SOLUTION BRIEF

Symantec Industrial Control System Protection USB Scanning Station

Solutions help protect against attacks to industrial control systems.

Symantec™

Overview

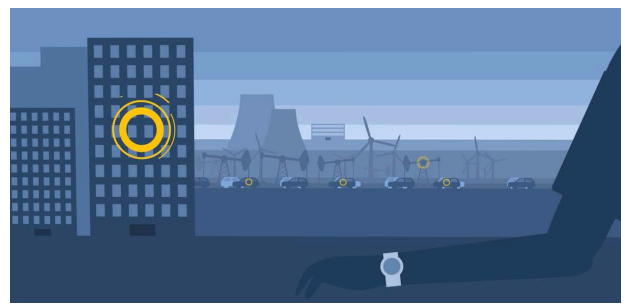
Today's industrial environments have become highly vulnerable to cyber-attacks as a result of USB-borne malware traversing the air-gap, and a dependence on outdated industrial technologies that have little to no security.

With recent cyber-attacks like Stuxnet, Industroyer and Triton, Industrial OT (Operational Technology) elements are now a major focus for cyber-attacks. Often these attacks are initiated from within the OT environment via removable media, such as USB devices.

A high degree of protection can be achieved by leveraging security for a transiting USB device between the OT and IT networks. These industrial environments include (but not limited to): manufacturing, pharmaceutical, oil & gas, shipping, drilling, and more against new and known threats inside this threat landscape. With cyber physical systems in a wide variety of facilities — increasing numbers of malware are traversing the air- gap into a critical environment.

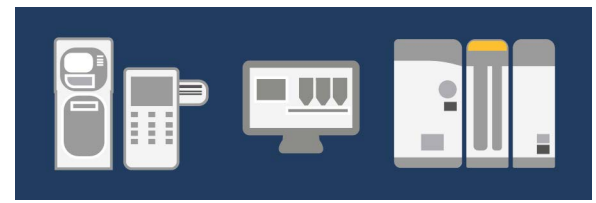
Malware infection and other types of attacks of Industrial Control System (ICS) resources can have serious implications including:

- Intel gathering
- Invalid data displaying to operations
- Invalid programming sent to controllers
- Downtime to production



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 assist in protecting your critical environments from USB-borne malware and attacks traversing the air-gap. ICSP is a solution that requires zero configuration on a target system with only a driver installation, and supports a wide range of industrial segments and Windows platforms.

ICSP addresses the need for secure removable media used on ICSs and is a solution tested on the Emerson DeltaV™, Rockwell, Honeywell Experion and more.



Operational Technology

Protect against the weaponized malware afflicting operational technology with complete protection through an award-winning security strategy.

Healthcare

Protect against USB-borne malware attacks to critical medical environments.

Explore more
www.symantec.com/internet-of-things

Attack Anatomy

1. **Compromise Internal System**
    a. Email intrusion, Watering hole, Trojanized software, Non-PE attacks
    a. USBs and other external storage media devices
2. **Pivot to OT**
    a. L2/L3 controllers can be accessed via USB or the network
    b. Not a time-bound activity
3. **Access to PLC**
    a. No authentication required to reconfigure logic
    b. Uses the protocol against itself
    c. f(X,Y)=z
4. **Profit**
    a. Now under your command
    b. Components can be entirely disabled or altered
    c. Alerts can be suppressed

Industry Challenges

In the wake of recent cyber-attacks like Stuxnet or Industroyer, 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. Combine the priority levels established between OT and IT environments and it becomes clear how difficult it is to secure these environments at design time.

Organizations that do not secure its ICSs are subject to risks that can be devastating to operations. Companies need an ability to augment customer's existing systems, old and new, against sophisticated cyber-attacks for secure removable media use.

Attacks in the cyber-physical world

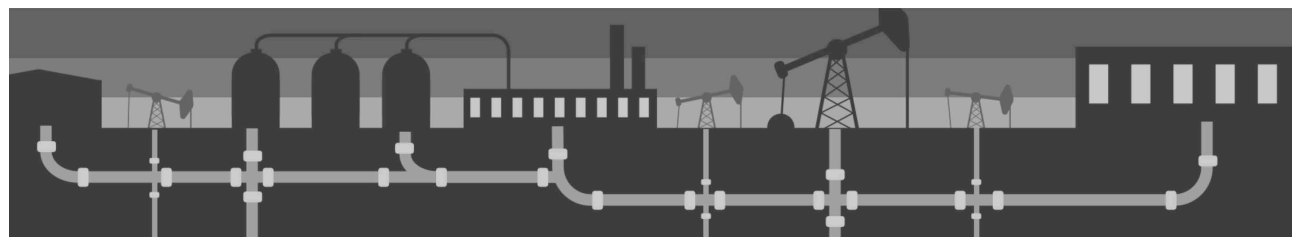
With increasing connectivity between industrial control systems and enterprise networks, the risks of cyber-attacks on OT can cripple operations and cost millions per day.

