Zingbox

CASE STUDY

WAUBONSEE COMMUNITY COLLEGE

INDUSTRY
Education

ENVIRONMENT
Open, interconnected multi-campus and virtual learning network

CHALLENGE

- Insight into every devices' type, baseline behavior, and risk status
- Ensure new solutions do not cause network downtimes or modify current hardware or software
- Adhere to strict security regulations while also encouraging open, flexible learning

SOLUTION

- Complete visibility into the entire IoT network, with categorization of 1,000 devices and their risk levels
- Seamless, phased implementation resulting in zero disruption or modification to current systems
- Real-time monitoring that keeps devices protected while enabling collaborative student engagement

IoT Guardian Gives Community College System-wide Visibility and Flexibility

When Unknown Devices Are at Uncertain Risk

Since 1966, Waubonsee Community College has offered high quality academic programs to equip lifelong learners with the skills necessary to meet the changing needs of today's economy. Providing students with cutting-edge resources and the freedom to explore their interests are core to Waubonsee's mission.

Across its four Illinois campuses and online community, students often require access to custom technological tools to conduct research and connect with one another. But operating open, digitally-enabled campuses introduces significant security risks, particularly when hundreds of IoT-enabled devices — from smart TVs to access control tags, security cameras to credit card machines — must be secured. Not doing so can put students' educational, employment, health, or finance records at risk, or even compromise their personal safety.

As information security manager at Waubonsee, Tarun Trivedi is charged with securing these devices and ensuring that students have a streamlined and safe educational experience. However, he found that definitively securing the entire Waubonsee network was difficult without visibility into the types of devices and their risk levels. *"We ran into a lot of unknowns,"* says Tarun. *"I had no way of knowing where these devices were communicating."* During his regular check-in meetings with Waubonsee's CIO, Tarun couldn't provide a full report of each device's risk status and overall assessment of network security.

A Custom Approach Provides Disruption-Free Visibility

As a team of one at the time, Tarun knew he needed a robust technological solution to monitor and manage Waubonsee's device security risks. He sought a platform that provided a clear baseline and assessment of risk for every device, an easy and seamless implementation process, an intuitive user interface, and great customer support. After considering several vendors, Tarun found that only Zingbox met all of these criteria.

In response to Tarun's concerns about the impact of implementing a new solution on the current system, the Zingbox team developed a personalized deployment plan, minimizing any concerns of downtime. Without modifying any hardware or software, the Zingbox team configured the IoT Guardian solution to monitor and secure specific sets of devices and VLANs at a time. After monitoring device statuses and being assured that the changes hadn't caused issues, they then sequentially expanded the coverage to other areas of the network. This phased approach enabled

> "Zingbox eased the concerns of our networking team and spoke their language from a technical perspective."
>
> – Tarun Trivedi, Information Security Manager

Tarun and his third-party security vendors to repurpose their existing security platforms while adding new levels of visibility and protection.

"Zingbox eased the concerns of our networking team and spoke their language from a technical perspective," says Tarun.

After the IoT Guardian configuration was completed, Tarun had full visibility into the type of devices in his network along with all the network traffic originating from the devices within and beyond the network. Zingbox's IoT Guardian helped him discover that the approximately 1,000 devices in his system consisted of 40 device types, including five different kinds of security cameras.

With its machine learning and three-tier profiling technology creating a unique "personality" for each device, Zingbox alerts Tarun and his team members whenever a device strays beyond its normal behavior. For example, Zingbox discovered that a printer was communicating with its manufacturer to receive software updates. This violated Waubonsee's security policy, which specified that devices should only install software updates via internal servers. Zingbox alerted Tarun that this device was engaging in high-risk behavior, allowing his team to promptly change the printer settings and reduce the risk of a breach.

The Power of Multi-Dimensional Risk Management

When Tarun provides a status report to his CIO, he is now able to show a comprehensive list of all devices at Waubonsee and their risk levels. The visibility that Zingbox provides clarifies any previously unknown risks, and he has confidence that he has an accurate picture of IoT security across Waubonsee's network.

As with many other industries involving sensitive user data, higher education is regulated by strict security standards. Educational institutions like Waubonsee invest heavily in security, since any vulnerability in smart building devices, cameras, payment machines, computers, and more could enable hackers to steal critical student data anywhere in the network.

However, ensuring security shouldn't come at the cost of facilitating open and collaborative learning. For example, in order to foster Waubonsee students' interest in pursuing programming careers in gaming, Tarun's team helped gaming clubs on campus create their own tendered file networks to support students' personal gaming consoles and files. With Zingbox, Tarun can easily monitor students' devices without disrupting their academics or recreational time.

In a digitally-interconnected system like Waubonsee, Tarun says that *"risk needs to be dealt with from all perspectives and not just one dimension."* As opportunities for users to engage with technology continues to grow, gaining visibility and control over multi-dimensional IoT security risks will be even more paramount for organizations in any industry.

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.