IoT Security Solution Deployment

IoT Secure™ IoT Security Solution Deployment

The IoT Secure™ 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.

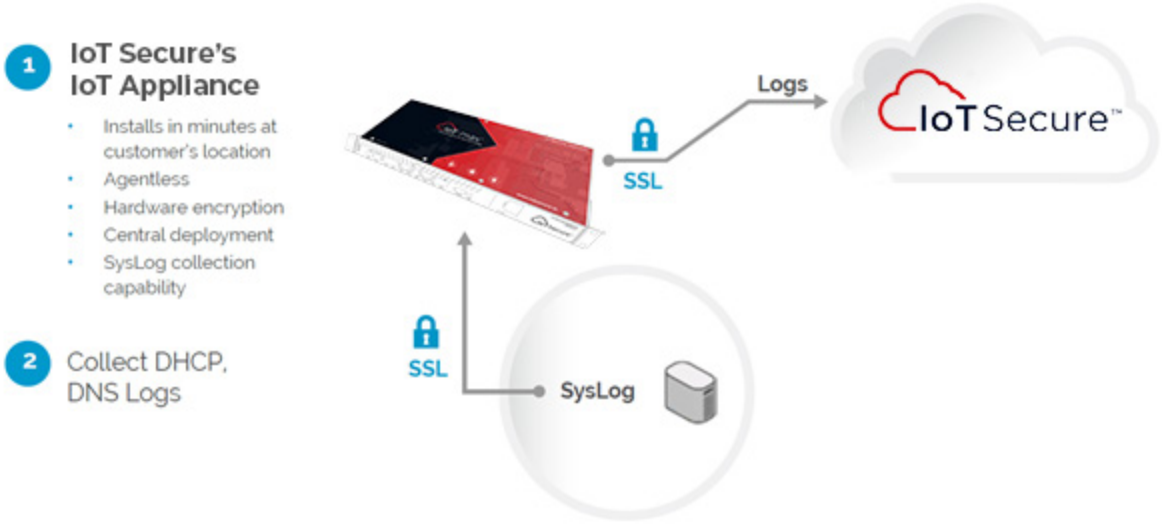
Simple, Safe, and Fast Deployment

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

Deployment Takes 2-Minutes

IoT Secures IoT-mini™ and IoT-max™ appliances **deploy in minutes without a network tap or collecting sensitive data**. Simply power up and connect the 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



sales@iotsecure.io | IoTSecure.io

IoT Security Solution Deployment

Implementing an Effective Solution is Not As Easy as it Seems

How it Works

We collect logs, which do *not* contain sensitive data. Once the logs are collected, proprietary data enrichment analytics, leveraging IoT Secure's 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. IoT-Secure™ Security Appliances

The IoT Security Appliances (IoTSA) are purpose built hardware appliances 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 CloudPortal™. Deploying the IoT-mini™ or IoT-max™ 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 Server / Servers Supporting syslog*: The IoT Secure™ IoTSA can act as a syslog collector. Simply syslog the DNS and DHCP logs to the IoT Secure™ IoTSA, which in turn will encrypt and send the logs to the CloudPortal™.

B. *For Microsoft Servers – IoT Secure™ 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 Cloudportal™ 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

sales@iotsecure.io | IoTSecure.io

IoT Security Solution Deployment

Implementing an Effective Solution is Not As Easy as it Seems

3. IoT Discovery and Threat Detection That's Safe for the Network and All 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, IoT Secure™ has developed unique and proprietary technologies that do not interfere with even very sensitive IoT like BioMed or SCADA devices.

1. IoT-Secure™ Device Library
2. PortSafe™ Technologies
3. IoT-Secure™ Device Behavior Engine

As logs are collected from the IoTSA and optionally from DNS and DHCP servers, the data is correlated in the CloudPortal™, leveraging the our proprietary IoT Device Library. Device Behavior 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.

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

Enter IoT Secure™

IoT Security Solution Deployment

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. IoT Secure™ 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

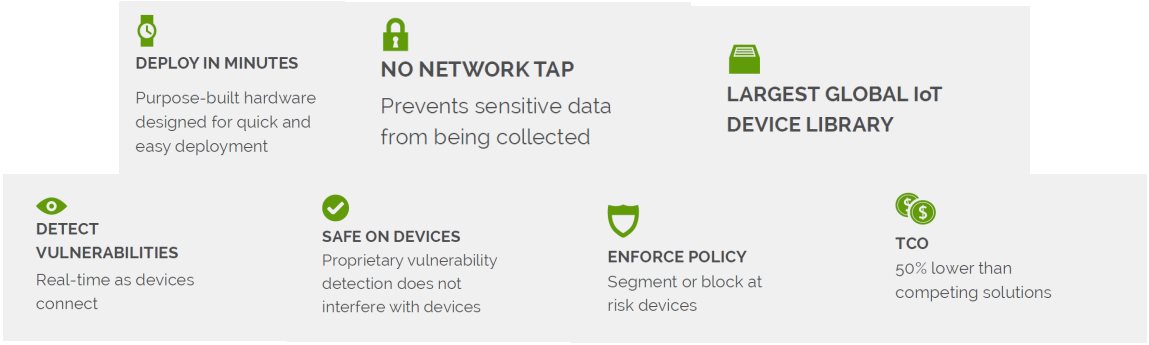
Competitive solutions are not as complete and have drawbacks. They:

- **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, IoT Secure™ 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 IoT Secure™ Difference:



sales@iotsecure.io | IoTSecure.io