SYNOPSYS®

CEVA：DSP 和 AI 处理器

借力新思确保标准遵从并降低许可风险

公司简介

作为20多年的行业领跑者，CEVA是无线连接、智能传感技术和共创解决方案领域的领先许可方，致力于打造一个更智能、更安全和互联的世界。许多世界领先的半导体系统公司和OEM厂商都在使用CEVA的IP，以此为移动、消费、汽车、机器人、工业、航空航天和国防以及物联网(IoT)等一系列市场构建节能、智能、安全、互联的设备。CEVA致力于承担其社会责任并恪守重视节能环保的价值观。

如想了解有关CEVA的更多信息，请点击这里。

挑战：执行编码标准并降低许可证风险

CEVA的DevOps/实时开发经理Ori Leibovich面临着双重挑战：在更高效地执行编码标准的同时降低许可证相关风险。近期，在给汽车行业的片上系统(SoC)设计开发AI处理器的过程中，Leibovich发现CEVA的安全计划需要符合汽车行业严格的安全要求。更有甚者，Leibovich报告称，“CEVA的软件开发在最近几个月增长迅速”，这使得能够跟上开发速度增幅的自动化解决方案变得尤为关键。

有了成熟的安全计划后，CEVA需要能够无缝适应现有开发活动和工具的解决方案，并且这个解决方案还能够支持当前的安全工作，而不会减慢现有计划或使其变得过于复杂。

Leibovich非常渴望通过汽车行业安全认证，这促使他对CEVA的安全计划进行了双管齐下的升级：部署强大的静态应用安全测试(SAST)和软件组成分析(SCA)工具。

解决方案：Black Duck SCA和Coverity SAST

CEVA选择将Black Duck® SCA和Coverity® SAST引入其现有开发管道中。Black Duck的自动策略管理解决方案使工作团队能够轻松地预先定义开源代码使用、安全风险及许可证合规策略，同时在整个软件开发生命周期(SDLC)中自动执行这些策略——所有这些均使用开发人员的现有工具来完成。Coverity是快速、准确且高度可扩展的SAST解决方案，使开发和安全团队能够在SDLC的早期阶段就轻松处理安全和质量缺陷。他们可以毫不费力地跟踪和管理整个应用组合中的风险，并确保符合安全和编码标准。

“新思科技Coverity和Black Duck解决方案使我们能够通过安全和质量标准认证。”

—Ori Leibovich,
DevOps/实时开发经理

Black Duck

Leibovich指出，他的团队“增长迅速，因此我们认为，开源代码自动检测工具对于规避法律问题至关重要”。CEVA将Black Duck部署到一个大约涵盖400名开发人员和数十万行代码的环境中，并开始每周运行Black Duck扫描。Black Duck与现有管道的无缝集成使CEVA能够将其轻松添加到现有的安全活动中，并让其识别软件中的所有开源代码。据Leibovich称，经过验证，CEVA认为市场上所有其他的SCA工具都“不可能实现这种级别的检查”。

Coverity

汽车行业的ISO 26262 ASIL-B标准和ISO9001质量/可靠性标准给CEVA提出了非常具体的安全要求。

ASIL是ISO 26262标准专为道路车辆功能安全定义的风险分类系统。该标准期望车辆“没有不合理的风险”，该期望一直延伸到操控车辆的应用代码质量。同样，ISO9001要求企业坚守高标准的诚信度和质量；企业必须能够证明其有能力持续提供符合监管要求的产品。作为值得信赖的行业领导者，CEVA希望快速确保并证明其有能力满足所有要求，并继续提供最优质的产品和解决方案，包括处理器、传感器集线器和数字信号处理器等。

Leibovich表示：“在考察了多款工具之后，我们发现Coverity最容易集成到我们的CI/CD流程中，并且最容易与我们内部开发的编译器一起使用。”现在，借助Coverity, CEVA可以全面跟踪和管理合规性，确保满足广泛的安全、质量和数据保护标准。

结果：轻松合规并降低风险

借助Coverity轻松实现合规

遵守行业标准和法规可能会令人生畏，尤其是随着开发速度的加快、发现和识别代码并确保其质量变得日益困难时，进一步，如何处理所发现的违规行为可能更加令人生畏。Coverity允许您按类别轻松筛选已发现的问题，查看趋势报告，根据严重程度确定漏洞修复的顺序，最重要的是，可以跨团队和项目来管理策略合规。

CEVA将Coverity快速集成到其CI/CD 流程中，然后证明其满足行业监管要求。Leibovich发现Coverity“提高了代码质量和安全性”，帮助“以低误报率发现缺陷”并“执行MISRA C和AUTOSAR C++等编码标准”。最重要的是，Coverity很容易“与内部开发的编译器相集成”，这意味着现有的开发活动不会受到这个新增方案的干扰。

借助Black Duck降低风险

如果没有应用组合中代码的完整视图，特别是开源代码，企业将会面临安全性、许可证合规和代码质量风险。许可违规可能给企业带来代价惨重的诉讼风险，或损害企业宝贵的知识产权。

Black Duck帮助CEVA消除了开发环境的许可合规证风险。在考察了数个工具之后，CEVA发现Black Duck最容易集成，对其蓬勃发展的安全计划破坏最小，同时还能立竿见影见到成效。Leibovich表示，Black Duck“将开源代码识别和管理功能集成到了我们的SDLC中”并帮助“识别我们正在使用的开源许可证”，所有这些都是有助于将许可证违规风险降至最低的关键活动。

新思科技帮助CEVA加强了安全工作，助力其解决方案实现了安全质量承诺。通过加强安全与合规工作，CEVA增强了客户对其产品的信任。谈到公司的最新安全态势，Leibovich指出“CEVA可以证明我们严格按照安全协议开展工作，我们没有因为使用开源代码而与客户产生问题。我们可以展示这些代码都要经过静态分析工具的分析，因此[我们]拥有质量更好的软件。我们可以证明CEVA是严格按照安全协议开展工作的。”

现在，Coverity和Black Duck扫描工具可在CEVA的开发管道中自动启动，并为开发人员和管理人员提供详细的报告，以便他们确保安全性与合规性。这样，开发团队便可以腾出时间专注于本职工作，集中精力开发他们所擅长的业界领先的处理器和平台IP解决方案。

新思科技与众不同

新思科技提供的集成解决方案，可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。与新思科技同行，您的开发人员可以在编写代码的时候快速兼顾安全。您的开发和DevSecOps团队可以在不影响速度的情况下在开发管道中自动进行安全测试。您的安全团队可以主动管理风险并将补救工作聚焦在对贵组织最重要的事情上。我们无与伦比的专业知识可以帮助您规划和执行所需安全计划。只有新思科技能够满足您构建可信软件的一切需求。

有关新思科技软件完整性小组的更多信息，请访问：www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road Mountain View, CA 94043 USA

美国销售热线：800.873.8193
全球销售热线：+1 415.321.5237
电子邮件：sig-info@synopsys.com