技术白皮书

ONEKEY
产品固件安全分析与合规管理平台

ONEKEY

TRINITY 创提信息

www.trinitytec.com.cn

ONEKEY 产品固件安全分析与合规管理平台

摘要： ONEKEY 产品固件安全分析与合规管理平台面向联网设备、嵌入式产品及软件供应链安全治理，通过对实际交付的 Firmware 进行二进制分析，识别其中的软件组件、版本、依赖关系和已知漏洞，并结合自动化影响分析进一步评估候选漏洞针对当前固件的适用性。在此基础上，平台提供 SBOM 管理、漏洞治理、合规证据映射、潜在零日漏洞分析、RTOS 分析、二进制加固检测及多种部署方式，帮助企业建立从软件成分可视性、漏洞发现和影响评估到持续治理与合规应对的产品网络安全能力。

一、平台概述

ONEKEY 是一款面向产品网络安全、嵌入式设备安全与软件供应链风险管理的固件安全分析与管理平台，可对固件、镜像文件、软件组件及各类二进制文件进行深入分析，建立从软件成分识别、漏洞发现与影响评估到持续治理的技术流程。

平台可帮助企业掌握产品中实际使用的软件组件、版本、依赖关系及潜在漏洞，并将原始技术发现转化为可执行的风险处置优先级，使研发、安全、合规与治理团队能够基于一致的技术信息开展协同工作。

二、核心价值

- 从二进制层面识别软件组件，提升 SBOM 与实际产品软件组成的一致性。
- 通过漏洞管理与风险优先级机制，帮助安全团队聚焦真正需要进一步分析和处置的问题。
- 以技术分析结果支撑法规与标准要求的证据准备，降低合规落地过程中的工作量。
- 支持多种部署模式，兼顾云端使用效率与本地化数据管控需求。

对企业而言，ONEKEY 的价值不仅在于发现潜在漏洞，更在于帮助建立从发现、分析、优先级判断、处置到合规证据准备的持续治理流程。

三、关键功能列表

功能面	说明	业务价值
二进制分析	针对固件与二进制文件进行深入分析，识别其中的软件组件、版本、函数库及相关已知风险。	提升软件成分可视性，补充仅依赖源代码或人工盘点的不足。
漏洞管理	将识别出的组件与漏洞数据库关联，支持漏洞追踪、优先级管理、状态管理及修复治理。	帮助安全与研发团队按照一致流程管理漏洞处置进度。
影响分析	结合架构、文件、二进制、符号、函数、模块、版本及补丁状态等 Firmware 技术证据，进一步评估候选漏洞针对当前固件的适用性。	减少明显不适用的候选漏洞，将人工分析集中到真正需要进一步确认的问题。
合规向导	将平台中的技术分析结果与 EU CRA、IEC 62443 等相关法规或标准要求建立映射，辅助合规证据整理。	降低要求梳理、证据映射和审核材料准备的工作量。

功能面	说明	业务价值
部署选项	支持 SaaS 与本地部署（On-Premises）等方式，可根据组织治理政策、法规要求和数据敏感程度灵活选择。	兼顾部署效率、扩展能力与数据控制需求。
潜在零日漏洞分析	针对自有或定制化程序代码，从程序行为、潜在弱点、攻击面及上下文条件等方面开展分析，帮助识别尚未被公开编号或现有漏洞数据库尚未覆盖的潜在安全问题。	补充仅依赖已知 CVE 或已知特征匹配的风险发现范围。
RTOS 分析	支持实时操作系统（RTOS）固件分析，可识别固件镜像中的架构、加载地址、组件与函数符号，并针对已识别组件进行 CVE 匹配。	扩展非 Linux 固件环境下的软件成分可视性和已知漏洞管理能力。
二进制加固	检查 ELF 二进制文件的加固保护机制，例如立即绑定（BIND_NOW）、Full RELRO、Stack Canaries、不可执行栈（NX）、PIC 及调试符号剥离等。	帮助团队掌握编译与执行层面的保护状态，识别需要改进的安全基线。

