物理层数据安全性
可防范内外部威胁

在当今的超连接智能楼宇中，每个网络连接都是进入公司或关键任务网络的一条途径。与此同时，当涉及到内部威胁时，攻击范围的大小与能够访问受保护数据的人数直接相关。

亚太地区的数字连接量大，但网络安全意识低，跨境数据传输不断增加而监管薄弱，因而成为网络犯罪分子肆意妄为的避风港。例如：在东南亚，所有经济领域都在进行数字化转型，且互联网接入成本在大多数人可承受的水平。

正如内部威胁是造成数据泄漏的一个被低估的原因，网络访问安全也是一个被低估的防御层。利用康普 Ruckus Cloudpath Enrollment System 之类的安全注册和身份验证系统，可轻松定义和管理基于角色的网络访问政策。此类系统使 IT 团队能够在检测到任何不当活动时切断网络访问。

除了采用安全引导流程系通过，以大大减少服务台票证相关的网络访问之外，企业还必须避免任何一层出现未经授权访问，并保护每个入口点（从应用级别的加密到身份验证、虚拟专用网络（VPN）、防火墙到最终物理层）的安全性。

物理层安全

企业网络中的数据泄露成本远不止是经济损失，企业可能需要数年时间才能重新获得信任并重建其声誉。据估计，60% 的数据安全漏洞都是由内部人员恶意或无意造成的。显然，物理层基础设施是任何针对内部和外部威胁的数据安全性计划的重要组成部分。

在医疗保健和金融等行业，网络安全问题催生了有关数据存储的法规和合规性要求。网络基础设施安全问题通常分为两类：

- 未经授权人员进行未经授权的访问可以通过部署与 IP 相连的摄像头、在场传感器、访问控制和所连接的其他物理安全组件来减少或预防。可以通过部署物理布线安保装置（如键控连接器、安全跳线和端口阻止器）来降低未经授权访问所带来的威胁。同样，自动化基础设施管理 (AIM) 解决方案可以记录和报告物理层上任何未经授权的活动。

- 检测和阻止授权人员进行未经授权的访问可能会更加困难。鉴于企业网络的深度和复杂性，网络管理人员可利用 AIM 系统从内部监控和管理网络连接。通过使用智能布线、连接器和配线架，AIM 系统可自动实时检测和映射端口和设备级的所有物理层活动。如果授权用户连接或断开连接设备，AIM 解决方案（如康普 imVision）会自动向 IT 人员发出警告。

室内无线

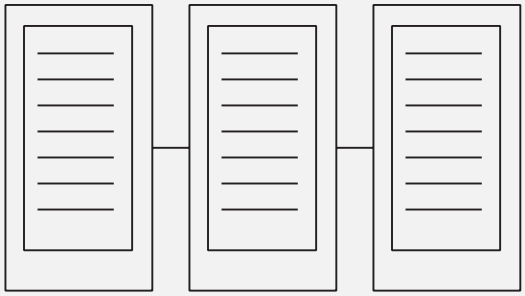
鉴于大多数移动流量都发生在楼宇内，室内无线网络对企业的重要性如同水或电一样。然而有一个令人担忧的趋势，就是黑客已经找到了利用大多数企业 Wi-Fi 系统使用的 WPA2 安全协议弱点的方法。

该协议的最新迭代 (WPA3-Enterprise) 具有相当于 192 位加密强度的功能。此外，由专用分布式天线系统 (DAS) 驱动的蜂窝或移动网络具有服务提供商集中管理和托管的安全性，可能在稳定性和响应速度方面会优于传统 Wi-Fi。

安全监控和光电混合缆/以太网供电布线

由 IP 安防摄像头和在场传感器组成的网络通常安装在智能楼宇中，可帮助发现未经授权的入侵者。借助适当的综合布线基础设施，就可以将这些采用以太网供电 (PoE) 的内部安全监控设备分布在楼宇或校园内的各个位置。

虽然 AIM 系统只能定位潜在的黑客，但摄像头可提供确凿的视觉证据。低压光电混合缆或 PoE 网络可为这些互连传感器、摄像头和控制器提供电力支持。如果主电源故障，AIM 系统和所有互连安保设备可继续运行，因为它们可以从交换机获电，而交换机通常由 UPS 电池和发电机供电。这种供电结构本身更易恢复运行，也更安全。



成功案例：越南河内证券交易所和澳大利亚的南澳大利亚健康医疗研究所

持续监控和警告可确保真正的安全网络

构建一个安全网络基础设施并确保其连接性能一直以来都是河内证券交易所和南澳大利亚健康医疗研究所 (SAHMRI) 关注的重点。

为方便系统管理人员实时查看网络物理层，加快故障排除速度并提高安全保障，同时减少网络宕机时间，提高维护的成本效益，实现智能基础设施管理十分重要。

解决方案

这两家机构都选择了结构化布线领域的领先供应商康普公司，并部署了 SYSTIMAX iPatch 系统，该系统由 System Manager 软件、iPatch Manager 和 iPatch 智能铜缆和光纤配线架组成，可满足其所有基础设施要求。

拥有全球支持网络和行业领先的 20 年质保是康普设施的坚强后盾。在河内证券交易所，完工后的基础设施将闭路电视与门禁控制系统连接起来。在数据中心内部，服务器与存储区域网络间的连接采用了 SYSTIMAX 布线。

与此同时，基于 SYSTIMAX 360 解决方案的网络基础设施连接 SAHMRI 的数据系统，并为超低电压系统提供支持，包括楼宇管理、安全性、VoIP 和照明控制。这些关键应用都依赖于具有高性能和可靠性的铜缆和光纤布线。

优势

这两家机构的 IT 管理员可实时查看并控制物理层。部署方案中的铜缆和光纤连接采用可监控网络连接和相连设备的 iPatch 配线架进行管理。

成功案例：越南河内证券交易所和澳大利亚的南澳大利亚健康医疗研究所

通过检测和定位未获授权的接入点，iPatch 软件可在发生任何变化时立即向管理员发出警告。System Manager 软件可通过标准网络浏览器记录和管理基础设施。

imVision AIM 平台

在 iPatch 系统的基础上，康普还采用了其 imVision AIM 解决方案，该解决方案可为影响网络物理层及与其相连设备的事件提供可以付诸实施的见解，并且能在实时智能和可视性的更高层面上查看此类事件。

AIM 解决方案采用智能布线、连接器和配线架实时监控互联环境。如果检测到未获授权或获授权设备试图访问未获授权信息，该系统会立即发出警告。

System Manager 可跟踪所有连接的终端设备，包括通过无线连接的移动设备。该软件还可以与 PoE 设备集成，确保为连接提供可用电源。此外，当 iPatch 智能配线架检测到网络中的意外变更时，会发出实时警告。

使用 Cat 6A 类布线解决方案部署 PoE 和光电混合缆技术还可以提高安防系统（如 IP 安防摄像头和基于 AIM 的智能系统）的恢复性能。