THOUGHT LEADERSHIP

Weblib

IoT devices: the weak link in your network?

How to simplify IoT device integration and security for your business?

Table of contents

How to simplify IoT device integration and security for your business? 3

The biggest challenges in managing IoT devices on your network 4

IoT security: a matter of organizational readiness? 5

The overlooked risks of using consumer devices 6

Best practices for securing your IoT ecosystem 7

Key Insights from our expert 8

How to simplify IoT device integration and security for your business?

Frédéric Kretzer,
Head of product, Weblib

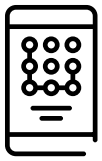
IoT covers a vast landscape, from simple sensors (temperature, motion, lighting) to complex systems like predictive maintenance or production control. What most of these devices have in common is the lack of a screen or keyboard—which means no captive portal—and the absence of a streamlined onboarding process to secure them with certificates (e.g., WPA3-Enterprise) or individual passwords. Their networking capabilities are, therefore, extremely basic, making them hard to integrate into secure environments. This diversity and lack of standard interfaces create real chaos when it comes to security and identification. According to a 2020 study by U.S. cybersecurity firm Palo Alto Networks, **nearly 98% of IoT traffic in business environments was unencrypted.**

Fast-forward to early 2025: cybersecurity experts witnessed a devastating comeback of the notorious Mirai botnet, known—quite fittingly—as "Mirai Resurrection". First emerged in 2016, Mirai exploited connected devices through weak authentication mechanisms, mainly default passwords. This time, the attack was supercharged by AI, enabling automated scans of billions of IoT devices with unprecedented speed and precision. **Over 5 million devices were compromised in just a few days*.**

In practical terms, taking permanent control of an IoT device and turning it into an attack vector is all too possible, just as easy as harvesting its data. Consider a retail store where a security camera is connected to the internal WiFi network ("Store-Internal") using its default credentials (admin/admin)." A nearby attacker logs in effortlessly through the camera's web interface and finds the company's WiFi key stored in plain text. With that key, they can join the internal network as a legitimate user. From there, it's open season: scanning servers, stealing sensitive data, or unleashing ransomware. **One small oversight on a seemingly trivial device can open the door to a major security breach.**

* Source: https://hoploninfosec.com/internet-of-things-iot-vulnerabilities/

The biggest challenges in managing IoT devices on your network



Heterogeneity

Devices come in all shapes and sizes, with different features, capabilities, and manufacturers.

Security

These devices are far more vulnerable to security flaws, and they require special attention.

Authentication

Without bulk onboarding, traditional authentication methods simply don't work.

Identification

Devices often lack clear identification, making it hard to know what's connected.

Which raises the question:
How can you simplify IoT integration and security for your business?

Here's our answer.

IoT security: a matter of organizational readiness?

From experience, we know that a significant proportion of IoT devices used in business environments are “non-compliant”—sometimes even the majority, depending on the sector or organization type (especially in retail and large, distributed organizations).

These are often consumer-grade devices, such as surveillance cameras, not designed for secure professional use. For instance, many SMEs and small branches of large corporations use consumer-grade network equipment like ISP-provided routers.

These routers ship with wide-open default settings: every port is open for outbound traffic, and there’s zero filtering. So even if your primary network password is strong—a hardcoded WPA2 key on the IoT device—storing it in plain text on a poorly secured secondary device makes that strength meaningless.

In general, most small businesses do not use proper solutions to secure their networks. They face a major challenge in network infrastructure security, mainly due to a lack of resources and security knowledge. Large enterprises are not immune either, as their distributed structures often result in inconsistent security levels, making the job just as tough.

The overlooked risks of using consumer devices

- **Use of default passwords and weak authentication**
  Many consumer-grade IoT devices ship with default credentials (e.g., "admin/admin") that users never change. Hackers know this and can easily guess or find these credentials online, granting them unauthorized access.

