Securing IoT Devices for PSTI Compliance

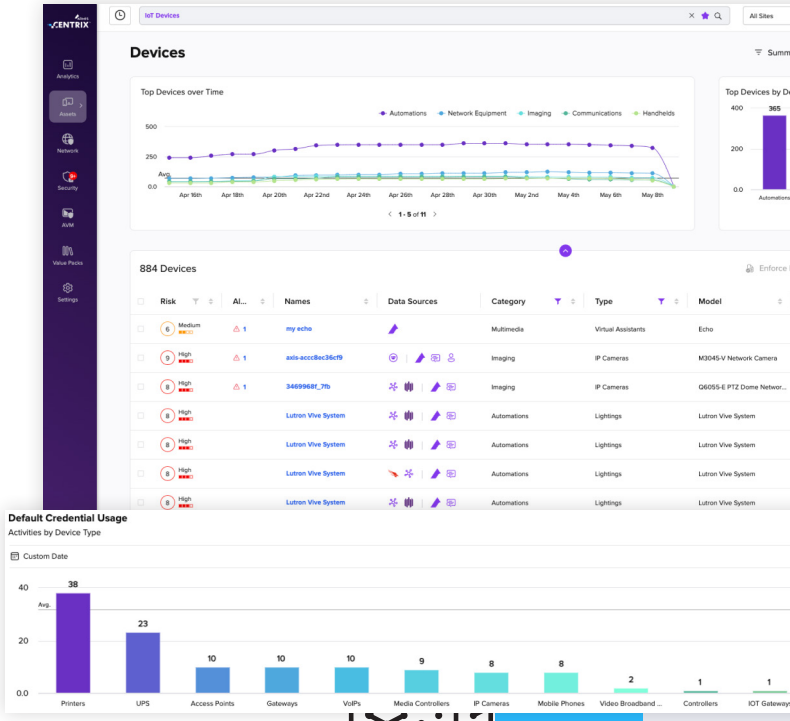
The Growth of Internet of Things (IoT) Devices is Transforming our Digital World

From smart thermostats to industrial sensors, IP cameras, and elevators, these innovations increase efficiency with new advancements. Yet, they also introduce significant security risks.

The UK has taken a leading role in enhancing IoT security with the UK's Product Security and Telecommunications Infrastructure (PSTI) Act, effective April 29 2024. This law makes the UK the first country to require the removal of default usernames and passwords in IoT devices.

This step is key as the number of IoT devices is expected to reach over 29 billion by 2030. The known security flaws of IoT devices emphasize the need for stronger security measures. The PSTI Act is a benchmark for IoT manufacturers and could inspire similar regulations worldwide.

The security of IoT devices is complex, with each device posing a risk for cyber threats. The vast and fast-growing array of IoT devices are often ignored or not prioritized by organizations, making them more susceptible to cyber-attacks. This issue underlines the importance of thorough visibility into all connected devices to strengthen an organization's security posture.



PSTI Requirements

Ban default passwords. Products that come with default passwords are an easy target for cyber criminals.

Require products to have a vulnerability disclosure policy. Security researchers regularly identify security flaws in products, but need a way to give notice to manufacturers of the risk they have identified, so that they can enable the manufacturer to act before criminals can take advantage.

Require transparency about the length of time for which the product will receive important security updates. Consumers should know if their product will be supported with security updates, and if so, what the minimum length of time is that they can expect that support to continue.

Armis is enabling PSTI compliance

1. **Discover and inventory all assets in a network** to which this act applies.
2. **List events** in real time such as when someone is logging into a IoT device with default credentials.
3. **Identify and track disclosed and undisclosed vulnerabilities** so you can better manage your Vulnerability Disclosure Policies with actionable threat intelligence.
4. **Improve transparency** around IoT security updates and lifecycle management.
5. **Track the use of common default passwords** used to access devices over unencrypted protocols.