四、技术特点

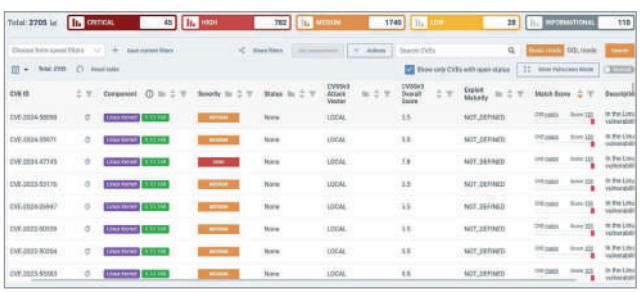
1. 通过影响分析减少不适用的候选漏洞

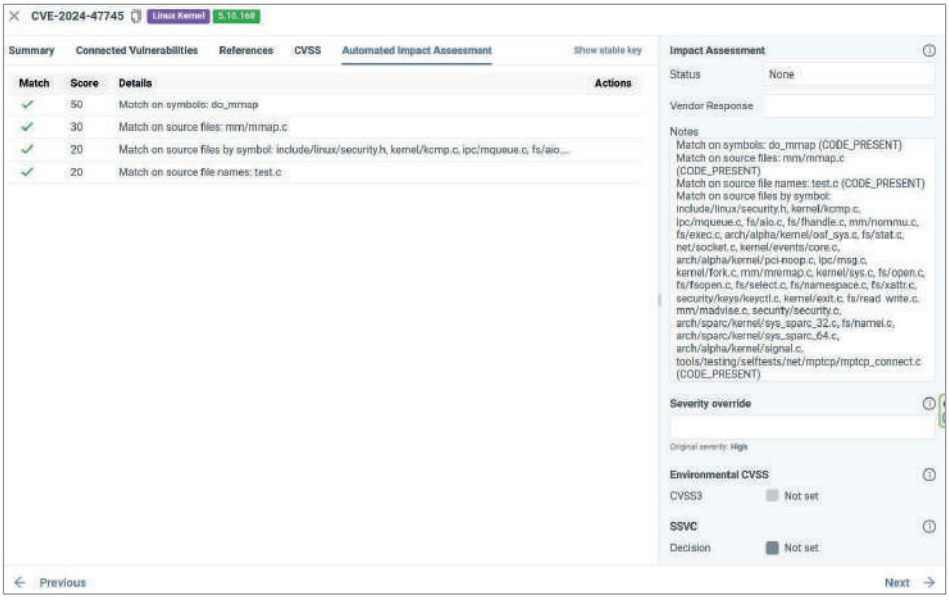
在漏洞管理实践中，常见挑战并非无法发现问题，而是组件与版本匹配后产生大量候选漏洞，其中相当一部分并不一定适用于当前产品或固件。若仅依据组件名称、版本与 CVE 信息进行匹配，研发与安全团队仍需要投入大量人工工作完成后续分诊与确认。

在完成组件识别与 CVE 匹配后，ONEKEY 的自动化影响分析可进一步结合固件中的架构、文件、二进制、符号、函数、模块、版本及补丁状态等技术证据，对候选漏洞针对当前固件的适用性进行评估。

不同技术证据可分别形成支持“可能适用”或“较不适用”的判断信号，并汇总形成匹配分数及相应证据记录。该分数反映的是漏洞针对当前固件的适用性判断信心，而非 CVSS 严重程度。通过这一过程，企业可以优先排除一部分明显不适用的候选项，将人工分析资源集中到真正需要进一步确认的问题上。最终漏洞处置仍需结合部署环境、攻击情报、业务影响以及安全团队的专业判断。

- 减少仅依据组件与版本匹配产生的无效候选项和误判。
- 提升漏洞优先级判断的可信度、可解释性与可沟通性。
- 帮助安全团队将有限资源集中于真正需要进一步分析和处置的产品网络安全问题。





