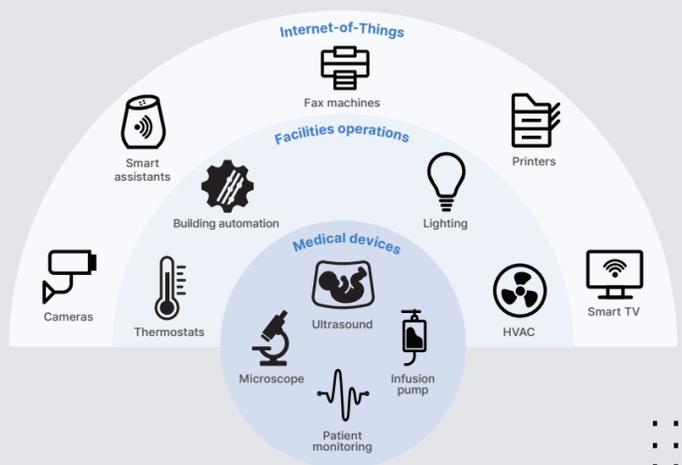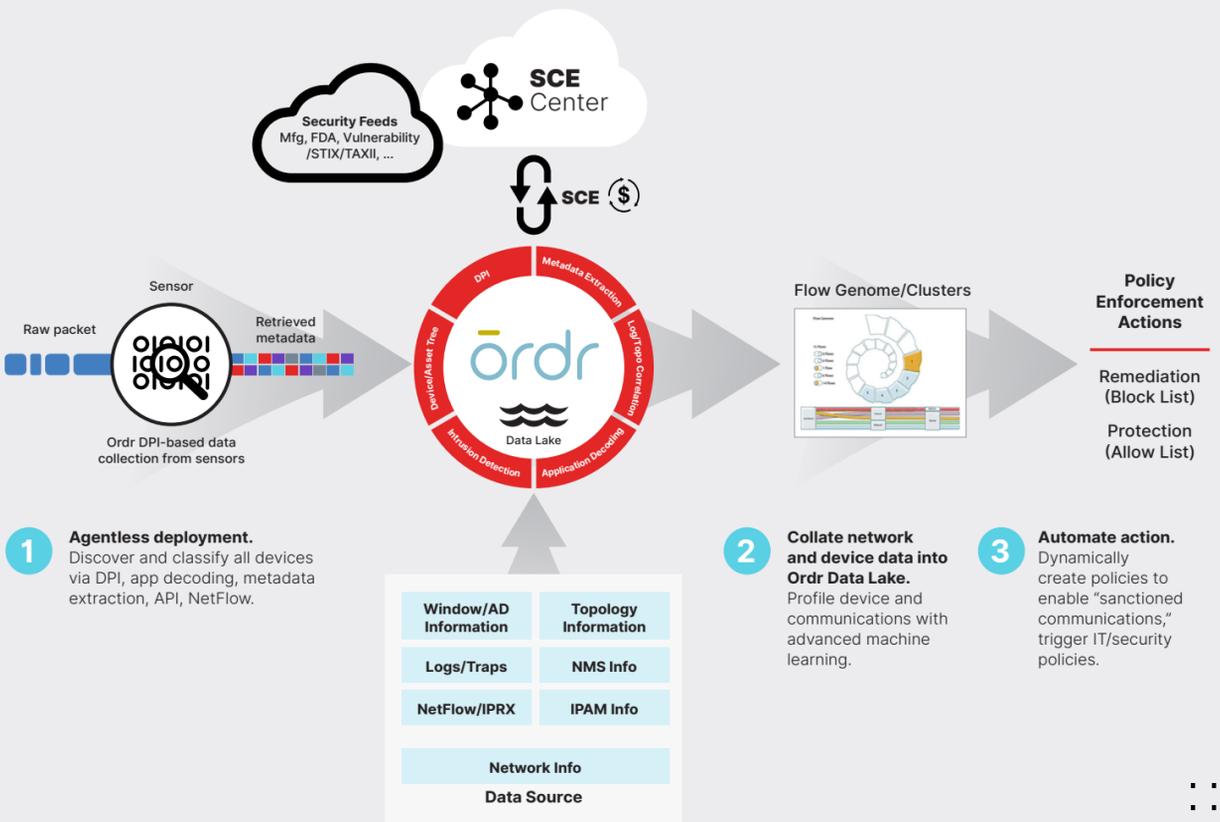# 3 Steps to a Whole Hospital Approach to Discover and Secure Every Device

The Fortinet FortiGate, FortiManager, and FortiNAC integration with Ordr SCE allows customers to reduce the amount of time spent on establishing a proper asset inventory, establishing where those assets are communicating, and creating firewall and NAC segmentation policies. Further, the integration allows for automated segmentation and microsegmentation.

Internet-of-Things
- Fax machines
- Smart assistants
- Printers

Facilities operations
- Building automation
- Lighting

Medical devices
- Cameras
- Thermostats
- Microscope
- Ultrasound
- Infusion pump
- HVAC
- Smart TV
- Patient monitoring

1 Discover and Classify IoMT, IoT, IT, OT Devices

SCE Center

Security Feeds
Mfg, FDA, Vulnerability /STIX/TAXII, ...

