



How SWISSCOM saves USD 400,000 per avoided IoT security incident through automated firmware analysis

Pioneering IoT Firmware Security as Key to Quality of Service, Vendor Relations, and Brand Reputation

Pioneer even in Times of Increased Complexity

Swisscom is Switzerland's leading telco and one of the country's largest IT service providers, with a market share of more than 60% in mobile and broadband, and a total revenue of CHF 11.5B (2019).

For over a century, Swisscom has served as the quality gateway for telecommunications products on the Swiss market. Thanks to the firmware analysis capacities provided by IoT Inspector, Swisscom runs tests that were previously neglected by manufacturers, and thereby enforces its pioneering position even as device security grows ever more complex.

Executive Summary

Swisscom analyzes around 80 firmware images per year with IoT Inspector, mainly during the purchasing process for new IoT devices, but also in continuous product development and support. Thus, Swisscom achieves a security ROI of up to 374k CHF per avoided firmware rollout by:

- Improving IoT security and strengthening its negotiating position with device manufacturers thanks to automated security analysis and compliance checks, which are often neglected by manufacturers.
- Minimizing repair and maintenance costs by systematically identifying critical security vulnerabilities prior to new firmware rollouts.
- Ensure world-class service and brand reputation by maintaining the highest security standards for customer premises equipment.

Swisscom started working with IoT Inspector in 2015. When the telco initially implemented the platform, it was mainly focusing on the analysis of customer-premises equipment (CPE) designed for its private and SME customers. As IoT device manufacturers struggle with short product lifecycles, heavy competition, complex supply chains, and intense focus on ever-evolving product features, security often falls short.



Bringing Transparency into Opaque Supply Chains

IoT Inspector serves as a quality gateway for CPE – be it for private and SME customers – such as Wi-Fi routers and repeaters, hotspots, and other devices that can be found in almost any home or corporate office in Switzerland.

IoT Inspector is seamlessly integrated in Swisscom's development process, where the systematic analyses of around 80 firmware images per year lead to increased supply chain visibility. The detailed firmware security and compliance analyses provided by IoT Inspector enable Swisscom to be well-prepared for negotiations with device vendors and manufacturers, and empower the telco to have informed and fact-based discussions with suppliers. Providing its vendors with the added value of previously unknown security issues identified by IoT Inspector, Swisscom has put itself into a unique position. Swisscom and its vendors have been working closely together to continuously raise the level of security of customer-premises equipment.

"IoT Inspector helps us significantly in the development and operation of customer premises devices. Checking software in "release candidate" status allows us to detect potential security-related errors earlier and report them to the supplier for correction or analysis. The assessment of the individual modules and plugins in IoT Inspector enables us to take risk-based decisions when negotiating new functions or interfaces." says Giulio Grazzi, Senior Security Consultant at Swisscom.

Saving Big Bucks Thanks to Effective Prevention

With some 1.8 million devices in play, each firmware upgrade implemented by Swisscom leaves a big support footprint. For a tiny percentage of devices that do not upgrade successfully (e.g. because the device lost power during the process), support technicians are sent to clients and devices repaired or replaced. On average, any firmware upgrade costs an estimated CHF 374,000 in support.

As a result, it is of the utmost importance that each upgrade is free of critical (and avoidable!) security vulnerabilities. Any problem arising may make it necessary to issue a new upgrade shortly after the previous release. By highlighting critical security and configuration concerns, IoT Inspector successfully contributes to this goal. By preventing only a single faulty upgrade (and the subsequent need to fix it), IoT Inspector already contributes to a security ROI of CHF 374,000.



Nearly at the same time it integrated IoT Inspector, Swisscom launched its bug bounty program. Thanks to the thorough in-house firmware security analysis – and thus elevated security level of its products – the quality of the submitted IoT bugs has continuously remained high, with bounty hunters being unable to grab the low-hanging fruits of security vulnerabilities.

Integrating IoT Firmware Security into New Business Models

Fueled by the success in its private and SME divisions, Swisscom decided to extend the use of IoT Inspector to new areas. The telco is putting an increased focus towards comprehensive IoT solutions for its industrial clients. Connectivity for IoT ecosystems as well as IoT gateways and IoT management solutions are at the core of those new service offerings. Throughout design, build, and ongoing maintenance of the service, IoT Inspector has played an integral part as a quality gateway for device selection, implementation, and release, as well as ongoing monitoring for emerging security threats, enabling Swisscom to build its IoT service on top of a secure stack.

The most recent example of such a service is Swisscom's "Gateway as a Service" offering, where the telco provides Wi-Fi or Ethernet gateways and connectivity for the IoT ecosystems of the pharma and manufacturing sectors. With this new service, manufacturers of barista coffee machines can now conveniently access their devices for remote support and predictive maintenance, and cable car providers operating information platforms in far-off locations can remotely manage their devices without having to travel inhospitable terrain. Operating in such central and exposed locations, as well as connecting sensitive and business-critical processes requires the gateways to be highly secure. IoT Inspector is the solution of choice as it can easily and transparently assess and monitor them.

About IoT Inspector

[IoT Inspector](#) is the leading European platform for IoT security analysis and enables automated firmware testing of IoT devices for critical security vulnerabilities in just a few clicks. The integrated Compliance Checker simultaneously uncovers violations of international compliance requirements. Vulnerabilities for external attacks and security risks are identified in the shortest possible time and can be remedied in a targeted manner. The solution, which is easy to use via the web interface, detects unknown security risks for manufacturers and distributors of IoT technology.

We are based in Germany, and global leaders from TÜVs, Swisscom, T-Systems and more already trust in IoT Inspector. [Request your free trial today.](#)