Cyber Security Solution for Industrial Control Systems

# Ensure the Safety and Integrity of your Operational Technology (OT) Environment

## MAIN BENEFITS

Ensure the safety of industrial assets and people.

Keep critical industrial processes undisrupted with adaptive policies and no need to patch systems.

Support compliance with OT cybersecurity regulations (e.g., NERC CIP, NIST 800-82 and ISA/IEC 62443).

## MAIN CAPABILITIES

Risk Analysis: expose all your OT related cyber-risks.

Auto-segmentation: minimize your risk exposure with auto-generated policies.

Threat Prevention: block attacks before they reach critical OT systems.

## Secure any Operational Technology (OT) Asset


## Tailored Solution for Different Industries

# Industrial Control Systems Are Attractive Targets for Threat Actors

The increasing connectivity of industrial control systems (ICS) and the convergence of OT and IT networks expands the attack surface of industrial manufacturing and critical infrastructure facilities. The advantages of interconnected ICS systems also work against them by providing opportunities for threat actors to damage infrastructure operations and processes. Attackers can alter commands sent to controllers, to change the controllers' logical sequence or to change sensors' readings, thereby disrupting the industrial processes. These disruptions can manifest subtly so while they may be difficult to detect initially, they will cause increasing damage to processes over time.

## ICS components are inherently vulnerable and easy to hack since:

- They usually can't hold endpoint protection.
- They run on legacy/proprietary software that lacks sufficient user and system authentication or data authenticity verification.
- Their software cannot be updated or patched frequently, due to access limitations, concerns over downtime or the need to re-certify systems.

## Crypto miners attacked 32% of the global utility providers

*according to Check Point's research in 2018.*

Crypto mining software overloads and negatively impacts the operation of ICS components.

## The Threat is Real: Cyber Attacks Against ICS Caused Major Disruption

Ransomware shut down a US Natural Gas-Compression facility for two days

Source: HackRead

Malware against SCADA systems left 1.4 Million Ukrainians without Power

Source: Independent

ASCO manufacturing plant was shut down completely for a month

Source: Cybersecurity Insiders

# Check Point Cyber Security Solution for Industrial Control Systems

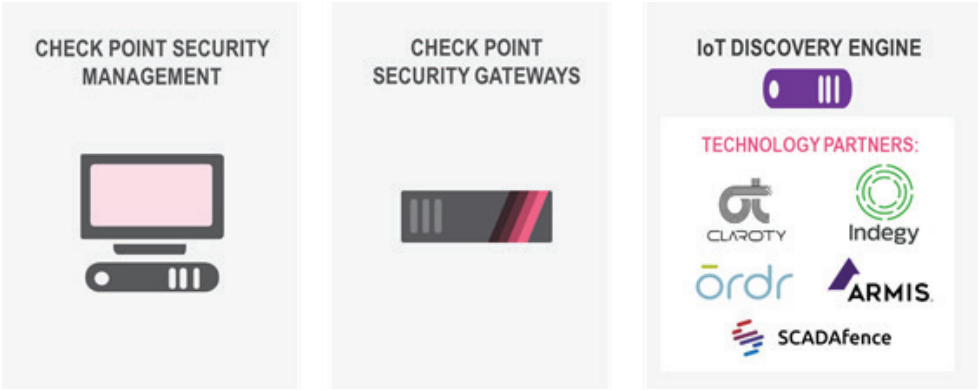
Check Point offers the industry's most comprehensive cyber-security solution for Industrial Control systems, keeping any connected asset on the Operational Technology network protected. That includes Industrial controllers, SCADA servers, and sensors.

With industrial domain expertise, the solution prevents OT related attacks and continually minimizes OT attack surfaces. All in a way that is easily scalable and non-disruptive to critical Industrial processes.

Main solution capabilities:

- IT/OT Network Segmentation
- Risk Analysis: Expose All your OT Related Risks.
- Auto-generated Policies: Minimize your risk exposure with auto-generated OT Policies.
- Threat Prevention: Block attacks before they reach critical OT systems.

## Solution components:



# How It Works

## 1. IT/OT Network Segmentation

Check Point Next-Generation Firewalls, available as physical or virtual appliances, provide boundary protection between the IT and the OT network and micro-segmentation among product lines and departments on the shop floor. With granular visibility into over 1,400 SCADA protocols and commands, these firewalls provide access control throughout the entire OT environment.

