SECURITHINGS

Technology Companies' Cyber Security Hinges on Physical Security Devices

Tech companies invest heavily in physical security devices – not only to protect their premises and staff, but also to secure their data and intellectual property. But in many cases these devices aren't delivering their full potential value, leaving companies 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57% are running on outdated firmware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 of 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40% of devices are vulnerable to attack due to outdated firmware

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

41% of cyberattacks exploit IoT device vulnerabilities

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"

90% of the market value of S&P 500 companies consists of "intangible assets" including intellectual property, as of 2022

$4.97 Million was the average cost of a data breach for a technology company in 2022

$8.4 Trillion The global cost of cybercrime in 2022

$11 Trillion The forecast cost of cybercrime in 2023

GDPR, CCPA and CPRA non - compliance can have severe consequences

Reputational damage from a data hack can be enormous, and hard to shake off – e.g. the Verkada hack

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.