OTA
Online Trust Alliance
an Internet Society initiative

# THE ENTERPRISE IOT SECURITY CHECKLIST

Best Practices for Securing Consumer-Grade IoT in the Enterprise

## CONSUMER-GRADE IOT IN THE ENTERPRISE

The Internet of Things (IoT) has found its way into all aspects of our lives. In particular, "consumer-grade" IoT devices such as smart TVs, thermostats, smart speakers, fitness trackers and other devices are now used regularly in enterprises, either purchased by staff or brought in by employees.

This IoT insurgence represents a unique challenge since many of these devices are not accounted for as a normal part of IT security planning, yet they have characteristics that can create serious vulnerabilities. While some IoT products are designed with strong security, many have a simple or non-existent user interface, default (or hardcoded) passwords, open hardware and software ports, limited local password protection, lack the ability to be updated, "phone home" frequently, collect more data than expected and use insecure backend services.

The consequences of using these devices range from unauthorized access to other enterprise systems, to surveillance via audio, video and data, to use of those devices to attack other connected devices or services. To help enterprise IT staff address these issues, the Online Trust Alliance, an initiative of the Internet Society, created this best practices checklist (ordered chronologically from installation through end of life) for use of consumer-grade IoT in enterprises.

Underpinning this list are several core concepts. Enterprises should: be proactive and fully consider the possible risks introduced by these devices; understand that IoT devices are likely more vulnerable than traditional IT devices; educate users on IoT device risks; and strike a balance between controlling IoT devices vs creating "shadow IoT."

## BEST PRACTICES CHECKLIST

□ Just as in guest networks, place IoT devices on a separate, firewalled, monitored network. This allows you to restrict incoming traffic, prevent crossover to your core network and profile traffic to identify anomalies.

□ Update all passwords (local and remote, if different) to strong passwords and use multi-factor authentication where possible. Do not use products with hard-coded passwords. Closely govern permissions for devices, delegating access only when necessary.

□ Turn off any functionality that's not needed. This includes cameras, microphones or even connectivity itself (e.g., if a smart TV is merely for display, not connectivity). It may also include physical blocking/covering of ports, cameras and microphones.

□ Verify that physical access does not allow intrusion (e.g., by simple restart, easily accessible hardware port or default password).

□ Don't allow (or severely restrict) automatic connections via WiFi or other means. This will restrict the ability of other devices to connect and infiltrate an IoT device.

□ If incoming traffic is not blocked, check for open software ports that may allow remote control and configure or restrict them as appropriate.

□ Enable encryption whenever possible so that data is never transmitted "in the clear." Consider buying only devices that support encryption. Otherwise, consider using a VPN or other means to limit data exposure.

□ Research the security and privacy characteristics of the controlling apps and back-end services. Do not use devices that rely on services with poor security and privacy.

□ Keep firmware and software updated (via automatic updates or monthly checks). Do not use products that cannot be updated.

□ Closely follow the lifecycle of the devices so that they can be removed from service when they are no longer updatable or secure.

For additional guidelines regarding IoT security, privacy and lifecycle issues, see the OTA IoT Trust Framework.

https://otalliance.org/IoT