SCE ($)

Raw packet

Sensor

Retrieved metadata

Ordr DPI-based data collection from sensors

ördr Data Lake

DPI · Metadata Extraction · Intrusion Detection · Application Decoding · Monitoring (Meta Data) · Device/Asset Tree

Flow Genome/Clusters

Policy Enforcement Actions

Remediation (Block List)
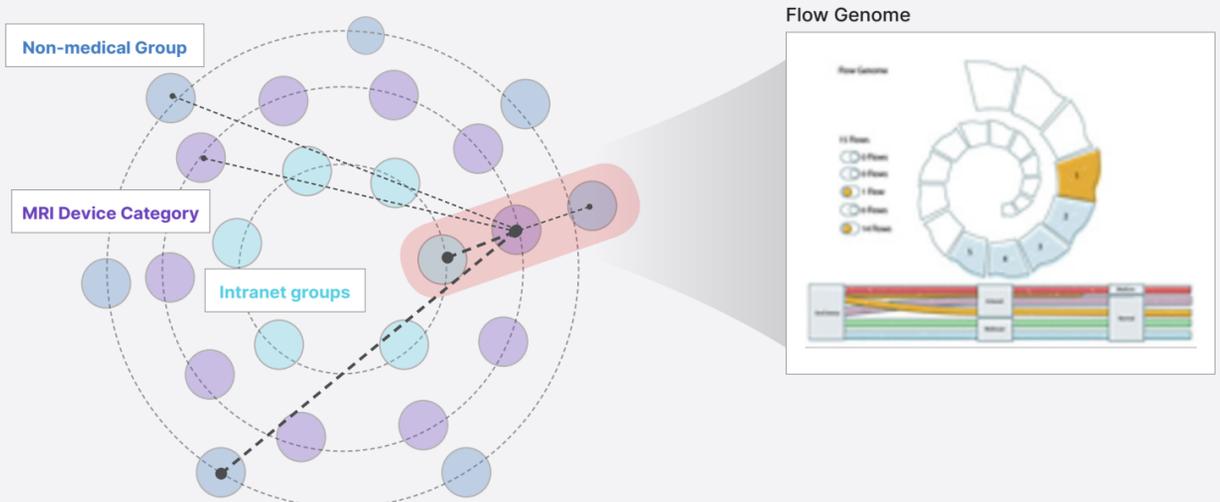
Protection (Allow List)

1 Agentless deployment. Discover and classify all devices via DPI, app decoding, metadata extraction, API, NetFlow.
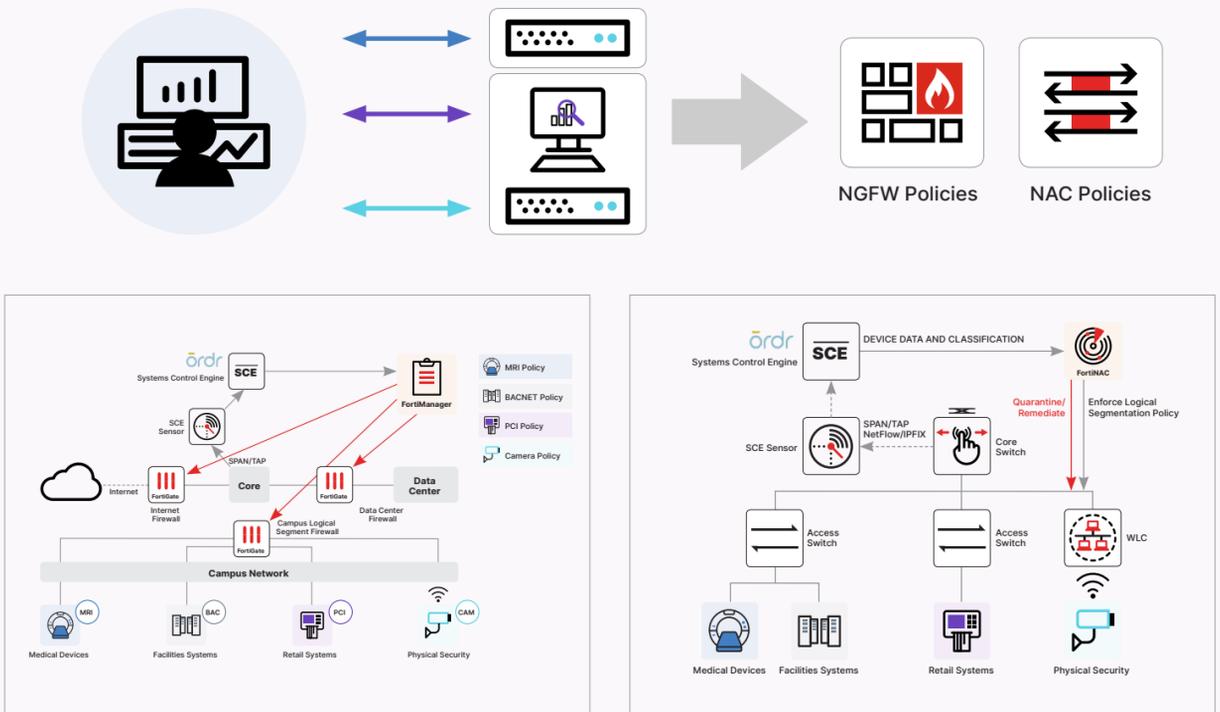
2 Collate network and device data into Ordr Data Lake. Profile device and communications with advanced machine learning.

3 Automate action. Dynamically create policies to enable "sanctioned communications," trigger IT/security policies.

Window/AD Information	Topology Information
Logs/Traps	NMS Info
NetFlow/IPRX	IPAM Info
Network Info	
Data Source	

2 Understand Behaviors and Set Baselines

- Non-medical Group
- MRI Device Category
- Intranet groups

Flow Genome

3 Automate Firewall and Segmentation Policies

NGFW Policies

NAC Policies

The largest private healthcare organization in the United States with 170 buildings and 500,000 devices uses Fortinet and Ordr for visibility and security of their network connected devices.

For more information, contact **FortinetFederal@Fortinet.com**.