4

Tips for Ensuring Security in Connected Devices

psacertified™

1

Prepare for Regulations by Utilizing Third-party Certification

- There is a growing recognition that devices must now be designed to protect consumer data and privacy

- This has led to increasing cyber security standards, regulations and baseline requirements that underpin how OEMs build IoT devices

- This can be confusing and costly, but third-party programs like PSA Certified are designed to help
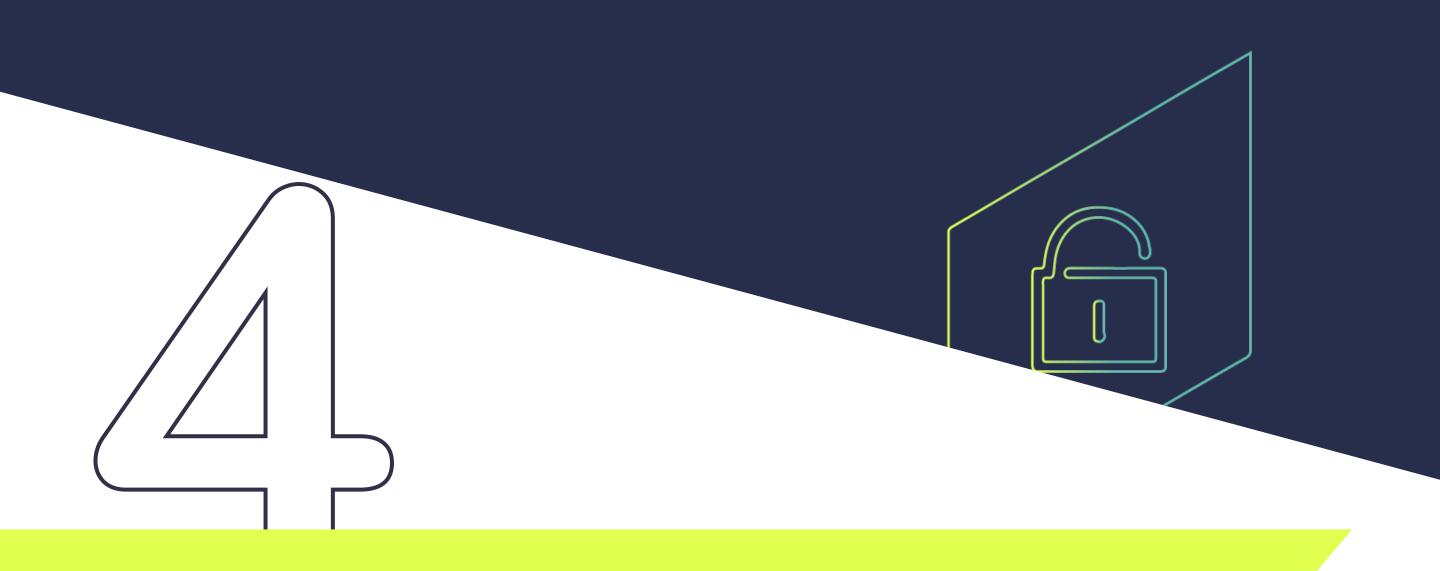
2

Show You Proactively Care About IoT Security

- Consumers today are far more knowledgeable buyers than in the past

- They want to know the devices they buy have security standards built in

- Seeking independent certification helps demonstrate that IoT security solutions have been built into devices correctly

3

Be Part of a Shared IoT Security Approach and Create a Security Community

- Manufacturers and OEMs all operate in distinct territories and jurisdictions

- This fragmented ecosystem leaves consumers unable to understand the cyber security standards built into their devices

- 96% of respondents in the PSA Certified 2022 Security Report are interested in an industry-led set of guidelines to help build IoT security

- Our guidelines have been built on collaboration by industry-leading security experts across the globe and give OEMs a fast track to deploying the best security requirements into a device's hardware and firmware

4

Follow the Industry-Backed Approach

- PSA Certified was developed to streamline and simplify standard device security for OEMs

- These products are built on a Root of Trust — a fundamental set of implicitly trusted functions that the system/device can rely on

- Together, the award-winning PSA Certified ecosystem is building security into devices and ensuring that consumers can safely enjoy their new connected products this Cyber Monday

Learn more about our approach for securing connected devices here