Ordr and Check Point IoT Defense:

Take Control of Your Connected IoT and OT Systems

IOT IS EXPANDING FASTER THAN IT CAN BE SECURED

IoT and OT devices present unique challenges to access control. Common traits include:

- No user, no authentication
- Highly vulnerable – typically run rudimentary or minimized versions of legacy operating systems without basic client protection software
- Closed systems – minimal or no patching capabilities to defend themselves; installation of posture or other device management agents is rarely an option
- Susceptible to scans – direct interrogation by profiling and other security assessment tools risky due to the fragile nature of device's OS or network stack

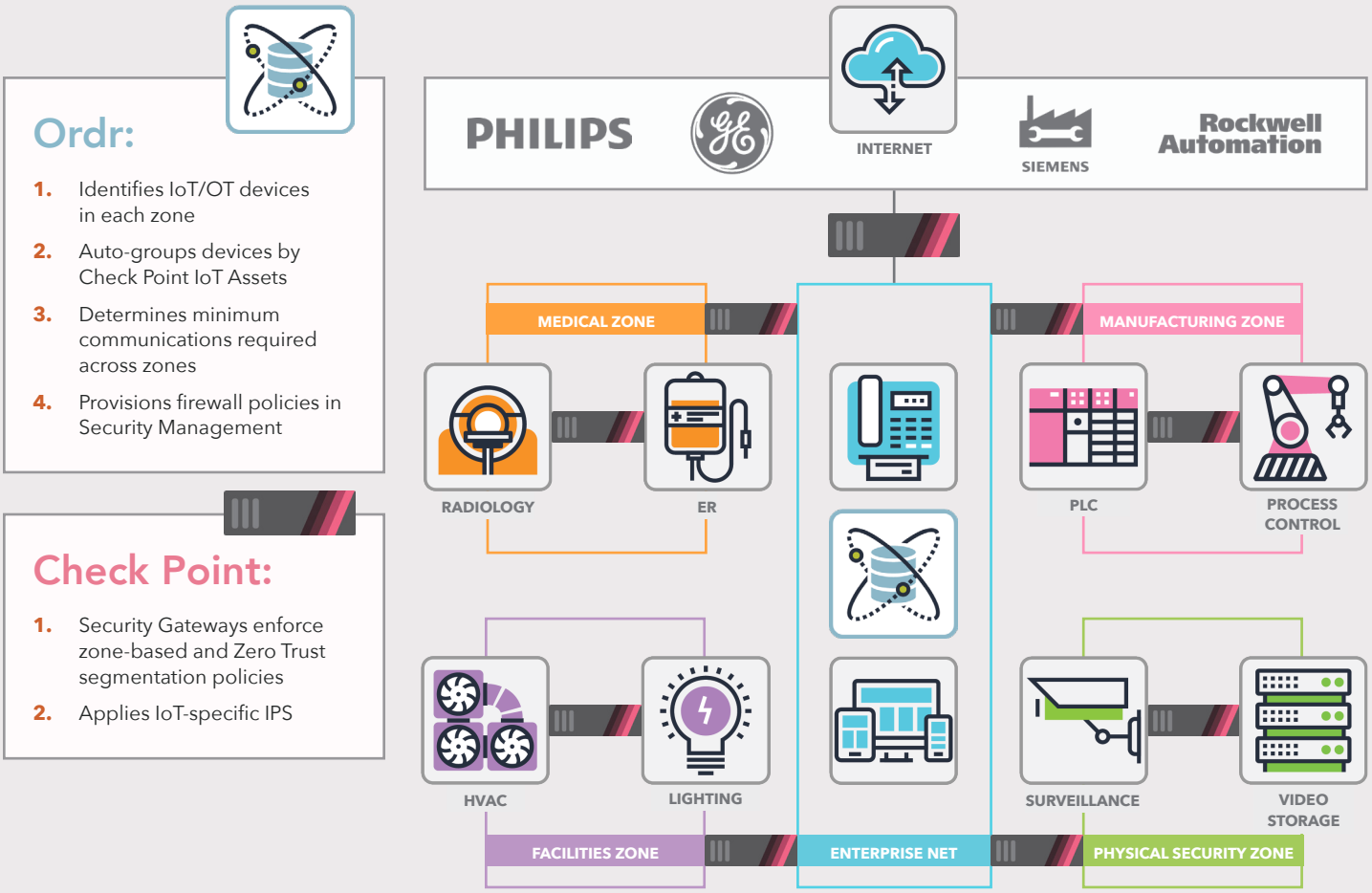
Conclusion: Critical devices are vulnerable to service disruption, data theft, or compromise for ransom or serve as a launchpad for other attacks.

