ivanti Neurons

医疗服务IT、生物医学、安全

医疗设备可视性和安全风险优化指南

内容

介绍

联网医疗设备对医疗服务IT、生物医学和安全企业构成了巨大挑战。这些设备的特点决定了它们易受网络威胁，而成功的网络攻击可能会造成严重后果。然而，传统的网络安全措施无法应用于这些设备，甚至可能会干扰关键的临床操作。

本指南将解释如何通过三个步骤来提升医疗设备的可视性，同时降低安全风险。为医疗设备建立多层面的网络安全是一个多阶段的持续过程，它的成功需要奠定坚实的基础，并采取有条不紊的系统化方法。

了解如何发现、评估和降低与联网医疗设备相关的网络安全风险。我们在本指南中提出的三个阶段并非一个一次性的过程，而应当被视为一个周期。医疗服务中心的IT和安全团队应持续执行这个周期中的步骤——日常检查环境、评估风险，解决发现的安全问题。

医疗设备在面对网络攻击时有多脆弱？

连接到网络或其他设备的医疗设备越来越多，为医院和医疗服务提供者带来了重大的安全隐患。其中许多设备并不安全，也没有得到主动管理，这就为各种网络安全威胁打开了大门。

为什么医疗设备会有漏洞？

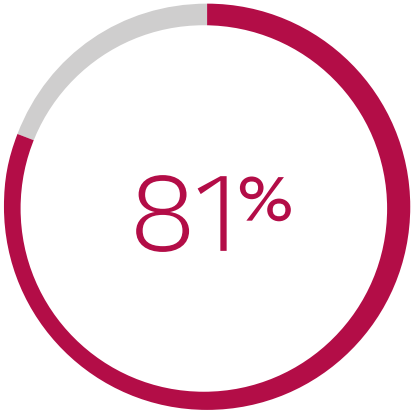
- 软件代码：没有经过安全审查
- 验证：薄弱或不存在
- 数据传输通道：往往不安全，没有加密
- 有限的可视性：无法充分了解正在使用的设备
- 无法监控：无法监控设备活动和安全事件
- 退役设备：没有得到安全处置
- 软件更新：没有，或很少部署

