CASE STUDY

Organization

Customer: Emerson

Site: www.emerson.com

Industry: Manufacturing

Headquarters: Ferguson, Missouri

Employees: 103,500

Challenge

The Emerson DeltaV™ Workstation is a modern and flexible industrial automation system that eliminates operational complexities to minimize project risk across various Industrial Operational Technology companies globally. As part of increased threats in Industrial IOT areas, customers who use Emerson DeltaV™ are subject to risk that can be devastating to operations. Emerson needed an ability to augment customer's existing systems, old and new, against sophisticated cyber-attacks.

Solution

Symantec Internet of Things

- Industrial Control System Protection (ICSP)

Benefits

- Leverages the best Symantec technologies against any USB-borne malware to ensure full protection of your IOT systems
- Ability to scan and clean USB drives before use in Emerson DeltaV™ systems and other IOT systems
- Supports a wide range of industrial segments and Windows platforms
- Enforces security policies for removable USB device usage

Symantec Secures Emerson customers using DeltaV™ Systems

Solutions Help Protect Against Attacks to Your Industrial Control System

Overview

Until recently the industrial control systems (ICS) market has paid little attention to securing its technologies. With recent cyber-attacks like WannaCry and Petya, Industrial OT (Operational Technology) elements have become highly vulnerable. As a result, ICSs are now a major focus for cyber-attacks. These attacks are most often made against the weakest points of the system and are initated from within the industrial environment. A major component that contributes to many of these ICS attacks are from removable media, often via UBSs.

Malware infection and other types of attacks of ICS resources can have serious implications including:

- Intel gathering
- Invalid data displayed to operations
- Invalid programming sent to controllers

With increasing connectivity between control systems and enterprise networks, the risks of cyber-attacks on ICSs can cripple operations and cost millions per day. Symantec's Industrial Control System Protection (ICSP) addresses the need for secure removable media used on ICSs and is a solution tested the Emerson DeltaV™ Workstation.

Challenges

In the wake of recent cyber-attacks like WannaCry, many cyber adversaries continue to target state owned critical infrastructure such as nuclear plants, power supplies, and other utilities. Securing those industrial environments against sophisticated cyber-attacks is part of the tremendous challenge for many organizations with operational technology. Add the priority levels established between OT and IT environments, and it's easy to see how difficult this task can be.

As part of this increased threat to Industrial OT environments, organizations that use ICSs, such as the Emerson DeltaV™ Workstation, are subject to risks that can be devastating to operations. Emerson needed an ability to augment customer's existing systems, old and new, against sophisticated cyber-attacks for secure removable media use.

Solution Overview

Symantec Industrial Control System Protection (ICSP) is a USB Scanner Station that acts much like a hand sanitizing station for USB drives. By leveraging the best Symantec technologies, ICSP can ensure that your critical environments are protected from USB-borne malware and attacks traversing the air-gap. Symantec ICSP is an available secure solution that requires zero configuration on a target system with only a driver installation, and a wide range of industrial segments and Windows platforms.

To help address the potential risks associated with USB-borne malware and attacks on OT systems, Emerson is partnering with Symantec Corporation to provide the world's best anti-malware USB scanning station. Symantec ICSP is a solution tested on the Emerson DeltaV™ Workstation for users who require use of removable media without completely exposing the endpoints to malware within the DeltaV Area Control Network (ACN).

Symantec ICSP also includes an enforcement driver that validates a USB was previously scanned and deemed clean. This validation is configurable with a time expiry and compatible with older operating systems (the driver is an optional add-on but recommended for assurance).

Once deployed, Symantec ICSP protects each DeltaV™ Workstation by allowing removable media to be accessed if previously verified by the ICSP Scanner Station.

The following use case can be considered to further explain how the protection is implemented as part of the ICSP deployment:

- The removable media is first checked by the USB Scanner Station and deemed clean
- The removable media can then be fully accessed by the DeltaV™ Workstation once it is connected to the workstation's USB port, including all files, folder and subfolders

- Files can be freely changed and accessed by the DeltaV™ Workstation where the removable media is still connected to
- Changed content will not be accessible by other DeltaV™ Workstations running the ICSP driver without re-scanning at the ISCP Scanner Station

Three key components of Symantec ICSP are:

1. USB Scanner Station is a physical appliance used to scan the removable media prior use of the workstations running the ICSP Enforcement Driver.
2. The ICSP Enforcement Driver is a software application that validates if the removable media was pre-scanned (and deemed clean) by the USB Scanner Station.
3. Symantec Malware Cleaner is used as a resource to clean malware found on removable media scanned by the USB Scanner Station (optional).

Symantec ICSP Features Overview

The key features of ICSP include:

- Whether the target ICS is 20 years old or modern-day machinery, Symantec ICSP grants a high degree of protection
- Integration with Symantec Critical Protection (CSP): Symantec ICSP can work in tandem with CSP, which protects against sophisticated unknown threats and network-borne attacks. CSP has a significantly small footprint and requires no content and signature updates
- Advanced Machine Learning: Using malware samples from hundreds of millions of endpoints around the world, the ICSP engine uses a trained, multi-dimensional behavioral model to identify large classes of malware. With a highly trained efficacy model by over 7 million data points, the ICSP engine is continuously learning with signature-less detection
- File Reputation: An analysis that determines the safety of files using techniques powered by Symantec's Global Intelligence Network. The safety score delivers another feed into the ICSP engine when rapidly processing files
- Emulation: For scripts, compressed files (zip) and other executables, the light sandbox detects polymorphic malware hidden by custom packers. The techniques used to hide from traditional signature-based only technologies can be uncovered immediately
- Signature: Symantec ICSP scans and eradicates malware that arrives via USB
- Two Ethernet NICs
- Broad compatibility: Supports various forms of USB drives
- Complete protection with multiple anti-malware technologies beyond signature

- ICSP satisfies diverse OT requirements, such as remote drilling sites or a container ship
- The update process can be done offline or online

Summary

The goal of the Symantec ICSP Scanner Station is absolute protection of your Industrial OT systems against USB-borne malware and attacks. Symantec ICSP helps address the need for secure removable media used on Emerson's DeltaV™ Workstations.

As a feature-packed station leveraging the most advanced Symantec threat technologies available, the ICSP engine is hardened against modern day threat actors and advanced adversaries.

For more information

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

To learn more about Symantec technology partners, please visit www.symantec.com/partners.

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