◉ • SECURI**THINGS**

LEADING UNIVERSITY STREAMLINES IOT OPERATIONS WITH SECURITHINGS HORIZON

For a Leading University with thousands of physical security IoT devices spread throughout its campus, the operational management of these devices was a major challenge. Without a single centralized system for the university's physical security team to monitor and control these devices from, they struggled to ensure that they were working consistently and securely. To bring a new level of visibility and reliability to the operational management of all these devices, the team started using SecuriThings Horizon. Today, Horizon continually provides the university's physical security team with the real-time information and control needed to manage its devices, in turn improving campus safety.

THE CHALLENGES

A Leading University wanted to bring a new level of reliability to the management of its thousands of security devices, which are spread over dozens of buildings across multiple locations. These devices play a critical role in campus security, with the campus safety officers relying on them for both real-time video streaming and recording of incidents. The role of these cameras is to keep students, faculty, and staff safe, but the way they were being managed presented a risk to the privacy and safety for those on campus – especially in case of lapses in cybersecurity best practices such as regular password rotation and firmware upgrades.

The main challenges:

- The lack of a single platform for the operational management of devices, as well as standardized and consistent procedures for their operational maintenance. Instead, these devices – including a wide variety of types and models from multiple brands – were being managed on an ad hoc basis.

- The university's security team lacked visibility and control over their devices. As a result, whenever a device malfunctioned, went offline, or encountered other expected or unexpected issues, the team would need to manually investigate the problem, which would often involve rolling out a truck to visit the location.

> **The ad hoc approach to operationally managing devices cost the university by creating extra manual work, while also creating a risk that devices could stop functioning or introduce a security vulnerability.**

Understanding the critical role of cameras in ensuring the safety of the university's students, faculty, and staff – in sensitive areas including dorms, locker rooms and clinics – the physical security team realized that they needed a more effective solution for managing the operational aspects of their devices. Realizing that automation could make a powerful difference in this regard, the team decided to start using SecuriThings' Horizon solution.

THE FINDINGS

Once Horizon was deployed, it immediately uncovered several high-severity security and operational risks – empowering the university's physical security team to mitigate these threats immediately.

Horizon's key findings included:

- 30% of cameras were running firmware versions that were not updated and had critical vulnerabilities, opening the university to potential security threats.

- Poor password rotation compliance had resulted in a cybersecurity breach where an external IP linked to a suspicious Russian server was communicating with the university's edge devices.

- An internal IP had been attempting to execute brute-force attacks on multiple devices.

THE HORIZON SOLUTION

Horizon brings the power of automation to IoT device management, providing the university's physical security team with the real-time visibility and control necessary to minimize camera downtime and ensure that each camera is running the way it should be. Additionally, by standardizing and centralizing the operational management of all these connected devices, Horizon empowers this team to ensure compliance with relevant privacy laws, while also increasing the efficiency of the management of on-campus cameras.

Specifically, integrated into one single, convenient platform, Horizon provides detailed and actionable analytics in real time, across all sites and all cameras. This allows the physical security team to constantly stay aware of the situation and respond rapidly when alerted.

Using Horizon enabled the campus security team to implement a password policy and regularly rotate all device passwords to a strong password generated by the platform, and also update all their firmware to the optimal version – automatically and seamlessly with just the click of a button.

In addition, the university's physical security team is now able to continuously monitor the health status of its devices, so they can tell whether any of these devices is reaching end of life or poses any risk – allowing the university to plan more effectively. They also use the system's automated alerts to identify when a device malfunctions, goes offline, or encounters other expected or unexpected issues.

"Thanks to SecuriThings, we finally have ongoing visibility into the security status of our large network of IP cameras. We are now looking to expand the scope of devices monitored by Horizon to additional IoT-enabled systems." Director of Campus Safety, A Leading University

THE BENEFITS

By using SecuriThings Horizon, the university has achieved the following business outcomes:

Improved system availability
Real-time device status data results in increased up-time of devices

Dramatic cost savings
Centralized automation of operational activities result in minimal manual, on-site maintenance work

Compliance you can count on
Device compliance achieved through implementation of internal policies

Protection from cyber threats
Exposure of devices to security vulnerabilities is prevented

Visibility for future planning
Health status of devices continually assessed, including end of life device planning