CASE STUDY FOR CAMPUSES' CONNECTED DEVICES

IVY LEAGUE UNIVERSITY MAXIMIZES SECURITY AND OPERATIONAL EFFICIENCY WITH **SecuriThings HORIZON**

Security and safety are key criteria for students and parents selecting an educational institution. Accordingly, universities have made **major investments in physical security devices** such as video surveillance and access control, as well as smart systems for behavior monitoring to mitigate security incidents and ensure student and staff safety (e.g., face and license plate recognition to track individuals and vehicles entering, etc.).

However, managing these large-scale deployments of connected devices has become a liability due to the **inherent vulnerability, physical accessibility and manual maintenance** of these devices. In fact, IoT devices are prone to failures and represent easy entry points for cyber-attacks. The challenge is even bigger as these devices are **remotely deployed in large campuses** within multiple buildings and assets (e.g., schools, libraries and administration buildings, streets, etc.).

A service breakdown resulting from either cyber-attack or any operational issue on a single device could have severe consequences – from generating huge reputation damage to threatening lives.

> "Thanks to SecuriThings, we finally have ongoing visibility into the operational and security status of our large network of connected devices"
>
> *Ivy League University, Director of Campus Safety*

PROTECT IoT DEVICES. MAXIMIZE OPERATIONAL EFFICIENCY.

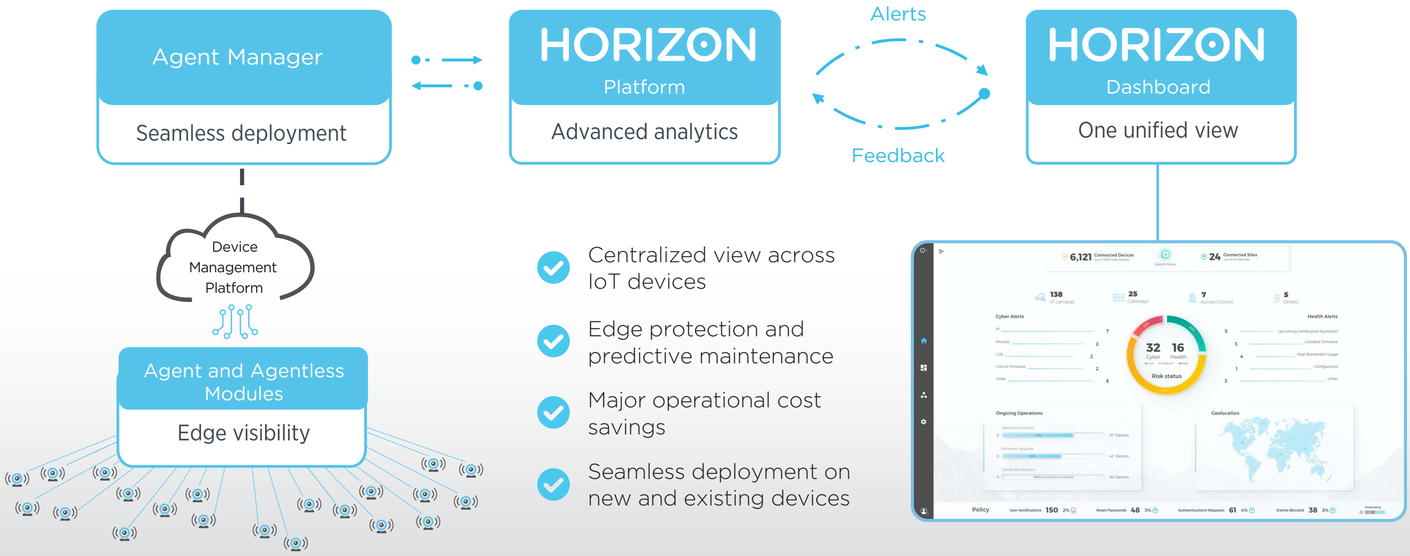
A renowned Ivy League university had a **complex network with many subnets** which made it **complicated to manage** from a security standpoint. Moreover, the university's IT department had **zero visibility and control over its connected devices,** deployed across large physical distances (including hundreds of cameras of various model types and firmware versions). The Director of Campus Safety sought an operational management solution for the police and IT departments to gain visibility over all physical security devices.

SECURITHINGS

SecuriThings Maximizes Security Efficiency

SecuriThings **HORIZON** is a software-only solution automating the operational management of connected devices deployed in large campuses. The software-only solution provides risk mitigation, predictive maintenance and automated operations.

Horizon's connection to the university's central Video Management System (VMS) enabled a seamless deployment on existing and new video surveillance devices. From that point on, Horizon performs 24/7 monitoring and analysis of all device operations.



Agent Manager

Seamless deployment

HORIZON Platform

Advanced analytics

Alerts

Feedback

HORIZON Dashboard

One unified view

Device Management Platform

Agent and Agentless Modules

Edge visibility

- ✓ Centralized view across IoT devices
- ✓ Edge protection and predictive maintenance
- ✓ Major operational cost savings
- ✓ Seamless deployment on new and existing devices

Fast and Actionable Results

Immediately following deployment, SecuriThings HORIZON raised several high severity alerts and discovered multiple security risks:

- Cameras running vulnerable or outdated firmware versions
- High-risk exposed services (FTP, UPNP, SSID, etc.)
- Internal and external suspicious communications
- Devices exposed and accessible from the internet
- Suspicious processes on the device level
- Legitimate processes listening on abnormal ports

Together with these findings, the university also received recommendations for mitigating the newly discovered risks on suspicious devices such as updating vulnerable firmware with patched versions, blacklisting IPs, etc.

Thanks to deploying SecuriThings Horizon, the Ivy League university had **full visibility and control over its video surveillance devices for the first time.** It is now looking to expand the scope of devices monitored by Horizon to additional IoT-enabled systems.