IoT Security

Protect Your IoT Devices and
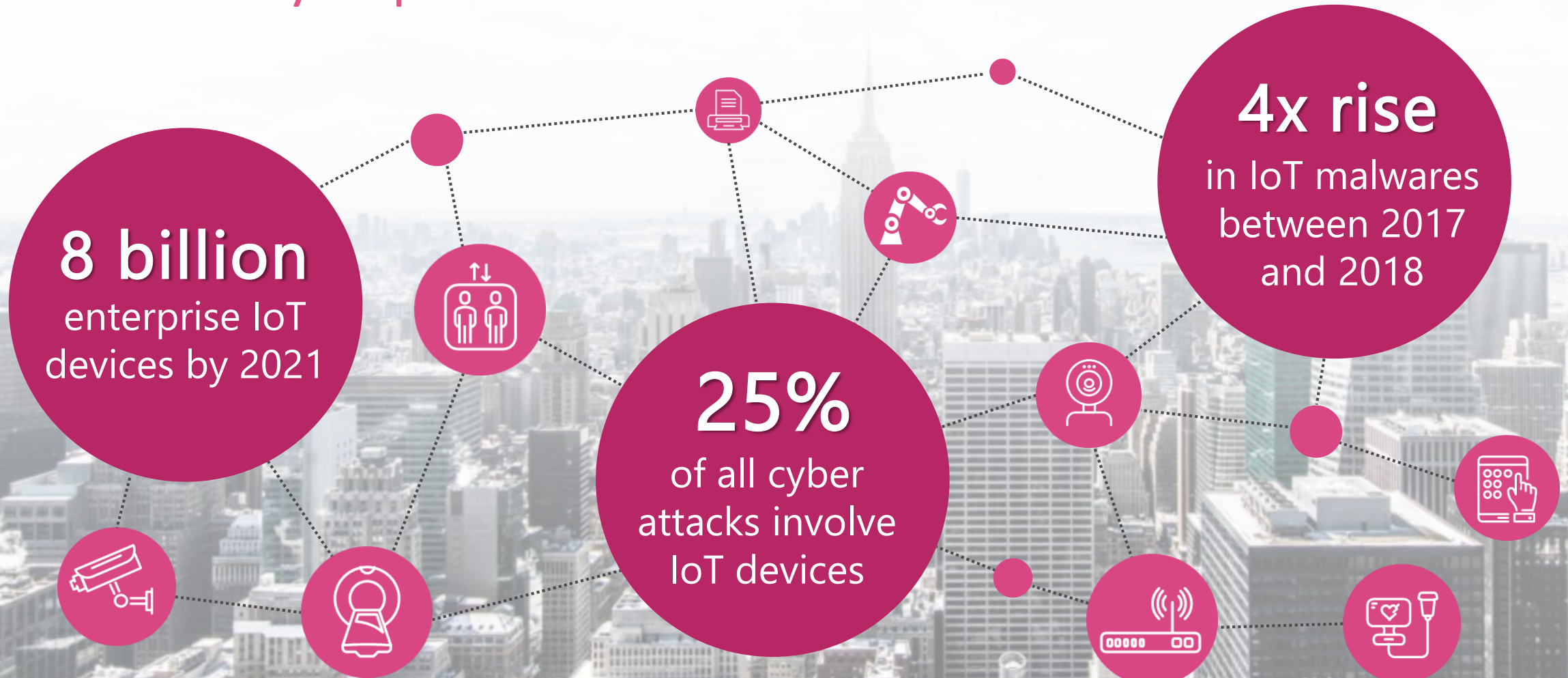Keep your Business Running

