Symantec Industrial Control System Protection

USB Scanning Station for secure information transfer.

Industrial IOT (Operational Technology) elements have become highly vulnerable as a result of dependence on operating systems that are not readily updated, and a lack of anti-malware due to interoperability issues or resource unpredictability.

While these can be solved with our ultra light-weight Critical System Protection, a high degree of protection can also be achieved by leveraging security for a transiting USB device between the OT and IT networks. This protects industrial environments in various segments such as 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 production and research & development — increasing numbers of malware are traversing the air-gap into a critical environment.

**ICSP features**

Symantec Industrial Control System Protection is a feature-packed station leveraging the most advanced Symantec threat technologies available. The station is hardened against threat actors and advanced adversaries and is consistently updated with new technologies to protect your environments from malicious USBs.

**Advanced Machine Learning**

Using malware samples from hundreds of millions of endpoints around the world, our engine uses this trained, multi-dimensional behavioral model to identify large classes of malware, both known and unknown. This technology significantly bolsters our ability to confidently convict malware potentially on the USB.

**File Reputation**

An analysis that determines the safety of files using techniques powered by our global intelligence network with advanced machine learning in the cloud. This safety score gives another feed into our engine when rapidly processing files.

**Emulation**

For scripts, compressed files (zip), and other executables, our light sandbox detects polymorphic malware hidden by custom packers. These techniques to hide from traditional signature-based only technologies can be uncovered immediately.

**Signature**

Scans and eradicates malware that arrives via USB.

* advanced technologies to be added in next release of ICSP via an included software update

**USB attack defense**

Symantec™ Industrial Control System Protection (ICSP) is a rugged USB scanning 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.

ICSP satisfies diverse OT requirements such as a remote drilling site, or a container shipping.

ICSP also includes an enforcement driver that can validate a USB was indeed scanned. This validation is configurable with a time expiry and compatible with older operating systems. This driver is optional, but recommended for assurance.

*Whether your industrial control system is 20 years old or is brand-new machinery, ICSP gives you a high degree of protection without change control.*
Enforcement Driver
Interoperable with various automation vendors HMI and workstations (Emerson DeltaV, Rockwell, and more) ICSP includes a lightweight enforcement driver to validate that a USB was scanned by the ICSP station.

This functionality requires no connection between the target system and the station and can preserve the disconnected, or air-gapped, state of the OT network.

Integration with Critical System Protection
ICSP pairs well with Critical System Protection which protects against sophisticated unknown threats and network borne attacks. This technology has a significantly small footprint and requires no content and signature updates.

Robust security
- **Rugged design**: Two ethernet NICs as well as multiple USB ports for longevity inside the OT environment.
- **Broad compatibility**: Supports various forms of USB drives
- **Complete protection**: Provides multiple anti-malware technologies beyond signature coming in 1H 2019 release of ICSP.

More information
To learn more about Symantec Critical System Protection, visit www.symantec.com/campaigns/embedded-security-critical-system-protection.

About Symantec
Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps businesses, 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 suite of products for protection at home and across all of 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.