## CLICK HERE TO VIEW FULL LIST OF THE SUPPORTED SCADA PROTOCOLS

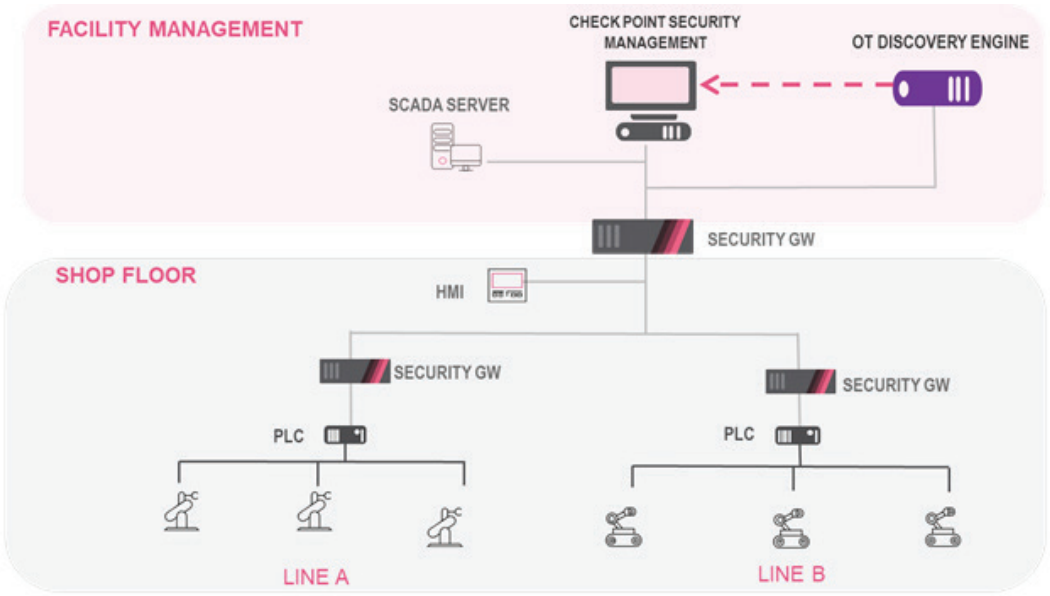



*Figure 1: Deployment example in Manufacturing Plant*

# 2. OT Risk Analysis: Exposing All your OT Related Risks

The solution continually performs a comprehensive risk analysis of your entire OT environment to expose all the risks associated with your assets at any given moment. From a single console, you can view all your connected assets classified based on their risk level, and even drill down for a risk analysis per asset.

OT Risk Analysis is based on:

a. **OT Network Discovery -** by integrating with third-party OT discovery platforms, the solution auto-identifies all your assets, tags them based on their attributes (e.g., device type, manufacturer, model, firmware version, and MAC address), and analyzes their behavior in real-time to detect anomalies.

b. **OT-specific Threat Intelligence –** the solution identifies OT threat trends and malicious patterns via Check Point's ThreatCloud, which aggregates threat indicators (IoCs) from over 100 Million gateways, endpoints, and OT assets worldwide.