David Galdran
Team Leader Industry, Telco and Goverment
ICS Security Expert

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT
INFINITY

CLOUD • MOBILE • THREAT PREVENTION

IoT Security Represent a New Frontier

8 billion enterprise IoT devices by 2021

25% of all cyber attacks involve IoT devices

4x rise in IoT malwares between 2017 and 2018

The Smarter Your Environment – The Higher the Risk

IoT Devices are Highly Vulnerable and Easy to Hack
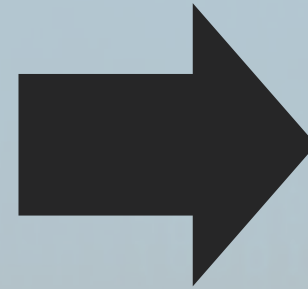
Outdated SW / Legacy OS / No OS

Basic Micro Controllers

No Security-by-Design

Unmanaged Devices

Shadow Devices

Operational Limitations

- Data Breaches
- Data Tampering
- Ransomwares
- Denial of Service
- Physical Damage

IoT Vulnerabilities are All Around Us

Healthcare IoT

Industrial IoT

Smart Building

Smart Office

END-TO-END IOT SECURITY

Reduce IoT Attack Surface, IoT Threat Prevention, Easy Deployment, Efficient and Unified

DISCOVERY & VISIBILITY

Identify and analyze IoT devices and traffic

POLICY MANAGEMENT

Apply granular IoT-based policies

THREAT PREVENTION

Identify and block IoT malicious intents

SECURITY ENFORCEMENT

Block unauthorized IoT access and IoT traffic

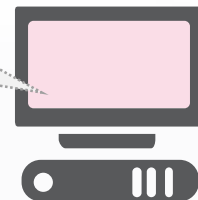HEALTHCARE IOT • INDUSTRIAL IOT • SMART OFFICE • SMART BUILDING

Quick and Easy Deployment

IoT Security Controller

- Configure and manage granular IoT security rules
- Auto generated policies based on customer's profile

IoT Security Controller

IoT Discovery Engine

- Monitors the IoT traffic
- Automatically identify IoT devices and provides deep insight information per device
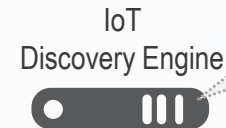
IoT Discovery Engine

IoT Security GW

Security Gateway with IoT support

- Control and restrict internal IoT traffic
- IoT application control: Identify and control IoT protocols and commands
- Integrated IPS designed for IoT devices

IoT Network

Check Point
SOFTWARE TECHNOLOGIES LTD.

