概览

优势

- 保护知识产权和有形资产免遭网络盗窃，借此**获得竞争优势**。
- **加快解决安全威胁的速度，减少停机时间，**从而推动所有工厂设施实现效率提升。
- 保护员工和您的信息，在内部和外部**树立良好的品牌声誉**。
- 凭借随时随地安全可靠地访问工厂资产的能力（包括对工厂非常重要的安全远程访问能力），**提高整体设备效率** (OEE)。
- 利用由思科服务及其业界领先的合作伙伴（如 Rockwell Automation）提供的验证设计和成熟方法，**有效建立稳固的工厂车间安全防线**。

思科互联工厂安全解决方案

万物互联的机遇和挑战

万物互联 (IoE) 的增长在提高整个价值链效率、节省成本的同时，也为制造商带来了价值 3.9 万亿美元[1]的商机。然而，连接数量的这种指数级增长以及人员、流程、数据和事物之间的紧密联系也带来了更高的安全风险。

制造业：一个遍布目标的环境

在制造商看来，数据安全是妨碍实现万物互联价值的最大障碍。而且，随着制造商开始采用新技术标准，并努力融合 IT 和运营技术系统与组织孤岛之间的传统边界，这种威胁也会不断加剧。

从统计数据可以看出，制造业所面临的安全形势极其危险：

- 2013 年，制造业是最容易受到攻击的行业；所有针对性攻击中，有 24% 是以制造业为对象 (Symantec[2])
- 在最容易遇到网络安全问题的系统排名中，工业网络位居首位 (McAfee)
- 2014 年，有超过 1000 个工业自动化和控制系统 (IACS) 成为 Dragonfly 间谍恶意软件程序的攻击目标[3]
- 从 2013 年到 2014 年，工业监控与数据收集 (SCADA) 系统所受到的攻击**增加了一倍**[4]
- “在未来几个月乃至几年内，老化的工业机械基础设施所带来的巨大安全挑战将持续增长。”[5]

从本质上讲，运营技术网络中的 IACS 非常容易受到攻击，因为这些系统会使用专有硬件和软件，而且传统工厂网络几乎没有（甚至完全没有）实施任何安全保护措施。实际上，随着制造商开始跨工厂实施 IoE 功能，并将工厂资产连接到更高级别的应用，这种易受攻击的情况也会加剧。

[1] 来源：思科咨询服务部，“IoE Value Index Survey”（万物互联价值指数调查），2013 年，*2013-2022
[2] 摘自联邦科技商业网在 2013 年 4 月发布的文章
[3] BBC，能源公司遭到“网络间谍团队 Dragonfly”入侵，2014 年 7 月 1 日，http://www.bbc.com/ news/technology-28106478
[4] 戴尔年度安全威胁报告，https://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708
[5] 戴尔年度安全威胁报告，https://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708

“当今世界充满了前所未见的网络威胁。如果能获得对这些威胁的可视性，我们的团队就能重拾信心，确信在我们的工业网络中添加入侵防御技术是合理的。”

Charles Harper
液化空气集团
全国供应和渠道运营总监

万物互联时代的安全性和业务灵活性

在万物互联时代，由不同的产品或技术拼凑而成的安全战略将不再有效。要想有效预防、检测并缓解公司知识产权、资本资产、声誉和隐私所面临的安全威胁，必须采用一种**着眼于整体**的方法来保护 IT 和运营技术数据的安全性。

您的企业正在努力转变，以求集成和部署融合式网络（IT 与运营技术相融合）、预测性维护工具、机器系统、工厂车间移动应用，以及基于云的服务。这些部署所产生的分析结果可以带来诸多优势。毫无疑问，您也希望充分利用这些优势。因此，在这些部署工作中采用一种**着眼于整体**的方法非常重要，该方法必须能推动实现由业务驱动的安全蓝图和安全战略，为整个制造价值链提供有效的防御。

行业领先的整体安全方法

为了帮助企业从整体视角应对万物互联部署所伴随的特定安全风险，我们精心设计了“思科互联工厂 - 安全解决方案”（参见侧栏）。该解决方案可以将各种制造流程转化到一个安全且紧密集成的统一通信系统之中，将基础设施、机器、流程和人员紧密联系在一起。借助该解决方案，企业可以获得以下优势：

- 安全地访问工厂车间的机器数据，将之汇总，然后应用数据分析算法确定最佳的运营和供应链工作流程，从而提高效率并降低成本
- 在员工、合作伙伴和供应商全球生态系统范围内安全地共享知识产权，扩大专家资源的覆盖面
- 利用终端安全评估功能为策略合规、操作系统更新和软件补丁部署提供支持，从而有效缓解风险
- 在远程位置安全地对机器进行故障排除，并解决与引入新产品相关的问题

工作原理

为了保护您的工厂，并且沿用以前发布的思科互联工厂自动化和互联工厂无线解决方案，互联工厂安全的最新版本包括以下融合访问安全产品、技术和服务。

安全身份服务

- 支持多种外部身份库，包括用于身份验证和授权的 Microsoft Active Directory
- 可使工厂管理员根据基于 Web 的 GUI 控制台上提供的身份验证和授权服务，配置并管理有线和无线用户访问
- 利用来自单一管理界面的集成管理服务简化管理工作

工业 DMZ

- 通过满足安全和业务需求的架构，建立着眼于整体的工业 DMZ 方法
- 为现代 IACS 应用中普遍使用的控制与信息准则、设备和装置提供标准的网络服务
- 包括各种防火墙、远程接入 VPN 服务、IACS 应用主机和网络基础设施设备，例如在经过验证的成熟架构中部署的交换机、路由器和虚拟化服务

执行下一步操作

思科拥有必要的基础设施专业知识和战略合作伙伴，可在不牺牲可靠性、安全性和网络响应时间的前提下保护企业 IT 和 OT 安全，推动更快作出决策，并为新业务模式提供支持。

如需了解有关“思科互联工厂 – 安全解决方案”的更多信息，或预约演示，请访问 www.cisco.com/go/factorysecurity，并联系您的思科代表。

网络地址转换 (NAT)

- 允许重复使用 IP 寻址（适用于规模生产型工厂车间机器和设备的寻址），可在简化集成的同时，避免在 IACS 应用架构中引入重复错误
- 由于可以配置为仅将一个单元或一个区域内的特定 IP 地址转换到工厂的更高层级，同时保持机器制造商通常会重复执行的 IP 寻址功能，因此有助于提高安全性
- 帮助用户利用规划和设计指南来部署支持 NAT 的网络，从而优化架构，以满足 IACS 应用的需求

互联工厂入门套件

- 允许您以最低限度的财务投资，小规模试用解决方案所包含的新技术和新功能
- 作为预打包且经过验证的成套设备和服务交付，可用于在工厂设施内建立实地实验室

C45-734463-00 05/15