securolytics® | IoT Security Solution Deployment

DATA SHEET

Securolytics IoT Security Solution Deployment

The Securolytics IoT Security solution is agentless, non-intrusive, not inline, and designed for rapid deployment. It will profile, discover and identify IT assets by category, type, make and model number. It also safely detects vulnerabilities in real-time as devices connect and monitors devices for abnormal or malicious behavior.

Say "No" to Network Taps

Competitive solutions that deploy using a network tap can:

- Collect and send sensitive network traffic to the vendor's solution which should cause data privacy concerns
- Require a complex, lengthy deployment that drains IT's time and resources.

Simple, Safe, and Fast Deployment

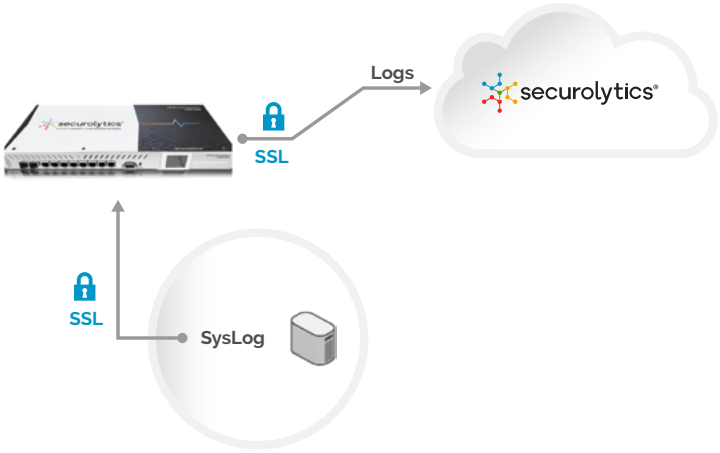
In comparison, Securolytics features a unique model that provides rapid deployment of the Securolytics IoT Security solution with minimal investment of IT resources and without collecting senstive data.

Deployment Takes 2 Minutes

Securolytics **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 maximum efficacy, forward DNS and DHCP logs to the IoT Security Appliance that can also act as a syslog collector.

No Network Tap, No Sensitive Data Collection

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

DEPLOY IN MINUTES

OUR PURPOSE-BUILT HARDWARE DESIGNED FOR QUICK INSTALL

NO NETWORK TAP

NO AGENTS

NO COLLECTION OF NETWORK TRAFFIC OR SENSITIVE DATA

SAFE & NON-INTRUSIVE – DOES NOT INTERFERE WITH OTHER DEVICES

PASSIVE - NOT INLINE

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

Other solutions were immediately discarded because they required a network tap and collected our network traffic, which was unacceptable. To ensure full visibility, it also meant a long, complex deployment with switch configurations and data collectors. This created even more work because we did not have an up-to-date and complete inventory of all our switches, nor did we want the additional deployment or maintenance work required with network taps.

We selected Securolytics. 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

Copyright © 2019 Securolytics, Inc. | All Rights Reserved

How it Works

We collect logs, which do not contain sensitive data. Once the logs are collected, proprietary data enrichment analytics, leveraging the Securolytics IoT Device Library, are applied to the logs to accurately identify devices, determine if they are vulnerable and continuously monitor the behavior of devices. The logs are easily collected.

1. Securolytics IoT Security Appliance

The Securolytics IoT Security Appliance (IoTSA) is a purpose-built hardware appliance designed for IoT. It deploys in minutes simply by powering up the appliance and connecting to any network port. It transparently collects profiling data about devices, then encrypts and sends the logs to the Securolytics cloud.

Deploying the Securolytics IoTSA is all that is needed to get started with IoT Asset Discovery and Threat Detection with up to 50% efficacy rates.

2. DNS and DHCP Log Collection

To further improve IoT Asset Discovery and Threat Detection efficacy rates approaching 100%, DNS and DHCP logs are needed. This can be achieved quickly using the following methods.

A. For Non-Microsoft Servers / servers supporting syslog:
The Securolytics IoTSA can also act as a syslog collector. Simply syslog the DNS and DHCP logs to the Securolytics IoTSA, which in turn will encrypt and send the logs to the Securolytics Cloud.

B. For Microsoft Servers – Securolytics Express Forwarder:
The Express Forwarder is a lightweight client that installs on Windows DNS, DHCP servers and, optionally AD servers if it is desirable to provide reporting on users who have logged into devices. Express Forwarder monitors, encrypts and forwards the Windows event logs to the Securolytics Cloud through two (2) separate services. These services are independent and can be disabled if the appropriate log forwarding is not desired. All forwarded logs are encrypted via TLS and forwarded to our public collector over TCP: 443.

--**Express-Forwarder Service (DNS, DHCP-required)**
C:\Windows\Sysnative\dns\debug-dns.log
C:\Windows\Sysnative\dhcp\DhcpSrvLog-*.log

--**AD-Express-Forwarder Service (AD-optional)** Logs and forwards Windows server events from collections: Application, Security, System

3. IoT Discovery and Threat Detection that's Safe on the Network, Safe on Devices

The problem with using Network Scanners like NMAP, Network Access Control (NAC) tools or Vulnerability Scanners to discover devices and detect threats is that they do not run in real-time and/or they can be too intrusive and even crash resource-constrained IoT devices. This means these tools are run only periodically or infrequently, if at all, and can leave large gaps in coverage. They can't provide continuous real-time monitoring and detection.

To address this challenge, Securolytics has developed unique and proprietary technologies that do not interfere with even very sensitive IoT like medical or SCADA devices.

1) Securolytics IoT Device Library

2) Securolytics DevicePrint and PortSafe Technologies

3) Securolytics Device Behavior Engine

As logs are collected from the Securolytics IoTSA and optionally from DNS and DHCP servers, the data is correlated in the Securolytics Cloud, leveraging the Securolytics IoT Device Library. DevicePrint technology uses and enriches this information to identify and profile devices on the network. PortSafe Inspection technology safely identifies open network services on each device.

In combination, these technologies deliver real-time, detailed device identification and vulnerability detection for issues like default credentials, insecure device configurations, ISC-CERT and CVE issued vulnerabilities, and devices at risk to ransom ware, as devices connect to the network. The Device Behavior Engine leverages this information during device-specific, continuous security monitoring to identify devices that are behaving abnormally or maliciously.

sales@securolytics.io | 1.404.260.7405 | www.securolytics.io
Copyright © 2019 Securolytics, Inc. | All Rights Reserved