Automatically Identify and Profile IoT Devices

HEALTHCARE

INDUSTRIAL
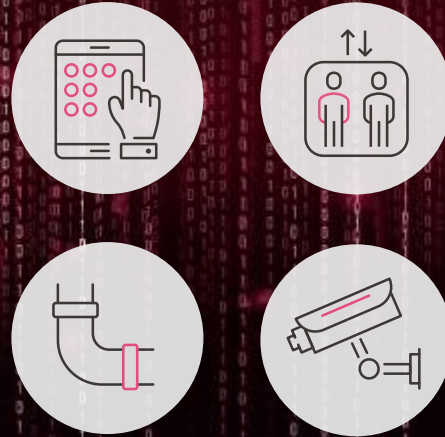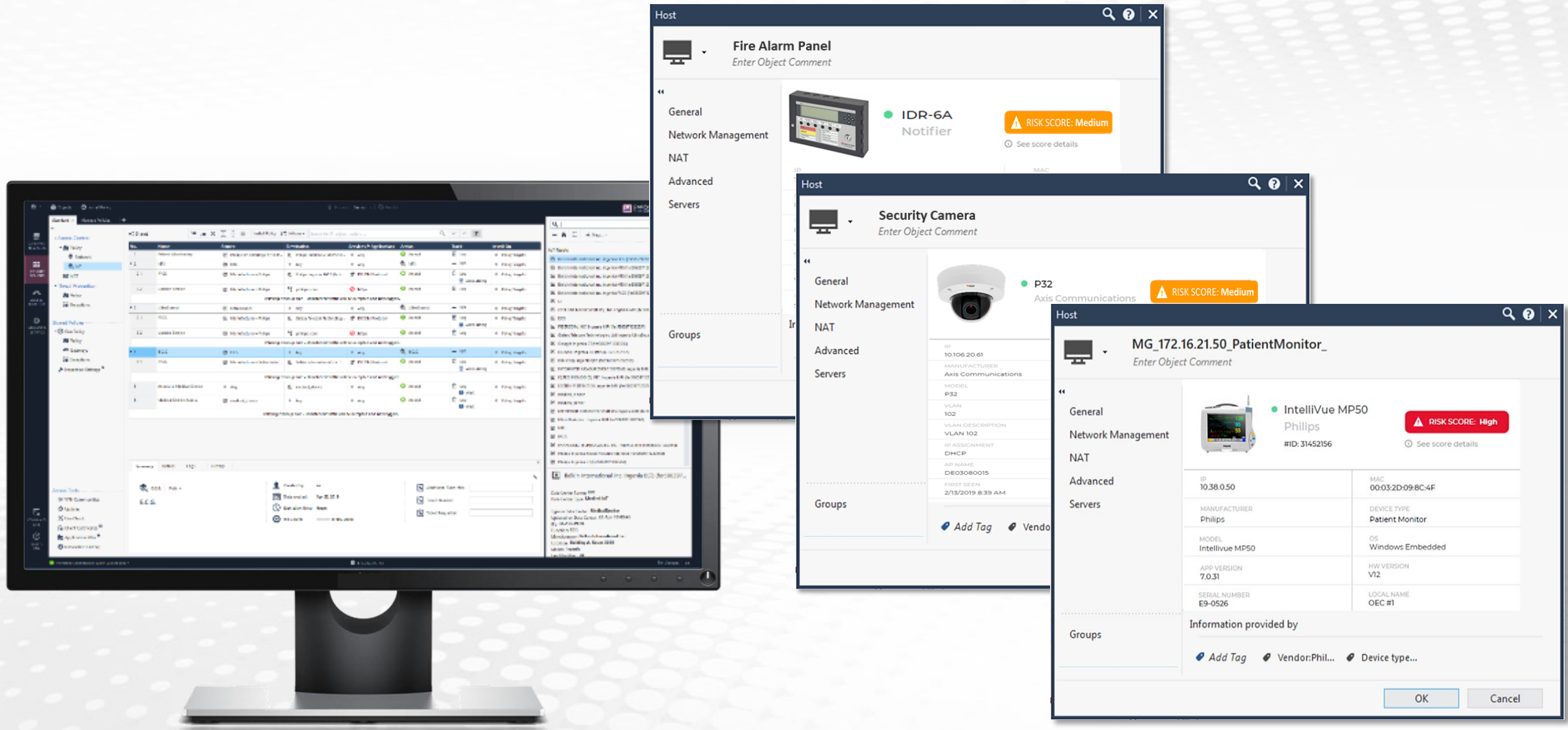
ENTERPRISE

