

ZYXEL
COMMUNICATIONS

A SUCCESS STORY

HOW ZYXEL SCALES FIRMWARE SECURITY AND CRA READINESS

With Automated Vulnerability
Management

REDUCING FALSE POSITIVES BY OVER 60%, DETECTING ZERO-DAYS EARLY, AND EMBEDDING SECURITY DIRECTLY INTO CI/CD WORKFLOWS

Executive Summary

Zyxel, a global leader in broadband and networking solutions, partnered with ONEKEY to modernize and scale its firmware security and vulnerability management strategy. By integrating ONEKEY directly into its GitLab CI/CD pipeline for continuous firmware image analysis, Zyxel automated the detection and prioritization of both known and zero-day vulnerabilities across its product portfolio.

The results: faster security assessments, significantly fewer false positives, improve engineering efficiency, and a scalable foundation for regulatory readiness under RED and the upcoming EU Cyber Resilience Act (CRA).

Background

Founded in 1989 and headquartered in Taiwan, Zyxel is a global provider of broadband access devices and networking solutions. The company works closely with telecommunications providers worldwide and enables high-speed connections via wired and wireless technologies such as Wi-Fi 7, GPON, FTTx, and 5G.

As Zyxel's product portfolio and customer expectations grew, so did the need for a more systematic, scalable, and proactive approach to firmware security—one that could keep pace with both innovation and regulation.

The Challenge: Scaling Security Without Slowing Innovation

Zyxel's customers increasingly demanded transparency and assurance around firmware security. At the same time, regulatory pressure was rising, driven by frameworks such as the Radio Equipment Directive (RED) and the upcoming EU Cyber Resilience Act (CRA).

Zyxel identified several key challenges:

- Manual and reactive vulnerability management did not scale with business growth.
- False positives consumed valuable engineering resources.
- Zero-day vulnerabilities needed to be identified before exploitation.
- Security checks had to integrate seamlessly into existing development workflows.
- Product needs to be compliant with regulations to avoid hefty fines.

Zyxel therefore looked for a solution that could automate vulnerability management end-to-end without disrupting development workflows and give security teams earlier and more reliable visibility into firmware risks.



Reducing Noise: Over 60% Fewer False Positives

One of the most immediate benefits for Zyxel was a dramatic reduction in false positives. ONEKEY’s advanced analysis and built-in triage capabilities reduced false positives by more than 60%, enabling Zyxel’s teams to focus on vulnerabilities that actually matter.

Instead of spending time validating irrelevant findings, engineering teams can now:

- Quickly assess real risk
- Prioritize remediation efforts
- Resolve issues faster with direct references and patch suggestions

This shift significantly improved operational efficiency and reduced unnecessary R&D effort

Supporting Decentralized Teams and Scalable Growth

Zyxel operates with a decentralized model in which individual business units are responsible for their own product security assessments. ONEKEY supports this approach by giving teams the autonomy to run analyses independently—while maintaining consistency and transparency across the organization.

Thanks to the flexible API interface, Zyxel can also integrate selected analysis results into internal dashboards and decision-making workflows, aligning security insights with business priorities.

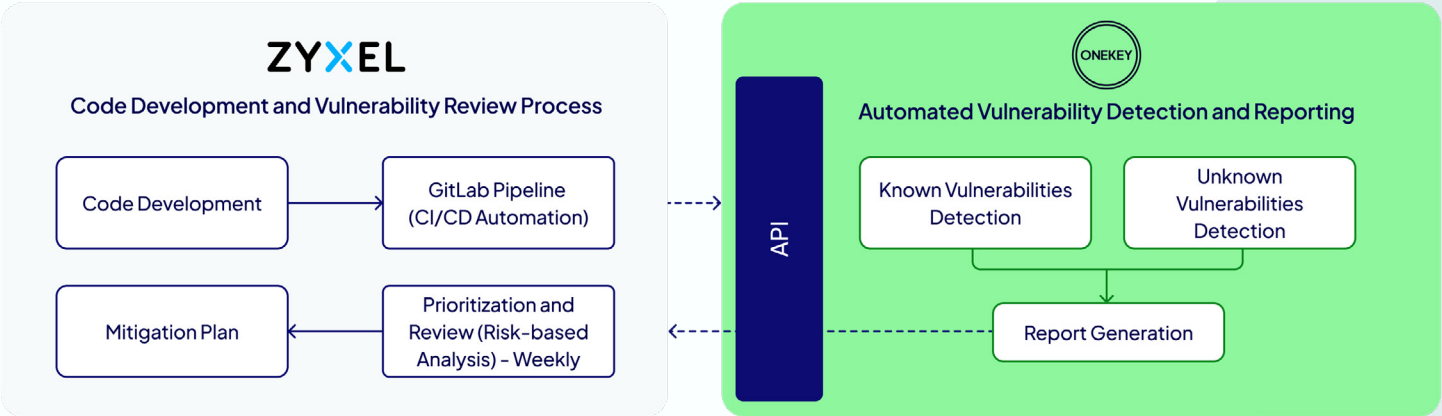
Overall, this automation allowed Zyxel to strengthen security without changing existing development workflows, address risks before products reach customers, and ensure alignment with regulatory requirements.

