电子实验记录本（ELN）该选择 SaaS 部署还是私有化部署？

电子实验记录本 (ELN) 如果按照部署方式来区分，可分为 SaaS ELN 和私有化 ELN。近年来，随着云计算等技术的飞速发展，SaaS ELN 成长迅速，大有与私有化 ELN 分庭抗礼之势，而两种部署方式到底该如何选择，往往令企业十分困惑。在了解如何选择之前，我们先来看一下什么是 SaaS 部署，什么是私有化部署。

SaaS 部署

SaaS，是 Software-as-a-Service 的缩写，意为软件即服务。SaaS 是一种通过互联网提供软件服务的模式。SaaS 软件供应商将应用软件统一部署在云服务器上，用户可以根据工作实际需求，通过互联网向厂商定购所需的应用软件服务。SaaS 本质上是一种服务。

私有化部署

私有化部署是为了满足特定用户单独使用软件的需求，用户需自行购买基础设施（服务器等），包括本地部署（将业务数据部署在企业局域网内）和私有云部署（将业务数据部署在第三方主机托管场所）。

SaaS ELN VS 私有化 ELN

两种截然不同的部署方式对上线 ELN 的企业意味着什么？SaaS ELN 究竟有什么无可替代的优势让越来越多的企业倾心呢？下方表格中，我们将二者从产品特性、功能迭代、实施周期、安全性、合规性、售后运维、总拥有成本等角度作了详细对比。

项目	SaaS ELN	本地/私有云 ELN
产品特性	产品化；大量用户带来多应用场景的适配；成熟稳定	定制化；不可控风险较大
功能迭代	持续迭代，基本以 1-3 个月为一个迭代周期，能够快速响应市场需求	迭代周期相对较慢或基本不迭代
实施周期	工作主要集中在开通账号、梳理业务流程、软件配置和培训层面，上线周期一般为 1-2 周	涉及软件、中间件、硬件的实施；环节多，周期长，上线周期一般至少 3 个月

北京创腾科技有限公司 | 北京. 苏州. 上海. 广州. 成都
地址：北京海淀区知春路 7 号致真大厦 A 座 12 层 1201 号
电话：(010)82676188
www.neotrident.com

安全性	SaaS 服务商作为专业的互联网企业，在安全性、备份和维护方面投入更多资金，拥有更加完善的安全管理体系以及足够多专业技术人员来保障系统及数据安全	一些勒索软件和其他恶意软件，更容易入侵企业内部网络；用户需要有能力投入足够的安全基础设施和人员支出方能确保服务器和数据的安全
计算机化系统验证	服务商会在放行 SaaS 系统前按照 GxP 要求执行 IQ 和 OQ，用户只需补充 PQ，验证周期将缩短 75%	用户需在产品设计环节开始执行 IQ，OQ 和 PQ，需配备验证专家团队，验证周期最少 2 个月
安全合规职责划分	SaaS 层为云服务商职责	用户职责
售后运维	服务商对产品运营十分重视，用户对运维及售后的满意度往往更高	对运营的依赖度较弱，保持用户正常使用即可；系统升级需支付额外费用
总拥有成本	不需考虑软硬件及人力成本，项目启动成本大幅降低，5 年累计费用节省至少 75%	除高昂的软硬件及人力成本外，还要考虑很多难以量化的隐性成本；总拥有成本非常高

通过对比，我们总结了 SaaS 5 个方面的优势：

✧ **数据安全保障更专业**

直观来看，私有化部署是直接部署在用户自己的服务器上，数据把握在企业内部；而 SaaS ELN 是用户通过购买服务获得所需功能，数据将保存在 SaaS 服务商的服务器中，用户对自己数据的可控性较弱。然而，数据在自己手中，就很安全吗？事实上，在**专业保障数据安全**方面，SaaS 才更有发言权。

尽管 SaaS 软件用户仍然容易受到攻击，例如试图收集登录凭证的网络钓鱼攻击，但对于勒索软件和其他恶意软件而言，入侵云软件的难度要大得多。同时，SaaS 服务商在系统安全防御方面的投入也远远高于其他传统行业公司。

	本地及私有云部署	SaaS部署
数据安全风险	高 (需大量软硬件投入，开发维护成本高)	低 (访问隔离+传输加密+存储加密+安全销毁)
网络安全风险	高 (网络规则多且复杂，维护困难)	低 (VLAN隔离+安全组+二层安全策略)
主机安全风险	高 (需进行大量硬件及基础设施建设投入)	低 (虚拟资源隔离+攻击防御+系统加固+安全监控)
运维安全风险	高 (需要ISO27000数据安全体系建设投入)	低 (行为检测+态势感知+风险清理及ISO2700规范)
三级及以上等保	需要大量投入建立三级等保体系	平台本身具备三级及以上等保能力
安全合规职责划分	租户职责	SaaS层为云服务商职责

SaaS 与本地/私有云部署安全风险对比

（1）SaaS 数据安全技术

- ✓ 采用行业主流云厂商提供的云安全产品（三级等保）
- ✓ 防火墙包括全天候安全漏洞检测及实时修复推送
- ✓ 秒级增量备份及定时全量备份
- ✓ 备份数据分布式存储