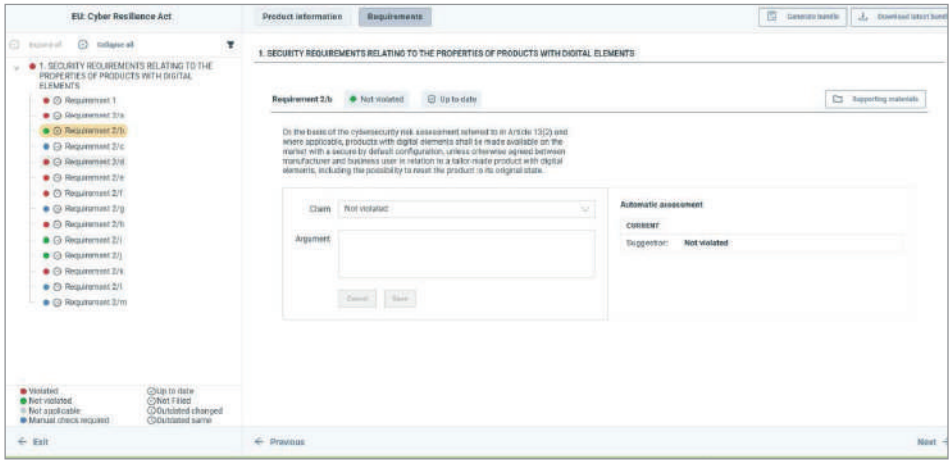
2. 合规向导辅助应对 EU CRA 与 IEC 62443 要求

随着产品网络安全法规与行业标准持续强化，企业不仅需要识别和管理技术风险，还需要形成能够说明安全活动、治理过程与技术结果的合规证据。ONEKEY 的合规向导可将平台中的技术分析结果与相关法规或标准要求建立映射，降低要求梳理、证据整理与合规材料准备的复杂度。

以 EU CRA 为例，企业需要围绕产品网络安全风险、漏洞处理、持续维护及安全开发实践形成相应的流程和证据；对于 IEC 62443，则需要结合工业网络安全场景中的流程、技术控制和生命周期要求开展相关工作。合规向导可作为辅助机制，帮助使用者将平台中的分析结果、漏洞状态与治理记录对应到相关条款或控制要求。

这种方式有助于将合规工作与产品网络安全治理过程结合起来，减少合规证据与日常安全活动相互割裂的情况。对企业而言，可降低法规要求梳理和材料准备的工作量，提高跨部门协作效率，并增强面对客户审核、第三方评估及市场准入要求时的应对能力。

- 降低法规要求梳理、证据映射与合规材料准备的工作量。
- 使技术分析结果能够更直接地支撑合规说明与审核准备。
- 帮助企业将 EU CRA 与 IEC 62443 的相关要求更有效地纳入产品网络安全治理流程。



3. 支持 SaaS 与本地部署（On-Premises）等多种部署模式

不同企业在部署安全平台时，对数据敏感性、网络隔离、运维责任和上线周期的要求并不相同。ONEKEY 支持 SaaS 与本地部署（On-Premises）等多种部署模式，使企业能够根据内部政策、法规要求与 IT 架构选择适合自身环境的部署方式。

SaaS 部署适合希望快速上线、集中运维并降低基础设施负担的组织，有助于缩短部署周期并支持跨团队协作。本地部署则更适用于数据敏感度较高、受到严格监管或需要强化数据管控的环境，例如工业控制、关键基础设施、国防、医疗及部分大型制造场景。

多种部署模式使 ONEKEY 能够适应不同安全成熟度、数据治理要求和 IT 环境，在部署效率、数据控制与长期扩展之间提供更灵活的选择。

部署模式	适用情境	主要优势
SaaS	希望快速部署、降低运维负担并支持跨团队协作的组织。	上线周期短、扩展灵活、运维集中。
On-Prem	重视数据敏感性、网络隔离、法规限制或内部安全管控要求的组织。	数据控制能力强，可配合内部政策，适用于高敏感场景。

