Ivy League University Maximizes Security and Operational Efficiency with SecuriThings Horizon

IoT Devices are Making Campuses Smarter and Safer

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.

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 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.

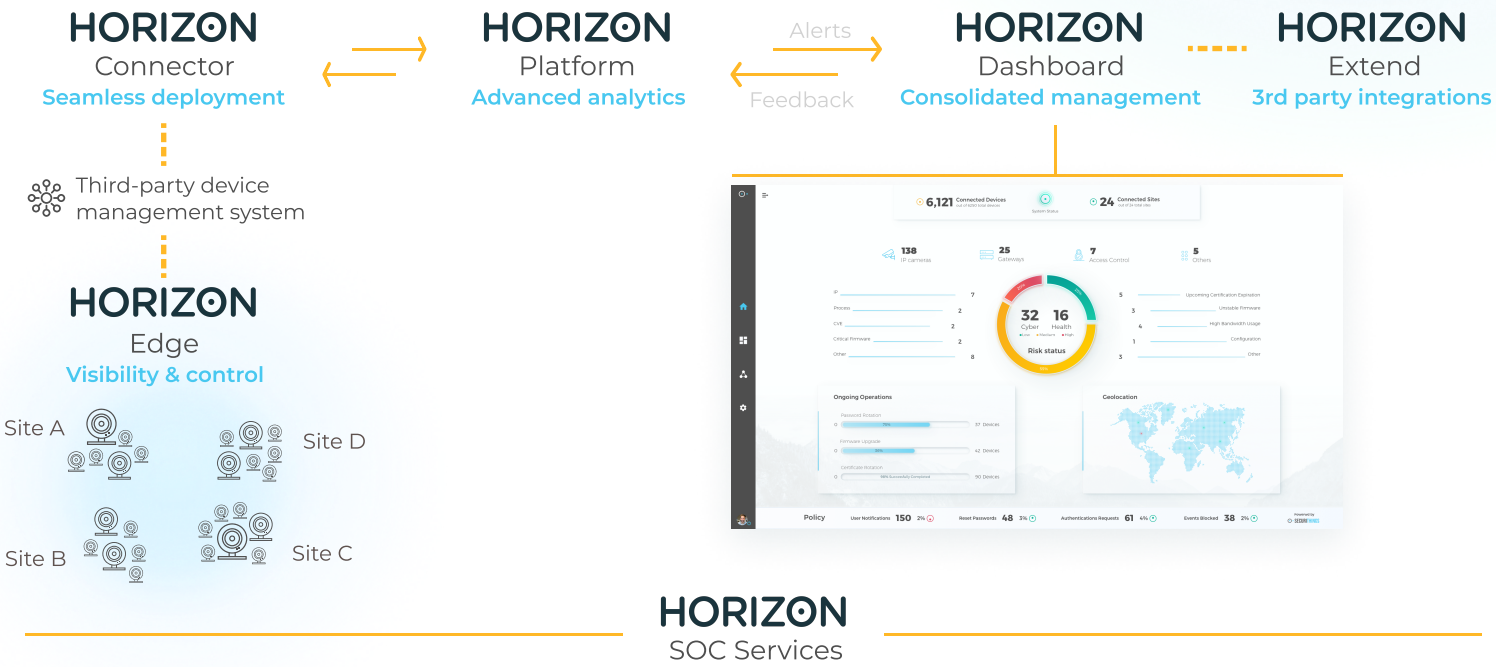
Case Study: Ivy League University

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 Horizon Maximizes Campuses' Security and Operational Efficiency

SecuriThings Horizon is **the first IoTOps solution** automating the operational management of connected devices. The software-only solution provides **risk detection, predictive maintenance and automated operations**. Horizon has been seamlessly deployed on existing and new video surveillance devices by connecting to the university's central Video Management System (VMS). From that point on, Horizon is performing 24/7 monitoring and analysis across all devices.



Fast and Actionable Results

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

- 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

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 SecuriThings, we finally have ongoing visibility into the operational and security status of our large network of connected devices"

Director of Campus Safety, Ivy League University