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

SANS

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

OWASP

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 Use of Insecure or Outdated Components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

sales@securolytics.io | 1.404.260.7405 | www.securolytics.io

securolytics® | IoT Security Solution

DATA SHEET

Implementing a True Solution is Not As Easy As It Seems

Gaps with a Traditional Network Scanner

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

Scan Results	Network Scanner Gaps with IoT Security
Hostname, IP and OS detected; Manufacturer detected by MAC address	**What exactly is the device? Scans don't tell you** • IP or hostname doesn't tell you • OS or MAC address doesn't tell you - They can have a 3rd party NIC & run Windows like everything else • What other devices are on the same network? • Is the device sensitive and should it be excluded for scanning? • Do you know if you have a device that comes under a CVE or ISC-CERT Advisory
Windows CVE-2019-xxxx detected	**What is the remediation priority? Scans lack context** • Is it Medical or SCADA device or a Windows machine?
Limited Coverage	**Did you even see the device? No dynamic/continuous monitoring** • It was off the network when you scanned • It was deployed in between scheduled scans • Human factor - didn't know about the network to include it in the scan configuration
Missed Vulnerabilities	**Is it vulnerable?** • Lack of IoT-specific threat checks like default credentials or outdated components • OS fingerprinting is not always reliable, so scanners may run generic instead of device- specific checks and miss vulnerabilities
Business Disruption & Trouble Tickets	**Device crashed or was interferred with - Scans are too intrusive** • IoT devices are resource constrained and scans can be too intrusive
Hard to Track and Locate Vulnerabile Device	**Where is the device now?** • It's vulnerable, but it got a new IP or moved around on the network - can you locate it?

So, how can organizations address these challenges to discover and secure IoT?

Enter Securolytics!

sales@securolytics.io | 1.404.260.7405 | www.securolytics.io

securolytics® | IoT Security Solution

DATA SHEET

Start With the Answer and Get it Fast

Our technology is purpose built for Enterprise IoT security. It is agentless, passive, and not inline. Securolytics 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

> "It was amazing!"
> —A Top 10 U.S. Hospital

After a 2-minute deployment, Securolytics identified over 100,000 devices, including medical devices, and gave new visibility into IoT-specific threats with zero reports of device interference.

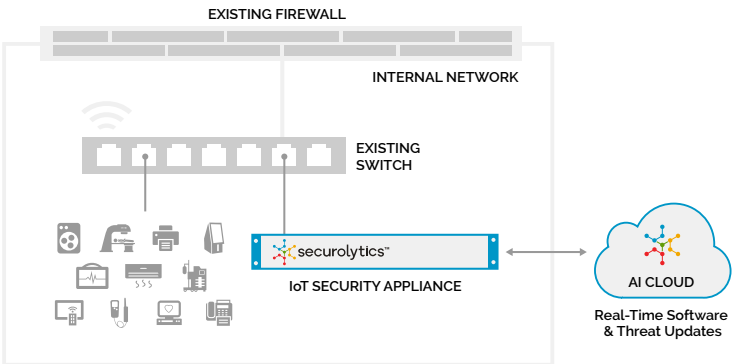
Competitive solutions are not as complete and have drawbacks. They:

- **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, Securolytics 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.

Securolytics IoT Security Appliance Deployment



The Securolytics Difference

DEPLOY IN MINUTES
Purpose-built hardware designed for quick and easy deployment

NO NETWORK TAP
Prevents sensitive data from being collected

LARGEST GLOBAL IoT DEVICE LIBRARY

DETECT VULNERABILITIES
Real-time as devices connect

SAFE ON DEVICES
Proprietary vulnerability detection does not interfere with devices

ENFORCE POLICY
Segment or block at risk devices

TCO
50% lower than competing solutions

sales@securolytics.io | 1.404.260.7405 | www.securolytics.io