了解环境
发现存在哪些IT和医疗设备，对它们进行准确分类，了解临床背景，确定联网需求

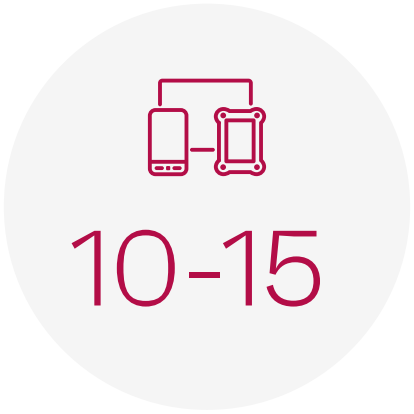
风险评估
识别设备漏洞和联网风险，为每个设备确定风险指数，并提供补救建议

保护设备
在设备层面解决安全问题，在局域网内隔离设备，阻止局域网/广域网上的非必要通信，制订战略以在发生安全事件时及时检测

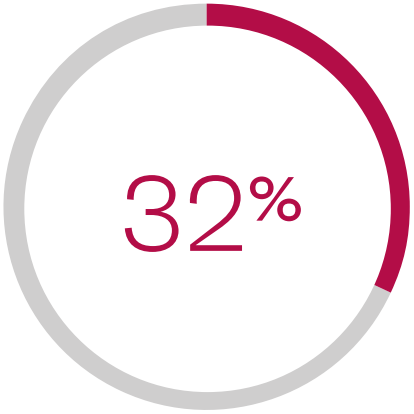
这个问题有多严重？



81%的医疗服务机构报告，在过去两年中曾在网络攻击下发生泄露。



每张医院床位的联网医疗设备数量保持在10-15台，共有370多万台设备正在使用。



32%的医疗服务机构表示，医疗设备是他们的首要安全顾虑。

来源：KPMG, Wired

哪些威胁向量会影响医疗设备？

恶意软件
医疗设备通常没有端点保护，在恶意软件攻击下尤其脆弱。

内部威胁
由于身份验证较弱，恶意的内部人员很容易进行未经授权的访问，并篡改设备。

网络应用攻击
一些医疗设备可以通过网络界面管理，并构成一系列的网络风险，例如代码注入、跨站脚本(XSS)、目录遍历等。

滥用设备
联网医疗设备通常基于Windows PC。医院工作人员可以使用这些机器浏览互联网或安装软件，从而带来额外风险。

如何才能评估网络安全风险和攻击影响？

FDA 医疗设备指南 就设备风险等级提供了非常有用的分类信息。

1级：较高网络安全风险	2级：普通网络安全风险
此类设备	**此类设备**
能够连接到其他医疗或非医疗产品、网络或互联网 或 影响该设备的网络安全事件有可能对一名或多名患者造成直接损害	能够连接到其他设备或网络，但不会对患者造成直接损害 或 能够对患者造成直接损害，但无法连接网络

您可以使用 CVSS 风险评分系统 CVSS 风险评分系统等框架进行更细化的风险评估。在评估网络安全风险时，应考虑以下因素:

- 软件漏洞
- 患者安全
- 验证
- 隐私
- 联网
- 服务中断

阶段 I:

了解联网设备环境

解决问题的第一步是认识到问题存在，并了解它涉及的范围。医院及医疗服务机构的IT、生物医学和安全团队对联网医疗设备的问题缺乏了解，是因为这些设备的可视性极其有限。

安全团队视医疗设备为黑箱，甚至根本无法看到

医疗设备安全正在逐渐成为临床工程团队和IT部门的共同责任。这些设备的信息存在于医疗服务机构中，但安全团队无法轻易获取。

以下重要问题无法得到解答：

1. 有多少台设备在联网？
2. 这些设备与其他哪些设备或网络通信？
3. 是什么类型的设备？
4. 其网络行为是正常有序还是异常？

为什么难以为联网医疗设备建立设备清单？

医疗设备无法像普通IT网络那样，轻松运行网络扫描即可完成设备识别。

- 这些设备很敏感——主动的网络扫描可能会扰乱医疗设备的运行，因此您必须使用被动检测。
- 对网络发现工具隐藏——传统工具无法发现绝大多数的联网医疗设备，或可能错判该设备为Windows工作站。大多数联网医疗设备不会公布它们的信息，要在网络上检测到它们，需要在应用程序层面进行仔细的流量分析。
- 设备数量大、种类繁多——也许有数万台不同类型、不同供应商和不同版本的设备。
- 持续的变化——设备不断地被添加、替换或从网络中移除，且通常不会通知IT人员，因此设备的发现和统计必须是一个持续性的过程。

第1步：发现

目的是建立包含每台设备数据的医疗设备数据库。重点放在能够协助确定风险和漏洞的高质量数据上。尤其是：

- 设备类型
- 部门和房间
- 销售商
- 型号
- IP地址
- 操作系统
- 应用软件版本
- 最新的安全补丁

第2步：网络映射和临床背景

了解设备的网络行为能够让您了解设备对内外威胁的暴露程度。请尝试为每台联网设备获取以下信息：

- 设备在与其他哪些通信？
- 设备是否拥有对其他设备、网络和互联网的不必要访问权限？
- 设备的网络通信是否通过虚拟局域网隔离？
- 设备使用何种协议？
- 设备在哪里发送或接收受保护的健康信息（PHI）数据？是哪种PHI？
- 设备是否通过互联网进行对外通信？
- 设备是否需要与供应商保持通信？
- 互联网通信是否属于此类设备的正常行为？
- 设备的互联网通信是否通过VPN隧道隔离？

