如果一流的医疗中心因网络过时而出现安全问题，会发生什么？

在某个行业处于全球领先地位的组织却在网络安全方面落后于人，这并不奇怪。我们这个案例的主角就是医疗行业中的这样一家企业。这个大型国有医院系统曾面临严峻的 IT 挑战。他们一再推迟网络方面的投资，直到暴露出了严重的安全漏洞。由于受攻击面极大，而且可视性有限，威胁很有可能成功侵入网络，并隐藏数月不被发现。这使得医院的关键系统、员工、患者和声誉面临风险。

> “由于缺乏重视，我们的网络基础设施沦落到无法支持业务服务的程度，我们因此尝到了苦果。”
>
> – 客户陈述

挑战

- 为 500 个站点和数千台设备提供安全保护。
- 支持网络分段，以实现 HIPAA 和 PCI 合规性。
- 获得对威胁的可视性与可控性。

解决方案

- 架构化网络更新和安全策略实施
- 网络即传感器 (NaaS) 和网络即执行器 (NaaE)
- 思科 IOS® NetFlow、思科® 身份服务引擎 (ISE)、思科 StealthWatch® 以及思科 TrustSec® 解决方案
- 思科咨询服务在每个阶段提供指导

成果

- 通过网络分段防止高级威胁的横向扩散
- 提供深层可视性，以改善访问、策略和控制
- 提高患者信息的安全性和可访问性

问题

随着时间的推移，在多种因素影响下，这家医院面临着严峻的风险。

平面网络

医院老化的网络基础设施，包括过时的交换机，都会使医院面临威胁。大多数医院采用并行网络，能够将临床系统、研究设施、访客访问和管理分离开来。理论上来说，不同的网络绝不应彼此接触。

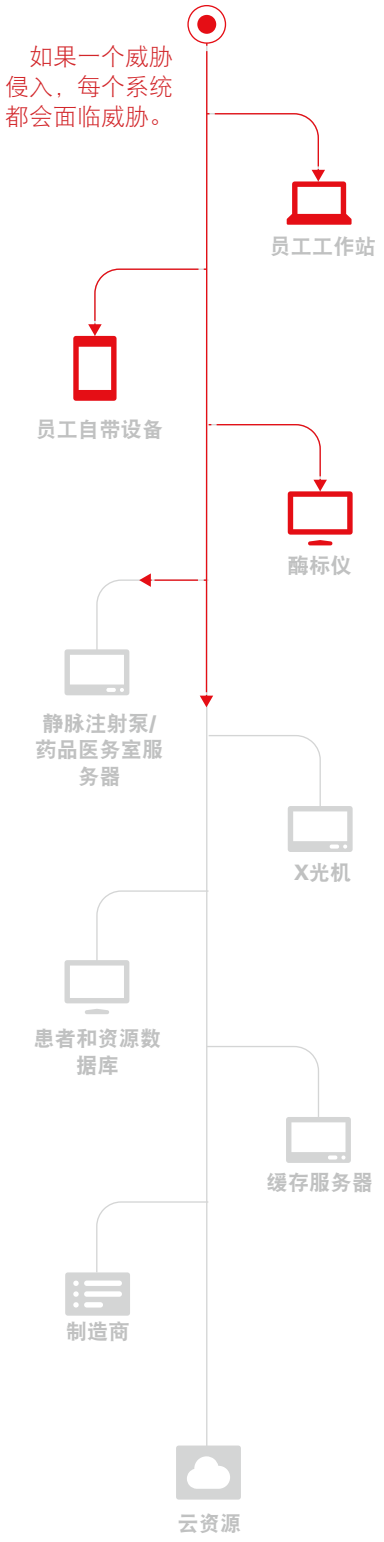
但是，这家医院只有一个平面网络，没有进行分离或网络分段。他们按楼层分配 VLAN，而不是按职能进行划分。医生、员工、学生和医疗设备共用同一个网络，这就扩大了受攻击面，使医院暴露在威胁之中。这家医院很难洞悉网络中的可疑行为，更不容易确保符合 HIPAA 及其他法规的要求。

设备过载

医院拥有超过 15,000 个不可升级的终端，并且许多终端是互连的。心率仪、呼吸机、质子束治疗仪和其他设备都连接到该网络甚至互联网。

该医院需要控制其平面网络暴露的环境。

某些终端运行的是早在 1992 年就安装的 MS-DOS 版本，因此网络容易受到高级或复杂威胁的攻击。医院网络中的 600 多台 Windows NT4 设备以及将近 7000 台 Windows XP 设备均面临支持服务终止和缺少补丁程序的问题，并且无法运行最新的防病毒软件。更糟糕的是，FDA 审批要求设备保持制造商最初交付的原样，因此系统升级就意味着不合规。



拼拼凑凑的无效解决方案

IT 曾试图提高网络的安全性。他们利用传统模式对网络进行分段，安装补丁并建立了 VLAN，甚至尝试采用透明防火墙，以限制用户访问相应的文件和资源，但并没什么成效。购买新设备意味着要花费大量资金，但这样做无法解决根本问题。该团队面临着严酷的现实：他们需要更高的可视性、洞察力和可控性，同时满足合规要求。

