

The Problem – IoT Security Challenges

The Internet of Things (IoT) are growing rapidly due to improved efficiencies and cost savings for organizations, but traditional security tools are not designed to address common IoT device challenges:


Reasons IoT Devices Lack Visibility and are Hard to Secure:

- Are easily deployed by Operational Technology and end users without involving IT for securing the device
- Automatically connect to the internet or other devices
- Can't run agents for centralized management and security
- Can't be patched or don't support a patching process
- Manufacturers:
 - Use open-source OSs like BusyBox or embedded Linux for quick time to market while lacking the effort or expertise to properly build in security
 - Lack methods of operation to convey what the device should/shouldn't be doing by default, so manual research of the device and building security rules are needed.
 - Incorporates 3rd party NICS so the device manufacturer can't be reliably identified by MAC address
- Don't produce logs for monitoring
- Have default risky behavior like insecure services, hard-coded passwords or automated data transmissions

Industry Guidance on IoT Security

Industry security organizations, SANS & OWASP, have provided guidance on the importance of knowing what IoT devices are on the network and what threats are most specific to IoT devices.


Know What's on the Network



You Can't Secure What You Don't Know About

“ One of the first things you need to do to secure the Internet of Things is to do an inventory — knowing what things you're connected to or what things are connected to you so you know what you need to protect. ”

Top 10 IoT Security Threats



1. Default or Hardcoded Passwords	5. Use of Insecure or Outdated Components	8. Lack of Device Management
2. Insecure Network Services	6. Insufficient Privacy Protection	9. Insecure Default Settings
3. Insecure Ecosystem Interfaces	7. Insecure Data Transfer and Storage	10. Lack of Physical Hardening
4. Lack of Secure Update Mechanism		

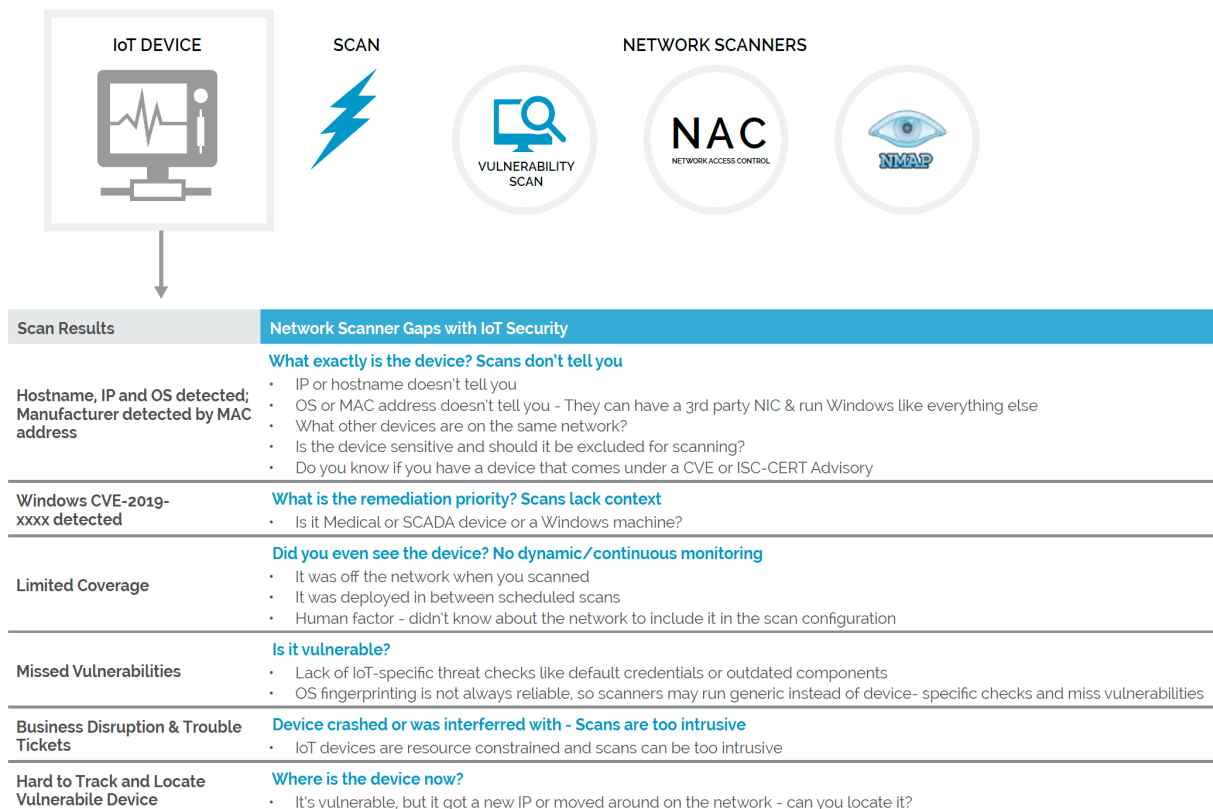
Implementing an Effective Solution is Not As Easy as it Seems

Gaps That Exist with Legacy Scanning Solutions

Organizations can no longer rely on traditional tools like NMAP, Network Access Control (NAC) tools or Vulnerability Scanners to identify IoT devices and detect IoT-specific threats.

Network scanners have gaps in device visibility, context and security with IoT because they:

- Don't tell you exactly what the device is, or exactly what other devices are on the same network. Manual IT asset inventory is not efficient or practical
- Weren't designed to detect IoT-specific threats
- Lack device context to determine remediation priority
- Are intrusive and can crash resource constrained IoT
- Are not continuous, so they miss discovering devices and vulnerabilities



How can organizations address these challenges to discover and secure IoT?

Enter IoTSecure™

Start with The Right Solution and Get It Fast

Our technology is purpose built for Enterprise IoT security. It is agentless, passive, and not inline. IoTSecure™ is safe and doesn't interfere with even sensitive devices, and it provides continuous threat monitoring and automated visibility to:

1. **Know what IoT devices are on the network** by discovering and identifying IoT devices by category, type, make & model, as they connect to the network.
2. **Know what IoT devices are vulnerable**, including coverage for the OWASP IoT Top 10, as devices connect to the network.
3. **Know where vulnerable IoT devices are.** Track vulnerable IoT devices, even as they move around the network or get new IPs.
4. **Protect IoT devices that can be compromised** through device-specific profiling & behavioral monitoring
5. **Enforce policy** by blocking or segmenting at risk IoT devices

Competitive solutions are not as complete and have drawbacks. They:

- **Deploy using a network tap**, sending sensitive network traffic to the vendor's solution which should cause data privacy concerns and deployment can drain IT's time and resources.
- **Lack proactive, IoT-specific security.** Instead, they only focus on reporting and anomaly detection which most firewalls already have, and they lack active vulnerability detection.
- **Lack active policy enforcement** to stop suspicious devices.

In contrast, IoTSecure™ is a complete IoT security solution, and deployment is a snap:

- **Deploys in minutes, No network tap, No collection of sensitive data.** Simply power up and connect the IoT Security Appliance anywhere on the network. It's preconfigured for DHCP and auto activates.

The IoTSecure™ Difference:

