Mayo Clinic Efforts to Secure Connected Medical Devices and HIoT

August 27, 2020

Keith Whitby

Pandian Gnanaprakasam

Keith Whitby, MBA, CHTM

About the speakers

Keith has worked at Mayo Clinic for over 22 years in several different support and leadership roles. He is currently the Section Head of Healthcare Technology Management Cybersecurity and Operations. Keith has also had several other positions in HTM, starting as a Unit Manager of the X-Ray equipment service group and most recently as the Section Head for Enterprise Lab, Research, and Ophthalmology Service. Prior to his roles in HTM, he worked in Surgical Services as a Core and Prosthesis Supervisor, and as a Surgical Process/Systems Analyst.

During his time at Mayo, Keith has had extensive experience collaborating on several multidisciplinary teams. He has demonstrated a commitment to customer service, strong leadership skills, and experience with process analysis, project management, and technical support. During his tenure in Surgical Services and HTM, he has been exposed to the depth and breadth of medical equipment in a large healthcare organization. This includes the use of, service and support on, and the operationalization of cybersecurity for a wide range of medical equipment and HIoT technology

Pandian Gnanaprakasam, MS

About the speakers

Pandian Gnanaprakasam currently serves as Chief Product Officer at ORDR Inc., an agentless devices security startup company, that he co-founded. Before the current role, he was the Chief Development Officer at Aruba, responsible for all of engineering and product management functions. Aruba, is an enterprise mobile wireless company, which got acquired by HPE for $3 Billion in March 2015.

With 20 years of engineering and product management experience, Pandian has held various engineering management roles in Cisco Systems, a computer networking company. During his long career at Cisco, Pandian worked on various networking products, that includes routers, switches, WiFi, security and others. Before departing for Aruba, Pandian served as the head of engineering for Cisco's WiFi product line taking the business unit to multi-billion dollar run rate. Before that, he was also the vice president of engineering for the low-end switching, a very successful product line, that has also reached several billion dollars' annual run rate.

Pandian graduated with a Master's degree in Electrical Engineering from IIT, Chennai, India and holds several patents to his credit in various networking technologies.

Mayo Clinic – At a Glance

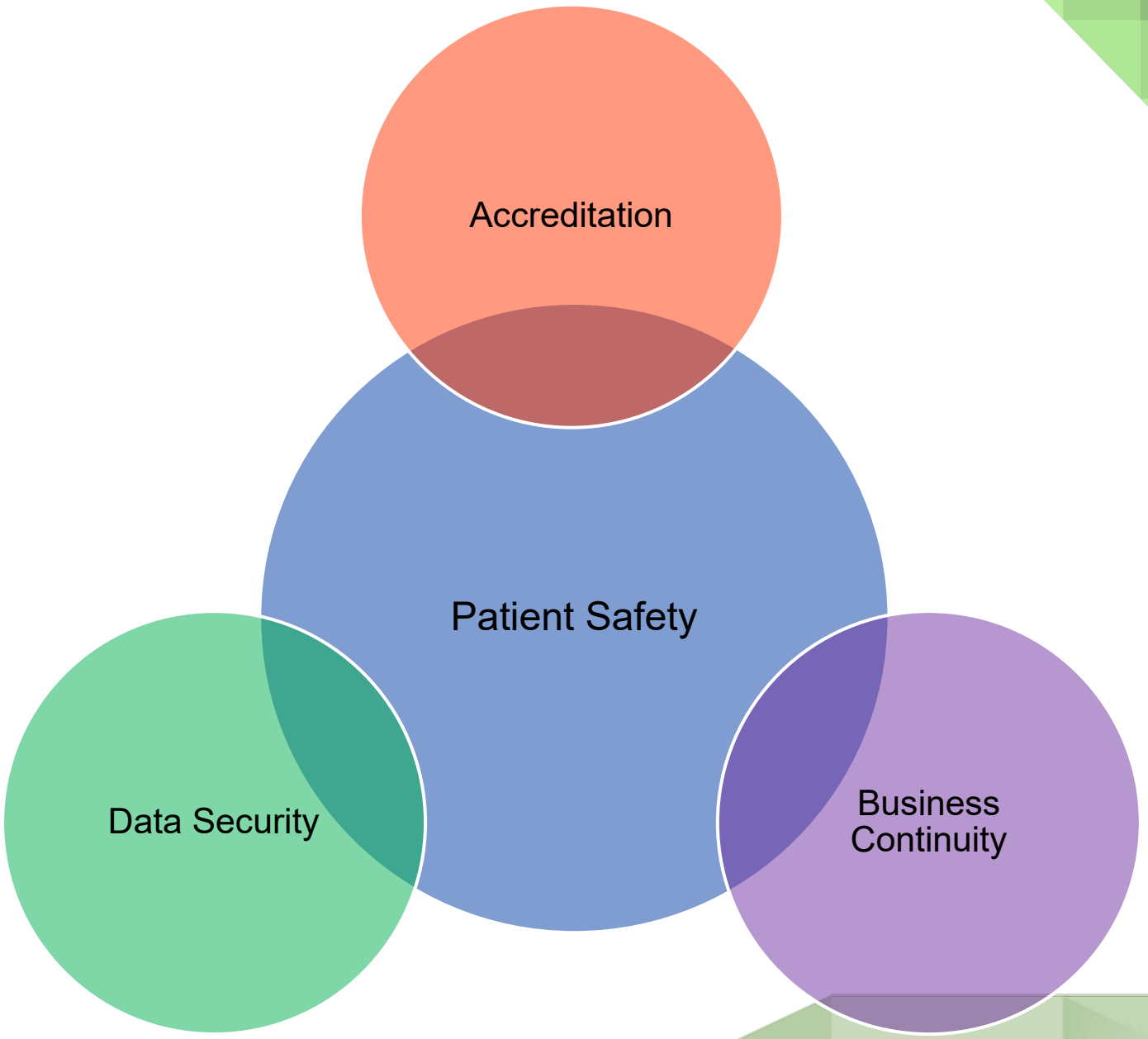
Mayo Priorities

Mission:

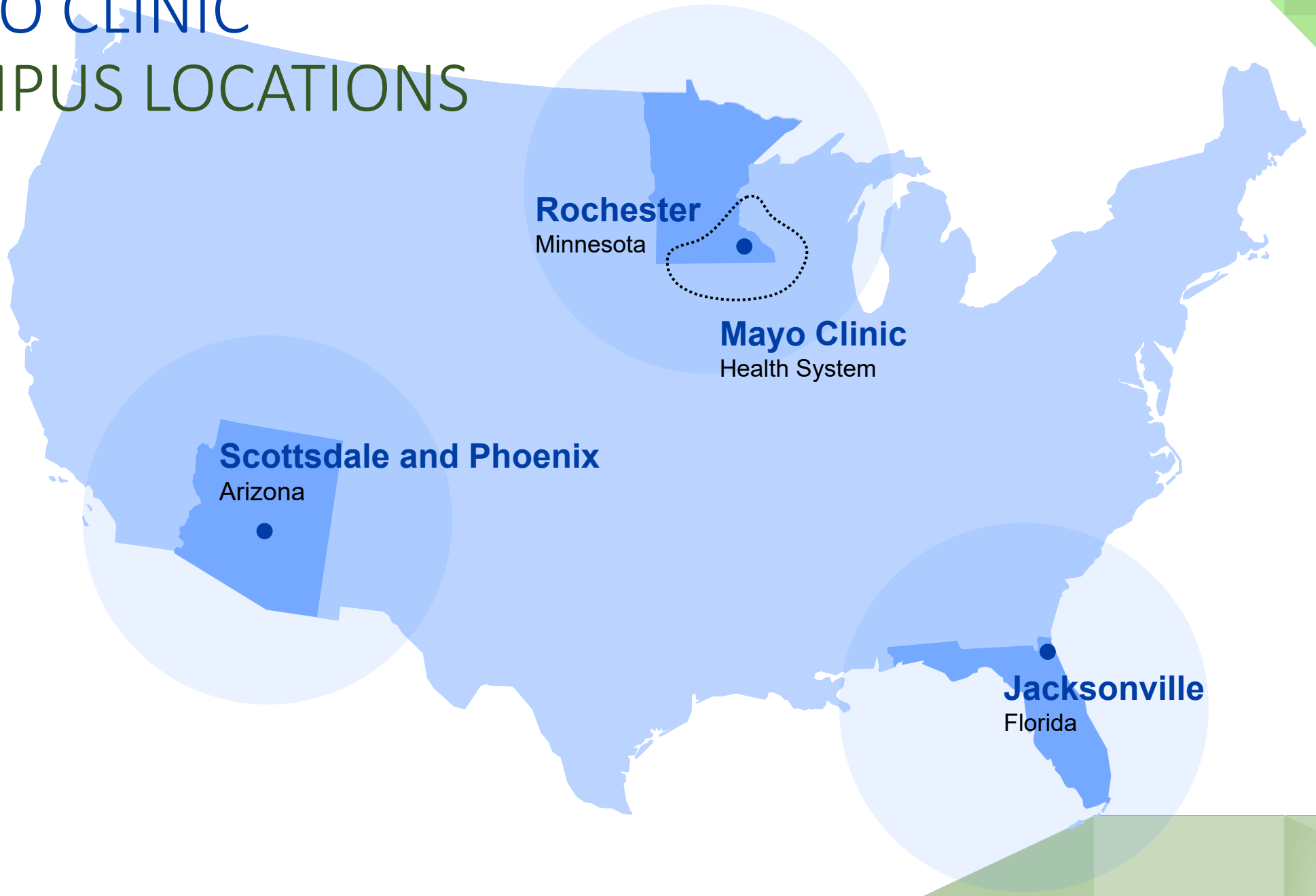
To inspire hope and contribute to health and well-being by providing the best care to every patient through integrated clinical practice, education and research

Primary value:

The needs of the patient come first.