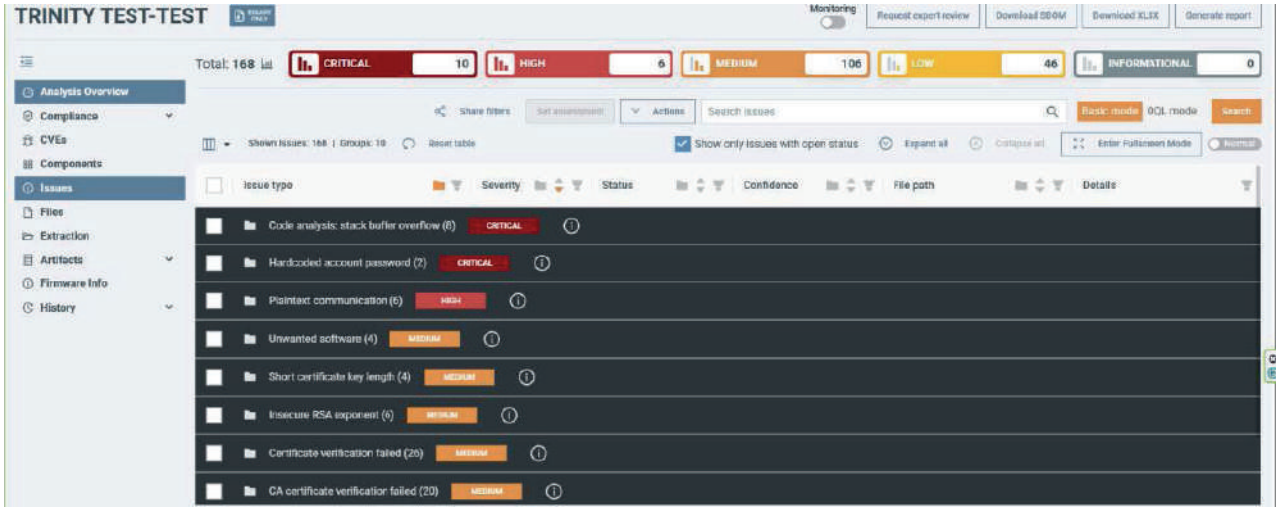
4. 支持自有程序代码的潜在零日漏洞分析

除开源组件和已知漏洞分析外，ONEKEY 还可针对自有或定制化程序代码开展潜在零日漏洞分析，用于补充公开 CVE、已知特征或传统组件匹配方式无法完整覆盖的风险发现场景。

对于许多产品团队，自行开发的程序逻辑、定制模块与专属功能无法通过公开 CVE 和通用组件数据库获得完整覆盖。通过对程序行为、潜在弱点、攻击面及上下文条件进行分析，平台可帮助团队发现尚未被公开编号或现有漏洞数据库尚未覆盖的潜在安全问题。

这一能力使安全分析从已知漏洞管理进一步延伸到潜在未知风险发现，补充传统漏洞管理偏重已知 CVE 的局限。对安全、研发与产品管理团队而言，有助于提升自有代码风险可见性，并在设计、测试与发布阶段更早开展分析和修正。

- 补充自有及定制化程序代码在传统组件漏洞管理中的可见性不足。
- 提升对潜在未知漏洞、逻辑缺陷与攻击面的早期发现能力。
- 使产品网络安全治理从已知漏洞管理进一步延伸到潜在未知风险分析。



5. RTOS 分析增强实时操作系统固件的可见性

除常见的 Linux 固件分析场景外，ONEKEY 还支持实时操作系统（RTOS）分析，可帮助企业覆盖更多嵌入式和工业设备的安全盘点需求。RTOS 分析可识别固件镜像中的架构、加载地址、组件及函数符号，使安全团队能够更清晰地了解固件内部的软件组成。

平台可识别多种 RTOS 环境中的常见软件组成，例如加密库、TCP/IP 协议栈、标准函数库及操作系统组件，并可覆盖 FreeRTOS、ESP-IDF、ThreadX（Azure RTOS）、Zephyr、C/OS II、C/OS III、eCos、VxWorks、QNX 与 Apache NuttX 等环境。完成识别后，可继续针对已识别组件进行 CVE 匹配，使 RTOS 固件中的已知漏洞能够纳入统一的漏洞治理流程。

这一能力使原本较难盘点、较依赖逆向工程经验的 RTOS 固件能够形成结构化的软件组成与漏洞信息，并进一步纳入持续的风险治理流程。对于 IoT、工业控制、网络通信及各类嵌入式设备制造商而言，可有效扩展非 Linux 固件环境下的软件成分可视性与已知漏洞管理能力。

- 支持 RTOS 固件中的组件、函数与架构识别，补充非 Linux 环境下的软件成分可视性。
- 可对已识别组件进行 CVE 匹配，并纳入既有漏洞治理流程。
- 适用于 IoT、OT、工业控制及各类嵌入式产品网络安全场景。

6. 二进制加固检测评估二进制文件的保护状态

ONEKEY 可检查固件中 ELF 二进制文件的加固保护机制（Binary Hardening），使团队在了解软件组件和漏洞之外，进一步掌握编译及执行层面的安全保护状态。这有助于企业建立产品网络安全基线、改进软件安全质量，并支撑安全开发规范的持续落实。

根据平台提供的检测能力，ONEKEY 可检查多项二进制加固机制，包括编译强化相关选项、立即绑定（BIND_NOW）、Full RELRO、Stack Canaries、不可执行栈（NX / No-Exec Stack）、位置无关代码（PIC），以及调试符号是否已剥离等。这些机制与降低部分内存破坏、代码执行及逆向分析相关风险有关。

