Symantec
A Division of Broadcom

Protecting Critical Infrastructure

Securing Operational Technology (OT) and Industrial Control Systems (ICS)

Table of Contents

Challenges of securing industrial environments

Recent computing advancements have increased device connectivity and automation in industrial environments. Security in these environments was once maintained through:

1. Lack of internet connectivity to operational technology (OT) systems
2. Lack of common infections that could plague OT environments

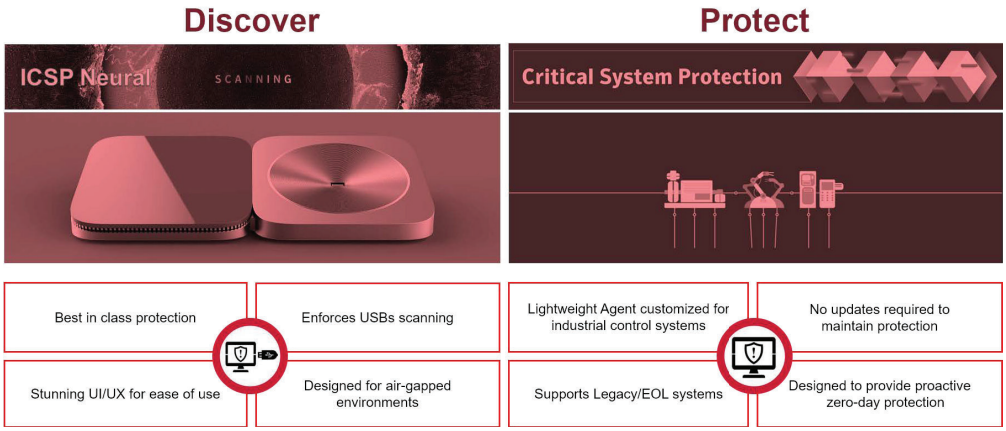
Times have changed in a connected world. The number and breadth of attacks have increased dramatically. The OT habitat does not help. A low priority given to security-related patches, unsuitable antivirus compatibility and connectivity requirements, and frequent USB usage further increase the likelihood of attack.

The downstream impact of a breach is unacceptable. The infection vector can be manipulated in ships, trains, or power grids to cause damage and casualties, even fatalities.

Industry attacks tell us that human-operated systems (human machine interfaces, or HMIs) are key attack vectors everywhere from utilities to nuclear power plants. 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 Symantec response

In this brochure, we describe two Symantec endpoint solutions that protect against network and USB attacks in industrial environments across a number of verticals (including manufacturing, pharmaceutical and healthcare, oil and gas, logistics, drilling, data centers, and travel and hospitality) and use cases.



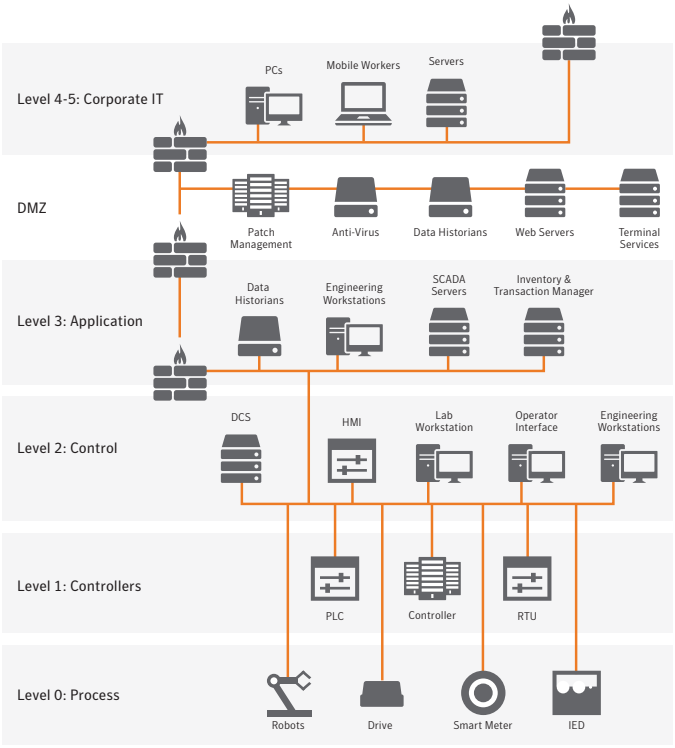
These solutions work together, and with the rest of the Symantec product portfolio, thanks to our Integrated Cyber Defense (ICD) platform, unify cloud and on-premises security to provide threat protection, information protection and compliance across all endpoints, networks, email, and cloud applications.

