Internet of Things: Protecting Against Industrial Cyber Attacks

Multidimensional security for industrial control systems and critical infrastructures

FAMILY BROCHURE

Symantec™

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.

- **Symantec Industrial Control System Protection (ICSP)**—USB scanning station cleans and sanitizes storage devices.
- **Symantec Critical System Protection (CSP)**—Works without internet connectivity and supports legacy operating systems.

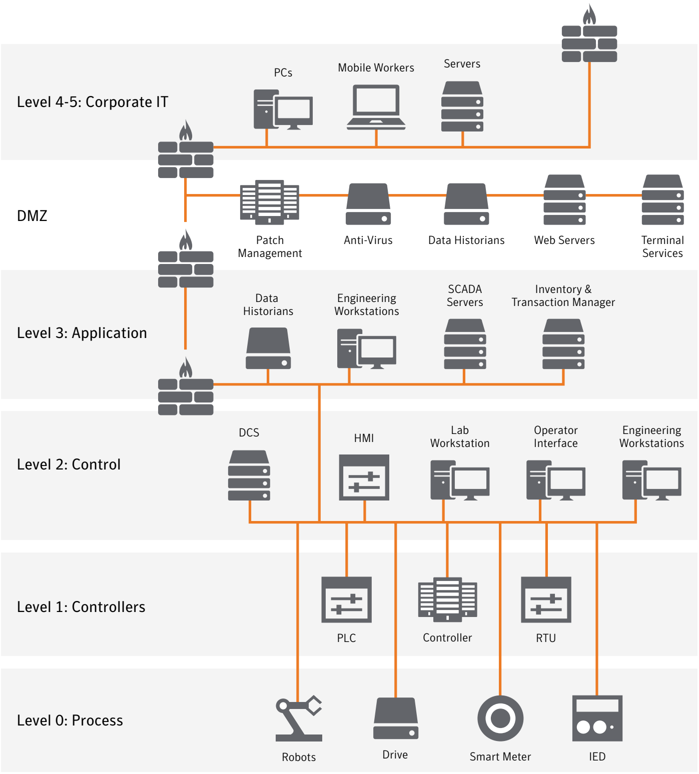
These solutions work together, and with the rest of the Symantec product portfolio, thanks to our Integrated Cyber Defense (ICD) platform, unify cloud and on-premises security to provide threat protection, information protection and compliance across all endpoints, networks, email, and cloud applications.

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

Stuxnet was one of the first attacks developed specifically for ICSs. Its purpose was to decimate the Iranian nuclear program. It is a remote-access Trojan with three main parts: A worm that executes the main payload; a rootkit that hides its presence; and a link file that automatically executes copies of the worm that it has spread on other devices. Stuxnet used four zero-day exploits as well as compromised certificates to spread and execute itself. It looked for the Windows operating system, Siemens S7 PLC, and Siemens PCS 7.

The Stuxnet malware was installed using a USB device. It then automatically propagated itself in the network, installing itself on all devices, and executing whenever it found software for which it had zero-day exploits. Then it executed its payload and infected the PLCs, gaining control of their actions. It also executed a man-in-the-middle attack so the system didn't shut down due to abnormal behavior.

Industroyer is a modular malware framework that took down Ukraine's electrical grid. It has five main components. The first is a main backdoor used to control all the malware components, and connect to the command and control server. The second part is an additional backdoor with the same functions, in case the original backdoor gets disabled. The third component is the launcher, which launches the payloads and the data wiper. The payload has four subparts. Each subpart was intentioned for a specific protocol; all, however, had the same effect: to map the network and then issue commands to specific devices. Last, the data wiper overwrites files with random binary code to render the system unbootable, thwarting recovery.

Industroyer showed that critical infrastructure is vulnerable and that hackers are not only willing to take it down, but they can take control of everything that's happening on it.

WannaCry is an IT security threat that also crossed over into the OT world. WannaCry targeted computers running Windows. It has two parts: A payload that encrypted the data and demanded ransom (Bitcoin payments) to get the data back, and a worm that propagated using EternalBlue, an exploit of Windows Server Message Block (SMB) protocol. It affected not only individuals but also services such as the United Kingdom's National Health System (NHS), Spain's Telefonica, FedEx, a German railway company, and more.

In August 2018, the world's largest chip supplier, Taiwan Semiconductor Manufacturing Co. Ltd. (TSMC), admitted that an attack that halted production was caused by unpatched Windows 7 systems. TSMC was infected by a virus akin to WannaCry via a USB device. The infection occurred when a supplier connected tainted software to TSMC's network without performing a virus scan. The virus spread swiftly, hitting facilities in Tainan, Hsinchu, and Taichung. The infected production tool was provided by an unidentified vendor.

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
• 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
ICSP/ CSP	

STAGE 3: ACCESS TO PLC	STAGE 4: PROFIT
• No authentication required to configure logic • Use the protocol against itself	• Now under your command • Systems can be disabled, changed • Alerts can be suppressed
CSP	

A trusted IoT 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 IoT 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 IoT security over the competition?

Startup 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.

Featuring technologies

- Signature
- Emulation
- File reputation
- Enforcement driver
- Advanced machine learning
- Neural Network

Signature—StarGate 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 (in-field update)—In early 2019, StarGate will include 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 provides a high degree of protection from unknown and known threats traversing the air gap.

Symantec Critical System Protection

Application Whitelisting—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.

CSP Features

- Streamlined application whitelisting
- Anti-exploit techniques
- Behavioral system hardening
- Web console
- Supports Windows 2000/XP/10 & Linux
- Memory footprint less than 20 MB
- CPU utilization less than 1 percent

Streamlined application whitelisting—The new streamlined application whitelisting policy 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 8.0:

- 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

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.

Web console—The new web-based management console presents an intuitive user interface, enabling you to:

- View and manage the Simplified Windows Policy and the Windows Null Policy
- Manage the CSP 8.0 agents operating under the Simplified Windows Policy
- View policies and agents in versions earlier than CSP 8.0

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).

Learn more

Working together, Symantec ICSP and CSP provide broad protection from Stage 1 and Stage 2 industrial control system attacks.

To learn more about Symantec Critical System Protection, visit:

https://www.symantec.com/products/embedded-security.

To learn more about IoT security, visit:

https://www.symantec.com/solutions/internet-of-things.

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.