Zingbox

CASE STUDY

> “Instead of having my head in the sand, I was able to take what I learned from Zingbox and secure our network.”

Educational Institution Gains Valuable Knowledge with Zingbox IoT Guardian

Fear of the Unknown

Brainerd Baptist School is a private school founded in 1953, serving urban, suburban and rural communities within a 30-mile radius of Chattanooga, Tennessee. The school serves hundreds of students from K to 5th grade.

Like many educational institutions, Brainerd Baptist School relies on a wide range of Internet-connected devices for its day-to-day operations. These devices include critical systems such as the HVAC and the campus security and surveillance system. Although the school felt confident with their network security posture, they noticed an alarming trend: An increasing number of vendors were requiring access to their campus network. This was a cause for concern.

“Most of the platforms that I was fearful of were not systems that I had purchased or from vendors that I was familiar with,” said Bradley Chambers, IT Director at Brainerd Baptist School. *“They were typically sourced through our facilities group.”*

Chambers came to realize that these devices weren’t built with network security in mind. In many cases, it was an afterthought. “*I just hoped and trusted that nothing was going bad,”* he said.

It became clear that the school needed a solution that provided visibility into how these systems were communicating and ensured they didn’t place the campus network at risk. Unfortunately, such solution was not easy to find. Many existing products were designed for IT devices, like laptops and servers, and assumed the devices could be easily patched or upgraded. Unfortunately, you can’t simply download a patch or install anti-virus on a HVAC system.

20/20 Vision for IoT Devices

When Chambers first learned of Zingbox and its security offering, IoT Guardian, he was cautiously optimistic. It promised unparalleled insight and visibility into the various IoT devices that many traditional solutions could not offer. *“It felt like it was security for a modern infrastructure,”* Chambers said.

Installing IoT Analyzer, the on-premise component of IoT Guardian, was a simple plug-and-play, requiring just few minutes. After installation, the solution was left alone to monitor the school’s network. To Chambers’ surprise, in less than one hour, IoT Guardian had discovered and identified close to 4,000 devices on the school’s network. The devices were automatically categorized into the following:

- Smart Building
- Printers
- Camera
- Security Surveillance
- IT Products
- Audio Video Conference
- Projectors
- Entertainment

"I don't have the option to just unplug our HVAC controller or our CCTV. I have to make it work. We're committed to these platforms."

By the second hour, Zingbox IoT Guardian completed the device vulnerability assessment and risk posture analysis for every single IoT device discovered. The wealth of information and insight turned out to be a double-edged sword. Chambers was glad to finally have his hands on the information he had been seeking, but he was surprised to learn the number of suspicious network connections originating from overseas.

IoT Guardian pinpointed the suspicious access on multiple IoT devices from malicious external destinations on the Internet. The affected IoT devices included:

- Security camera DVRs
- Security and fire alarm panel
- Smart building devices for HVAC control and monitoring

Because IoT devices are interconnected throughout the network, malicious access to any of these devices meant that cybercriminals could have moved laterally on the school's network bypassing traditional perimeter security solutions, gaining access to high-value assets and even taking over the entire network.

Better Visibility Empowers Better Security

Backed by detailed visibility into how the IoT devices were connecting to the outside world, Chambers had the necessary information to start tightening up his network. He reached out to vendors with specific questions—backed by real data—about how their devices were behaving. And with the help of Zingbox, he was able to methodically cutoff access to suspicious connections.

"Using Zingbox's enforcement capability was a fast and easy way to fix issues. It was just a matter of clicking on the alerts sent by the tool to plug the holes in the firewall," Chambers said.

Confidence in an Increasingly Connected World

Today Chambers is once again confident in the school's security posture. Armed with weekly reports from Zingbox's IoT Guardian, Chambers can partner with other departments to incorporate new technologies without fear of compromising the school's network.

"We're going to see more connected devices. I see that going up. Big time. Well now I can do it without fear. I don't have to worry about what these things are doing," Chambers said.

About Zingbox

Zingbox IoT Guardian is an Internet of Things security solution that provides visibility into and protection for enterprise IoT assets against cyber and insider threats. A **non-intrusive, agent-less, signature-less** solution, IoT Guardian uses machine learning for asset discovery, risk assessment, baselining the normal behavior of devices, and discovery of threats. Zingbox was founded by Silicon Valley IT industry leaders and experts in networking, big data, IoT, and security.