Recent attacks include:

- **Stuxnet**, a highly sophisticated piece of malware whose worm components exploit and target ICSs
- Executed not one but **four zero-day exploits** upon discovery
- Successfully attacked Iran's nuclear program
- Spreads stealthily through systems running Windows – including systems not connected to the Internet
- First U.S. vertical to be infected was Oil & Gas (Chevron)

ПРИКАРПАТТЯ ОБЛЕНЕРГО

- Ukraine powergrid was successfully attacked for the past two years, latest with **Industroyer**
- **230,000** customers lost power.
- 8 provinces without power.



Three key components of Symantec ICSP

1. A physical appliance scans removable media (USBs) for infectious malware.

2. Enforcement Driver validates removeable media was scanned and cleaned by ICSP.

3. Symantec Malware Cleaner is used to clean a target system in case of prior infection.

Symantec Industrial Control System Protection Scanner Station

The goal of the **Symantec ICSP Scanner Station** is absolute protection for Industrial OT systems against USB-borne malware and attacks. The ICSP Scanner Station helps address the need for secure removable media and has been tested on ICSs from the following organizations:

- **Emerson**
- **Yokogawa**
- **Honeywell Experion**
- **Rockwell**
- **Siemens**
- **GE**
- **Schneider/ Invernsys**
- **ABB**

Whether the target ICS is 20 years old or modern-day machinery, Symantec ICSP grants a high degree of protection.

ICSP features

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

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 trillion 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.

Enforcement Driver

Interoperable with various automation vendors', HMIs and workstations, ICSP includes a lightweight enforcement driver to validate that a USB was scanned by the ICSP Scanner Station. This functionality requires no connection between the target system and the station and can preserave the disconnected, or air-gapped, state of the OT network.

Signature

ICSP scans and eradicates known malware that arrives vis USB.

Integration with Critical System Protection (CSP)

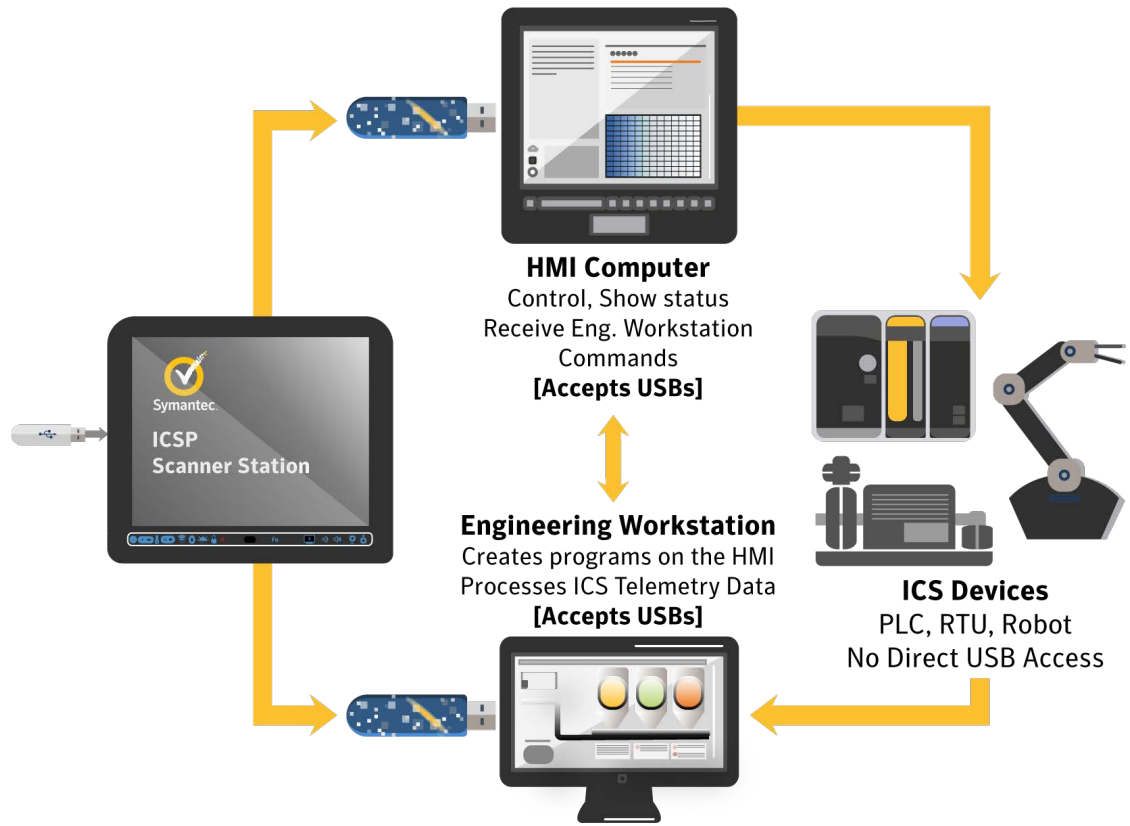
Symantec ICSP can work in tandem with CSP, which protects against sophisticated unknown threats and network-borne exploits. CSP is compact, behavioral security engine that provides comprehensive and in-depth security for your IoT devices.