（2）SaaS 网络安全技术

- ✓ 采用 DMZ 技术，确保数据中心安全隔离
- ✓ 管理网络与数据网络分离

（3）SaaS 数据访问及安全测试

- ✓ 所有数据访问需要授权，敏感数据进行脱敏存储
- ✓ 所有应用程序接口都配备授权访问
- ✓ 应用程序调用使用 https 协议
- ✓ 测试完成后需经过安全扫描（防注入、防渗透和防攻击等）才可发布

（4）SaaS ISO27001 数据安全体系规范

- ✓ 版本迭代及故障处理需要根据 SOP 指导手册进行审批和操作
- ✓ 运维登录生产环境需要经过堡垒机并且全程录屏；并且针对所有执行过的操作提供审计报告

✧ 总拥有成本断崖式下降

在私有化部署模式中，用户需购买大量的硬件设备（物理服务器、防火墙、建设或租用机房等），需要招聘专业的运维人员、制定运维规范、考虑系统灾备等问题。除此之外，往往还有很多难以估量的隐性成本。

首先，随着 SaaS 的大范围推行，软件供应商将更加注重云软件的功能开发，私有化部署系统的发展可能将陷于停滞；其次，企业如果固守笨拙的劳力密集型系统，而不

是积极部署高性能系统和高效流程，那企业文化会受到影响，不利于吸引优秀人才；第三，如果采用私有化部署，企业除了为确保数据安全需要耗费大量安全基础设施和人员支出外，可能还要考虑购买虚拟专用网络，以便从办公室以外位置访问应用等方面，这些可能导致每年数千美元的成本和更多其他管理开销。

相比之下，SaaS 软件的安全保护和备份工作均由软件商负责，用户需要的全部基础设施只是用来运行浏览器的设备以及让该设备可以访问互联网的简易网络，这使得 SaaS ELN 的启动成本大幅降低。有关数据表明，相较于私有化部署，SaaS 部署模式将缩短 75%的上线周期，5 年可帮助企业节省 75%的投入。

✧ 部署优势

（1）提供高度可复制的“标准化”解决方案

SaaS ELN，能够为特定领域提供具有高度可复制的“标准化”解决方案，该解决方案也早已经过大量用户经验的积累与迭代，是成熟的、可靠的，是“产品化”的；而私有化部署需要用户自行实施解决方案，而且过多的定制化往往存在很多不可控的风险，一个功能的更新往往波及整个系统，可谓“牵一发而动全身”。

（2）快速上线，部署成本大幅降低

私有化 ELN 的实施一般包括需求调研、软件硬件的安装、配置、人员培训等，此外，在高度受监管的制药行业，为降低合规风险，药企须从产品设计环节开始就要同步执行计算机化系统验证，因此，实施验证过程涉及环节多、周期长、成本高。而 SaaS ELN 主要的实施内容为开通账号、梳理业务流程、配置产品基本参数，工作主要集中在软件配置和培训层面，实施复杂度明显低于私有化 ELN。对于合规层面，供应商会在放行 SaaS 系统前按照 GxP 相关要求执行 DQ、IQ 和 OQ，企业只需补充部分验证活动（PQ）。

（3）更有利于跨系统的数据交互

传统信息化软件部署在企业内部，系统间相互孤立。而 SaaS 软件相互一次性打通后，理论上所有的用户均可使用打通后的产品能力，能够摊薄系统间打通的成本，而传统软件间对接的方式会带来大量的研发、协调和实施工作，成本远高于 SaaS 模式。

SaaS 部署更有利于做场景延伸产品和上下游协同产品的打通，从而有助于构建起 SaaS 生态，为用户带来更好的效率提升和体验提升。

✧ 快速迭代与多应用场景的适配

私有化 ELN 交付后，迭代周期相对较慢；而 SaaS 产品一般都需要持续迭代，基本以 1-3 个月为一个迭代周期，能够快速响应市场需求。

相比而言，私有化 ELN 可以提供更好的可定制性，其定制开发比例相对较高；而

SaaS ELN 则可以通过大量用户经验以及产品的快速迭代覆盖更多应用场景。

✧ **用户满意度更高的运维服务**

传统 ELN 对运营的依赖度较弱，保持用户正常使用即可，而 SaaS 产品本身就是一种服务，SaaS 产品快速的可持续性迭代，让用户可以享受到未来软件产品升级带来更优体验或价值提升。SaaS 服务商比较重视续费率，因此更加重视用户的使用和反馈情况，会配备专门的运营团队，让用户可以享受到更加专业、便捷的服务。

SaaS ELN 正在成为主流

近年来，SaaS 作为软件服务的颠覆性创新技术，正在得到研发企业和机构的青睐，并逐步从中小企业走向大型企业。当前，国际上对 SaaS 软件的认可度非常高，数据表明，国际上 TOP 50 的生物医药公司中超过 50%的企业已转型 SaaS 数字化研发平台；超过 80%的生物医药初创企业首选 SaaS 数字化研发平台。在中国，SaaS ELN（电子实验记录本）正在撼动传统 ELN 在企业心目中的地位，成为市场主流。

如果您想了解更多关于「电子实验记录本」的应用，欢迎来电咨询

电话：010-82676188

邮箱：market@neotrident.com

官网：www.neotrident.com