**镜像安全**

1. Clair (定期从一组配置的CVE源中刷新其漏洞数据库，对可用的容器映像进行仔细检查，并对安装的软件包进行索引)
2. Anchore (对Docker镜像进行深度检查。还可以探索其丰富的剖析公共映像库，充分了解其内容、构建过程和发现CVE威胁)
3. Dockerscan (审计环境变量、添加攻击模块)
4. Oscap-Docker (审计镜像，同时评估运行的容器和云端镜像)
5. AquaSec [商用] (安全审计、容器镜像验证、运行时保护、自动策略学习或入侵预防)
6. BlackDuck Docker Security [商用] (专门负责容器库存和报告镜像库存，将已知的安全漏洞映射到镜像索引和跨项目风险报告)

**内核安全**

1. Dockscan (简单的Ruby脚本，用于分析Docker安装和运行容器，既针对本地主机，也针对远程主机)
2. Sysdig Falco (Sysdig Falco是一种开源的行为监测应用，旨在检测基于其技术的异常活动, Falco是一种与众不同的审计工具，它在用户空间中运行，使用内核模块来拦截系统调用，而其他类似的工具在内核级执行系统调用过滤/监视)
3. NeuVector [商用] (NeuVector专注于运行时的实时安全保护。自动发现应用程序、容器和服务的行为，以及与其他Linux Id类似方式检测安全升级和其他威胁。NeuVector“强制”容器部署在每个物理主机上，并完全访问本地的Docker守护进程)
4. Twistlock [商用] (用于支持容器化环境的商业安全套件：漏洞管理、访问控制、分析和对安全标准遵从性的取证)

**网络安全**

1. docker-bench-security (是一个元脚本，用于检查生产中部署Docker容器的数十种常见的最佳实践)
2. drydock (和Docker-Bench-security相似，Drydock是Docker的安全审核工具。而Drydock的独特之处在于，Drydock允许它的用户创建自定义的审核配置文件。这些配置文件可消除生成报告（噪声警报）中那些引起大量杂乱的审核，从而调整审核过程。此外它还可用于停用和环境无关、会产生虚假警报的审核测试)
3. Cilium(基于一种称为eBPF的新Linux内核技术，允许根据容器/pod身份定义并执行网络层和http层安全策略, Cilum利用BPF执行核心数据路径过滤、管理、监视和重定向)