Symantec's Integrated Cyber Defense Platform is powered by the largest civilian threat intelligence network, deep security research and operations expertise, and a broad technology ecosystem – working together to enhance security controls, improve visibility, and reduce cost and complexity for businesses worldwide.

Industrial control system architecture

The Purdue model presents a sample architecture of an industrial control system environment. The various levels guide engineers in designing functional cyber-physical systems.

- **Level 0:** Physical aspects of OT, which gather data or drive analog movement.
- **Level 1:** Programmable logic controllers (PLCs), which manipulate physical processes and convert analog to digital.
- **Level 2:** Distributed control systems (HMIs), which provide fine-tuned control over physical processes, and a method for operators to interact with the ICS.
- **Level 3:** Supervisory control and data acquisition (SCADA) components, which can be used for high-level process supervisory management.



Key challenges in securing an ICS

- Old cyber-physical systems are vulnerable and more susceptible to infections.
- These systems are difficult and expensive to replace or patch, and configuration is highly customized.
- Poor antivirus compatibility results from resource sensitivity; everyday USB usage can infect these OT environments.

Implications of an ICS attack

Malware infections in the various types of ICS resources have serious implications including:

- Intelligence illicitly gathered
- Production downtime
- Invalid data displayed to operations
- Invalid programming sent to controllers

ICS attack anatomy

A common denominator of the ICS malware described above is a lack of sophistication. While purposed for cyber attacks, the malware simply used the very protocols defined by the manufacturers. The following flow demonstrates the path of a typical ICS attack.

STAGE 1: COMPROMISE INTERNAL IT SYSTEM	STAGE 2: PIVOT TO OT	STAGE 3: ACCESS TO PLC	STAGE 4: PROFIT
• Email intrusion • Watering hole • Trojanized software • Non-PE attacks	• L2/L3 controllers can be accessed • Typically via USB or network • Not a time-bound activity	• No authentication required to configure logic • Use the protocol against itself	• Now under your command • Systems can be disabled or changed • Alerts can be suppressed
ICSP/ CSP		CSP	

A trusted strategy

Symantec solutions promote security by preventing attackers from infecting OT systems.

- Organizations that do not take proper measures to secure OT environments are subject to large liabilities.
- Business stakeholders need a clear understanding of the risks in their environment.
- Only monitoring at a network level does not enable organizations to prevent even accidental infections.
- Intrusions pivot through the endpoints and, therefore, must be at the heart of an organization's OT security strategy.

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.

Why choose Symantec over the competition?

Some competitors focus on post-attack detection and visibility into an OT environment. More established competitors do not focus on OT pain points but, instead, assume IT solutions will function adequately in OT environments.

Symantec ICSP and CSP prevent both known and unknown attacks. Working together, they protect against Stage 1 and Stage 2 ICS attacks. Moreover, they build on existing Symantec investments in threat protection.

Symantec ICSP and CSP implement control points to protect against USB-borne malware, network intrusion, and zero-day exploits to industrial control systems.

Symantec Industrial Control System Protection

Plug-and-play USB scanning

The Symantec ICSP USB scanning station is a self-contained aluminum-unibody appliance that scans your critical IoT environments to detect, and protect you from, USB-borne malware and attacks traversing the air gap.

For secure media transfer, the ICSP scanning station uses and visualizes the Symantec machine learning stack, cross-hatched with signatures and emulation, to provide the highest levels of protection against weaponized malware.

Signature - StarGate Technology 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.

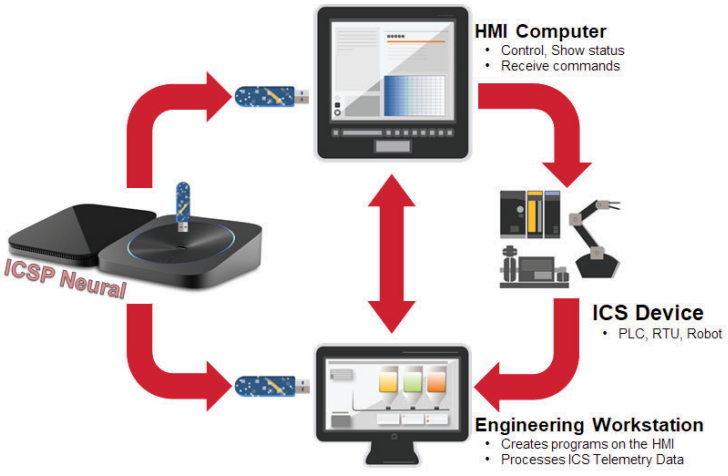
File Reputation - Based on anonymized information from innumerable deployed instances, StarGate identifies good and bad software and websites based on billions of associations/relationships in our customer base. Symantec uses these reputation ratings in products to block entirely new attacks, and to 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. It's 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. StarGate thus effectively blocks malicious software that it has never seen before.