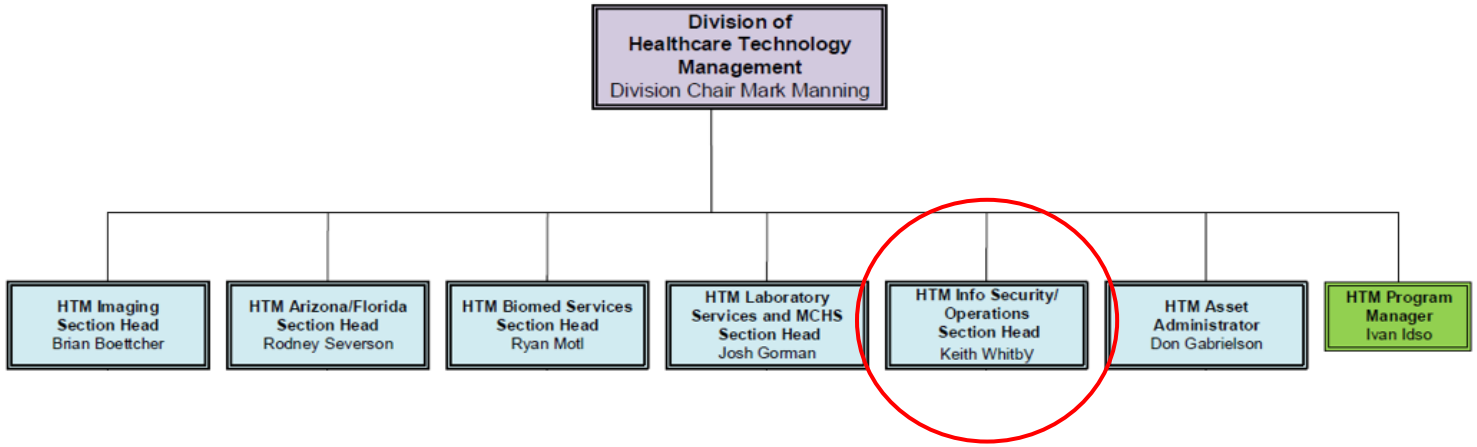


MAYO CLINIC
CAMPUS LOCATIONS



HTM Organizational Structure

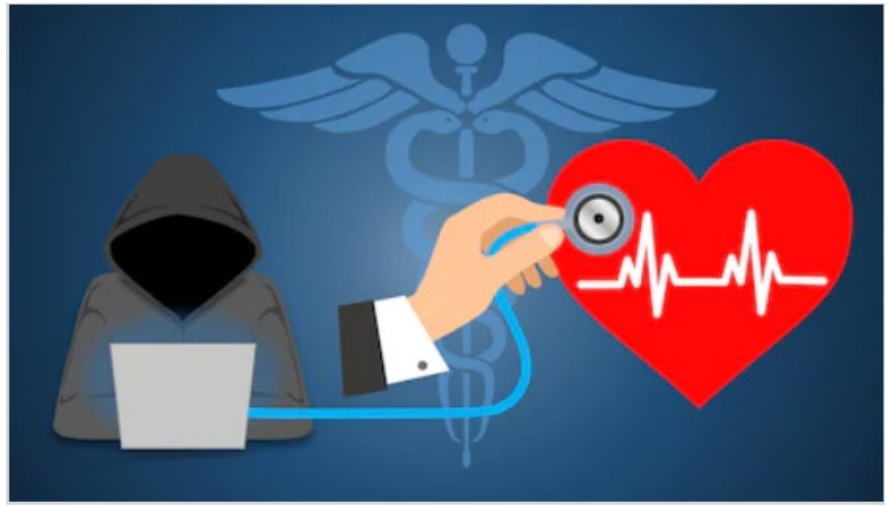
- **~280 HTM Staff: ~220** Biomed technicians, **~20** Managers & **~40** Support staff
- **26 Shops** providing services in over **66** communities, and spanning **5** states
- **Over 130,000** medical devices and systems inventoried, and valued at approximately **$2B**
- **Heavy focus on in-house service and support, contract reduction/elimination, cost avoidance**



Historical Gaps and Challenges Related to Medical Device Cybersecurity

GAPS

- OIS--Industry leading intake and assessment process
- Excellent security knowledge, but limited operational resources or expertise
- Asset specific security assessment with findings:
  - –Mitigating control requirements
  - –Many were vendor dependent
  - –Many could never happen
  - –Asset by asset approach had very limited impact on fleet risk
  - –Who should be “doing the new work”?
  - –No standard operational framework or processes



