I

Internet of Things (IoT): Examples, Risks, and Security

The Internet of Things connects devices that sense or affect the physical world. Their long lifecycles, data collection, and limited controls require planning.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What makes a device IoT?
02 Why IoT security is different
03 What to check before buying
04 Secure deployment checklist
05 Monitoring and incident response
06 Manufacturer responsibilities
07 Sources

Quick answer: The Internet of Things (IoT) is the ecosystem of connected devices that sense, process, communicate, or affect the physical world. Examples include cameras, thermostats, medical devices, industrial sensors, smart speakers, vehicles, and building

controls. Secure IoT use requires product evaluation, unique credentials, updates, segmentation, monitoring, and a retirement plan.

01 What makes a device IoT?

An IoT product usually combines a physical device, software or firmware, network connectivity, and often a cloud service or mobile application. The device may collect environmental or personal data, receive commands, or change physical conditions. A traditional computer can run many applications, while an IoT device is often designed for a narrower purpose, but the boundary is not absolute.

IoT security includes more than the device. The app, cloud API, vendor update service, account, home or business network, and third-party integrations all affect risk.

02 Why IoT security is different

- Devices may remain installed for years after the vendor stops security updates.
- Owners may not know the device contains software or exposes a network service.
- Interfaces, storage, memory, and logging can be limited.
- A compromise can affect privacy, safety, operations, or the physical environment.
- Default credentials and identical fleet configurations can turn one weakness into a large botnet.
- Cloud shutdown or account loss can remove important functionality even when hardware still works.

03 What to check before buying

1. Confirm the published support period, update mechanism, security-contact process, and vulnerability-disclosure policy.

2. Check whether credentials are unique, passwords can be changed, MFA is available, and local operation is possible if cloud service ends.
3. Understand what data is collected, where it is stored, who receives it, and how it can be deleted or exported.
4. Verify that unnecessary interfaces can be disabled and configuration can be backed up or securely reset.
5. For organizational purchasing, require an asset identifier, software or component information where appropriate, logging, secure updates, and documented end-of-support.

04 Secure deployment checklist

Change default credentials and use a unique password stored in a password manager. Enable automatic verified updates when operationally safe. Place IoT devices on a separate network or VLAN with only the communication they need. Block unsolicited internet access to management interfaces; avoid port forwarding and disable unused remote management and universal plug and play.

Inventory the model, serial number, owner, location, IP and MAC addresses, firmware, data handled, dependencies, support date, and reset procedure. Configure privacy and recording settings deliberately. Review integrations and remove unused vendor or voice-assistant links.

05 Monitoring and incident response

Monitor DNS, outbound destinations, bandwidth, configuration changes, failed logins, and traffic when the device should be idle. A security alert, unexpected reset, new administrator, abuse complaint, or connection to unfamiliar infrastructure requires investigation.

1. Isolate the device without causing a safety or operational hazard.
2. Record network, account, configuration, and alert evidence; coordinate with the responsible operational owner.
3. Reset credentials and revoke cloud sessions from a clean device.

4. Install trusted firmware or factory-reset and reconfigure manually. Do not restore an unverified configuration.
5. Replace the device if it is unsupported, cannot be securely updated, or lacks controls needed for its risk.

06 Manufacturer responsibilities

Security cannot be shifted entirely to customers. NIST’s IoT baseline identifies capabilities such as device identification, secure configuration, data protection, logical access control, software update, cybersecurity-state awareness, and device security. Manufacturers should also provide documentation, vulnerability reporting, and security information throughout the product lifecycle.

07 Sources

Current manufacturer guidance is in NIST IR 8259 Revision 1; device capabilities are listed in the NIST IoT Cybersecurity Capabilities Catalog.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com