



# The Enterprise IoT Security Challenge

While connecting Internet-of-Things (IoT) devices to your corporate network delivers clear benefits, it also creates new attack surfaces that can expose your network to cyber-threats. From IP cameras, and smart elevators, to medical devices and industrial controllers, IoT devices are extremely vulnerable and easy to hack. Many of these devices run on unpatched software, are misconfigured, or use unsecured communication protocols. These issues increase the risk of a successful cyber-attack where critical devices can be shut down, damaged, manipulated, or used to infect other systems on the network.

Most traditional security solutions cannot see these devices. The solutions that can see these devices, lack the context of what the devices are or how they are expected to function. You need more than just an IP address to secure IoT networks effectively, without disrupting your critical processes.

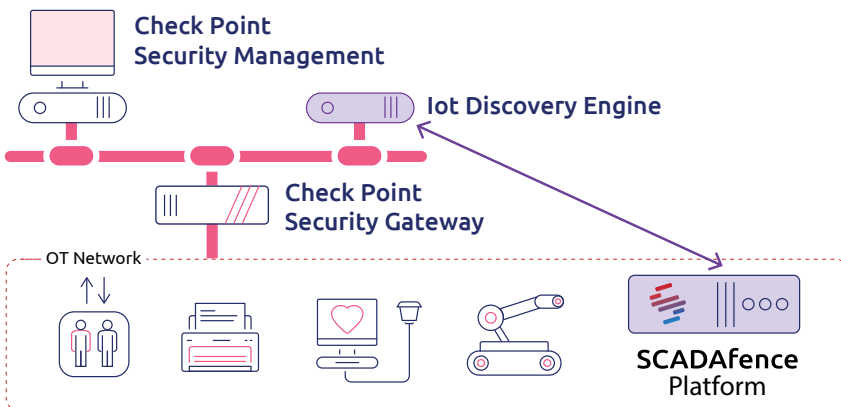
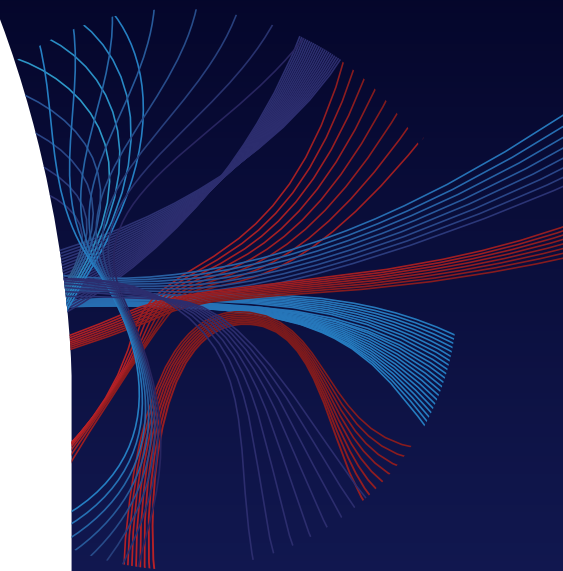


Figure 1: Architecture Diagram

## Minimize the IoT Attack Surface with a Zero Trust Policy for Every Device

The SCADAfence Platform discovers IoT devices connected to your environment and provides you with granular visibility into their attributes such as manufacturer, model, operating system, MAC address, and more, including a device risk analysis and a contextual understanding of its behavior.

Using the Check Point IoT Security Manager, you can configure a security policy based on these device attributes and even leverage auto-generated policy recommendations. This allows you to reduce your risk proactively, by ensuring that your security gateway has a policy for any device in your environment. One that automatically adapts to any changes in its attributes, behavior, and risk level.



## Key Benefits

*The SCADAfence & Check Point integration extends Check Point's reach into OT networks. It provides Check Point's customers with asset visibility and security policies for OT networks.*

- **Visibility into the OT Network:**

*Security teams are now able to see the full OT asset inventory on the Smart Console's UI. This includes all discovered properties such as asset vendor, model, firmware, and many other parameters. For each asset, the list of corresponding CVEs will be displayed, to understand which assets are exposed.*

- **Securing the OT network:**

*Users can now get concrete recommendations for firewall rules, based on the detection of security events in the OT network.*

## IoT Auto-Segmentation: Minimize Your Risk Exposure With Auto-Generated Policies.

The joint solution automatically generates and enforces a policy for every device in your environment. The SCADAfence Platform's detection engine detects OT security threats and automatically sends policy recommendations to the Check Point IoT Security Manager.

This automated process saves you months of manual policy configurations and ensures that your IoT devices are secure from the first moment that they connect to your network. The auto-generated policies instantly minimize your IoT attack surfaces by creating network segmentation, one that allows only authorized access to (and from) your IoT devices and ensures that devices use only communication protocols they were designed to use. They can address system or user defined scenarios, including the detection of malware, unauthorized access, application level anomalies, and deep packet inspection of OT industrial protocols (for example, commands that attempt to change PLC configurations or that stop production processes).

### Example Policy Use Cases:

- Allow AC systems to communicate only with the building management system.
- Allow medical imaging devices to communicate only with PAC servers.
- Prevent badge readers from communicating with HR systems.