Unique Nature of Medical Devices/Systems and HIoT

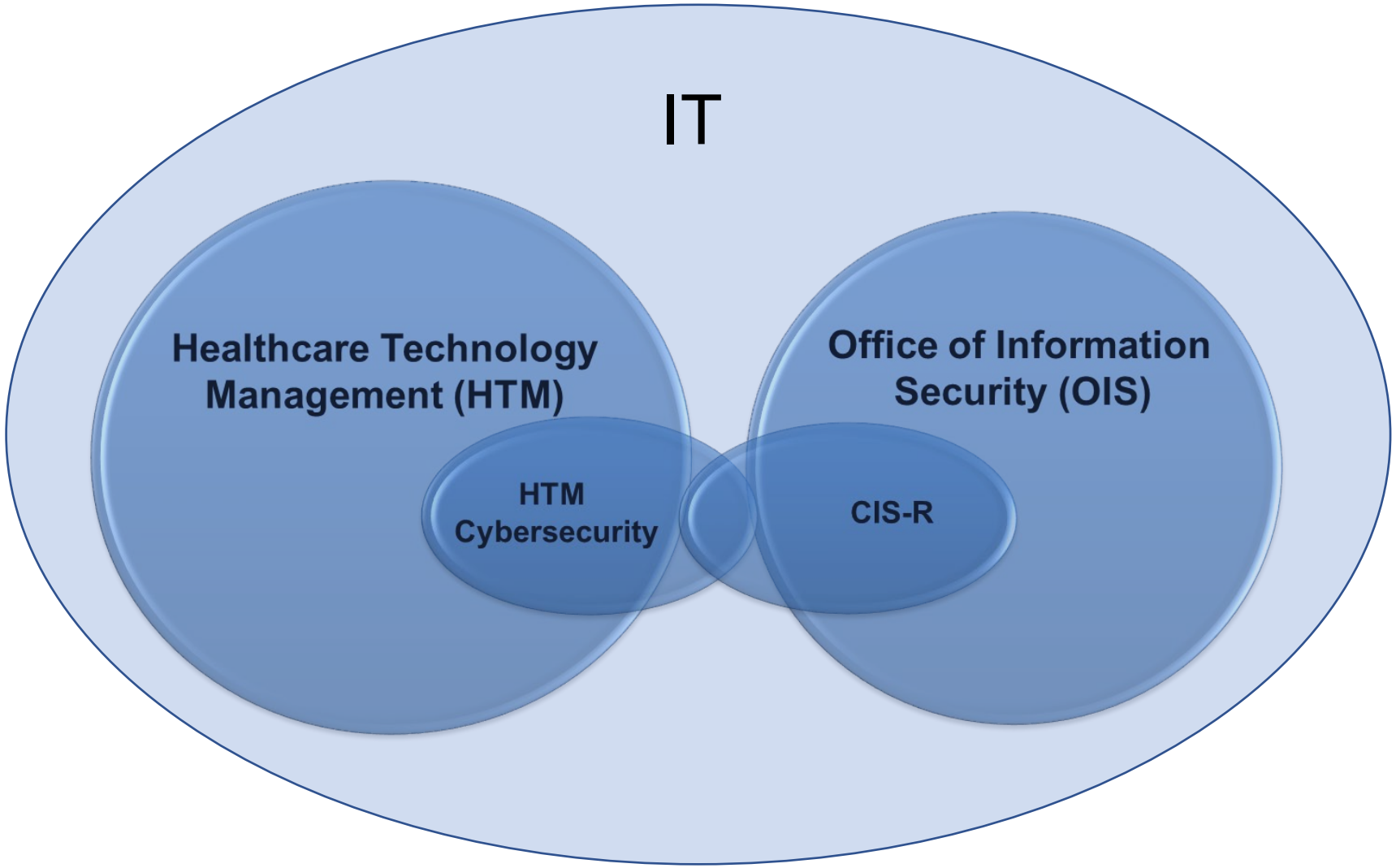
- **Regulatory guidelines (FDA, CAP, JCAHO)**
- Complex systems
- Critical to patient care
- Research and testing
- Vendor validation prior to Mayo action
- **Manual, resource intensive patching process**
- Access to devices
- Lack of “IT” like deployment options
- Specialized skills required
- **Lack of vendor urgency**
- Outdated/Unsupported Devices
- **Largely unable to scan with standard tools**
- Service keys required
- **Unable to load agents**

Security Challenges
HDO Size and Scope

- Significant geographical implications—5 States, 26 Shops, Over 300 Buildings
- Roughly 50,000+ Network Connected Medical, Lab, Research, and HIoT Devices
  - Hundreds of Vendors
  - Thousands of Models
- Inventory discrepancies
  - Determining ownership: Who's responsible for capturing, verifying, and maintaining critical attributes? Who's responsible for tracking, documenting, and applying controls/patches?
  - Mismatched data—CMMS vs. Cisco ISE
  - Are all network connected medical devices inventoried?

