Symantec
A Division of Broadcom

Product Brief

# Industrial Control System Protection Neural

## USB Scanning Station for Secure Information Transfer

## At a Glance

Industrial OT elements have become highly vulnerable as a result of:

- Everyday USB usage that can infect OT environments
- Dependance on legacy operating systems that are not easily updated or expensive to replace
- Poor anti-virus compatibility due to resource sensitivity or interoperability issues

A high degree of protection can be achieved by leveraging security for a transiting USB device between the OT and IT networks.

ICSP Neural offers high efficacy USB cleaning without changes to an OT environment through a feature-filled scanning station that is hardened against threat actors and advanced adversaries.

### Pioneering Design

- Innovative high-density display and industrial grade finish provides a modern experience for remediation and user entry of USB devices.

### Broad compatibility

- Supports various forms of USB media and the enforcement driver for OT systems has broad legacy OS support.

### Complete protection

- Our high intensity threat detection engine enables detection at near-zero false positives at less that 1/100th of a percent.
- Prevents both known and unknown attacks and implements control points to protect against USB-borne malware, network intrusion, and zero-day exploits.

## Challenges of securing industrial environments

Recent computing advancements have increased device connectivity and automation in industrial environments. Security in these environments has historically been only maintained through the lack of:

- Internet connectivity to operational technology (OT) systems
- Common infections that could plague OT environments

Times have changed in a connected world. The number and breadth of attacks have increased dramatically. The downstream impact of a breach is unacceptable. The infection vector can be manipulated in environments like ships, trains, or power grids to cause damage and casualties, even fatalities. The implications of an industrial control system (ICS) attack from malware infections in the various types of ICS resources have serious implications, including:

- Illicitly gathered intelligence
- Production downtime
- Invalid data displayed to operations
- Invalid programming sent to controllers

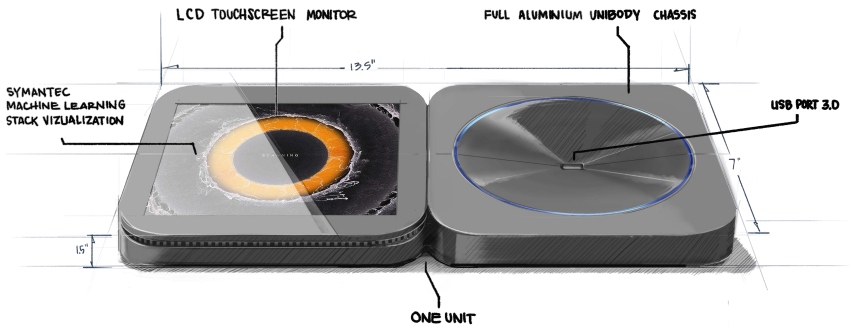
Industry attacks tell us that human-operated systems (human machine interfaces, or HMIs) are key attack vectors. Attackers compromise HMIs because they are frequently used for data transfer. Common malware (even dated infections such as WannaCry) and advanced adversaries infect these systems regularly via network and USB exploits.

The challenges are even more acute when it comes to protecting older cyber-physical systems, which are difficult and expensive to replace or patch, and where configuration is highly customized. Everyday USB usage (to update systems, for example) can easily infect these environments and some malware protection may not support legacy operating systems or low resources on OT Systems.

## Symantec's defense arsenal

Symantec fosters uninterrupted business operations without requiring you to replace existing equipment, software, or downstream operations. Our Endpoint solutions solve customer pain points with enterprise-ready, proven offerings.

The Industrial Control System Protection (ICSP) Neural USB scanning station is a self-contained aluminum unibody appliance that prevents both known and unknown attacks to OT environments through detection of and protection against malicious malware that exists on USB devices.




For secure external media transfer, ICSP Neural leverages and visualizes our most advanced Symantec threat technologies. A machine learning stack cross hatched with signatures, emulation, and reputation provide the highest levels of protection against weaponized malware.

## Key Features

**Signature –** Symantec's STARGate security service puts to work a vast collection of malware and threat intel feeds to rapidly produce signatures that identify and block threats. It maintains information on prevalent threats and can retrieve information on all known threats when cloud access is available.

**Emulation -** Samples are executed in a lightweight virtual machine to cause threats to reveal themselves. Because this emulated environment is similar to a real operating system, malicious software is detected within milliseconds of virtual execution, keeping performance impact low.

**File Reputation -** Based on anonymized information from innumerable deployed instances, STARGate identifies good and bad software and websites based on billions of associations/relationships in our customer base. Symantec uses these reputation ratings in products to block entirely new attacks and to provide additional context to other protection technologies so they can be more aggressive.

**Enforcement Driver -** The scanning station is interoperable with products from various automation vendors and includes a lightweight enforcement driver to validate that a USB was scanned and cleaned. This functionality requires no connection between the target system and the station. Also, its memory footprint is less than 5 MB.

**Advanced machine learning -** Hundreds of characteristics related to a file's intent are evaluated using advanced machine learning models and an automated back end that perpetually retrains the machine learning to prevent in-field evasion. ICSP Neural thus effectively blocks malicious software that it has never seen before.

**Neural Network -** ICSP Neural technology includes an unprecedented deep learning component, known as Neural Network. It will not only offer higher detection rates, but also orthogonally increase functionality in three new areas.

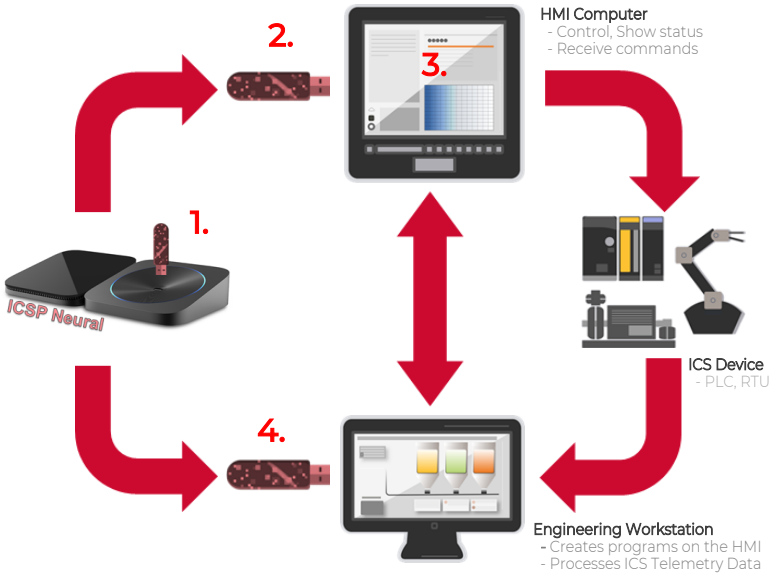
- **Longevity:** Extended ability to maintain efficacy over longer durations
- **Adversarial machine learning:** Ability to uncover advanced adversaries attempting to fool a model by transfiguring a malicious payload
- **Self-improvement:** Organic ability to improve detections by itself

Whether the target system is decades-old or modern-day machinery, ICSP Neural provides a high degree of protection from unknown and known threats traversing the air gap.

## Customer Use Case

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 folders, 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.




## Additional Information

Learn more about ICSP Neural by reviewing our Video Overview and Product Documentation.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com