医疗机构如何确保符合 HIPAA 标准 保障网络安全

www.isdecisions.com

医疗机构如何确保符合 HIPAA 标准 保障网络安全

随着美国新修订的**联邦隐私和安全条例**（HIPAA 总括最终法规）在上月 23 号正式生效，公民的**个人健康信息安全**再次被广泛关注。

该条例的产生是源于**健康技术条件下经济和临床医疗（ HITECH ）法案**所做出的修改。自这一法案于 2009 年颁布以来，美国已投资数以百亿的资金来创建一个全国性网络的**电子健康记录**。而 HITECH 这一法案的修改在保护公民个人电子健康记录（即**电子病历**）方面对医疗机构也提出了新标准。（注：HIPAA 指健康保险流通与责任法案）

任何医疗机构或人身保险机构，无论是存储、处理或传输个人健康信息，必须遵守 HIPAA 法案，并保障所有受保护数据的安全。

HIPAA 的规定虽没有特定的安全技术要求，但也指定了一套原则来引导这类机构的技术选择。当涉及到 **Microsoft Windows** 和 **Active Directory** 网络的安全时，机构应该着眼于维护和保障他们的 **Windows 基础架构**，不单单是本机 Windows 上的安全控制。因为 Windows 上的安全控制有其自身的局限：

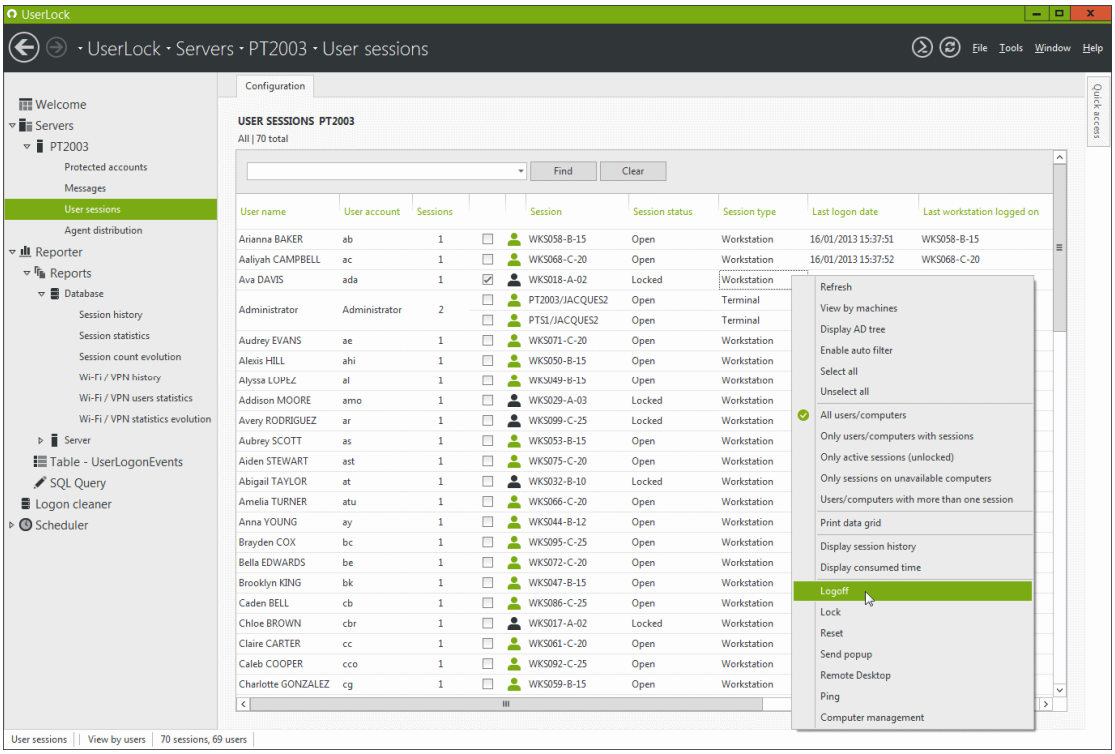
- 微软的服务器易因不当的用户访问受到攻击。
- Windows 不禁止并发登录，对于不当的文件访问不能提醒 IT 人员。
- Windows 不为管理员提供监控或智能访问和登录的功能。

那什么样的才是有效的解决方案呢？

看 ISDecisions 如何帮助医疗机构满足 HIPAA / HITECH 标准

ISDecisions 是全球顶尖的软件企业，专注于提供针对 **Microsoft Windows** 和 **AD 域控**的安全和访问管理解决方案。ISDecisions 的解决方案帮助**防止安全漏洞**，并确保遵守 **HIPAA 标准**，保护网络内部的数据和信息不受授权用户（或使用同一账号进行登录的用户）的破坏，并禁止未经授权的网络访问。

1. UserLock 提供对所有员工访问网络及其中数据的可见性和全面监控



使用 UserLock 你可以设置并执行粒状登录限制：

- 防止并发登录，以确保对数据的访问是来自是单个员工。限制并发登录有助于防止用户共享他们的密码，并阻止流氓用户使用有效凭据成为合法所有者。
- 限制基于多种标准的网络访问，包括工作站访问和使用/连接时间。

2. FileAudit 通过监测、归档和报告所有文件和文件夹的访问，保护 Windows 环境下的所有文件服务器

使用 **FileAudit** 你可以：

- 识别所有受访问的文件/文件夹、访问类型、文件所有权变更或权限修改。
- 实时监控——你可以快速搜索、警惕、报告和归档发生在一个或多个 Windows 系统上的所有文件访问事件。

UserLock 和 FileAudit 为企业提供超乎本地 Windows 功能所能提供的网络安全保护，并广泛的报告和审计，由此，医疗机构可以借助二者来助其确保符合 HIPAA 的监管审计，实现更高的综合效益。