The Cybersecurity Team Within HTM

Organizational Fit



HTM Role in Cybersecurity

- Operationalize Security on Medical Equipment and Systems
  - Structured
  - Standardized approach
  - Economies of Scale
- Also….Facilities Operations and HIoT
- Ensure that equipment is functional and optimized in order to meet organizational--patient safety, business continuity, regulatory, and cybersecurity requirements.
- Accountability through the entire technology lifecycle
  - Visibility
  - Monitoring
  - Action

Align Efforts to Industry Standards

Mapping of HTM Activities to NIST and AAMI Guidelines

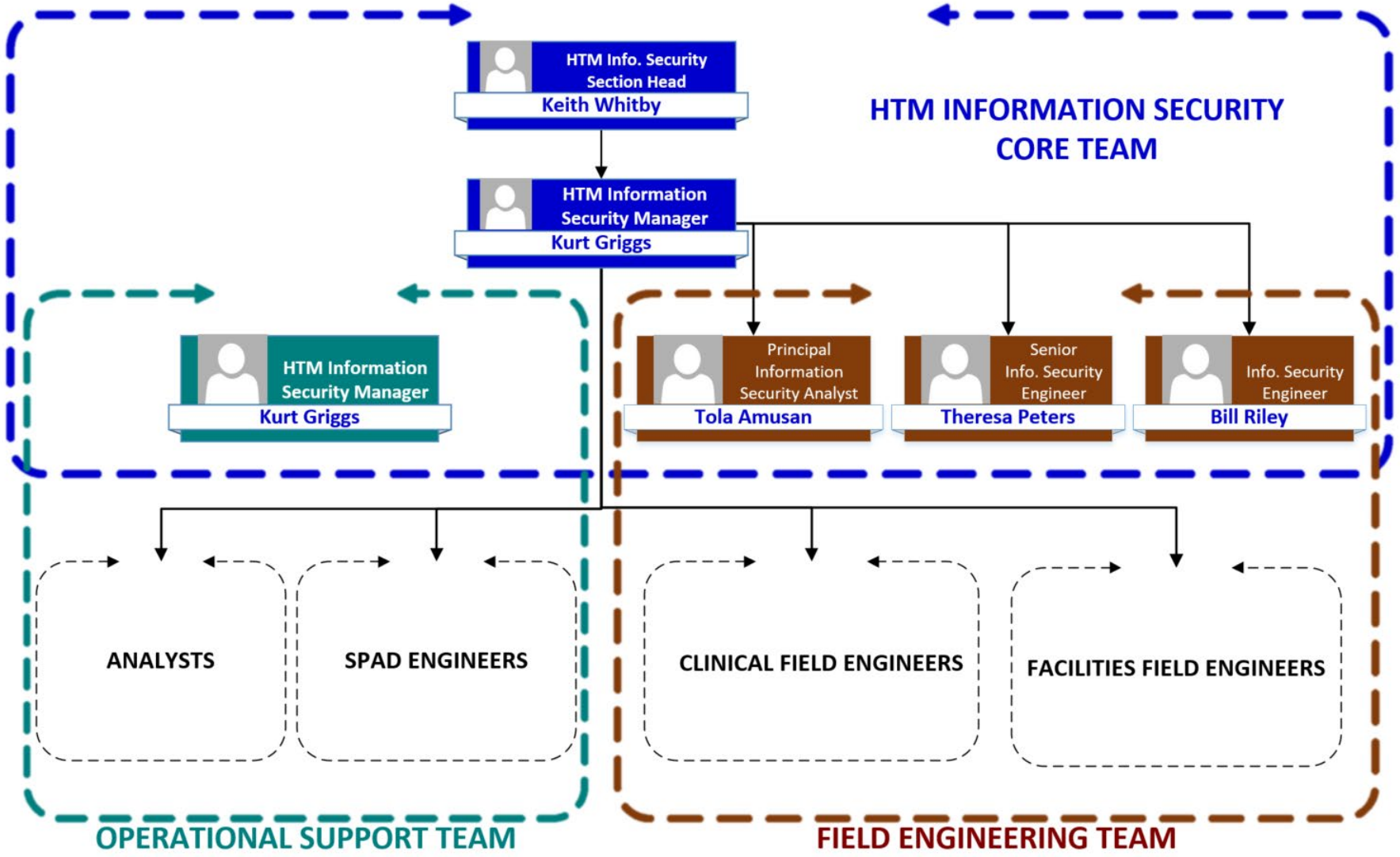
- Matching will not always be explicit
- Identify unmatched activities
- Reverse map to close gaps
- Identify lines of responsibility (OIS, HTM)

Many of the Mayo activities leverage automated asset, flow identification and security tools (Ordr)

