Industrial Security in The Connected Enterprise

Building secure infrastructures
Minimise risks in
The Connected Enterprise

Protect against internal and external threats
Cybercriminals targeting companies or internal threats from suppliers, contractors or employees are a major concern in today’s manufacturing environment.

- Tamper Detection
  Detect & record unwanted activity & modifications to the application

- Secure Network Infrastructure
  Control access to the network, and detect unwanted access and activity

- Content Protection
  Protect viewing, editing, and use of specific pieces of control system content

- Access Control & Policy Management
  Control who, what, where and when access is allowed, to which application and device

How Rockwell Automation can help
Rockwell Automation can help you manage industrial security with a comprehensive portfolio of product solutions, partners and implementation guidance. In addition, a range of security services are available to assess, implement and help manage your network infrastructure.

Securing your network and your business
The Connected Enterprise enables manufacturers and suppliers to share data in a smart and secure way. Ensuring the right access to the right level of data for the right people is critical and requires a secure network.

- For Machinery / Equipment Suppliers
  - Enable Intellectual Property security to protect your assets
  - Secure access to your machines, allowing you to support your customers remotely

- For Plant Operations
  We can help you assess, design, implement and audit a comprehensive program and architecture, against security standards.

- For Enterprises
  We have robust solutions to maintain your network security while optimizing your productivity.

Security challenges to consider
- Effective and efficient risk management
- Management of assets
- Maintaining system availability
- Protection integrity of operations and the safety of personnel
- Internal and external threats
- Control of critical data and intellectual property
Industrial Security Infrastructure

ENABLING THE CONNECTED ENTERPRISE

1. Assess and Inventory the System
   - Inventory all devices using FactoryTalk AssetCentre
   - Establish and maintain a device inventory

2. Segment your Zone from your Industrial Zone
   - Leverage customized, pre-built solutions and recommended security solutions
   - Implement validated network designs from Rockwell Automation or Cisco
   - Establish a perimeter using an Industrial Demilitarized Zone

3. Segment your Network from the Enterprise
   - Control access to sensitive zones with VLANs
   - Implement port blocks, cable locks, and locking mechanisms
   - Ensure valid firmware with digital signatures
   - Prevent unwanted applications from running on computers by using partner solutions like Microsoft Patch Qualification efforts

4. Build Access Control into the Network
   - Segment your network using firewall technology
   - Control access to sensitive zones with VLANs
   - Implement port blocks, cable locks, and locking mechanisms
   - Ensure valid firmware with digital signatures
   - Prevent unwanted applications from running on computers by using partner solutions like Microsoft Patch Qualification efforts

5. Physical Security
   - Implement physical security measures such as access control

6. Device Hardening
   - Implement port blocks, cable locks, and locking mechanisms
   - Prevent unwanted applications from running on computers by using partner solutions like Microsoft Patch Qualification efforts

7. Change Detection and Threat Detection
   - Implement change detection mechanisms
   - Monitor user activities with FactoryTalk Audit
   - Identify and help mitigate network based threats
   - Prevent configuration changes by putting policies in place

8. Device Hardening
   - Implement port blocks, cable locks, and locking mechanisms
   - Prevent unwanted applications from running on computers by using partner solutions like Microsoft Patch Qualification efforts

9. Incident Recovery
   - Manage systems by key configuration

10. Monitor and Audit
    - Monitor network traffic for anomalies
    - Monitor user activities with FactoryTalk Audit
    - Establish a perimeter using an Industrial Demilitarized Zone

11. Automate and Schedule
    - Automate and schedule the backup process for directories on PCs
    - Automate and schedule the backup process for directories on PCs

12. Control Network Access
    - Control network access with 802.1x, Identity Management, and Access Control Lists (ACLs)
    - Implement validated network designs from Rockwell Automation or Cisco
    - Establish a perimeter using an Industrial Demilitarized Zone

13. Control User Permissions
    - Control user permissions with FactoryTalk Application Servers
    - Control user permissions with FactoryTalk Application Servers

14. Implement Port Blocking
    - Implement port blocking with Firewalls
    - Implement port blocking with Firewalls

15. Segment Traffic Based on Policy
    - Segment traffic based on policy with Access Control Lists (ACLs)
    - Implement validated network designs from Rockwell Automation or Cisco
    - Establish a perimeter using an Industrial Demilitarized Zone

16. Protect Code from Change
    - Protect code from change with High Integrity AOI
    - Protect code from change with High Integrity AOI

17. Prevent Tampering with Message Packets
    - Prevent tampering with message packets by using partner solutions like Cisco Security DLP
    - Prevent tampering with message packets by using partner solutions like Cisco Security DLP

18. Minimize Denial of Service (DoS) Impacts
    - Minimize Denial of Service (DoS) Impacts with Quality of Service (QoS)
    - Minimize Denial of Service (DoS) Impacts with Quality of Service (QoS)

19. Extend Security Controls
    - Extend security controls with managed switches, routers, and firewalls
    - Extend security controls with managed switches, routers, and firewalls

20. Leverage Deep Packet Inspection
    - Leverage Deep Packet Inspection to implement application whitelisting on computers
    - Leverage Deep Packet Inspection to implement application whitelisting on computers

21. Integrate Management of User Accounts
    - Integrate management of user accounts with Active Directory
    - Integrate management of user accounts with Active Directory

22. Block Unwanted Traffic
    - Block unwanted traffic in the network
    - Block unwanted traffic in the network

23. Control Network Access
    - Control network access with 802.1x, Identity Management, and Access Control Lists (ACLs)
    - Control network access with 802.1x, Identity Management, and Access Control Lists (ACLs)

24. Automate Asset Inventory
    - Automate asset inventory with Firewalls
    - Automate asset inventory with Firewalls

25. Access Control
    - Build Access Control into the Network
    - Build Access Control into the Network

26. Site Operations
    - Site Operations
    - Site Operations

27. Remote Access and Connectivity
    - Remote Access and Connectivity
    - Remote Access and Connectivity

28. Physical Security
    - Physical Security
    - Physical Security

29. Change Detection and Threat Detection
    - Change Detection and Threat Detection
    - Change Detection and Threat Detection

30. Device Hardening
    - Device Hardening
    - Device Hardening

31. Incident Recovery
    - Incident Recovery
    - Incident Recovery

32. System Operations
    - System Operations
    - System Operations

33. Remote Access and Connectivity
    - Remote Access and Connectivity
    - Remote Access and Connectivity

34. Change Detection and Threat Detection
    - Change Detection and Threat Detection
    - Change Detection and Threat Detection

35. Device Hardening
    - Device Hardening
    - Device Hardening
Rockwell Automation, Inc. (NYSE:ROK), the world’s largest company dedicated to industrial automation, makes its customers more productive and the world more sustainable. Throughout the world, our flagship Allen-Bradley® and Rockwell Software® product brands are recognized for innovation and excellence.

Follow ROKAutomation on Facebook & Twitter. Connect with us on LinkedIn.

For more information about our industrial security solutions, please visit:
www.rockwellautomation.com/global/products-technologies/security-technology