No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
Smart Building (5-6)							
5	IP CAM	IP CAM	* Any	* Any	IP CAM	NA	* Policy Targets
5.1	IP CAM to BMS	IP CAM	BMS	ONVIF Protocol	Accept	Log	* Policy Targets
5.2	Hikvision updates	Manufacture=Hikvision	.hkvs.updates.com	https	Accept	Log	* Policy Targets

Figure 2: Auto-generated Policy Example for an IP Camera

In the auto-generated policy example (in figure 1): rule 5.1 allows IP cameras to communicate with a BMS (Building Management System) controller using only the ONVIF protocol and rule 5.2 allows Hikvision cameras to communicate with a specific internet domain (for a firmware update).

The policies are highly granular and adaptive to any change in devices' attributes, behavior, and risk level so they can secure thousands of IoT device profiles without disrupting critical processes.

Every policy can be manually modified within the Check Point security management console, in a separate IoT policy management layer (so that you can avoid confusion and conflicts with the security policies of your entire network).

### Detect Firewall Policy Violations and Bypass

The SCADAfence Platform can also alert if the firewall's policy is violated or bypassed. The SCADAfence Platform can detect communications to/from unauthorized IPs or via unauthorized ports/protocols. All OT network alerts can be sent to the Check Point Smart Console and be shown on Check Point's user interface.

# Block IoT Related Attacks with Virtual Patching

The joint solution accurately detects threats and vulnerabilities relevant to your IoT devices (i.e., CVEs, legacy OS, anomalies) using continuous device behavior analysis, and information from the Check Point ThreatCloud, harnessing globally shared threat intelligence.

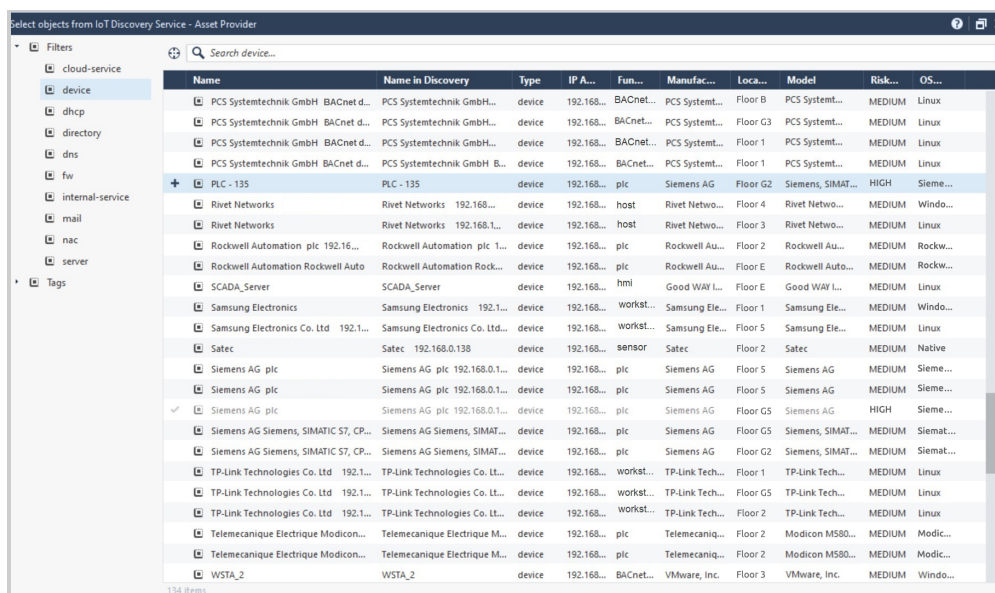
Following input from The SCADAfence Platform's detection engines, the Check Point IoT Security Manager can automatically activate security protections against

detected threats, whether through virtual patching (by installing the appropriate IPS signatures on the gateways) or through policy enforcement to isolate infected devices.

This allows effective protection against unpatched devices or devices that are running on unpatchable OS's and software; without disrupting critical processes and business operations (as in the case of medical and industrial devices).

## Provide Security Teams With Comprehensive Device Information

The SCADAfence Platform automatically creates a comprehensive and detailed OT asset inventory, and shares it with the Check Point IoT Security Manager. Security teams can now see a wealth of information about each device directly in Check Point's IoT Security Manager (e.g., device risk score, manufacturer, model, serial number, location).



The screenshot displays a web interface titled "select objects from IoT Discovery Service - Asset Provider". It features a search bar and a table of discovered devices. The table columns include Name, Name in Discovery, Type, IP A..., Fun..., Manufac..., Loca..., Model, Risk..., and OS... The table lists various industrial devices such as PLCs, Rivet Networks, Rockwell Automation, SCADA\_Server, Samsung Electronics, Satec, Siemens AG, TP-Link Technologies, and Telemecanique.