TAKE CONTROL OF YOUR ENTERPRISE

The Ordr Systems Control Engine (SCE) provides the most effective solution to identify, classify, regulate, and secure IoT and digital OT devices from unauthorized access and cyber-attack:

- Passively discovers every connected device with high-definition detail and without agents
- Automatically classifies IoT/OT assets in Check Point Security Management and maintains membership
- Rapidly deploys zone-based segmentation per NIST and IEC 62443 with AI-created policies for Check Point Security Gateways
- Continuously monitors device security risk, application, and behavior; vulnerable and compromised devices are quickly spotted so they can be quarantined
- Enables Virtual Patching – Deployment of Check Point IPS signatures relevant to connected IoT assets
- Verifies segmentation policy is effective using simple, graphical tools

The Joint Solution



The most effective means to protect IoT and digital OT devices is through zone-based segmentation and Zero Trust policy rules. Check Point Security Gateways provide scalable policy enforcement and zone controls for the enterprise. Ordr Systems Control Engine discovers, classifies and groups all devices and automatically maps them into their respective zones, areas, and cells using Check Point IoT Asset groups, and then dynamically generates Security Gateway policy rules based on these groups to deliver streamlined microsegmentation.

For example, building automation devices are seamlessly mapped to the Facilities Zone and facility devices within this zone are further segmented from each other. Security policy rules are enforced by Security Gateways to restrict access between zones, areas, and cells based on the minimum access required to allow devices to properly function while protecting them from insider or outsider attack. An HVAC system can talk with a trusted smart-building controller using approved protocols and applications such as BACnet, but blocked from communicating to the Internet or to another HVAC system.

Ordr and Check Point IoT Defense in Action

Ordr SCE integrates natively with Check Point Security Management for multi-gateway policy enforcement. Security Gateways enforce zone-based segmentation policy to protect all devices inclusive of IoT and digital OT in the enterprise campus or manufacturing plant, the data center, as well as securing communications traversing the Internet edge.

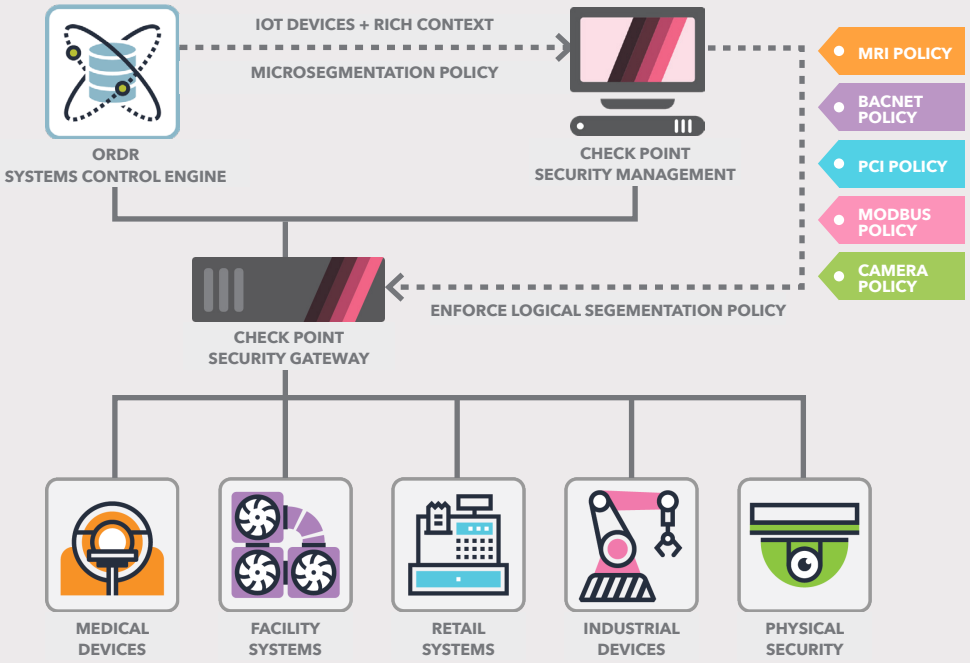
When new devices are connected to the network, they are automatically classified and updated in Check Point Security Management and Security Gateways with the proper IoT Asset membership. Through its network and device awareness, Ordr SCE maintains current IP addressing for IoT Assets in all Security Gateways.

