securolytics®

IoT Security: Securolytics vs Competitive Solutions

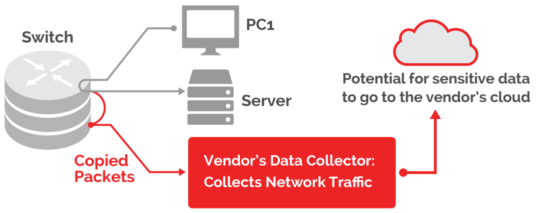
In comparing Securolytics to competitive solutions for Medical & IoT device security, Securolytics stands out with unique advantages with (1) Deployment and Data Privacy, (2) Proactive Security, (3) Policy Enforcement and (4) Lower TCO.

Deployment & Data Privacy

Competing Solutions - Network Tap Deployment

Risky Way: Collects Sensitive Data, Complex deployment

Competing solutions **deploy using a network tap,** sending sensitive network traffic to the vendor's solution which cause data privacy concerns. It also can require a complex deployment involving multiple switch configurations and deploying multiple vendor collection devices that can drain IT's time and resources.

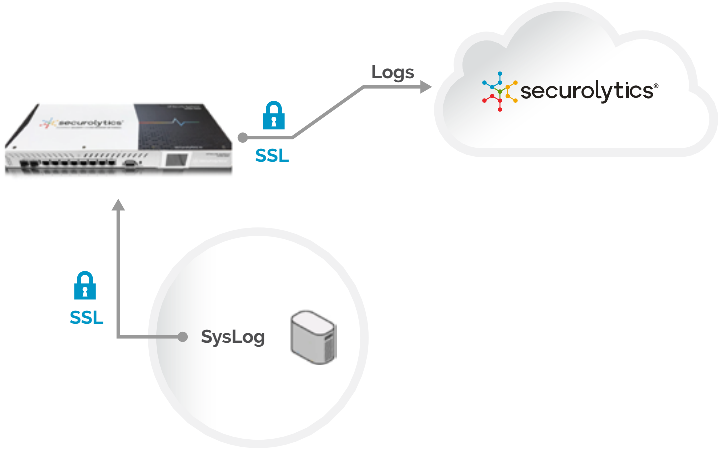

Switch
PC1
Server
Potential for sensitive data to go to the vendor's cloud
Copied Packets
Vendor's Data Collector: Collects Network Traffic

Securolytics Deployment

Safe Way: No Sensitive Data Collection, Simple & Fast Deployment

In contrast; **It's safe and easy to get started** with Securolytics, which deploys in minutes without a network tap or collecting sensitive data. Simply power up and connect the Securolytics IoT Security Appliance anywhere on the network. It's preconfigured for DHCP and auto activates. For full efficacy, just forward DNS and DHCP logs to the IOT Security Appliance which can act as a syslog collector, or for Microsoft servers, use the Securolytics Express Forwarder to securely send Windows Event Logs. Securolytics is agentless, passive and non-intrusive and is not inline.

1. Securolytics IoT Security Appliance
   - Installs in minutes at customer's location
   - Agentless
   - Hardware encryption
   - Central deployment
   - SysLog collection capability
2. Collect DHCP, DNS Logs



The Securolytics Difference

INSTALL IN MINUTES

Our Purpose-Built hardware designed for quick and easy deployment

NO NETWORK TAP

Prevents sensitive data from being collected

LARGEST IoT DEVICE LIBRARY

Medical
- Infrastructure
- Industrial / SCADA

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 IS 50% LOWER

1/2 the cost of competing solutions

— A Top 10 Largest U.S. Hospital - from their Security Analyst...

"Other solutions required a network tap and collected our network traffic, which was unacceptable. To ensure full visibility, it also meant a long and resource-intensive deployment that required many switch configurations and data collector deployments. This created even more work because we did not have an up-to-date and complete inventory of all our switches.

We selected Securolytics. Without a network tap and after a 2-minute deployment, Securolytics identified over 100,000 devices and gave us new visibility into both managed and unmanaged devices, including medical and other IoT devices, with zero reports of device interference."

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

IoT Security:
Securolytics vs Competitive Solutions

Proactive Security - Know if devices are vulnerable, as they connect!

Most solutions, including Securolytics are able to detect compromised devices via behavioral monitoring. But, other solutions fail to provide proactive threat detection to stop attacks before they occur. Traditional network scanners have gaps because they can be too intrusive and interfere with resource-constrained, sensitive medical and IoT devices, and they lack IoT-specific threat detection.

Securolytics' PortSafe technology is the only solution that provides real-time and IoT-specific vulnerability detection, as devices connect and doing so safely, without interfering even with sensitive IoT devices. Securolytics also provides:

- Coverage for OWASP's IoT Top 10
- Immediate visibility into restricted devices, or devices that come under ICS-CERT or CVE security advisories

Unique Policy Enforcement

Securolytics provides the option to block or segment at risk devices and offers multiple deployment models for policy enforcement with or without 802.1x integration. Also, Securolytics' Smart Block Technology provides a way to keep devices to stay online, but blocks any malicious or abnormal traffic.

— A Top 5 Largest U.S. Children's Hospital-from their Information Security Manager...

> **"We looked at other solutions** but they all required a network tap which was a non-starter for us because of data privacy concerns. Securolytics was an easy choice. **It deployed** in minutes **without a network tap. And, it delivered** a complete and detailed device inventory, while giving us the added benefit of safe and real-time vulnerability detection on not only medical and IoT devices, but all devices on the network – both managed and unmanaged. Now anytime a device connects to the network, we immediately know it's there and if it's vulnerable. Securolytics also gave an option to actually block devices and the cost was over 50% lower than other solutions."

Criteria		Securolytics	Competing Solutions
Deployment and Data Privacy	Deploys without Network Tap	✓	✖
	Deploys without collecting sensitive network traffic	✓	✖
Proactive Security	Safe, Vulnerability Detection designed for IOT and as devices connect	✓	✖
	Identify devices that come under ICS-CERT or CVE advisories	✓	✖
	Tracks vulnerabilities to devices as devices get new IPs	✓	✖
	OWASP IoT Top 10 Security Compliance	✓	✖
Policy Enforcement	Segment or block at risk devices	✓	✖
	Smart Block Technology	✓	✖
TCO	Sub-$10K Entry Point	✓	✖
	Costs 40% - 50% less	✓	✖
Other	Medical Device coverage	✓	✓
	Integration with other systems (SIEM, CMMS, Help Desk, etc.)	✓	✓
	Device Behavior Monitoring and Anomaly Detection	✓	✓
	Device Identification by category, type, make, model	✓	✓
	Reporting on device communications	✓	✓
	Integrated SOC for threat tracking	✓	✓

The Securolytics Difference

OWASP

Safe, Proactive, Real-Time coverage for the OWASP Top 10 IoT Security Threats

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