidentified and unmanaged devices and missed vulnerabilities.

This paper explains why traditional profiling approaches must be supplemented for more complete IT asset inventories and vulnerability detection, especially on xIoT devices.

Limitations with Traditional Approaches

1) Active scanners:
   - rely on endpoint agents or by connecting to open ports to gather profiling information, but IoT devices often don't support agents and have no/limited open ports
   - are intrusive and risk overwhelming resource-constrained devices

2) Passive monitoring and profiling:

   - commonly relies on collecting/analyzing network packets which can:
     a) leave these solutions blind to devices that encrypt traffic, and
     b) cause data privacy concerns by sharing packets with 3rd parties
   - fails to detect xIoT device vulnerabilities & exploits that require active inspection

3) Asset management solutions inherited the limitations of scanning and passive monitoring.

4) Manual inventory management quickly becomes outdated and doesn't scale.

IoTSecure's unique approach overcomes limitations with traditional approaches

IoTSecure combines a) active inspection (designed to be safe on even sensitive IoT devices), b) passive profiling (that doesn't rely on collecting network packets) and c) a huge library of profiled devices and IoT manufacturers' backend services which accelerates device identification.

The result is enhanced device profiling that delivers more complete and accurate device inventories and vulnerability detection. It's continuous, always on and always up to date.

- Proprietary multi-faceted, agentless approach integrates non-intrusive active scanning with AI-enhanced passive monitoring and service profiling for enhanced device profiling
- Extensive library containing millions of device fingerprints for accurate profiling and vulnerability detection
- Simple, rapid, set it and forget it deployment without relying on endpoint agents, network TAP/SPAN ports, sensitive data, or packet collection
- Safe on the network and safe on even resource-constrained IoT devices
- Continuous discovery and profiling of ALL devices, with detailed device identification (category, type, manufacturer, ports, OS, manageable or unmanageable)

- Seamless integration of device context with existing tools and processes (Asset Management, SIEM, ITSM, CMDB, CMMS, NAC, etc.) for increased efficiencies in IT asset management & inventory supplementation, segmentation, and remediation prioritization

IoTSecure's unique combination of profiling techniques improves profiling to help eliminate device inventory blind spots.

Profiling Techniques for xIoT	Traditional Scanning	Passive Monitoring: SASE & SIEM	IoTSecure™
Scan open ports	✓	✗	✓
Endpoint agent	✓	✗	not used
Utilizes identity services (SNMP)	not used	✓	✓
TAP/SPAN port	not used	✓	✓
- fully functional without TAP/SPAN	not used	✗	✓
Monitor cloud communications	not used	✓	✓
- including encrypted traffic (HTTPS)	not used	MAYBE	✓
- profile & identify cloud endpoints	not used	✗	✓

IoTSecure goes to great lengths to profile xIoT devices because they have different network profile characteristics than traditional devices.

Device Profiling Characteristics	Active Scanning	Endpoint Agents	Passive Monitoring	IoTSecure™
Traditional: (i.e. Computers, Servers, Laptops, etc.)				
Common OS & services	✓	✓	✓	✓
Numerous open ports	✓	✓	not used	✓
Support identity services	not used	not used	✓	✓
Common:				
Communicates to cloud	not used	✓	✓	✓
Encrypts outbound traffic	not used	✓	✗	✓
xIoT:				
Custom OS & Services	MAYBE	✗	MAYBE	✓
Few/No Open Ports	✗	✗	not used	✓
Lack IT identity services	✗	✗	✗	✓

With IoTSecure, you can revolutionize the way your organization manages device inventories and threat detection in an IoT world with confidence, clarity and complete automation.

Try it free, it takes just 5 minutes!

Experience the power of IoTSecure today with our no-obligation, 30-day free trial of the IoT-mini evaluation unit! Visit: **https://iotsecure.io/iotmini**

Note: Outside of the scope of this paper, IoTSecure also provides dynamic Zero Trust for xIoT that automatically detects/blocks anomalous/malicious communications, device access and lateral movement without VLANs, building policy or disrupting intended device functionality.