网络安全指南

概述

因美纳 （Illumina）推出此网络安全最佳实践指南，涵盖客户现场产品的整个生命周期：从部署和配置，到补丁管理，以及报废或转售。因美纳建议客户将以下内容应用于因美纳产品中。

安全要求推荐

为了持续维护部署在客户现场的因美纳产品的受保护安全状态，因美纳建议遵循下列安全要求，以避免网络安全风险上升：

1) 确保因美纳仪器被放置在受保护的、良好分隔的网络中，仅服务于内部客户组织，只允许授权人员访问。
2) 确保因美纳仪器物理上位于客户设施内受控制的环境中，只允许授权人员访问。
3) 确保与客户提供的网络存储/服务器/PC 的通信配置为使用了因美纳仪器提供的最新安全协议之一。安全协议将确保连接的身份验证，并提供传输数据的完整性和保密性保护。一个强健的安全协议实例可以是启用了加密和签名的 SMB v3.1.1 或更新版本。
4) 确保除了仪器特定文档中描述的内容和默认配置外，无任何其他连接在因美纳仪器上的额外配置：
    a. 对于那些运行本地运行管理器（Local Run Manager） 的仪器，请确保仪器操作软件上的 Local Console 模块的入站连接（用于预配置测序运行），仅允许通过 TLS 1.2 或更高版本。
    b. 对客户提供的网络存储的出站连接仅允许使用安全协议（参见以上第三条）。该连接用于使因美纳仪器产生的结果和分析对客户可用。
    c. 向因美纳云服务器的可选单向出站连接仅允许通过 TLS 1.2 或更高版本。
    d. 向因美纳云服务的出站连接（适用于相应产品）仅允许通过 TLS 1.2 或更高版本，该连接用于将测序仪产生的数据发送并进行二级和三级分析。
    e. 对于 VeriSeq NIPT Solution，请确保来自连接于客户提供的电脑的 SMB 服务器的入站连接仅允许使用安全协议（参见以上第三条）。

5) 确保因美纳仪器不被用作通用电脑，避免其中操作系统级别的访问被滥用以执行诸如浏览互联网、下载和安装其他非因美纳软件等操作。
6) 因美纳建议在将仪器加入目录管理（Active Directory）时谨慎行事。目录管理策略可能会覆盖因美纳的产品安全控制。如果决定将因美纳的产品加入目录管理，请确保通过组策略对象（GPO）推送的安全配置不会覆盖仪器的安全设置。
7) 如果您认为您的仪器受到潜在网络安全事件的影响，请尽快通过 chinasupport@illumina.com 联系因美纳并报告。

安全设备报废/二次销售协议

因美纳提供以下关于通过清除因美纳仪器中的敏感、机密和专有数据和软件来安全报废设备的指导：

• 对于希望报废因美纳仪器的客户，必须取出硬盘，可将其保留给客户，根据客户政策进行数据存档或应该将其物理销毁。如需帮助，请通过 chinasupport@illumina.com 联系因美纳技术服务以请求付费现场访问。

• 如果因美纳仪器将被重新销售，客户应通过 chinasupport@illumina.com 联系因美纳技术服务，必须对敏感、机密和专有数据以及软件进行清除。

补丁管理

因美纳致力于为其产品提供持续的网络安全支持，包括及时沟通有关支持软件和网络安全特定应用程序补丁的维护和更新。对于 Dx/IVD 仪器，因美纳仪器软件的软件更新和网络安全补丁将由因美纳的现场服务团队提供并安装。对于已由因美纳测试并在此页面上提供的操作系统补丁（例如 Microsoft、RedHat、Oracle），请与您的 IT 团队合作将补丁应用到因美纳的产品上。因美纳致力于在产品达到其服务寿命终止（EoSL）日期之前为最新版本的仪器软件提供此支持。

定期进行关键的安全更新有助于保护因美纳仪器免受最新的安全威胁和漏洞的影响。

网络安全指南

安全审计

对于支持审计跟踪的因美纳仪器，包括 IVD/Dx 仪器，审计追踪提供了在操作系统（Microsoft Windows）和应用程序（例如 Local Run Manager）级别的安全日志记录的。当启用时， Local Run Manager（LRM）界面可供客户的管理员角色进行日志导出（请参阅 LRM 管理设置和任务章节以获取更多详细信息）。安全日志的导出和分析应根据客户内部安全政策确定的频率进行。

安全状态

因美纳仪器随附一套软件、功能和配置，可在操作系统级别实现强健的安全性，例如：

• 反病毒工具（基于 Windows 的仪器）。

• 配置防火墙仅允许必要的连接。

• 启用了安全审计日志记录， Dx 仪器中的日志以受保护的方式存储。

因美纳建议客户：

• 遵循 Antivirus Software Page 中提供的说明，并以手动扫描模式启用反病毒工具。

• 一旦启用并配置了反病毒工具，请不要修改任何安全配置，或者如有必要，请在进行此操作之前与因美纳技术支持联系进行咨询，以避免在产品上引入额外的网络安全风险。

因美纳仪器随附了用户管理功能，遵循最佳的安全实践，包括：

• 强大的基于角色的访问控制和用户与管理员角色的分离（请参阅仪器说明书“ LRM 管理设置和任务”）。

• 密码复杂性规则的介绍和执行。

• 引入和执行暴力攻击保护。

• 能够维护基于身份的账户。

• 密码的存储。

• 对启用 LRM 的仪器进行基于身份的安全审计日志记录。

因美纳建议充分利用提供的系统用户管理功能，并且仅使用非共享账户，每个用户关联有唯一的登录账户和密码。因美纳还建议使用美国国家标准与技术研究院（NIST）建议的密码规范，这些规范包括不要重复使用其他系统的密码，不要将字典词汇作为密码的一部分，以及使用足够长度和复杂性的密码（至少 10 个字符，其中包括一个大写字母、一个小写字母、一个数字和一个特殊字符）。

技术支持

如需技术支持，请联系因美纳技术支持。

网站: www.illumina.com

电子邮件: chinasupport@illumina.com

安全数据表（SDSs）—可在因美纳网站 support.illumina.com/sds.html 上获取。

产品文档—可从 support.illumina.com 下载。

修订历史

文档	日期	变更描述
200055146 v00	2024 年 4 月	首次发布.

网络安全指南

Document # 200055146 v00