Name	Name in Discovery	Type	IP A...	Fun...	Manufac...	Loca...	Model	Risk...	OS...
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH...	device	192.168...	BACnet...	PCS System...	Floor B	PCS System...	MEDIUM	Linux
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH...	device	192.168...	BACnet...	PCS System...	Floor G3	PCS System...	MEDIUM	Linux
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH...	device	192.168...	BACnet...	PCS System...	Floor 1	PCS System...	MEDIUM	Linux
PCS Systemtechnik GmbH BACnet d...	PCS Systemtechnik GmbH B...	device	192.168...	BACnet...	PCS System...	Floor 1	PCS System...	MEDIUM	Linux
PLC - 135	PLC - 135	device	192.168...	plc	Siemens AG	Floor G2	Siemens, SIMAT...	HIGH	Sieme...
Rivet Networks	Rivet Networks 192.168...	device	192.168...	host	Rivet Netwo...	Floor 4	Rivet Netwo...	MEDIUM	Windo...
Rivet Networks	Rivet Networks 192.168.1...	device	192.168...	host	Rivet Netwo...	Floor 3	Rivet Netwo...	MEDIUM	Linux
Rockwell Automation plc 192.16...	Rockwell Automation plc 1...	device	192.168...	plc	Rockwell Au...	Floor 2	Rockwell Au...	MEDIUM	Rockw...
Rockwell Automation Rockwell Auto	Rockwell Automation Rock...	device	192.168...	plc	Rockwell Auto...	Floor E	Rockwell Auto...	MEDIUM	Rockw...
SCADA_Server	SCADA_Server	device	192.168...	hmi	Good WAY L...	Floor E	Good WAY L...	MEDIUM	Linux
Samsung Electronics	Samsung Electronics 192.1...	device	192.168...	workst...	Samsung Ele...	Floor 1	Samsung Ele...	MEDIUM	Windo...
Samsung Electronics Co. Ltd 192.1...	Samsung Electronics Co. Ltd...	device	192.168...	workst...	Samsung Ele...	Floor 5	Samsung Ele...	MEDIUM	Linux
Satec	Satec 192.168.0.138	device	192.168...	sensor	Satec	Floor 2	Satec	MEDIUM	Native
Siemens AG plc 192.168.0.1...	Siemens AG plc 192.168.0.1...	device	192.168...	plc	Siemens AG	Floor 5	Siemens AG	MEDIUM	Sieme...
Siemens AG plc 192.168.0.1...	Siemens AG plc 192.168.0.1...	device	192.168...	plc	Siemens AG	Floor 5	Siemens AG	MEDIUM	Sieme...
Siemens AG plc 192.168.0.1...	Siemens AG plc 192.168.0.1...	device	192.168...	plc	Siemens AG	Floor G5	Siemens AG	HIGH	Sieme...
Siemens AG Siemens, SIMATIC S7, CP...	Siemens AG Siemens, SIMAT...	device	192.168...	plc	Siemens AG	Floor G5	Siemens, SIMAT...	MEDIUM	Siemat...
Siemens AG Siemens, SIMATIC S7, CP...	Siemens AG Siemens, SIMAT...	device	192.168...	plc	Siemens AG	Floor G2	Siemens, SIMAT...	MEDIUM	Siemat...
TP-Link Technologies Co. Ltd 192.1...	TP-Link Technologies Co. Lt...	device	192.168...	workst...	TP-Link Tech...	Floor 1	TP-Link Tech...	MEDIUM	Linux
TP-Link Technologies Co. Ltd 192.1...	TP-Link Technologies Co. Lt...	device	192.168...	workst...	TP-Link Tech...	Floor G5	TP-Link Tech...	MEDIUM	Linux
TP-Link Technologies Co. Ltd 192.1...	TP-Link Technologies Co. Lt...	device	192.168...	workst...	TP-Link Tech...	Floor 2	TP-Link Tech...	MEDIUM	Linux
Telemecanique Electrique Modicon...	Telemecanique Electrique M...	device	192.168...	plc	Telemecaniq...	Floor 2	Modicon MS80...	MEDIUM	Modic...
Telemecanique Electrique Modicon...	Telemecanique Electrique M...	device	192.168...	plc	Telemecaniq...	Floor 2	Modicon MS80...	MEDIUM	Modic...
WSTA_2	WSTA_2	device	192.168...	BACnet...	VMware, Inc	Floor 3	VMware, Inc	MEDIUM	Windo...

Figure 3: Auto-Discovered OT Asset Inventory, Synchronized from The SCADAfence Platform

With rich log records and dedicated IoT event reports, you gain a contextual understanding of device behavior and forensics for event investigations. This helps you make well-informed decisions without impacting critical devices, without ever having to leave the Check Point console.

## About SCADAfence

SCADAfence is the global technology leader in OT cyber security. The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and user experience with minimal false-positives. SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in manufacturing, building management and critical infrastructure industries to operate securely, reliably and efficiently. To learn more, go to

[www.scadafence.com](http://www.scadafence.com)

### Our offices

Headquarters: Tel Aviv

Regional: New York, Munich, Tokyo

Contact us: [info@scadafence.com](mailto:info@scadafence.com)

[www.scadafence.com](http://www.scadafence.com)



**SCADAfence**