BLOCK IOT ATTACKS WITH VIRTUAL PATCHING

IoT and OT devices are particularly vulnerable, often running trimmed-down versions of legacy operating systems. Patching of these systems is commonly not an option or spotty at best. Check Point Security Management matches the IoT and OT devices learned from Ordr SCE to download and apply dedicated IoT/OT signatures specific to the devices present on the network, thus further reducing the attack surface over approved communication channels.

ORDR PROVIDES:

1. Dynamic IoT Device Classification
2. Automated flow, application, and behavior analysis
3. Agentless Security Assessment
4. Dynamic mapping of IoT devices by group/business role
5. Automated microsegmentation policy based on observed flows



Providing advanced IoT device classification and IoT Asset updates to Check Point Security Gateways is only one piece of the puzzle. To move to microsegmentation and the enforcement of Zero Trust policy rules, administrators must understand which traffic to allow and deny. Ordr SCE provides this insight to fully automate the provisioning of security

and segmentation policy. Ordr SCE policy rules are translated into the syntax required to directly update Check Point Security Management and Security Gateways.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Auto-Generated (1-4)								
1	Ordr-Policy-Hospira-Plum A+-Infusion Pump-16	Function=HospiraPlumA+I...	Any	Any	Any	from HospiraPlumA+	N/A	Policy Targets
2	Ordr-Policy-Picker-PQ5000-CT Scanner-27	Function=PickerPQ5000CT...	Any	Any	Any	from PickerPQ5000CT	N/A	Policy Targets
3	Ordr-Policy-Philips-MRI-3	Function=PhilipsMRI	Any	Any	Any	from PhilipsMRI#	N/A	Policy Targets
3.1		Any	ip_192.168.101.241	Any	domain-udp	Accept	Detailed Log	Policy Targets
3.2		Any	ip_192.168.101.108	Any	tcp-104	Accept	Detailed Log	Policy Targets
3.3		Any	Any	Any	Any	Anomalies	N/A	Policy Targets
4	Ordr-Policy-Baxter-35700BAX-Spectrum Infusion Pump-23	Function=Baxter35700BAX...	Any	Any	Any	from Baxter35700BA	N/A	Policy Targets

Ordr SCE's job is still not done. While monitoring all devices for known threats and vulnerabilities, it is also keeping close watch on communication flows and anomalous traffic. Here Ordr SCE can reassign at-risk, vulnerable, and compromised devices to quarantine VLANs that map to restricted firewall zones, or flag high-risk devices in Check Point Security Management to block attacks and the spread of malware.

Together, Ordr and Check Point allow you to Take Control of your IOT and OT security by implementing segmentation across your hyper-connected enterprise.

ordr

Check Point
SOFTWARE TECHNOLOGIES LTD

About Ordr

At Ordr, we're energized by the explosive growth in network-connected systems and devices. We recognize the tremendous opportunities that this represents for the hyper-connected enterprise. Improved delivery of care, efficient logistics and operations, quality enhancements in manufacturing, more stable and intelligent business-critical systems. We're energized because we give you the power to take control and realize these myriad opportunities.

Learn more at **www.ordr.net**.

About Check Point

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Find out more at **www.checkpoint.com**.