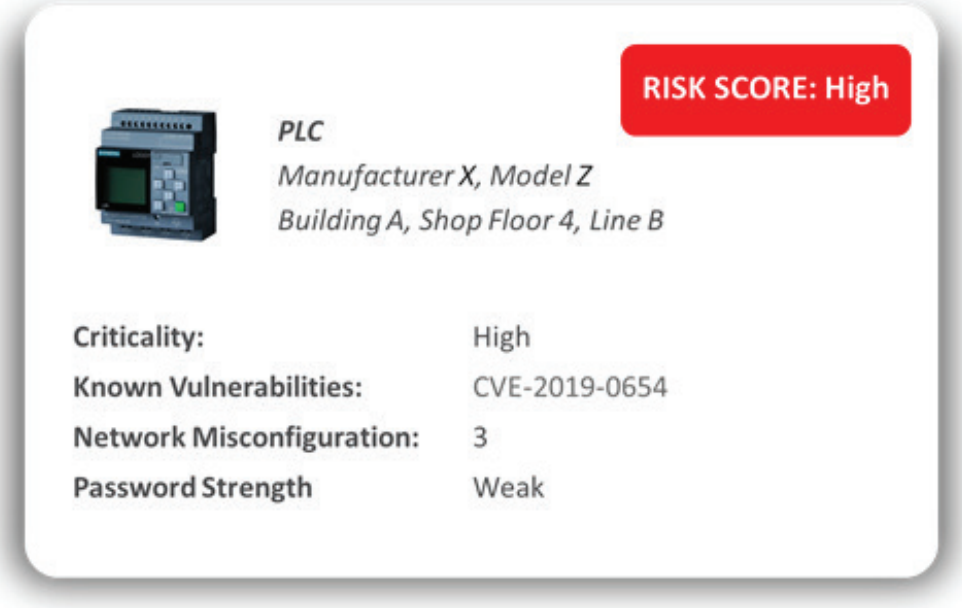
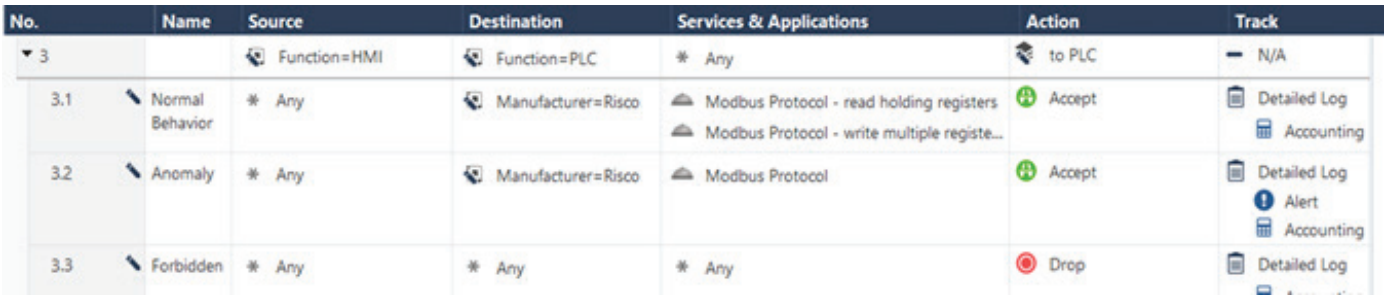



*Figure 2: Drill down for a risk analysis per device*

# 3. Auto-generated OT Policies: Instantly Minimizing your Risk Exposure

Based on the OT risk analysis, the solution automatically generates and enforces a policy for every device in your environment. This automated process saves you months of manual policy configurations and ensures your OT assets are secure from the first moment they connect to your network.

These auto-generated policies instantly minimize your OT attack surfaces by creating network segmentation, one that allows only authorized access to (and from) your OT assets and ensures they use only communication protocols they were designed to use.



| No. | Name | Source | Destination | Services & Applications | Action | Track |
|---|---|---|---|---|---|---|
| 3 | | Function=HMI | Function=PLC | Any | to PLC | N/A |
| 3.1 | Normal Behavior | Any | Manufacturer=Risco | Modbus Protocol - read holding registers<br>Modbus Protocol - write multiple registe... | Accept | Detailed Log<br>Accounting |
| 3.2 | Anomaly | Any | Manufacturer=Risco | Modbus Protocol | Accept | Detailed Log<br>Alert<br>Accounting |
| 3.3 | Forbidden | Any | Any | Any | Drop | Detailed Log |

*Figure 3: Auto-generated Policy Example for HMIs.*

In the policy example in Figure 2, rule 3 defines authorized/unauthorized communication between HMI and PLC assets.

- Rule 3.1 allows HMIs to communicate with PLCs manufactured by Risco using two specific commands of the Modbus Protocol.
- Rule 3.2 allows HMIs to communicate with PLCs manufactured by Risco using other Modbus commands but sends an alert for anomaly behavior.
- Rule 3.3 prevent from Dell HMIs to communicate with other PLCs or to use application/protocol other than Modbus.