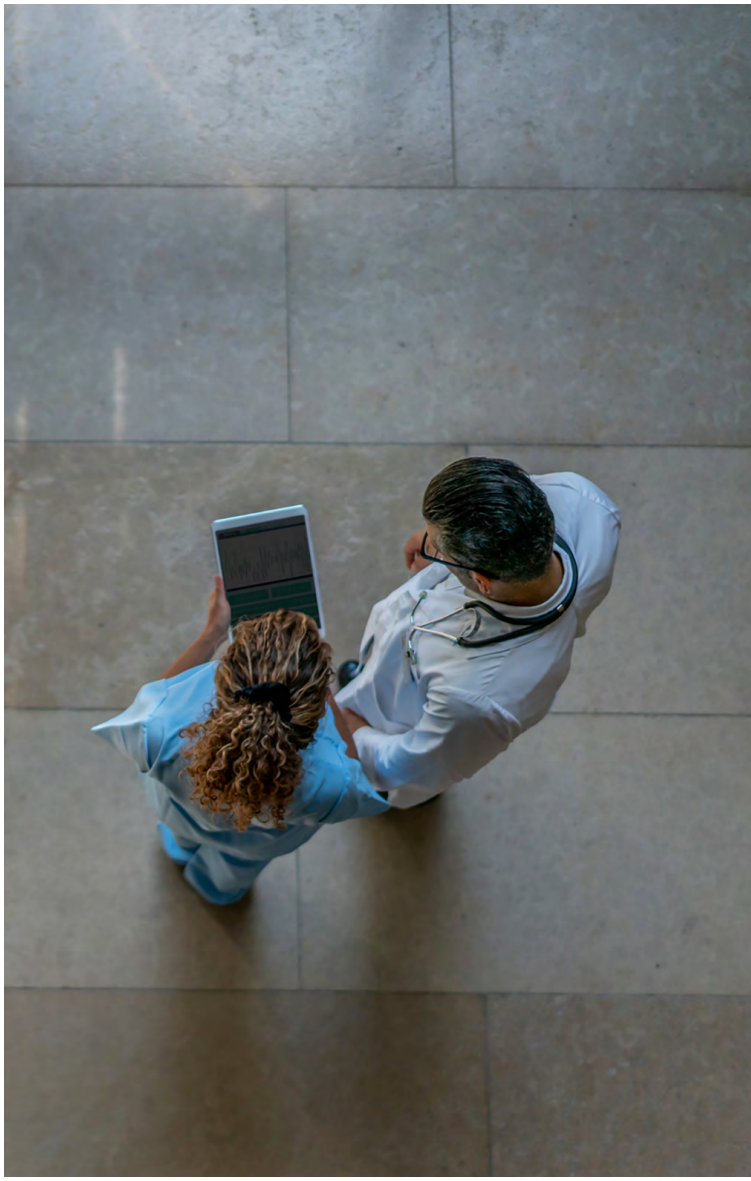
明确每台设备的临床用途，并进一步明确其风险暴露情况。如果没有自动化工具的帮助，要获得这些数据是非常困难的。

临床背景信息

- 设备发出或接收的连接中哪些用于临床数据传输？哪些是控制信道等非临床通信？
- 设备是否传输或保存受保护的健康信息（PHI）？
- 设备是否与患者护理直接相关？例如：患者监护仪、输液泵、心脏起搏器等。设备是否属于FDA规定的III类器械（用于维护或支持声明的器械）？

作用

- 任何安全措施都必须避免干扰关键的数据流。
- 通过识别临床工作流，您可以准确地识别可能影响重要信息流的异常情况。
- 包含PHI的设备更容易成为网络罪犯的目标。
- 既要保证数据的安全，也要保证设备本身的安全。
- 设备需要符合相关的标准和规定。
- 优先考虑与患者护理直接相关或可能对患者造成直接伤害的联网设备安全。



阶段 II:

风险评估

一旦您对您的联网医疗设备有了更好的了解，并建立了设备、设备背景和网络行为的清单，您就可以利用清单来评估每台设备的风险及其对您的机构的影响。

第1步：识别设备漏洞和可能的补救措施

收集漏洞数据，包括您的每台设备型号、操作系统和应用程序版本。

同样重要的是，确认设备的所有者和您的权限，以补救安全问题。

软件漏洞的影响
使用CVSS 风险评分系统来了解您的联网设备中已知软件漏洞的影响。

错误配置
检查一般性漏洞，例如硬编码或默认密码、未打补丁的操作系统或软件。

设备验证
确定设备是否具有验证功能，如果有，强度如何，是否设置了安全密码。

联系点
谁来管理设备：临床工程、IT、制造商还是第三方承包商？

访问权限
安全团队是否有权访问此设备以执行安全控制或应对事件？

备份
设备是否有备份或冗余，服务中断会有何影响？

第2步：识别网络层面的风险

医疗设备漏洞只是风险的一个方面。分析网络连接性，识别攻击者可以借以连接到您的设备的向量。

互联网连接
检查设备是否通过互联网连接到其他系统，例如连接到第三方公司或制造商进行维护或更新。

与较低安全设备的连接
检查设备是否可以连接到较低安全的设备或端点，例如医生的工作站等，以及是否会暴露管理或数据服务，如FTP或SSH。

加密
检查设备是否传输或接收未加密的数据流 。

不安全协议
检查设备是否使用弱认证、无认证或有漏洞的协议。

第3步：识别风险严重性

仔细考虑：如果您的每一台设备分别遭受了成功的网络攻击，会造成什么影响？与对医疗服务IT系统的攻击不同，联网设备攻击的影响不仅仅是数据安全和隐私。成功的网络攻击可能会干扰临床护理，对患者造成直接伤害。

我们建议您采用CVSS风险评分系统的三个影响指标来查明风险的严重性。

- 保密性——代表设备存储或传输的受保护健康信息(PHI)的风险暴露
- 完整性——针对直接用于患者护理的设备，代表患者安全所面临的风险
- 可用性——代表服务中断的风险

患者安全	隐私	服务中断
低：FDA I类医疗器械；对患者或用户产生低度至中度风险	低：设备不储存PHI	低：设备故障不会影响患者护理
中：FDA II类医疗器械；中度至高度风险	中：设备在测试或治疗的有限时间内储存少量PHI	中：设备故障可能会影响患者护理，但不会影响关键的医学治疗
高：FDA III类器械；高风险，用于维系或支持生命、植入体内或存在较高的疾病或伤害风险	高：设备储存大量PHI，覆盖多项测试或治疗	高：设备故障可能会干扰关键的医学治疗，如手术、呼吸设备或维持生命的药物输送

阶段 III:

保护联网医疗设备

我们为您提供结构化的发现和风险评估流程，其优势在于，您可以根据设备的风险程度对其进行排序。每台设备都应有一个风险影响评分（基于患者安全、隐私和服务中断）。

您的机构可指定一个可接受的风险水平。安全团队便可专注于保护风险评分超出可接受水平的设备，并可针对不同风险评分的设备采取适当的安全措施 。

我们建议通过四个步骤保护联网医疗设备：

1. 保护设备层面——打补丁，禁用易受攻击的服务，采纳模范配置
2. 保护网络层面——在局域网层面隔离，阻断本地网络内的非必要通信，以及在广域网层面隔离，仅允许设备与已知的外部实体通信
3. 事件检测——制定发生安全事件时的检测策略
4. 量化和分析——持续分析安全方案的结果、调整、改进

第1步：设备加固

与任何计算设备一样，联网医疗设备也必须确保拥有最新的安全补丁和软件升级。必须对配置进行加固，以实现安全验证。关闭不使用的端口，限制不必要的功能——总之，减少攻击面。

大多数医疗设备都通过Windows操作系统运行。然而，对它们补丁不像工作站或Windows服务器那样简单

加固医疗设备的挑战

- Windows安全补丁必须经过设备制造商的验证和批准
- 临床工程部门必须证实补丁或更新不影响医疗设备功能

指导原则

- 部署所有的安全补丁，或加固所有的设备是不可能的
- 把重点放在高风险评分的设备上
- 优先处理针对您在风险评估中发现的已知漏洞的安全补丁或配置更改

第2步：网络隔离

保护联网医疗设备的一个重要策略是，尽可能把它与非关键的临床通信隔离开来，以此减小攻击面。这包括两个部分：

- 定义网络分段，确保联网医疗设备只能与同属一个临床流程的设备或系统进行通信
- 阻断外部通信，确保联网医疗设备永远不会连接到互联网，除非有必要与设备供应商或其他已知实体进行通信

隔离医疗设备的注意事项

- 隔离临床数据流与非临床数据流
- 临床通信是必不可少的，但其他任何通信都应被阻断

指导原则

- 制定严格的访问策略和网络分段，以限制设备发出/接收的非必要通信
- 制定分段策略，以解决您在影响分析中发现的风险和漏洞
- 阻止设备连接到互联网，绝对必要的情况除外，且只能连接到已知实体
- 与临床工程和医疗技术管理（HTM）团队密切合作，确保您不会造成关键数据流中断

第3步：事件检测和响应

对于大多数联网医疗设备而言，抵御所有的潜在威胁是不可能的，因为总有一些关键的遗留设备无法被替换，也无法完全打补丁或隔离，这意味着您可以减小攻击面，但无法彻底消除。此外，隔离可能会是一个漫长的过程，在此期间，一些设备将仍然易受攻击。所以，监控设备并在发生异常活动时立即检测和报警是至关重要的。

监控安全事件的注意事项

- 使用网络TAP或镜像端口等被动监测，以避免中断设备操作。
- 利用您收集到的每台设备的临床背景信息，了解什么是正常的临床通信。
- 将当前行为与供应商规范、过往行为以及您的环境和其他机构中的同类设备的行为进行比较。

指导原则

- 持续监测所有设备，重点关注高风险评分的设备。
- 建立策略，比较进行中的通信与正常临床通信。
- 在发生任何重大异常行为时通报安全部门。
- 与第三方整合，通过远程操作执行快速修复，如按需网络分段等。

第4步：量化和分析

维护医疗器械网络安全是一个长期的过程，需要逐步维护和改进，以应对不断变化的威胁。

记录您的进展有助您了解自己的工作方向是否正确，如果您所做的工作并没有改善安全状况，您可以修正。以下是记录医疗设备安全项目进展的一些指导原则。

- 建立记分卡，记录医疗器械风险评分和时间线，确保风险随时间的推移而降低
- 明确操作，明确改善KPI和降低总体风险指数的操作和策略
- 设定KPI，以重要设备的风险为基础，并监控改进情况；将KPI与业务目标（如患者安全和服务可用性）联系起来，以获得领导层的支持
- 收集数据，收集设备的风险指数和历史行为数据，并将其用于更好的采购决策

选择Ivanti Neurons 神经元医疗服务，提高医疗设备的资产可视性，缓解安全风险

Ivanti® Neurons 神经元医疗服务为您提高医疗设备的资产可视性，缓解安全风险。这款解决方案可发现并智能剖析医疗设备和医疗物联网(IoMT)，评估安全风险，报告威胁，并在多个数据源之间协调设备信息。更确切地了解您的设施中的各种特殊医疗设备，包括设备分类、使用信息和详情，以降低安全风险或应对异常情况。采集和核对供应商数据，为您的所有医疗设备创建单一可靠的信息源。

要进一步了解，请访问
ivanti.com.cn/products/ivanti-neurons-healthcare

ivanti Neurons

ivanti.com.cn/neurons
+86 (0)10 85412999
ContactChina@ivanti.com