ACT ID	ACTIVITY	NIST CSF	AAMI
ACT.1	Governance Framework (HTM, MDOG, Security Committee)	ID.BE-3-5; ID.GV-3-4; ID.RM-2-3; RC.CO-1-2	A-2
ACT.2	Security Framework	ID.BE-2; ID.BE-3	A-2, A-4
ACT.3	Human Resources	ID.AM-6	A-2, A-4
ACT.4	How do we use (7 FTEs)		
ACT.5	Quantifying Effort		
ACT.6	Roles & Responsibilities (HTM, Stakeholders)	AM-6; ID.GV-2; PR.AT-1-2,4-5; RS.AN-1; RS.CO	A-2, A-4
ACT.7	CIS vs HTM (HTM Security vs. HTM Techs)		
ACT.8	Accountability	PR.IP-8; RC.CO-2,3	A-2, A-4, A-7
ACT.9	Develop Definitions and Service Support Levels for Med. Device and Interne		
ACT.10	Metrics		
ACT.11	Development of Information Security Policies	ID.GV-1,3-4; ID.RM-1	A-2
ACT.12	Develop HTM Specific Policies		
ACT.13	Alignment with IT/IS Policies		
ACT.14	Alignment with Industry Policy		
ACT.15	Develop Information Security Processes	ID.GV-1,3-4; ID.RM-1	A-2, A-4
ACT.16	Develop HTM Specific Processes		
ACT.17	Exception Processes		
~~ACT.18~~	~~Approval Processes~~		
ACT.19	Develop HTM Specific Procedures	ID.RM-1	A-2
ACT.20	Incident Response Plan (Including NIST DE/RS event impact related assessm	4; PR.IP-9-10; RS.RP-1; RS.AN-1-2; RS.CO-1; R	A-2, A-6
ACT.21	Emergency Vulnerability Response Plan		
ACT.22	Asset Inventory (Manual, Automated, Granularity)	ID.AM-1; ID.AM-2; ID.AM-4	A-1, A-2, A-4, A-7
ACT.23	Discovery Tool		

One-to-One mapping

MAYO/HTM Information Security Team



Core Team

- Develop NIST and AAMI based security framework for HTM and HIoT
- Develop standardized security processes and procedures
- Assist with projects (NAC and Segmentation Efforts, med device security tool testing)
- High End Resource for Associate Eng, Technicians, and Clinical Groups
- Develop and guide HTM vulnerability management program
- Construct and maintain fleet-level comprehensive cyber risk scoring
- Engage with industry groups and participate in initiatives (FDA, SBOM, CISA)
- Ordr Implementation and Administration
- Automate security workflows

HTM Associate Info Sec Engineers

- Embedded within the local HTM shops
- Security SME for Biomed Techs
- Security point of contact for vendors
- Create procedures for:
  - Compensating Control application
  - Vulnerability mitigation/remediation
- Apply controls to medical devices (as possible)
- Network connectivity SME (NAC, Segmentation, Onboarding)
- Training and education for HTM shops
- Local incident response SME

SPAD (Security, Privacy, Architecture, Data)—”Security Assessment”

- Initial intake triage of all capital and non-capital medical device purchases (~1500 per year)
  - Hardware
  - Software
- Route through the appropriate level of intake assessment
- “White glove” service for purchase proponents
  - Guide proponents through the purchase assessment process
  - Work with vendors to acquire review deliverables
- Collaborate with OIS and the proponent to determine mitigating controls
- Construct Security Lifecycle Profiles (Model Specific Roadmap/Template)

Execution

Proactive Security

Strategic Approach

- Leverage Known Security Incidents (e.g. Malware attack, Ransomware, etc.)
- Leverage Zero Day Vulnerabilities (BlueKeep, DejaBlue, Ripple20)
- Leverage Regulatory Compliance and other Business Opportunities
- Internal Audit Observations
- Next Level of Security Operations
- Governance

Thought: What do we want to do better?

Proactive Security

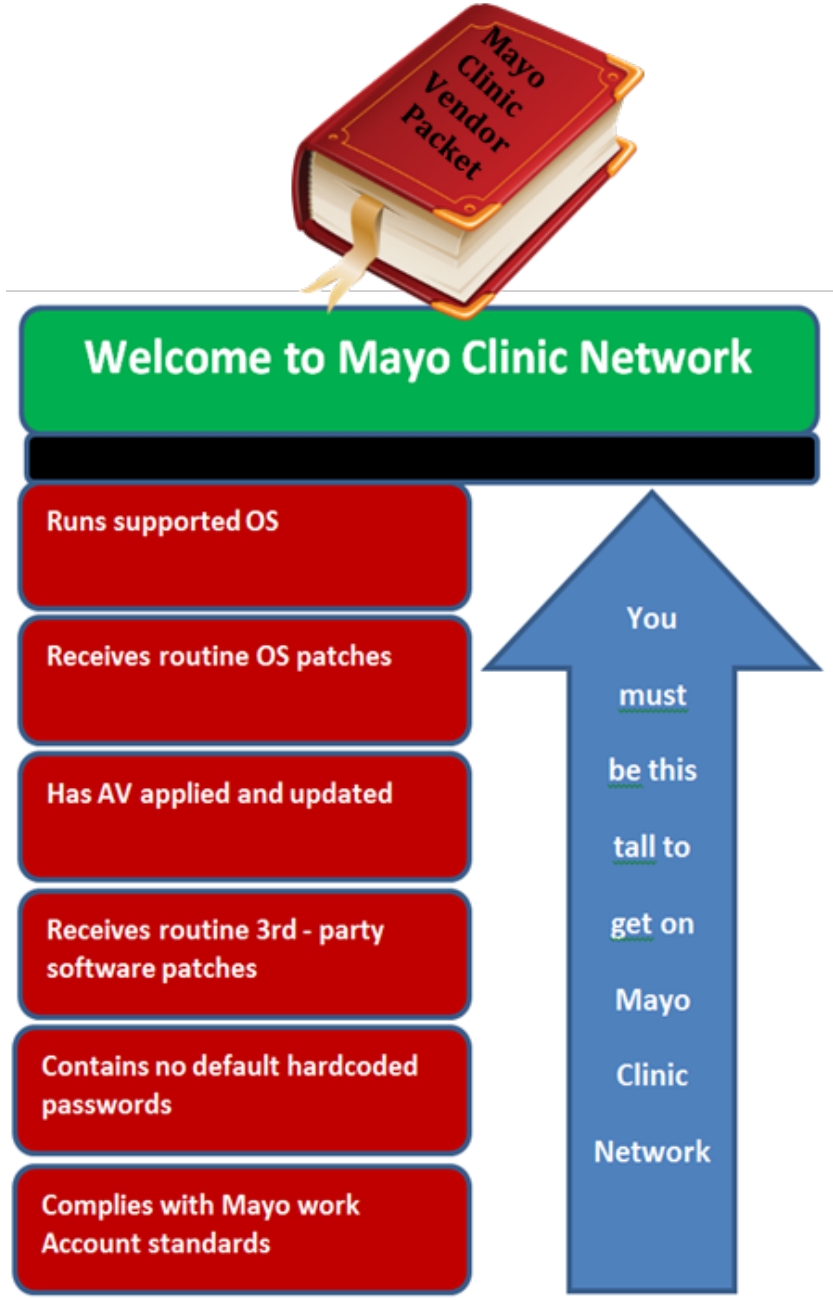
Security Operations within the Equipment Lifecycle

