



Cisco ISA 3000

工业安全设备

在工业环境中获得可视性并降低风险

制造、能源、运输及其他工业领域的企业正在利用物联网 (IoT) 技术来取得优良的业务成果：提升效率、更好的供应链可视性和增强的员工安全。但是，安全性仍然是首要考虑因素。

现在，我们正在使用 Cisco IoT 系统安全产品组合中的新产品 Cisco ISA 3000 工业安全设备来解决安全问题。

Cisco ISA 3000 安全设备：

- 利用强化设计实现恶劣环境中的运行，同时还会遵守 OT 最佳实践。
- 提供跨壁垒的可控性与可视性：传统 OT 环境中，特定于供应商的基础设施之间有壁垒，它们具有独立的管理系统。Cisco ISA 3000 提供跨 IT 和 OT 系统通用的安全流程和网络安全管理。这一结合使得公司可以使用其现有 IT 安全专业知识，同时还能满足 OT 特定需求。
- 简化合规性：不断增加的内部规定、行业和政府规范给运营商带来了压力。Cisco ISA 3000 有助于进行所需的一致策略实施和分段，从而简化合规性和缩小审核范围。
- 缓解风险：当客户打开其 OT 环境以利用 IoT 效率时，他们不能让其系统可用性受影响。Cisco ISA 3000 安全设备融合了应用感知、OT 协议理解以及高级工业控制系统 (ICS) 威胁检测。这种融合增强了跨 IT 和 OT 环境的可视性，支持一致的策略实施，并且降低了系统可用性风险。

主要特点

Cisco ISA 3000 工业安全设备和带有 FirePOWER 服务软件的 Cisco ASA 采用相同的安全机制。它还在 DIN 导轨或机架式外形中配有四个高性能以太网数据链路。而且 3000 提供针对恶劣环境的访问控制、威胁检测和应用可视性功能。

主要特点包括：

- 恢复力：可以容忍 -40° C 到 60° C 的温度，经受得住振动、碰撞、电涌和电气噪声
- 合规性：符合有关工业自动化、ITS 和变电站环境的多种行业规范

优势

- 打破工业环境中的壁垒，获得跨越不同系统的可控性与可视性。
- 降低风险，利用应用感知、操作技术 (OT) 协议理解和高级威胁检测实现。
- 提高并扩展安全性，通过跨 OT 和 IT 网络基础设施的一致策略实施实现。
- 简化合规性和缩小审核范围，通过高效的网络分段和完整的 OT 应用可视性实现。

- 耐用性：采用不包含活动件的无风扇对流冷却设计，使用寿命更长
- 易用性：允许跨网络的多设备管理
- 身份验证：提供特定于用户的访问和控制
- 威胁检测：跟踪 25000 多条规则以提供特定于 OT 的保护
- 可视性与可控性：监控 DMZ 基础设施、IoT 应用和协议
- 高性能：提供经由 VPN 的远程访问
- DMZ 基础设施：支持包含 DHCP、DNS、AAA 和 IP 路由服务的 DMZ 基础设施

对垂直行业的好处

Cisco ISA 3000 工业安全设备为供电设施和制造工业提供以下好处：

- 供电设施通过场域网 (FAN) 和变电站自动化方案获得增强的应用可视性。网络分段功能和策略实施缩小了 NERC-CIP ([北美电力稳定性委员会关键基础设施保护](#)) 的审核范围。而且通过在同一地方实施策略，简化了合规性。
- 制造商可以借助 Cisco ISA 3000 同时跟踪 OT 应用行为、异常流量模式和恶意攻击的能力，提高安全性并获得可视性。Cisco ISA 3000 可与 Cisco IoT 系统网络连接产品集成，协同控制 OT 制造单元与 IT 数据中心和 / 或云之间的交互。

后续计划

有关 Cisco ISA 3000 工业安全设备的更多信息，请访问 www.cisco.com/go/isa3000。