LISTEN.
THINK.
SOLVE.®

Protecting the Connected Enterprise

Industrial security for machine and equipment builders

Rockwell Automation

Allen-Bradley • Rockwell Software

$400 billion:
the annual cost of cybercrime to the global economy

The opportunities are out there, and so are the risks.

Enterprise connectivity represents a massive opportunity for progressive machine builders and their customers. By connecting control systems and making information available and actionable, you give your customers the scope to make unprecedented operational improvements.

But the risks associated with having a complex, interconnected system – from cybercriminals and competitors – are growing. Almost one in two companies has experienced illicit copying of entire machines.

Fundamental to today's production environment is the ability to provide secure, remote access for end customers, protecting their critical production data from internal and external threats, while keeping intellectual property equally secure.

1 in 5 manufacturers have suffered security breaches leading to intellectual property loss

1 INTELLECTUAL PROPERTY: *protect yourself and your customers*

Reliable and secure network infrastructures keep operations running, support critical information-sharing priorities within the enterprise, and protect the intellectual property of machine builders and customers alike.

Effectively developing a complete Connected Enterprise requires a comprehensive approach to industrial security that extends beyond the control system to include policies and procedures that address people, process and technology-related risks.

Security Scenario

Are you looking to expand your market globally? When considering an expansion to new regions, you need to think about intellectual property including the custom AOIs on your machines: critical information that, if released or hacked, can cause major competitive issues.

Solutions…

- **GOOD** – Prevent access via the network to your machine assets by unauthorized assets and users, through Firewall and Access Control Lists policies.
- **BETTER** – 'Good' solution + deploy FactoryTalk® Security
- **BEST** – 'Better' solution + license-based source protection functionality enabled through Studio 5000 Logix Designer™

Learn more about FactoryTalk Security
literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm016_-en-p.pdf

71% of companies are affected by intellectual product or brand piracy

2 UNAUTHORIZED ACCESS AND CHANGES: *monitor your machines*

The Connected Enterprise relies on a layered, defense-in-depth approach to security, and policies that control human interaction with end user systems.

To protect yourself and your customers from breaches, externally and internally, you need to build appropriate security measures into your machines: securing network infrastructures, collecting, assessing and reporting critical data, and ensuring compliance with appropriate standards.

Authorized access can also create safety risks and needs to be monitored to alleviate dangerous machine movement or injury.

Security Scenario

Do you need to better manage warranty costs? How can you better monitor customer access during the warranty period and validate a warranty claim based on access history and change history?

To understand if there is a case for a warranty claim, or if your customer has been making changes to the machine, you need to be able to continuously monitor networks for configuration changes, traffic overload and unauthorized access.

Solutions…

- **>** **GOOD** – Maintain consistency and revision control with High Integrity Add-on Instructions
- **>>** **BETTER** – 'Good' solution + Logix Change Detection Audit Value Feature
- **>>>** **BEST** – 'Better' solution + Logix Controller Logging feature

Learn more about Change Detection features
literature.rockwellautomation.com/idc/groups/literature/documents/pm/1756-pm015_-en-p.pdf

Over **25%** of companies suffer illicit warranty claims on fake products

3 REMOTE ACCESS: *reducing costs and solving problems faster*

With the correct security procedures and architectural systems in place, remote monitoring through open standard networks gives you an unprecedented ability to remotely oversee operations, perform real-time diagnostics, troubleshoot the control system and keep your customers' maintenance costs low.

Security Scenario

Historically, remote support might have incorporated individual connections outbound to public space or even cellular modems. Today's technologies improve access and problem-fixing ability, and give you another potentially valuable revenue stream.

Every connection represents a risk for end users, giving a direct path into their facility and your machines. As customers look for ways to centralize and better control access to their facilities, you need to provide optimal support while giving customers the peace-of-mind that their systems are secure.

Solutions…

> **GOOD** – Virtual Support Engineer Standard version, including a feature-rich hardware platform that supports secure remote access and alarming on tag-based devices

>> **BETTER** – Virtual Support Engineer Enhanced version, including a remote access solution that allows for alarming on any Ethernet-based device while providing multiple security levels and integration to customer firewall

>>> **BEST** – Virtual Support Engineer Enhanced version, leveraging customer Industrial Demilitarized Zone and Terminal Services

How to create scalable, secure remote access in your environment
www.RockwellAutomation.com/go/oem/br002a-en

ACTIONABLE STEPS YOU AND YOUR CUSTOMERS CAN TAKE NOW

1. Control who has access to various areas of the network, using features such as Access Control Lists and port blocking features.
2. Ensure robust and reliable operations, by limiting and managing network traffic through the use of firewalls and intrusion detection and prevention systems.
3. Develop security policies to manage the 'human factor'. For example, managing and protecting passwords, and managing removable media and use of personal devices.
4. Implement a level of physical control by putting the key-switch on controllers in Run Mode, and removing the key.
5. Limit access to automation equipment by implementing physical controls such as locking cabinets and doors.

Discover how Rockwell Automation can help you to build more secure machines and reduce risk
literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp031_-en-e.pdf