# CHECK POINT INDUSTRIAL CONTROL SYSTEMS CYBER DEFENSE

Check Point next-generation security platforms secure industrial control processes found in manufacturing and critical infrastructure industries including power systems, water utilities, transportation, communication systems. Our integrated security suite reduces the cost and complexity of securing and monitoring distributed SCADA systems, aligns Operational Technology (OT) with Information Technology (IT) security and ensures maximum system uptime of operational processes.

Our comprehensive Industrial Control System (ICS) security solution provides end-to-end, multi-layer threat defense and is also available in form factors designed for the extreme conditions of process control environments.

- Full visibility and granular control of SCADA traffic
- Comprehensive security with SCADA-aware threat detection
- Deploy SCADA security in harsh environments and remote locations

## ALIGN IT AND OT SECURITY

Deploy our security platforms across your enterprise IT and OT networks for a unified end-to-end security architecture to protect critical assets from threats. Threats to IT networks are protected from OT networks that are not updated or patched as frequently as enterprise systems and do not have the same level of security. OT networks are protected from Advanced Persistent Threats that target IT networks.


**Threats Target IT and OT Networks in Different Ways**

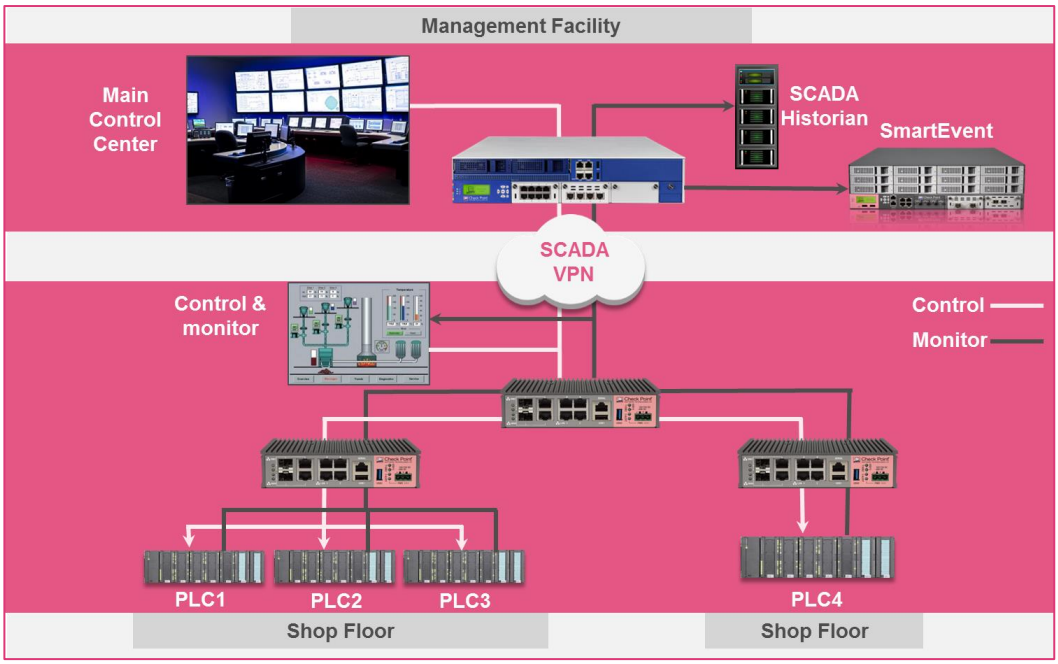
## NEXTGEN SECURITY FOR INDUSTRIAL CONTROL SYSTEM ENVIRONMENTS

## HARDENED SECURITY APPLIANCE AND GRANULAR SCADA PROTOCOL SUPPORT ENABLES INDUSTRIAL CONTROL SYSTEMS CYBER DEFENSE

## TIERED ARCHITECTURE ENABLES BOUNDARY DEFENSE

Implement granular protection to segment and isolate connectivity to and between facilities and production areas, following the ISA-99 zones and conduits model. Ensure the security of the SCADA network devices perimeter and interface points. Ensure that all endpoints and portable equipment used for management is secured with port control protection and free from malware. Our complete IT-OT security solution protects the corporate perimeter, the bridge between IT and OT networks and operator workstations and SCADA devices within the OT network.