The Solution: Automated Firmware Security with ONEKEY

To address these challenges, Zyxel integrated ONEKEY directly into its GitLab CI/CD pipeline via API. This API-first approach established a tight connection, ensuring scalable, reliable, and structured data exchange without manual setups.

Every week, firmware builds are uploaded automatically and analyzed by ONEKEY, allowing Zyxel to:

- Detect relevant known vulnerabilities at scale
- Identify previously unknown (zero-day) vulnerabilities through deep binary analysis
- Prioritize risks based on real impact, not noise
- Maintain continuous security visibility across development, pre-release, and post-release phases



KEY BENEFITS FOR ZYXEL



Significant Time Savings with Fewer False Positives

Reduced false positives free up engineering capacity and improve operational efficiency.



Faster Vulnerability Resolution

Built-in references and patch guidance shorten response times, resolve issues faster, and strengthen Zyxel's security posture.



Reliable, Automated Security at Scale

Automation minimizes manual effort and human error while ensuring consistent and scalable approach to managing known and unknown vulnerabilities.



Regulatory Readiness

ONEKEY supports Zyxel's compliance strategy for RED and the EU Cyber Resilience Act—today and in the future.

WHY ZYXEL CHOSE ONEKEY

Zyxel selected ONEKEY for its unique combination of:

- Automated and efficient analysis of known vulnerabilities
- Advanced zero-day vulnerability discovery through deep firmware analysis
- Clear, actionable security insights for technical and business teams
- Cost-effective integration without added complexity
- Decentralized usage with centralized consistency across teams
- API-first architecture enabling scalable CI/CD automation



"With ONEKEY, we save valuable time by reducing false positives and triaging vulnerabilities more effectively. The platform's automatic impact assessment makes it easier for our teams to prioritize what matters most and helps us reduce R&D costs."

— Jason Wu, Associated VP, Zyxel

”

CONCLUSION: FROM REACTIVE SECURITY TO SCALABLE ASSURANCE

With ONEKEY, Zyxel transformed vulnerability management into a proactive, automated, scalable, and cost-effective security strategy. The company now benefits from earlier risk detection, reduced operational overhead, and a strong foundation for long-term compliance.

By embedding security directly into its development pipelines, Zyxel strengthens product security, meets growing regulatory demands, and builds lasting confidence with customers and partners.

Facts

100s of Scans
Available Throughout the Year

Over 60%
Reduction in False Positives

API-First
Approach Driven Solution

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



© 2026 ONEKEY. All rights reserved. Reproduction only permitted with the approval of ONEKEY. All brands listed are the brands of the respective owners. Errors, changes, and availability of the listed products, services, characteristics, and possible applications reserved. Software & services will be provided by ONEKEY. ONEKEY makes no guarantee for the information of third parties regarding characteristics, services and availability. ONEKEY reserves the right to make changes to products and services as a result of product development, even without prior notification. None of the statements and depictions represents legal advice or may be interpreted in such a manner. In case of deviations from the contract documents and general terms and conditions of ONEKEY and their affiliated companies and subsidiaries in conjunction with this document, the contract documents and general terms and conditions always have precedent over this document.

VZ02660001EN