- **Neglected firmware updates**
  Manufacturers of consumer-grade hardware often overlook firmware security (the device's built-in software) or fail to release regular updates to patch known vulnerabilities, leaving devices wide open to attacks.
- **Weak or missing encryption**
  Data exchanged between IoT devices and their servers or apps is often poorly encrypted—or not encrypted at all—making it easy for attackers to intercept and read sensitive information (such as video streams from cameras).

- **Software vulnerabilities**
  Embedded software frequently contains exploitable flaws, giving attackers a path to remotely control the device.

Another key point: Shadow IT and BYOD (Bring Your Own Device). In other words, employees using personal devices on the corporate network, with smartphones being the most common example.

"By using their personal devices, some employees effectively bring their home network into the company, without realizing the consequences. The issue often isn't budget, but awareness. In most cases, it's not negligence; it's a drive to innovate, meet time-to-market pressures, or compensate for the lack of simple solutions provided by their IT department."

Best practices for securing your IoT ecosystem

Combining insecure IoT devices with a weak network infrastructure creates a potential disaster scenario. What's more, configuring network rules (e.g., firewall policies) is often seen as complex, leading to an "open bar" approach. **Yet a minimum level of security is often enough to deter opportunistic hackers.**

The first step is to demystify IoT security and show that an initial layer of protection is easy to implement. **The first rule of IoT security is network segmentation.** Isolating IoT devices on dedicated networks (physical or virtual) can really limit threat propagation. Ucopia makes segmentation easy, with a major advantage: simple configuration compared to other solutions. Only basic network configuration skills are required.

To kick off this process, Ucopia can run an instant traffic and device audit. This provides instant visibility into network activity, identifying all IoT devices, including those introduced through Shadow IT. **It's the critical first step: taking inventory before applying security measures.**

- **Device identification and registration:** Ucopia detects IoT devices and provides administrators with tools to register them on the network. This includes assigning details such as name and description, and linking each device to a Ucopia profile.
- **Ucopia profile creation for IoT devices:** Just like users, IoT devices receive Ucopia profiles that define their network access rights, such as zones, services, and connection schedules. This ensures granular control over security and usage.
- **Activity logging:** Ucopia logs all IoT device activity, giving administrators complete visibility into network usage by both users and devices.

With Ucopia, securing consumer IoT devices takes less than two hours per site. Ucopia connects to your network infrastructure and, within minutes, starts monitoring traffic and automatically detecting all connected devices. **No more tedious manual inventory.** Your team gains instant, full visibility into everything that's actually on your network. With signature and behavior analysis, Ucopia goes well beyond basic MAC address detection. It identifies and profiles devices, instantly recognizing a Samsung TV, a Google Chromecast, or an Arlo security camera. **This automatic classification is the key to applying the right security policies with minimal effort.**

Key Insights from our expert

“Ucopia can serve as an initial onboarding gateway for IoT devices, simplifying a step that’s often a real challenge for IT teams.”

Frédéric Kretzer,
Head of product, Weblib

Passionate about technology from the start, Frédéric draws on his IT expertise to tackle your challenges with a fresh, innovative perspective.

Here’s how to get started on the right track:

- **Raise awareness and educate employees about security**, since lack of knowledge is often a barrier to implementing best practices..
- **Emphasize the importance of network segmentation** for security, as most IoT traffic is unencrypted. Isolating IoT devices on separate networks is essential.
- **Choose solutions that are easy to configure** to simplify IoT device onboarding into a secure network. Deployment should be straightforward and accessible, enabling businesses of all sizes to effectively secure their IoT devices.

Ucopia, Europe’s leader in wireless connectivity

INTEGRATIONS

Thanks to its global network of technology partners, Ucopia integrates seamlessly with most existing systems, without disrupting your current infrastructure.

SUPPORT

Ucopia offers outstanding technical support and a team of wireless connectivity experts who provide personalized assistance, guidance, and recommendations tailored to your specific needs.

Weblib | +33 (0)1 88 40 52 15 | weblib.com

TALK TO OUR EXPERTS

All rights reserved WEBLIB / UCOPIA. This document is for informational purposes only and may not be reproduced in whole or in part without prior authorization from WEBLIB / UCOPIA, under penalty of legal action.