



Safety & Compliance: Why Device Management is Critical to the Transportation Industry

The transportation industry invests heavily in physical security devices to make sure that key infrastructure such as airports, seaports, and railroads are protected from a range of dangers, including terrorism, cyberattacks and other criminal activities. But in many cases these devices aren't delivering their full potential value, leaving campuses open to enormous risks.

Are Your Devices Properly Maintained?

On average:

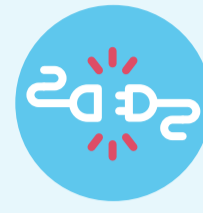


8% of devices are misconfigured



57% are running on outdated firmware

In a typical week:



6% of physical security devices are disconnected from their network



4% of cameras are disconnected from their video management system

Unmanaged devices = An Open Door For Cyber Attacks

On average:

40% of devices are vulnerable to attack due to outdated firmware



41% of cyberattacks exploit IoT device vulnerabilities

15% devices have reached their end of life, and therefore no longer supported by their manufacturers - including security patches

Weak device passwords are commonly exploited by attackers, due to unchanged manufacturer - set passwords and poor password security practices

The Cost of "The Status Quo"



2.56 Million passengers a day pass through TSA checkpoints



\$3.59 Million The cost of the transportation industry's average data breach (2022)



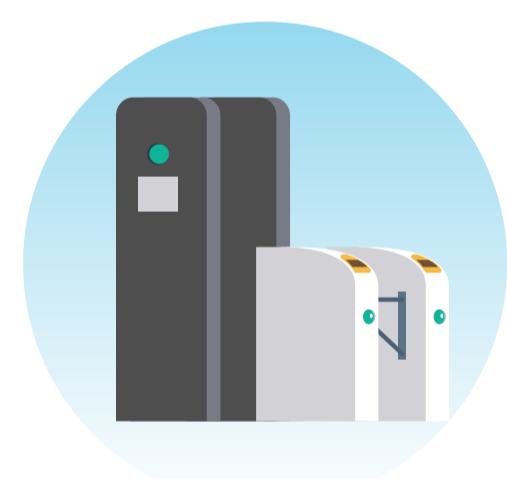
\$8.4 Trillion The global cost of cybercrime in 2022



\$11 Trillion The forecast cost of cybercrime in 2023



Reputational damage from a data hack can be enormous, and hard to shake off



TSA has demanded proactive steps to minimize the aviation industry's vulnerability to cyberattacks

The Need for an Effective Physical Security Solution



At the end of the day, the transportation industry's top priority is protecting people from the risks of terrorism, smuggling, and other crimes - without leaving them vulnerable to cybercriminals. That's why physical security managers need to operationally manage their devices consistently, making sure they run reliably.



So, What Can You Do?

With the SecuriThings platform you can gain full visibility and control of all your physical security devices and the power to respond rapidly whenever necessary, whether remotely or on site.



Improved system availability

Minimize device downtime. Get real-time data on device status and manage operational issues whenever they arise.



Ensured compliance

Ensure organizational compliance with automated maintenance processes set based on organizations' internal IT policies and relevant legal regulations.



Significant cost savings

Reduce manual labor and on-site visits, as well as other expenses related to managing physical security devices. Diagnose and resolve all issues, all in one consolidated platform.



Protection from cyber threats

Detect and prevent security vulnerabilities from compromising your devices. Automate crucial maintenance activities such as password rotation and firmware upgrades.



Visibility for future planning

Plan for device end of life, and prioritize your maintenance activities and budget accordingly.