二进制加固检测能够提供可视化的保护状态，使研发与产品安全团队快速识别哪些二进制文件缺少预期的保护机制、哪些编译安全选项尚未落实，并据此将相关安全要求更早纳入构建与发布流程。

- 快速盘点 ELF 二进制文件的安全加固机制启用状态。
- 帮助建立更一致的编译安全基线与发布质量要求。
- 使二进制层面的安全保护状态成为可持续评估和改进的治理指标。

五、适用对象与应用环境

- 嵌入式产品与 IoT 设备制造商，需要在产品上市前后持续掌握软件组成与风险暴露情况。
- 工业控制与 OT 相关产品供应商，需要兼顾产品网络安全与 IEC 62443 等行业标准要求。
- 受到 EU CRA 或其他产品网络安全法规影响的企业，需要建立更加系统化的技术证据与治理流程。
- 产品网络安全、PSIRT、DevSecOps 与合规团队，希望通过统一平台整合分析、管理与报告工作。

在上述场景中，ONEKEY 适合需要同时提升技术分析能力、风险治理效率与合规应对能力的组织。

六、结论

ONEKEY 产品固件安全分析与合规管理平台并非单一的漏洞扫描工具，而是将固件二进制分析、软件成分识别、漏洞管理、自动化影响评估、合规证据支持及多种部署方式结合起来的产品网络安全分析与治理平台。

其中，自动化影响分析可帮助减少不适用的候选漏洞并降低人工分诊工作量；合规向导可辅助 EU CRA 与 IEC 62443 等要求的证据映射与材料准备；潜在零日漏洞分析可补充自有程序代码的未知风险发现；RTOS 分析扩展了对实时操作系统固件的软件成分与已知漏洞可视性；二进制加固检测则帮助团队评估编译和执行层面的保护状态。结合 SaaS 与本地部署等模式，ONEKEY 可支持不同企业在产品网络安全分析、持续漏洞治理和合规应对方面的实际需求，为提升产品安全治理效率提供具有落地价值的技术选择。

七、关于ONEKEY与创提信息

关于 ONEKEY

ONEKEY 是一家总部位于德国杜塞尔多夫的产品网络安全与合规自动化厂商。其平台源于 2020 年推出的 IoT Inspector，并于 2022 年更名为 ONEKEY，核心方向是通过固件二进制分析和自动化技术，帮助联网产品制造商与运营方持续掌握产品中的软件成分、已知漏洞、潜在未知风险及合规状态。围绕产品全生命周期，ONEKEY 提供 SBOM 管理、漏洞管理、自动化影响评估、潜在零日漏洞分析、持续监测及 Compliance Wizard® 等能力，并支持 EU Cyber Resilience Act（CRA）、IEC 62443、RED 等多项产品网络安全法规和标准的技术分析与合规证据准备。ONEKEY 的能力重点面向 IoT、OT、工业设备、网络通信设备和医疗器械等具有长期生命周期和复杂软件供应链的联网产品。

关于创提信息

创提信息科技（上海）有限公司（Trinity Technologies）成立于 2012 年，长期服务于高可靠、高安全软件和嵌入式产品研发领域，为汽车电子、工业自动化、轨道交通、医疗器械、航空航天、通信等行业客户提供研发工程化、自动化测试、产品网络安全及合规相关的工具链、解决方案与专业技术服务。公司已服务超过 400 家大中型企业和科研机构，并持续将软件工程、产品安全与行业合规实践结合到客户的研发与产品生命周期中。

在产品网络安全领域，创提信息围绕安全开发生命周期（SSDLC）、威胁建模、代码安全分析、软件成分分析（SCA）与 SBOM、固件二进制分析、漏洞管理、模糊测试、渗透测试及持续监测等环节构建解决方案，并面向汽车网络安全、工业网络安全、医疗器械网络安全及 EU CRA 等常见产品网络安全法规和标准提供技术支持。针对 CRA，创提信息重点关注制造商在软件供应链可视性、漏洞持续管理、影响判定、事件响应和合规证据准备等方面的实际挑战，结合 ONEKEY 等专业平台，帮助企业将产品级技术证据与安全流程、漏洞治理及合规要求衔接起来。

地址:上海市浦东新区毕升路299弄3号101A
邮编:201204
电话:+86-21-68580866
E-mail:info@trinitytec.net
网站:www.trinitytec.com.cn

企业服务号