> “客户曾问，现如今他们的基础设施中有多少能实现策略分段？答案：他们当前网络中不到 10% 的基础设施可进行策略分段。”
>
> – 思科顾问

解决问题

第三方顾问、医院 IT 专业人员和医院高管同意必须采取措施，并且他们应该退一步全面地审视安全问题。正确的战略性方法是设法了解应用、用户和设备如何连接并将网络控制措施落实到位。

思科安全顾问会同工程师、业务分析师和高管召开了为期 2 周的研讨会。最终达成的结论是，医院需要能够支持分段的更高级的网络，于是该团队制定了高级网络设计、为期 18 个月的推广计划以及详细的监管模式。最智能的方法是使用支持网络 (NetFlow) 的架构将安全性和网络连接在一起。

该计划非常简单：

- 升级传统交换机、路由器和无线技术，以并入包括 NaaE 和 NaaS 在内的关键安全解决方案，从而实现可视性、分段和可控性。
- 委聘思科高级服务团队，确保在指定的时间内成功实施解决方案。
- 标准化流程，以便将新组件添加到网络中。

解决方案

思科能够保护网络的安全。

思科 NaaS 将您的网络转变为威胁监控器或传感器。它采用已经嵌入了大多数思科 IOS 网络设备的 NetFlow 技术；思科 StealthWatch 解决方案；以及思科身份服务引擎 (ISE)。

- 思科 IOS NetFlow 由思科创建，可提供网络可视性。NetFlow 通过包含来源、目标、时间和协议信息的记录跟踪每个网络对话，以提供深入的可视性。通过它可以得知对话对象、使用工具、来源位置、对话时长，包括交换了多少数据，以及存储数月的信息。
- 思科 StealthWatch 将分析得出的威胁情报添加至 NetFlow 数据中，以加快响应速度。思科 StealthWatch 解决方案可以分析网络审计跟踪，识别异常活动并锁定攻击的根源。借助该解决方案，您可以检测与高级持续性威胁 (APT)、分布式拒绝服务 (DDoS) 攻击和内部威胁相关的网络流量及行为。
- Cisco ISE 可提供情景数据，包括参与者、事件、位置、时间、用户及设备的连接方式与访问网络资源的方式。

思科 NaaE 实施安全策略。它通过激活思科 ISE 中内嵌的思科 TrustSec 技术扩展功能。

- 思科 TrustSec 技术可与 ISE 配合使用，以遏制攻击的范围。思科 TrustSec 技术利用安全组标记功能创建虚拟网络分段，并由 ISE 在网段上实施策略。通过分段可以隔离威胁，从而限制恶意活动。

“如果一家偏远诊所在关门后还有医生在下午 5:30 访问大量记录，这就属于异常情况。

如果我启用了 NetFlow，系统将会标记出这种情况。”

– 思科顾问

这些解决方案不仅能帮助医院识别威胁，还能帮助其了解合法数据流和逻辑流量分组，以确定网络分段。

思科 TrustSec 技术可轻松地与较新的交换机、接入点和防火墙集成。使用思科 TrustSec 解决方案，医院不必再担心 IP 地址问题，并可以专注于分类。凭借 NetFlow 提供的精确分类，该团队能够制定一套有意义的规则。ISE 创建用户策略并对用户进行分组。医院可以通过精细的业务和策略规则实施访问，实现适当设备的适当通信。

医院必须能够将医疗设备和数据与网络上的其他设备和数据隔离开来，从而使医院可以通过实施分段和用户访问来阻止攻击。现在，即便攻击者入侵了网络，他们也只能访问一个网段。

成果

其他优势：
卓越的安全性推动了创新。

- 提升了员工满意度
- 提高了工作效率
- 实现高质量研究
- 改善了患者体验

除了拥有即时安全和合规性优势之外，医院还获得了意料之外的巨大优势：运营效率。他们减少了手动更新次数、人为错误和重复任务，并且网络团队现在可以快速地识别应用、服务器和网络性能问题。

全新的敏捷网络满足了患者和员工最迫切的需求：安全、速度、可用性和更完善的服务。这为将来采用其他技术奠定了基础。有了安全保障，医院可以开始推出新的应用，以创新的方式建立员工之间以及员工与患者之间的联系。全新的移动性、信息共享和协作应用有可能进一步简化运营。

详细了解相关思科解决方案的信息：

cisco.com/go/stealthwatch

cisco.com/go/ise

cisco.com/go/trustsec

技术优势

- 将安全性融入到每一层：交换机、路由器和接入点
- 升级整个医院的网络架构
- 针对未知设备和异常流量模式提供深入广泛的可视性
- 验证用户和设备
- 在有线、无线和 VPN 拓扑之间实施策略

业务优势

- 保持与不断增长的新用户、设备和应用之间的同步。
- 减少手动更新次数、人为错误和重复性任务。
- 轻松达到 HIPAA、PCI 及其他法规的审计要求。
- 减少停机成本及责任。
- 最终提供更准确、可靠的患者护理。

只有思科无线网络产品拥有美国医院协会 (AHA) 的独家认证。

美洲总部
思科系统公司
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰，阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站上列有各办事处的地址、电话和传真，其网址为 **www.cisco.com/go/offices**。