- Perform security risk assessment on device using Mayo's **six baseline security criteria** prior to making purchase decisions. Know what is in the device if to be connected to the network (**sBoM**)
- Work with the vendors to address **device weakness** prior to use
- Deploy, track and apply security mitigations using **device Security Lifecycle Profile** (SLP)
- Address ongoing security issues through a **vulnerability management process** (patching, mitigating controls, etc.)
- Sanitize device after use to prevent unintentional disclosure. Adopt a robust disposition policy and procedure

Proactive Security

Device Security Standard – Pre-Purchase

- Mayo's Six Baseline Security Standard for connectable new device purchases
  - Runs supported OS
  - Receives routine OS patches
  - Has AV applied and updated
  - Receives routine 3rd - party software patches
  - Contains no default hardcoded passwords
  - Complies with Mayo work Account standards
- Test/Assess new device before purchase
- Document security weakness and work with vendors to address the weaknesses



Proactive Security

Security Lifecycle Profile (SLP) – Deployment

- Document the device onboarding procedure
- Include pre-determined security controls as part of the deployment
- Assign ownership
- Address device risk by type and by model
- Reduce deployment variation- standardize and centralize the process
- Work Orders are tied to remediation tasks
- Remediation ties back to the findings
- Support risk model and quantification

Thought: Security-specific Service Manual

< Device Name> - Security Lifecycle Profile Procedure

Scope

The scope of this procedure is for the Healthcare Technology Management (HTM) staff responsible for the lifecycle management related to the device security.

Purpose

This procedure documents the lifecycle management security activities from deployment to disposal, to mitigate the security risks specific to the device/system.