Additional features

1. **Portable ICS Endpoint AV scanner** – ability to scan OT assets via up-to-date AV engine ported on USB devices
2. **Targeted Folder scans** for targeted Scan and Expose of USB devices on ICS Systems
3. Scan supports across major **Archive formats**
4. **Encrypted Drive Support***
5. Update process can be **offline** or **online**

*Kingston DataTraveler Vault Privacy v3 and v3

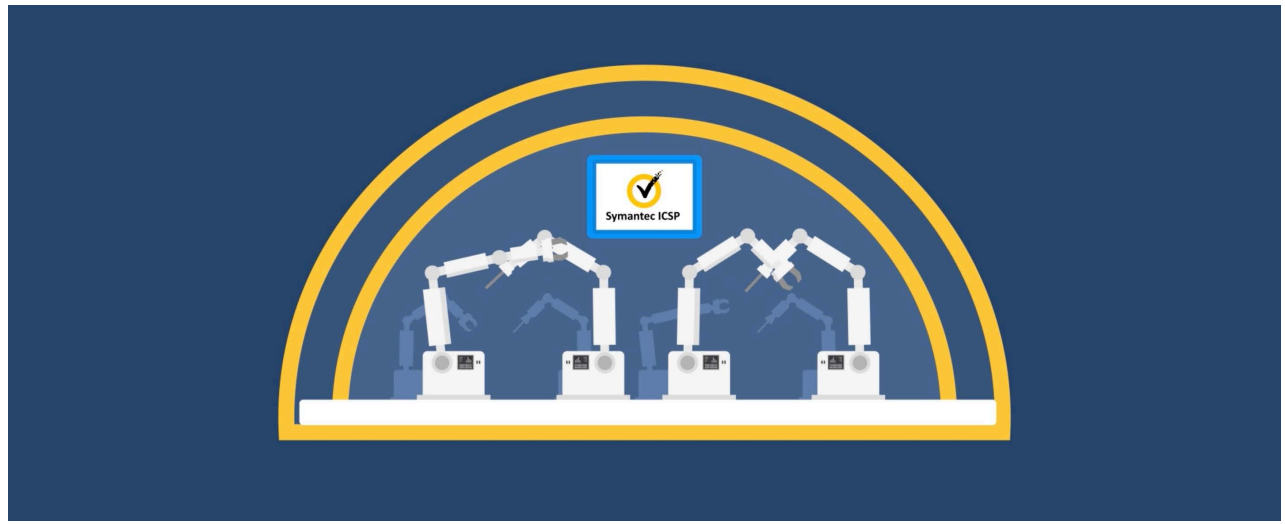
ICSP Workflow Deployment



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

1. The removable media is first checked by the USB Scanner Station and deemed clean.
2. The removable media can then be fully accessed by the targeted ICS once it is connected to the system's USB port, including all files, folder and sub-folders.
3. Files can be freely changed and accessed by the targeted ICS where the removable media is still connected to.
4. Changed content will not be accessible by other ICSs running the ICSP driver without re-scanning at the ISCP Scanner Station.

Industrial security made easy.



Explore more at ›symantec.com/iot

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.

Symantec™

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

SYMC-SB-IOT-ICSP-v 1