Dedicated discovery engines perfectly suited for the different IoT environments

Deep Insight Information per Device

Set Risk Score for each Device

Risk Parameters

CVE

OS & Firmware

Password

Connection Type

Network Risk

Functionality & Severity

Risk Analyzer

⚠ RISK SCORE: **High**

⚠ RISK SCORE: **Medium**

⚠ RISK SCORE: **Low**
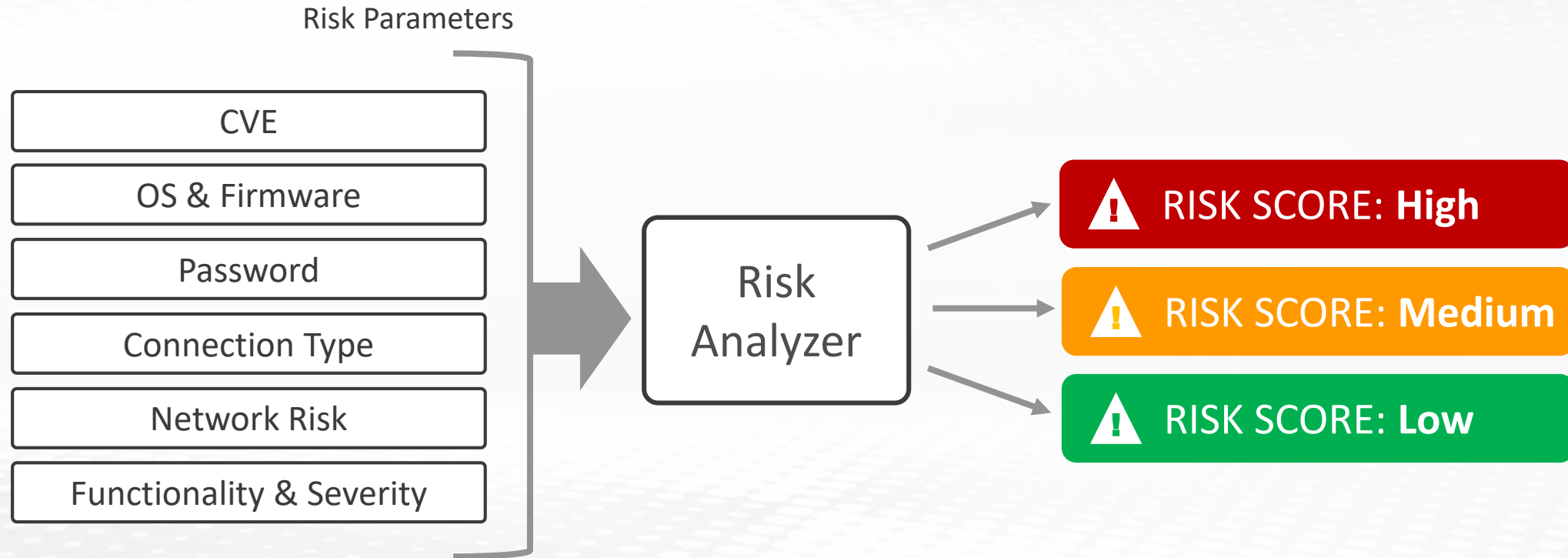
Standard ✕ | Manage Policies | +

Access Control
- Policy
  - Network
  - **IoT**
  - NAT
- Threat Prevention
  - Policy
  - Ex...

Separate IoT Security Layer

Shared

Install Policy | Actions ▾ | Search for IP, object, action, ...

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Patient Monitoring	Philips IntelliBridge EC10 P...	Philips IntelliVue MX450 P...	Any	Accept	Log	Policy Targets
▾ 2	MRI	MRI	Any	Any	MRI	N/A	Policy Targets
2.1	PACS	Manufacturer=Philips	Philips Ingenia PACS (fer5...	DICOM Protocol	Accept	Log / Accounting	Policy Targets
2.2	Update Service	Manufacturer=Philips	.philips.com	https	Accept	Log	Policy Targets
				Missing cleanup rule - Unmatched traffic will be accepted and not logged.			
		UltraSound	Any	Any	UltraSound	N/A	Policy Targets
		Manufacturer=Philips	Galaxy Telecom Technolog...	DICOM Protocol	Accept	Log / Accounting	Policy Targets
		Manufacturer=Philips	.philips.com	https	Accept	Log	Policy Targets
				Missing cleanup rule - Unmatched traffic will be accepted and not logged.			
▾ 4	E.C.G.	ECG	Any	Any	E.C.G.	N/A	Policy Targets
4.1	PACS	Manufacturer=Belkin Inter...	Belkin International Inc. I...	DICOM Protocol	Accept	Log / Accounting	Policy Targets
				Missing cleanup rule - Unmatched traffic will be accepted and not logged.			
5	Access to Medical Device	Any	medical_device	Any	Accept	Log / Alert	Policy Targets
6	Medical Device Access	medical_device	Any	Any	Accept	Log / Alert	Policy Targets
				Missing cleanup rule - Unmatched traffic will be accepted and not logged.			

