思科打造万物互联制造云服务

工业互联网作为新一代信息技术与制造业深度融合的产物，不仅能为制造业乃至整个实体经济数字化、网络化、智能化升级提供新型网络基础设施支撑，而且催生了网络化协同、个性化定制、服务型制造等新模式新业态，有力促进了传统动能改造升级和新动能培育壮大。目前，全球制造业龙头企业、ICT 领先企业、互联网主导企业基于各自优势，从不同层面与角度搭建了工业互联网平台。思科也全面加速云平台的布局，积极推动工业物联网市场的变革与发展。思科大中华区资深副总裁、创新事业部总经理江慧瀛介绍说，思科万物互联智造云平台定位于工业互联网平台，其不仅提供工业的云应用，还可以提供 IoT（物联网，Internet of Things）互联、App 应用商店等能力，比工业云提供了更广泛的服务。

思科“制造云生态体系”

“智造云”以思科全球领先的全数字化网络架构（DNA）、云计算、企业协作、信息安全和工业互联网解决方案为核心，以思科以及全球合作伙伴智能制造解决方案为抓手，聚焦电子、汽车、智能装备等行业，为制造企业在设计、研发、供需双方精准对接，供应链管理、数字化制造、全渠道客户服务和节能减排等领域提供智能制造服务支持。基于思科的万物互联智造云，江慧瀛表示，“思科可以提供全球化一键式部署解决方案，支持跨平台的公有云服务、用户自建的私有云平台和思科的云平台的混合云部署模式，从而满足中国公司走向国际的需求。”

在思科创新研发总部及创新研发中心的强大技术支撑下，思科将在中国建立万物互联的“制造云生态体系”。配合思科转型业务全球发展，打造面向制造业全产业链的“云生态体系”，提供制造业业务转型所需的大数据、云计算、各种 App 的服务和应用。思科很多合作伙伴比如 TCL、浪潮等，它们都会参与到生态体系建设中来，为制造企业在上下游（设计、研发、供应链管理、全渠道销售、培训等）领域提供云技术服务支持。

据了解，思科的制造云生态体系，在广东吕顺智能科技有限公司就得到了很好的应用。在过去的市场推广中，该公司主要的产品是 AGV 小车和定制化的生产线，虽具备很强的机械化能力，但是极度缺乏信息化和智能化的能力。在经过多次走访和现场勘查之后，思科为

其量身制定了四步走的战略。第一步，完成该公司内部的信息化、办公设计的自动化。第二步，逐步完善装备的智能化和云端管理，具备实时了解系统状态的能力，实现初步的可预测运维。第三步，重点打造智能仓储解决方案，打通上下游合作伙伴，实时了解订单情况。第四步，使广东吕顺智能科技有限公司具备打造无人工厂的能力。经过半年的联合工作，该公司利用思科提供的解决方案完成了前三步，目前正在向第四步迈进。

思科为广东吕顺智能科技有限公司提供基于思科 UCS 的虚拟化共享设计平台，同步设计和提供更为强大的功能，可以实现云端共享授权码，使用正版软件和实现服务外包。便于该公司只需按照协同设计任务栏要求完成图纸设计就等同于正常上班的状态，解放设计者的空间和灵感，提高了设计者的自由，使其工作更有效率，便于自动考核绩效和成本。同时从设计内容的安全性考虑，思科将所有的设计文件存储在云端，在本地工程师的本地电脑中不存储设计文件，避免由于工程师跳槽引起的知识产权泄漏的风险。

结合思科联合合作伙伴提供的工单管理的云服务平台，自动分配设计任务，使广东吕顺智能科技有限公司软件投入成本是原来的十分之一，硬件投入成本是原来的三分之一，效率也提高了一倍，最重要的是也提高了员工工作的积极性。思科定制的云服务平台实现互联网工业升级，设计研发投入降低，也使该公司帮助客户有效降低投入成本，从而获得了客户的迅速认可。

思科安全解决方案保障万物互联

在万物互联时代，会有越来越多的智能化设备成为可以被攻破的入口。信息安全也显得尤为重要，因此，工业互联网平台信息安全更应得到重视，从而保障工业互联网平台健康发展。

随着制造商开始跨工厂实施万物互联功能，并将工厂资产连接到更高级别的应用，其更易受攻击者侵入系统。一次攻击可能导致企业损失数百万美元的故障停机、生产计划中断以及造价昂贵的机器设备损坏。在最严重的情况下，工人的健康或安全也可能受到威胁。甚至，会给制造企业带来错失创收和增加市场份额的机会。

思科针对万物互联下的攻击与威胁，其安全解决方案和服务旨在通过以威胁防护为中心

的集成安全架构，覆盖攻击前、中、后的整个过程，构建连接基础设施、机器流程和人员的整体安全模式，实现最佳的投资回报率和可衡量的业务成果，包括以下内容：

（1）资产可视化和监控。思科能使企业识别和监控其网络中的所有资产和用户，并为安全的远程访问奠定坚实的基础。

（2）识别和访问管理。这些解决方案为供应商和承包商访问、设备加入合理化和动态策略实施提供便利。

（3）工业 DMZ。思科的工业隔离区提供先进的外围网络缓冲区，在可信和不可信的网络之间执行数据安全策略。

（4）网络地址转换 （NAT）技术。这些 IP 解决方案精简了工厂范围内的机器设备网络，并提供额外的安全性，防止网络入侵。

（5）工业网络安全服务。思科能分析网络风险、评估安全漏洞并设计和实施可减轻风险的网络及物理安全控制，借此帮助制造商保护工业资产和防止网络中断。

（6）安全的运营托管服务。此项针对运营环境的模块化网络安全和合规解决方案可随企业需求的变化扩展，提供经济实惠的服务化交付选择。

（7）ICS 网络架构和设计服务。思科与制造商紧密合作，提供不仅能交付新一代安全性，而且能确保提升运营绩效和投资回报率的解决方案。

伴随思科万物互联制造云生态体系的建设，相信不久的将来，思科将会联合国内及全球合作伙伴加速转型和创新，建设高标准智慧产业体系，为社会创造更多的价值。