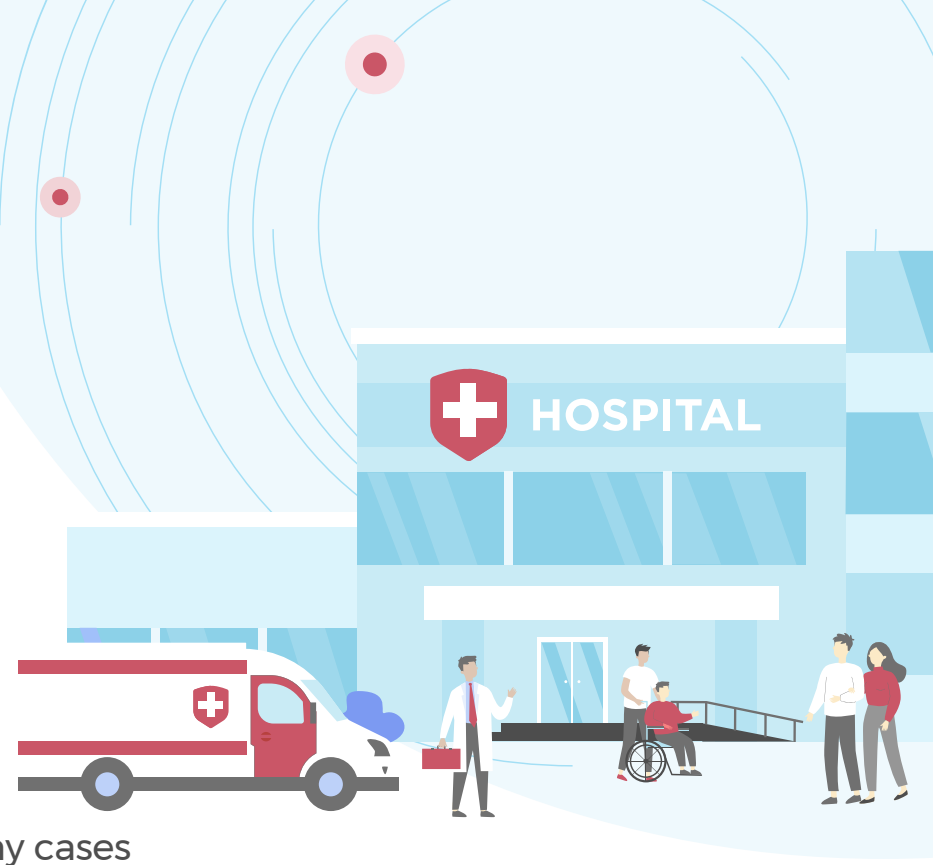# SECURITHINGS

Healthcare Institutions Face Unprecedented Physical and Cyber Security Threats – How to Overcome Them?

Hospitals invest heavily in physical security systems. But in many cases these devices aren't delivering their full potential value – leaving hospitals vulnerable to threats both physical and cyber in nature.

Physical Security Must Remain a Top Priority

Workplace accidents, violence and crime are a sad reality

Injuries from violence higher among medical professionals than any other profession
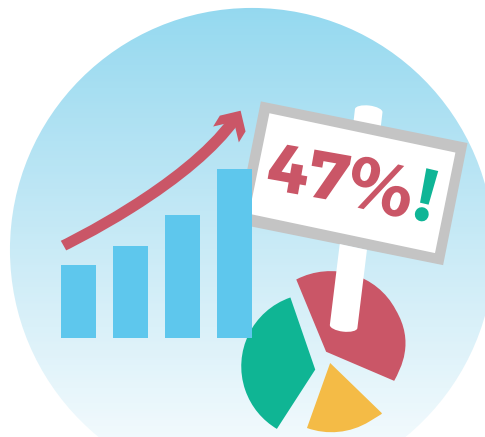
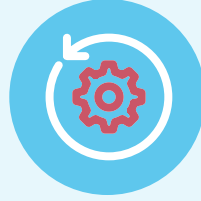**47%** increase in violent crime in U.S. hospitals in 2021

221,400 work-related injuries and illnesses at U.S. hospitals in 2019 alone

Are Your Devices Properly Maintained?

On the average:

8% of devices are misconfigured

57% are running on outdated firmware
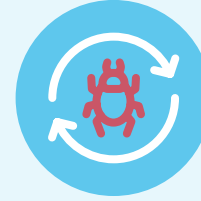
46% have passed their end of life

In a typical week:

6% of physical security of devices are disconnected from their network

4% of cameras are disconnected from their video management system

40% of physical security devices have at least one cybersecurity vulnerability

The Cost of "The Status Quo"

$7.8 Billion was lost to data breaches at U.S. medical organizations in 2021

19.76 Million patient records were compromised in data hacks

$10.1 Million Is the average cost of a data breach for an organization in the healthcare sector as of 2022

⚠ *HIPAA non-compliance can have severe consequences

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.