IoTSecure™

K-12 School District Gets Full Visibility, Security and Control of Connected Devices

CASE STUDY

IoTSecure helps to elevate a technology-leading school district’s security posture

CUSTOMER PROFILE

K-12 public school district
in Dallas - Fort Worth, TX Metroplex

INDUSTRY

Education

IT ENVIRONMENT

Approximately 40,000 devices,
including IoT devices
14,000 students
1,900 employees
20 school campuses

Introduction

Having been invited to attend the 2023 National Cybersecurity Summit for K-12 schools at the White House was a testament that this school district took cybersecurity very seriously.

This large K-12 public school district in the Dallas-Fort Worth Metroplex wanted to ensure they had full visibility into all devices that were connected to their network, and especially, a strategy in place to secure unmanaged and IoT devices at scale, across all locations.

After centrally deploying IoTSecure's agentless solution within 1 hour, the school district had complete coverage for all 20 campus locations. IoTSecure's solution armed the school district with new, detailed visibility into all connected devices and threats, as well as a way to mitigate these threats to better protect their network.

The school district's IT team wanted real-time visibility into all connected devices. This meant not only traditional computers, laptops, tablets, etc., but also non-traditional IoT devices like IP cameras, HVAC controllers, power management, building automation, smart TVs and video conferencing, including any rogue devices that had gotten connected without IT's knowledge by both students and staff.

Also paramount to the project was to close security gaps into the growing number of unmanaged and IoT devices that were being connected, especially since:

- thousands of these devices did not run endpoint agents
- traditional tools were not effective and did not scale.

IoTSecure™

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2023 IoTSecure, Inc. | All Rights Reserved

Challenges:

- Lack of continuous visibility into devices connecting to the network
- No detailed information about connected devices
- Vulnerabilty scans too often crashed IoT devices, leaving them untested on the network
- Vulnerabilty scans struggled to fingerprint IoT devices resulting in missed vulnerabilities.
- Had no way to automatically monitor anomalous behavior on devices that could not run endpoint agents
- Needed an easy, scalable way to mitigate threats, especially on devices that could not be patched
- Had budget limitiations and needed an inexpensive solution.

Overcoming Challenges ... in Minutes

Detailed, Complete & Continuous Device Inventory

After the school district's IT team saw a demo of the IoTSecure solution, they decided to conduct an initial evaluation on a small network. The initial test was plug-n-play and:

- took only 5 minutes to deploy
- provided a detailed device inventory by device types, model, OS, ports and network

Next, IT completed a full deployment in less than 1 hour to get a complete, continuously-updated inventory of all campuses.

New Visibility into Vulnerabilities

Traditional vulnerability scanners work great on managed devices that can run endpoint agents, but not so much on unmanaged devices that don't. The agents allow the scanners to accurately fingerprint devices so that the fingerprint can be matched to vulnerabilities in the scanner's database.

But on devices that don't run endpoint agents, scanners rely on connecting to open ports, in hopes of getting enough information from the device's banner response to fingerprint the device.
The problem is that IoT devices commonly:

1. don't run agents and don't have any open ports
2. easily crash under traditional scanning, so they end up on a scanner exclusion list and left untested on the network

To combat these limitations, the school district's IT team enabled IoTSecure's unique PortSafe Inspection, which is designed to

- be safe on IoT devices without any interference
- fingerprint IoT devices to detect threats that traditional scanners miss
- automatically run as devices connect to find vulnerabilities in near real-time

The result: The school district got new visibility into vulnerabilities they didn't know about to better protect their network.

IoTSecure™

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2023 IoTSecure, Inc. | All Rights Reserved

I've never seen a tool that gave such detailed visibility into devices and was as simple to deploy as IoTSecure

IT Manager
Large K-12 School District
Dallas - Fort Worth, TX

IoTSecure's Key Differentiators:

Data Privacy
-No TAP/SPAN ports
-No packet collection
-No agents

Deployment
-Centralized deployment in minutes
-Typically a single appliance covers all locations and VLANs

Threat Detection
-Unique PortSafe Inspection is safe on IoT devices
-Monitoring without tuning

Control & Mitigation
-Unique Firewall Mode provides 1-click mitigation

Low Cost
-IoTSecure is priced at a fraction of the the cost vs. other leading competitors

IoTSecure™

Automated, Agentless Device Behavior Monitoring

The school district's IT team also realized the challenges with monitoring unmanaged devices that don't run endpoint agents, produce logs for monitoring and that commonly lack documented methods of operation detailing where the device communicates. This meant manual effort and tuning that just didn't scale.

Armed with IoTSecure's massive library of millions of profiled devices, the IT team closed this gap automatically with:

- device-level anomalous behavior detection that's context-aware and knows where devices should/shouldn't be communicating
- no tuning, set it and forget it
- malicious communication detection

Actionable Control and Mitigation

After identifying all the devices on the network, the IT team's strategy was to segment the unmanaged IoT devices into their own VLANs. They also realized that many of these devices can't be patched when vulnerabilities are detected, so they required a way to easily mitigate any discovered vulnerabilities.

IoTSecure's solution allows them to:

1. First do a complete device inventory in passive mode and identify the IoT devices they wanted to segment.
2. Segment the IoT devices behind the IoTSecure appliance, which can be configured to function as an inline firewall option on specific ports.
3. Single-click to block devices entirely or to block only vulnerable services while leaving the device operational.

IoTSecure also support integrations into network infrastructure solutions to provide them with rich device context and threat data or to automatically generate ACLs for device control.

With IoTSecure, the school district has closed visibility, security and control gaps on unmanaged and IoT devices to advance its security posture.

sales@iotsecure.io | 1.404.260.7405 | www.iotsecure.io
Copyright © 2023 IoTSecure, Inc. | All Rights Reserved