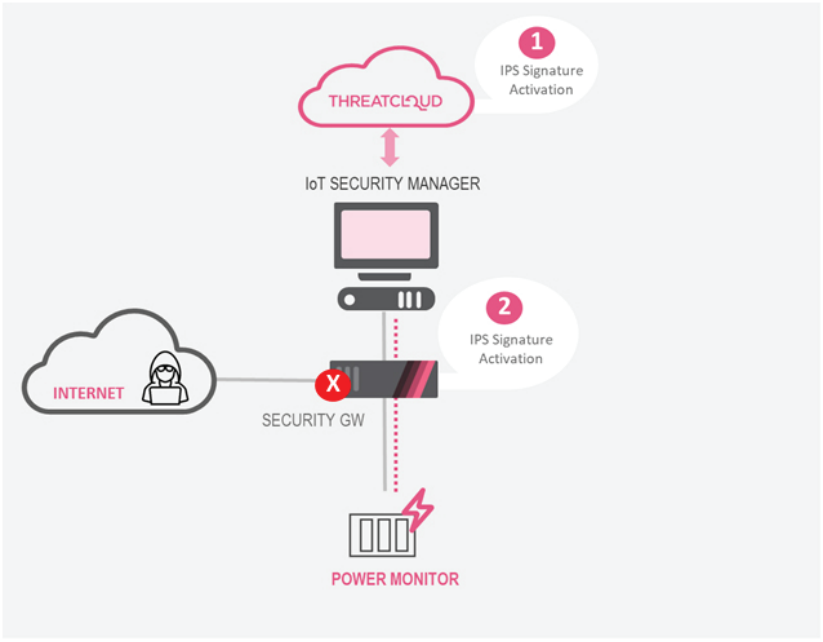
# 4. Virtual Patching: Blocking Known Attacks Before they Reach Critical Assets

The solution protects unpatched ICS systems from known exploits. It automatically activates security protections against known CVEs through virtual patching, by installing the appropriate IPS signatures on the gateways. That allows effective protection against unpatched systems or systems running on legacy operating systems and software; without disrupting critical processes and business operations.

Click here for the full list of Check Point's IPS signatures for OT related threats.

The diagram in Figure 4 shows how our solution identifies and mitigates a threat related to a known vulnerability in Rockwell Allen Bradley Power Monitor 1000.

1. A vulnerability related to a power monitor 1000 of Rockwell Allen Bradley is received from ThreatCloud, CVE-2018-19615
2. The appropriate IPS signatures is activated on the gateway.
X. A malicious connection attempt from the internet to the Power Monitor is blocked.



# Cyber Security Solutions for OT/IoT Manufacturers

## Release IoT innovations while providing your customers with security peace of mind

### On-Device Protection (BETA)

Check Point's revoluzines IoT Security by enabling you to develop connected devices with built-in-security. With our lightweight and easy-to-embed IoT Nano Agent, you can harden and protect OT asets and Industrial IoT devices in a simple and a rapid manner. The embedded nano agent delivers on-device runtime protection that blocks known and zero-day device-level attacks. It monitors the devices behavior and blocks attacks (such as shell injection, memory corruption, and control flow hijacking), before the device is compromised.

### IoT Firmware Risk Assessment (BETA)

Whether you develop IoT devices or deploy them in your organization, with the Check Point IoT Firmware Risk Assessment, you can reduce your exposure to the IoT risk in advance. The Risk Assessment exposes ALL of the inherent security flaws associated with your IoT device firmware (and also with embedded third-party components).

By the end of the assessment, you will receive a comprehensive report that includes insights on:

- Weak credentials: easily brute-forced, publicly available, or unchangeable credentials.
- Known vulnerabilities: list of all CVEs classified based on their severity and attack vector (Network/ physical attack).
- Suspicious listed domainsHardcoded security flaws, such as operating system misconfiguration.
- Key recommendations to mitigate security flaws

Read a sample report to get a preview of the scope of information you will receive

and click here for a free trial

# Summary

While Industrial Control Systems are inherently vulnerable, they are also poorly protected. Check Point offers the industry's most comprehensive solution for OT and ICS environments, enabling manufacturing, utilities, and critical infrastructure facilities to reduce their exposure to OT cyber-risks and block attacks before they reach critical systems. All without disrupting critical Industrial processes.

In addition, Check Point offers cyber security solution for Industrial IoT and OT manufacturers, enabling them to release IoT innovations while providing their customers with peace of mind.

**Worldwide Headquarters**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

**www.checkpoint.com**