Neural Network - StarGate 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.

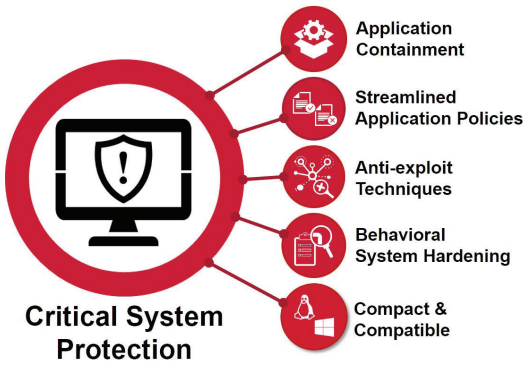
- Longevity: Extended ability to maintain efficacy over longer durations
- Adversarial machine learning: Ability to uncover advanced adversaries attempting to fool a model by transfiguring a malicious payload
- Self-improvement: Organic ability to improve detections by itself



Symantec Critical System Protection

Application Control - No Internet connectivity required

Symantec Critical System Protection is a flexible and compact behavioral security engine built with intrusion prevention and intrusion detection features for managed or standalone IoT devices. Symantec CSP uses a signatureless policy-based approach to endpoint security and compliance, which secures IoT devices from known and unknown zero-day exploits and attacks.



Application containment - Using proprietary auto-isolation technology, Critical System Protection restricts applications to sandboxes that provide the least privilege access required on a per-application basis, without any code changes or functional limitations.

Streamlined application whitelisting - Simplifies policy configuration by significantly reducing the number of decision points. The policy includes a new set of exploit prevention techniques along with system hardening, a network firewall, and USB whitelisting.

The CSP policy library contains prevention and detection policies; customize them to protect your network. A prevention policy is a collection of rules that governs how processes and users access resources. A detection policy is a collection of rules that are configured to detect specific events and take actions. Agents are installed on devices to enforce policies that protect the devices from malicious activity.

Anti-exploit techniques - The policy includes a new set of anti-exploit techniques (tripling the number in the previous version) to protect operating systems from exploits and attacks. The anti-exploit techniques are implemented to detect any malware action. Some of the latest techniques added to Symantec CSP:

- Enforce data execution prevention
- Data execution prevention override protection
- Stack pivot attack protection
- Buffer overflow protection
- Stack-based execution attack protection
- Heap-based execution attack protection
- Heap-based ROP attack protection
- ROP caller check
- Null page dereference protection
- VBS God Mode (IE)

Behavioral system hardening - System hardening enables you to lock down operating systems, applications, and databases, and prevent unauthorized executables from being introduced to, or run on, a target system.

Thousands of prebuilt rules are provided that monitor and harden the complete operating system and require minimal tuning. They monitor files, settings, events, logs, application behavior, and more, essentially covering the entire system. This ensures the immediate detection of any attempted malware actions.

CSP prevents intrusions from causing damage. It has granular control over the entire operating system, blocking any attempts at unauthorized behavior and rendering attackers powerless.

Compact and compatible - Optimized for embedded systems and resource-constrained environments such as industrial control systems and operational technology, CSP can augment EOL/EOS and new operating systems without content, signature or any need for a cloud connection. It is qualified and interoperable with many automation vendors and robots today.

CSP is not resource intensive and consists of a kernel level protection engine that runs in ~20MB on Windows and Linux at less than 1% CPU utilization. It has broad compatibility and operates on any Windows OS since windows 2000 and on Linux in headless or unmanaged mode.

CSP protects and isolates IoT systems against Stage 2 kill chain attacks when the CSP engine is installed on existing automation stacks and engineering workstations (such as Rockwell Automation Systems).

Symantec™
A Division of Broadcom

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