ONEKEY.COM

swisscom

A SUCCESS STORY

HOW SWISSCOM SAVES USD 400,000

Per avoided IoT security incident through automated firmware analysis

ONEKEY

PIONEERING IOT FIRMWARE SECURITY AS KEY TO QUALITY OF SERVICE, VENDOR RELATIONS, AND BRAND REPUTATION

Executive Summary

Swisscom analyzes around 80 firmware images per year with **ONEKEY** (formerly known as IoT Inspector), mainly during the purchasing process for new IoT devices, but also in continuous development and support. Thus, Swisscom achieves a Security ROI of up to CHF 374K per avoided firmware rollout:

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

Pioneer even in Times of Increased Complexity

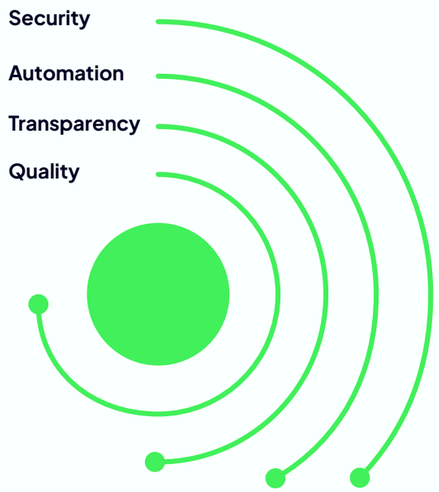
Swisscom is Switzerland's leading telco and one of the country's largest IT service providers, with a market share of more than 60% in mobile and broadband, and a total revenue of CHF 11.5B (2019).

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 ONEKEY, Swisscom runs tests that were previously neglected by manufacturers, and thereby enforces its pioneering position even as device security grows ever more complex.

Swisscom started working with **ONEKEY** 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

ONEKEY 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.

ONEKEY 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.

"**ONEKEY** 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 ONEKEY enables us to take risk-based decisions when negotiating new functions or interfaces."

— Giulio Grazzi, Senior Security Consultant, Swisscom

The detailed firmware security and compliance analyses provided by ONEKEY 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 ONEKEY, 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.

Swisscom saves 374 K CHF per Avoided Incident

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, **ONEKEY** successfully contributes to this goal. By preventing only a single faulty upgrade (and the subsequent need to fix it), **ONEKEY** already contributes to a security ROI of CHF 374,000. Nearly at the same time it integrated **ONEKEY**, 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 lowhanging fruits of security vulnerabilities.

75% of the companies would like to have a SBOM for all software.*

37% of the companies had already an IoT related security incident.*

[1] Secuity Report 2022

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 **ONEKEY** 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, **ONEKEY** 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. **ONEKEY** is the solution of choice as it can easily and transparently assessed and monitored them.

ABOUT ONEKEY

ONEKEY is the leading European specialist in Product Cybersecurity & Compliance Management and part of the investment portfolio of PricewaterhouseCoopers Germany (PwC). The unique combination of the automated ONEKEY Product Cybersecurity & Compliance Platform (OCP) with expert knowledge and consulting services provides fast and comprehensive analysis, support, and management to improve product cybersecurity and compliance from product purchasing, design, development, production to end-of-life.

Critical vulnerabilities and compliance violations in device firmware are automatically identified in binary code by AI-based technology in minutes – without source code, device, or network access. Proactively audit software supply chains with integrated Software Bills of Materials (SBOMs) generation. "Digital Cyber Twins" enable automated 24/7 post-release cybersecurity monitoring throughout the product lifecycle.

The patent-pending, integrated ONEKEY Compliance Wizard already covers the EU Cyber Resilience Act (CRA) and requirements according to IEC 62443-4-2, ETSI EN 303 645, UNECE R 155 and many others.

The Product Security Incident Response Team (PSIRT) is effectively supported by the integrated automatic prioritisation of vulnerabilities, significantly reducing the time to remediation.

Leading international companies in Asia, Europe and the Americas already benefit from the ONEKEY Product Cybersecurity & Compliance Platform (OCP) and ONEKEY Cybersecurity Experts.

onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

V2022080DEN