IoT Security Rules

Shared Po...
- Geo...
  - Policy
  - Gateways
  - Exceptions
  - Inspection Settings

Summary | Details | Logs | History

E.C.G. | Rule 4

E.C.G.

Created by: aa
Date created: Apr 22, 2019
Expiration time: Never
Hit Count: 0 (0%, Zero)

Additional Rule Info:
Ticket Number:
Ticket Requester:

Access Tools
- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application Wiki
- Installation History

GATEWAYS & SERVERS
SECURITY POLICIES
LOGS & MONITOR
MANAGE & SETTINGS
COMMAND LINE
WHAT'S NEW

IoT Assets — 37

- Belkin International Inc. Ingenia ECG (fer5863971282557)
- Belkin International Inc. Ingenia MRI (fer5863971282566)
- Belkin International Inc. Ingenia MRI (fer5863971282566)
- Belkin International Inc. Ingenia MRI (fer5863971282566)
- Belkin International Inc. Ingenia PACS (fer5863971282566)
- CT
- CYCLONE MICROSYSTEMS, INC. Ingenia MRI (fer586397128255d)
- ECG
- FIBERCOM, INC. Ingenia MRI (fer586397128255f)
- Galaxy Telecom Technologies Ltd Ingenia UltraSound (fer586397128...
- Google Ingenia CT (fer5863971282556)
- HUAWEI Ingenia US (fer5863971282555)
- IBM Corp Ingenia Tyto (fer5863971282559)
- INTEGRATED MEASUREMENT SYSTEMS Ingenia MRI (fer58639712825...
- IQ TECHNOLOGIES, INC. Ingenia MRI (fer586397128255e)
- LECTRA SYSTEMES SA Ingenia MRI (fer5863971282562)
- medical_device
- medical_server
- METAPHOR COMPUTER SYSTEMS Ingenia MRI (fer5863971282563)
- MicroBrain,Inc. Ingenia MRI (fer5863971282560)
- MRI
- PACS
- PANASONIC TECHNOLOGIES, INC. Ingenia MRI (fer586397128255b)
- Philips Ingenia Blood Pressure Monitor (fer5863971282558)
- Philips Ingenia CT (fer5863971282554)

Belkin International Inc. Ingenia ECG (fer586397...)

IoT Assets

Data Center Name:
Data Center Type: M
Type in Data Center: **MedicalDevice**
Updated on Data Center: **22-Apr-19 09:45**
IPs: **34.233.39.94**
Function: **ECG**
Manufacturer: **Belkin International Inc.**
Location: **Building A, Room 5030**
Model: **Ingenia**
Last Modifier: aa

Simple and Unified IoT Policy Management

Medical Devices (1-4)

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Patient Monitoring	☐ Philips IntelliBridge EC10 P...	☐ Philips InteliVue MX450 P...	✳ Any	⊕ Accept	🗒 Log	✳ Policy Targets
▾ 2	High Risk	☐ Risk=HIGH	✳ Any	✳ Any	≋ High Risk	— NA	✳ Policy Targets
▾ 2.1	Wireless	☐ Connection=Wireless	🏰 External Zone	✳ Any	⊙ Drop	🗒 Log	✳ Policy Targets
▾ 3	MRI	☐ MRI	✳ Any	✳ Any	≋ MRI	— NA	✳ Policy Targets
▾ 3.1	Wired	☐ Connection=Wired	✳ Any	✳ Any	≋ Wired	— NA	✳ Policy Targets
3.1.1	Philips PACS	☐ Manufacturer=Philips	☐ Philips Ingenia PACS (fer...	⊞ DICOM Protocol	⊕ Accept	🗒 Log 🖩 Accounting	✳ Policy Targets
3.1.2	Philips updates	☐ Manufacturer=Philips	⌁ .philips.updates.com	🌐 https	⊕ Accept	🗒 Log	✳ Policy Targets
▾ 4	E.C.G.	☐ ECG	✳ Any	✳ Any	≋ E.C.G.	— NA	✳ Policy Targets
4.1	E.C.G. PACS	☐ Manufacturer=Belkin Inter...	☐ Belkin International Inc. I...	⊞ DICOM Protocol	⊕ Accept	🗒 Log 🖩 Accounting	✳ Policy Targets