- Segment networks and hosts grouped on common security requirements
- Enforce the principle of least privilege with full protocol inspection
- Secure data in transit between segments with VPNs
- Secure remote access into the control network with multifactor authentication

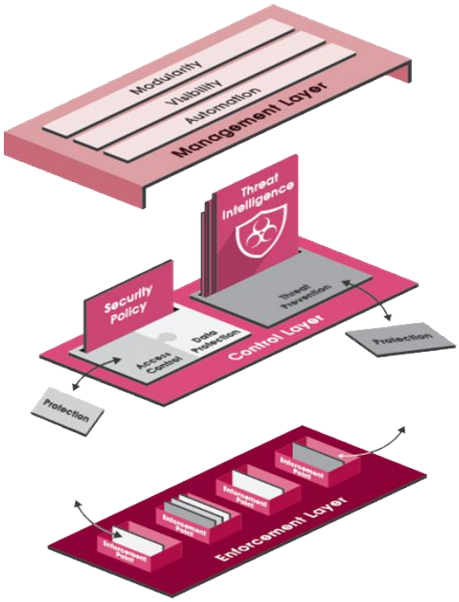



## REAL-TIME MONITORING AND PROTECTION

Unified reporting detects any threat to the application, process or network, providing granular visibility of SCADA traffic and facilitating attack forensics.

1. Log all SCADA activity out-of-band and independent of the ability of SCADA devices to send logs
2. Baseline normal behavior and alert on deviations from the baseline to prevent undesired network operations based upon policy
3. Integrated network and endpoint threat forensics reveals the entire sequence of an attack event
4. Security and events are centrally managed, providing a complete view and consistent policy deployment across your enterprise and control networks

## PRAGMATIC SECURITY ARCHITECTURE AND METHODOLOGY



## BROADEST ICS/SCADA PROTOCOL SUPPORT

Check Point Application Control has broad support for specialized SCADA and ICS protocols with granularity for over 800 SCADA specific commands. Support for additional protocols is available on request.

This enables protocol-specific controls with directional awareness. For instance administrators are able to create a policy to prevent monitoring and reporting systems from performing write operations to control systems.

Our protocol decoders enable granular control at the command level, for example read/write/get for specific units, function codes and address ranges.

**Protocol Support[1]**

- BACNet
- CIP
- DNP3
- EtherCat
- IEC-60870-5-104
- IEC 60870-6 (ICCP)
- IEC 61850
- MMS
- Modbus
- OPC DA & UA
- Profinet
- S7 (Siemens)

[1] For the latest protocols, see the AppWiki

## SCADA-AWARE THREAT DETECTION AND PREVENTION

Industrial Control Systems (ICS) from leading vendors are vulnerable to exploits that are now freely available on the Internet. Our threat detection technologies protect highly vulnerable, unpatched legacy and embedded systems found in Operational Technology (OT) environments.

The same threat prevention technologies with the best catch rate in the industry that you would deploy in prevent-mode in IT environments may be deployed in detect-mode to minimize disruption of operational processes. Granular visibility, control and protection identify unexpected communications and detect known and unknown threats to contain threats before significant damage is done.

## THREAT EMULATION (SANDBOXING)

Preventing today's sophisticated malware requires innovation and investigation. Check Point Threat Emulation quickly quarantines and inspects files, running them in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution prevents infection from undiscovered exploits, zero-day and targeted attacks.


