Symantec

CASE STUDY

Organization

Customer: Rockwell Automation

Site: www.rockwellautomation.com

Industry: Manufacturing

Headquarters: Milwaukee, WI

Employees: 22,000

Challenge

Rockwell Automation provides industrial automation products around the world to various Industrial Operational Technology companies. As part of increased threats in Industrial IOT areas, customers who use Rockwell are subject to risk that can be devastating to operations. Rockwell needed an ability to augment customer's existing systems, old and new, against sophisticated threats.

Solution

Symantec Internet of Things

- Critical System Protection (CSP)
- Industrial Control System Protection (ICSP)

Benefits

- Timeless system hardening using Critical System Protection against zero-day vulnerabilities, unknown malware, and advanced adversaries
- Zero impact to operational efficiencies and no dependence on cloud connection or content/signature updates
- Ability to scan and clean USB drives before use in Rockwell systems
- Complete cyberphysical security posture uplift

Rockwell Automation

Symantec Secures Rockwell Automation Industrial Control and Business Intelligence Solutions

Solutions Help Protect Against Attacks to Your Industrial Control System

Overview

Until recently, cyber attacks against industrial control systems (ICS) have not been very visible, and purportedly less frequent than IT attacks (though many ICS attacks don't get reported). However, industrial control systems have recently become a major focus for attacks and are now among the top targeted sectors worldwide.

These attacks are most often made against the weakest points of the systems. Malware infection and other types of attacks of ICS resources can have serious implications including intel gathering, invalid data displayed to operations, and invalid programming sent to controllers. With increasing connectivity between control systems and enterprise networks, the risks of cyber attack on ICS endpoints are increasing. Following best practices for network design can help mitigate some of the risk, but a misconfigured firewall, or improper usage of removable media can lead to compromised assets. For example, attacks against Human Machine Interfaces (HMI) have included modules that search out any network connected file shares and removable media for additional lateral movement within the affected environment.

Challenges

Securing industrial environments against these types of attacks is a tremendous challenge. Control and information systems are constantly changing and evolving. Each end user must be able to secure multiple networks, including their enterprise IT systems, SCADA networks, and ICS. Each of these systems has its own technical challenges, and in many cases regulatory controls require compliance. Add to that the critical job of ensuring the “lights remain on” one-hundred percent of the time, and it’s easy to see how difficult this task can be. With the aging of assets typically deployed in an industrial environment, enhancing or upgrading these systems with security solutions is sometimes difficult. Off the shelf solutions aren’t able to see what is happening within an industrial infrastructure, and do not understand the unique vocabulary of that environment. Therefore, the question of how to protect an ICS must be asked.

Security Solutions

To help address the risk to computer-based endpoints in automation systems, Rockwell Automation is partnering with Symantec Corporation to provide endpoint level security. Symantec’s Critical System Protection (CSP) solution has been tested by Rockwell Automation for protecting its ICS host endpoints.

Symantec’s CSP solution provides policy-based behavior control and detection for hosts/devices. This approach is attractive in ICS because Operating System (OS) patching isn’t always possible, AV signatures don’t get updated regularly, and other procedural processes can’t always be executed in a timely and effective manner. Symantec CSP controls application behavior, blocks identified incoming and outgoing traffic, and generally provides host-based intrusion prevention and detection. Symantec CSP agents control application behavior by allowing and preventing specific actions that an application or user might take. For example, a prevention policy can specify that a certain application may not spawn other processes, including dangerous processes like viruses, worms, and Trojan horses. The application can still read and write to the files and directories that it needs to access.

Symantec CSP is ideally suited to protect Rockwell Automation’s ICS host endpoints - not only because of the security features described below, but also because the signatureless, policy-based approach does not require any corporate or Internet connectivity. It does not need any updates and can run in an unmanaged mode (without the need for a management console) as required. This enables the operator to install the CSP agent on a host endpoint, and once turned on will not require any further integration to a management interface (unless so desired).

The key features of CSP include:

- Signatureless, policy-based security
- Application Whitelisting – Policy with a default deny strategy that prevents execution of all the applications that are not explicitly whitelisted or sandboxed
- Application Sandboxing – Granular application control by restricting applications' access to system resources while continuously protecting critical OS resources
- Machine Learning – Learning from the end user usage of an application to help define the application sandbox
- Protection against zero day attacks by preventing malware from executing
- Limit the system access through least privilege access control
- Host firewall to define network perimeter for the device to control inbound and outbound network access both at the application as well as the device level
- File, System and Admin Lockdown - Harden Rockwell's DCS and HMI systems to maximize uptime and minimize operational expense
- File Integrity Monitoring - Identify changes to files in real-time, including who made the change and what changed within the file
- Configuration Monitoring - Identify policy violations, suspicious administrators or intruder activity in real-time

Symantec CSP allows security policies to be applied from install time or remotely post-installation. You can remotely update agent software, and CSP can run in a standalone mode or can be connected to a management server.

Qualified Platforms and Configuration

Interoperability between Symantec CSP and Rockwell Automation host endpoint software is important to ensure ease of installation and operation by end users, machine and equipment builders, and system integrators. Rockwell Automation and Symantec collaborated to test interoperability with Symantec's CSP solution and the following Rockwell Automation products:

- FactoryTalk Service Platform
- FactoryTalk Activation Server
- FactoryTalk View Studio
- FactoryTalk View SE HMI Server
- FactoryTalk View SE Client
- RSLogix 5000
- Studio 5000
- RSLinx Enterprise
- RSLinx Classic

There were some important learnings when the interoperability testing was performed. To successfully install and configure the Symantec CSP solution to work with the above Rockwell Automation solutions, the implementer needs to consider the following:

- Interoperability qualification is specific to the software products that were tested
- The recommendations for interoperability are more qualitative than prescriptive; the implementer must ensure the integration meets the requirements of the application
- Configuration of the test bed required extensive network configuration that is not directly related to qualification of the software products, but should be considered when determining the requirements for a complete system

Good practices when integrating the Symantec and Rockwell Automation solutions for interoperability include:

- Proper installation and setup of both Symantec and Rockwell Automation Software products
- Assure all Rockwell Automation Software is operating properly and fully functional prior to enabling Symantec CSP
- Configure your Symantec CSP Policy and ensure all Rockwell Automation Software is still functional
- Monitor all Symantec and Windows Event Logs to assure all products are working as desired
- Edit the CSP Policy as needed based on the Log file findings
- Maintain proper CSP Policy Backup's along the way

A Rockwell Automation Knowledgebase article will be prepared in the future to help users configure Symantec CSP with Rockwell Automation products.

Summary

Symantec CSP helps address the need for endpoint security on Rockwell Automation's host endpoint solutions. Symantec CSP can provide an effective defense against unknown and unwanted attacks and is useful in allowing you to help protect your industrial environment.

Before implementing Symantec CSP in your production environment, you should verify your configuration on a non-production system, or when the facility is non-active, to ensure that there are no unexpected results or side effects. This will ensure an effective security implementation.

For more information

Symantec and Rockwell Automation will continue to qualify host endpoint protection technologies to help you achieve ICS solutions that meet your security needs.

For further information on how to obtain Symantec's CSP solution, please contact iot_security@symantec.com or call +1 (800) 745 6054 from within the United States.

For further information on how to obtain the recommended Rockwell Automation solutions, please contact encompass@ra.rockwell.com.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com