Smart Building (5-6)

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
▾ 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

Security Rules Based on IoT Devices Attributes

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
▼	**Medical Devices (1-4)**						☰
1	Patient Monitoring	☐ Philips IntelliBridge EC10 P...	☐ Philips InteliVue MX450 P...	✳ Any	⊕ Accept	▤ Log	✳ Policy Targets
▼ 2	High Risk	☐ Risk=HIGH	✳ Any	✳ Any	≋ High Risk	— NA	✳ Policy Targets
▼ 2.1	Wireless	☐ Connection=Wireless	⛃ External Zone	✳ Any	◉ Drop	▤ Log	✳ Policy Targets

Medical Devices **High Risk Devices** **Wireless Connected** **Block External Internet Connection**

▼	**Medical Devices (1-4)**			
▼ 2	High Risk	☐ Risk=HIGH	✳ Any	✳ Any	≋ High Risk
▼ 2.1	Wireless	☐ Connection=Wireless	⛃ External Zone	✳ Any	◉ Drop

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
	Philips updates	☐ Manufacturer=Philips	⛃ .philipsupdates.com	⊕ https	⊕ Accept	▤ Log	✳ Policy Targets
▼ 4	E.C.G.	☐ ECG	✳ Any	✳ Any	≋ E.C.G.	— NA	✳ Policy Targets
4.1	E.C.G. PACS	☐ Manufacturer=Belkin Inter...	☐ Belkin International Inc. I...	▦ DICOM Protocol	⊕ Accept	▤ Log 🖩 Accounting	✳ Policy Targets
▼	**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

Security Rules Based on IoT Devices Attributes

Smart Building

Devices

Source = IP Cameras

Destination = BMS

Accept only ONVIF protocol

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
▼ Medical Devices (1-4)							☰
1	Patient Monitoring	▣ Philips IntelliBridge EC10 P...	▣ Philips InteliVue MX450 P...	✳ Any	⊕ Accept	▤ Log	✳ Policy Targets
▼ 2	High Risk	▣ Risk=HIGH	✳ Any	✳ Any	⧈ High Risk	— NA	✳ Policy Targets

▼ Smart Building (5-6)				☰
▼ 5	IP CAM	▣ IP CAM	✳ Any	✳ Any	⧈ IP CAM
5.1	IP CAM to BMS	▣ IP CAM	▣ BMS	⠿ ONVIF Protocol	⊕ Accept
5.2	Hikvision updates	▣ Manufacture=Hikvision	⤳ .hkvs.updates.com	🌐 https	⊕ Accept

▼ 4	E.C.G.	▣ ECG	✳ Any	✳ Any	⧈ E.C.G.	— NA	✳ Policy Targets
4.1	E.C.G. PACS	▣ Manufacturer=Belkin Inter...	▣ Belkin International Inc. I...	⠿ DICOM Protocol	⊕ Accept	▤ Log	✳ Policy Targets
						▦ Accounting	

Source = Hikvision Cameras

▼ 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

Accept only https

Destination = Hikvision Updates Server

WELCOME TO THE FUTURE OF CYBER SECURITY

©2019 Check Point Software Technologies Ltd.