### GRANULAR MODBUS CONTROL

**UNIT ID**

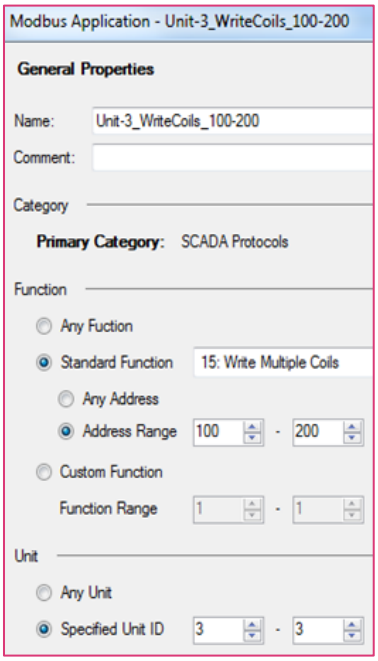
- **UNIT ID 3**

**FUNCTION CODES**

- **WRITE MULTIPLE COILS**

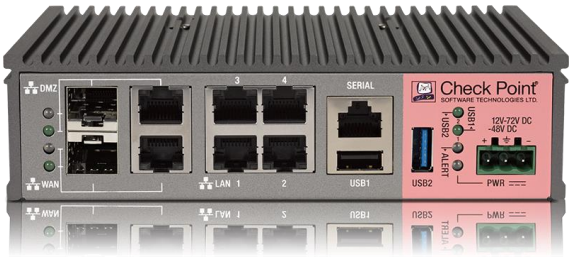
**RANGES WITHIN MODBUS**

- **ADDRESSES 100-200**



## WIDE RANGE OF APPLIANCES FOR IT AND OT NETWORKS

Hardened appliances complement our extensive appliance family to support a diverse range of deployment environments and meet specialized requirements. Our 1200R rugged appliance complies with industrial specifications such as IEEE 1613 and IEC 61850-3 for heat, vibration and immunity to electromagnetic interference (EMI). In addition the 1200R is certified for maritime operation per IEC-60945 and IACS E10 and complies with DNV 2.4. And it operates in extreme temperatures from -40°C to 75°C using a compact fan-less design with no moving parts. All features are available across all appliances so any appliances can be used in the CI/ICS environment.




**1200R Rugged Appliance**

## BEST-IN-CLASS MANAGEMENT

Our unified, integrated management platform supports distributed IT and OT deployments, providing operational consistency, simple administration and powerful analytics and forensics improving the efficiency of managing end-to-end (E2E) security.

Administrators can define security policy for the entire network — including internal security, main sites, and remote sites — from a single, centrally located Check Point Security Management server. With SmartProvisioning™, a profile-based management approach designed for large- scale deployments, administrators can define a single security and device profile and apply it simultaneously to thousands of appliances — dramatically reducing deployment time and administrative overhead.

With compliance built-in, Critical Infrastructure providers are enabled to meet and exceed emerging regulatory and other cyber security requirements such as NERC-CIP (US) and EPCIP (EU) and other regulatory requirements. Both CI and Manufacturing providers get the advantage of hundreds of best practices that define and recommend the optimal security configuration. The Compliance Software Blade constantly monitors the compliance status of the organization, enabling network security managers to quickly assess the strength of the current policy settings and where improvements are needed.

## WANT MORE INFORMATION?

Your network offers access to valuable and sensitive information. Can you be sure there aren't any hidden "surprises" threatening your most precious assets? No stealthy malware, back doors, data leaks or other security vulnerabilities? Don't be caught unprepared. Uncover potential risks on your enterprise network with a **Security Check Up**.

**"THE CHECK POINT COMPLIANCE SOFTWARE BLADE HAS MADE ALL OF OUR AUDITS AN ORDER OF MAGNITUDE EASIER. IT NOT ONLY MAKES THE AUDITING PROCESS FASTER,**

**BUT INSTILLS CONFIDENCE IN OUR CLIENTS THAT WE TRULY KNOW WHAT WE ARE DOING.**

**IN THE COMPLIANCE WORLD,**

**CONFIDENCE IS EVERYTHING."**


CONTACT US

**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