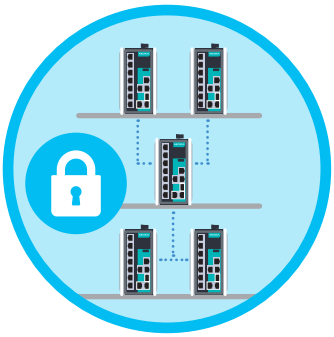
工业网络安全防护措施清单

Moxa 为您罗列了网络安全深度防御的诸项措施，谨作提醒。

安全设备

请问您部署安全的主要目的是：

- ☐ **识别和管控具有设备登录权限的账户**
- ☐ **符合的等保《信息系统安全等级保护》**
- ☐ **行业内对于网络安全的明确要求**
- ☐ **企业内部对于网络安全的重视**
- ☐ **提高密码的复杂程度，**加强访问控制
- ☐ **先验证设备权限，**再开放网络访问和跨设备通信功能
- ☐ **加密串口机密数据，**保证数据完整性
- ☐ **加密配置数据，**增强保密性
- ☐ **甄选设备供应商：**一能**快速响应**漏洞报告，二能**及时修复安全漏洞**



安全网络
基础设施

- ☐ **将大型网络分割**成若干小型子网，防止网络问题造成操作中断或全网瘫痪
- ☐ **滤除未经授权的数据包，阻止未经授权的访问，**加强访问控制
- ☐ **创建加密数据安全传输隧道，**保证数据完整性
- ☐ **部署工业防火墙、VLAN 或 ACL，**以最具可行性、**最具成本效益的方案**为工业控制系统提供安全防护

安全管理

- ☐ **制定正确的安全策略，**满足您的网络需求
- ☐ **确保所有网络设备**的配置达到**同一安全级别**
- ☐ **持续监测设备安全状态，**维护全网安全
- ☐ **定期监控网络，检查**是否存在新增设备
- ☐ **储存所有事件日志，**为查找安全漏洞提供参考
- ☐ **比较网络配置**在安全事件前后的差异，查找故障根本原因

如需更多关于 Moxa 工业网络安全解决方案的信息，请下载

《加强工业网络安全的案例分析》

了解更多

MOXA®
Reliable Networks ▲ Sincere Service

www.moxa.com.cn/security

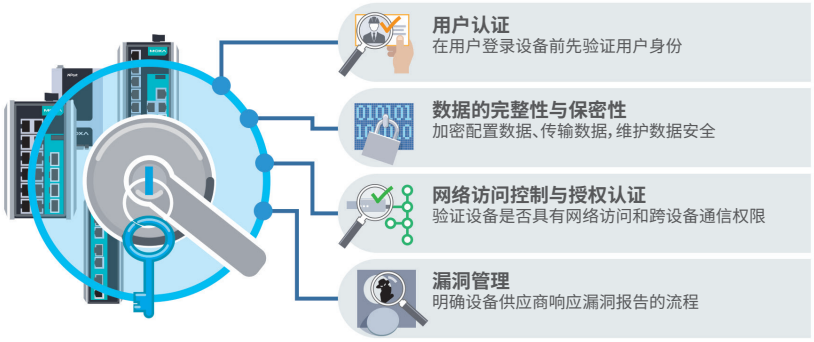
工业网络安全深度防御方案

Moxa 立足深度防御机制，推出工业网络安全解决方案，为您的工业网络安全保驾护航。

安全设备

为了降低工业控制网络面临的风险，您需要功能更强大的安全设备。

抵御侵入和攻击



用户认证
在用户登录设备前先验证用户身份

数据的完整性与保密性
加密配置数据、传输数据，维护数据安全

网络访问控制与授权认证
验证设备是否具有网络访问和跨设备通信权限

漏洞管理
明确设备供应商响应漏洞报告的流程

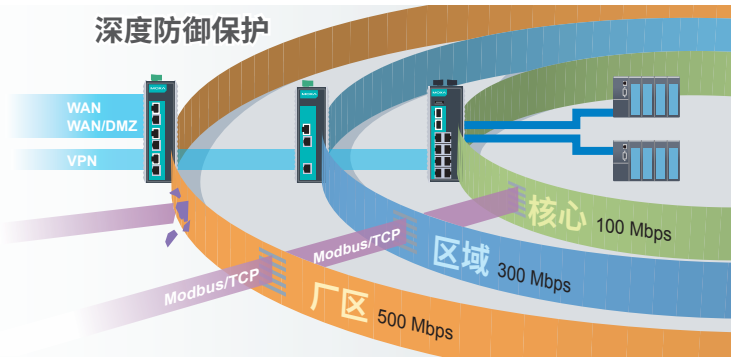
EDS-510E 系列
工业网管型以太网交换机

NPort 6000 系列
安全型终端服务器

安全网络基础设施

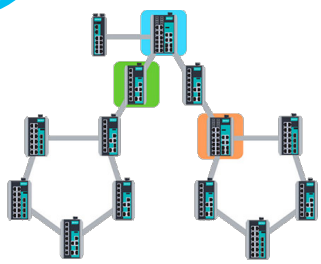
要实现高度可靠的持续运行，您需要安全性能更出色的工业级网络设备和工业防火墙。

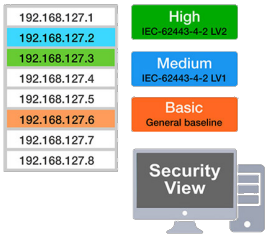
EDR-810/G902/G903 系列
工业级安全路由器



安全管理

要直观查看网络安全状态，您需配备网络管理软件。





MXview
工业网络管理软件

如需更多关于 Moxa 工业网络安全解决方案的信息，请下载

《加强工业网络安全的案例分析》

了解更多

MOXA
Reliable Networks ▲ Sincere Service

www.moxa.com.cn/security