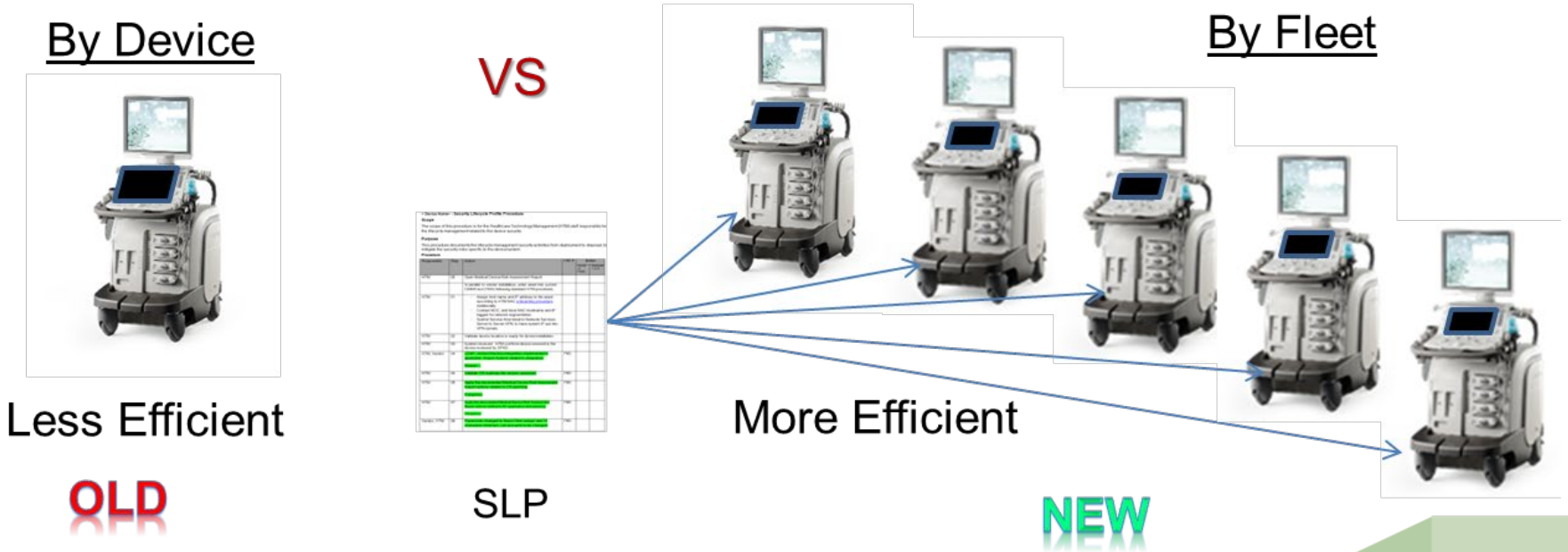
Procedure

Responsible	Step	Action	FND #	Action	
				(Asset or Fleet)	Deployed Y or N
HTM	00	Open Medical Device Risk Assessment Report.			
		In parallel to vendor installation, enter asset into current CMMS tool (TMS) following standard HTM processes.			
HTM	01	- Assign host name and IP address to the asset according to HTM NAC onboarding procedure. Additionally: - Contact NOC, and have NAC Hostname and IP tagged for network segmentation. - Submit Service-Now ticket to Network Services: Server to Server VPN, to have system IP put into VPN tunnels.			
HTM	02	Validate device location is ready for device installation.			
HTM	03	System received. HTM confirms device received is the device reviewed by SPAD.			
HTM, Vendor	04	LDAP - Active Directory integration implemented if applicable. Report Actions related to integration. Reason –	FND-		
HTM	05	Validate OS matches the version assessed.	FND-		
HTM	06	Apply the documented Medical Device Risk Assessment Report actions related to OS patching. Frequency	FND-		
HTM	07	Apply the documented Medical Device Risk Assessment Report actions related to AV application and patching. Frequency:	FND-		
Vendor, HTM	08	Passwords changed to Mayo Clinic unique and 15 characters minimum. List accounts to be changed.	FND-		

Proactive Security

Adopt Fleet Approach to Security Remediation Efforts

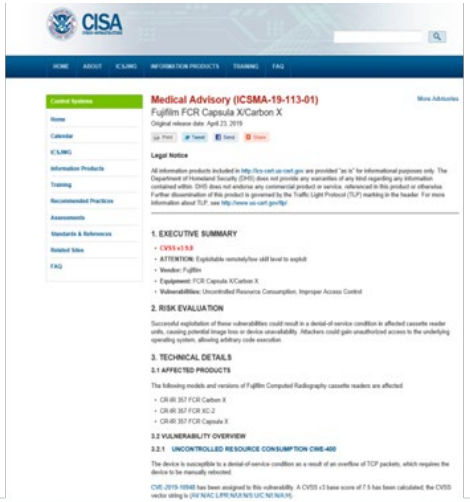
Vendor: ABC Manufacturer
Make: ABCD-123-EXY-Patient-Station
Model: 200/WXseries/Win10SP1



Proactive Security

Vulnerability Management & Remediation Program - Maintenance

- Enhance CMMS asset inventory with attributes for VM activities (e.g. OS, 3rd software, firmware, protocol, etc.)
- Track software vulnerabilities from various sources (Internal or external)
- Prioritize remediation in the context of impacted asset and patient impact, exploitability, exposure, etc.
- Standardize patching procedure; by model, by type; creating work order for tracking completion and status
- Monitor and track status of all remediation
- FDA Post Market Guidance for Patching



Major Activities	HTM Vulnerability & Remediation Management Plan			
	Detect/Discover	Prioritize	Remediate	Report
Asset Inventory/Status	Asset Inventory/Status			
Vulnerability Notification	Vulnerability Notification & Assessment			
Patching/Mitigation	Patching			
Device LifeCycle Risk Profile		Security LifeCyce Profile		
Work Order		Work Order		
Report	Report			

Tools

Key Tools

Operational Tools to Execute and Automate Security Operations

- **Robust CMMS Solution (Lifecycle Maintenance)**
  - Enterprise Asset Management Solution
  - Flexible and robust Work Orders
  - Support Risk scoring and modeling
  - Support vulnerability management module
  - Create device SLPP approach for mitigations efforts
  - Integrate with CMDB and other Enterprise Security tools

nuvolo

Key Tools

Operational tools to execute and automate security operations

- **Modern Asset Discovery (Foundational)**
  - Improves quality of data for Asset inventory
  - Capability to detect networked medical devices (including legacy)
  - Robust medical device asset classification
  - Provides insight into connected device actions
  - Supports device security operations
  - Integrates with other Enterprise Security tools
  - Micro-Segmentation

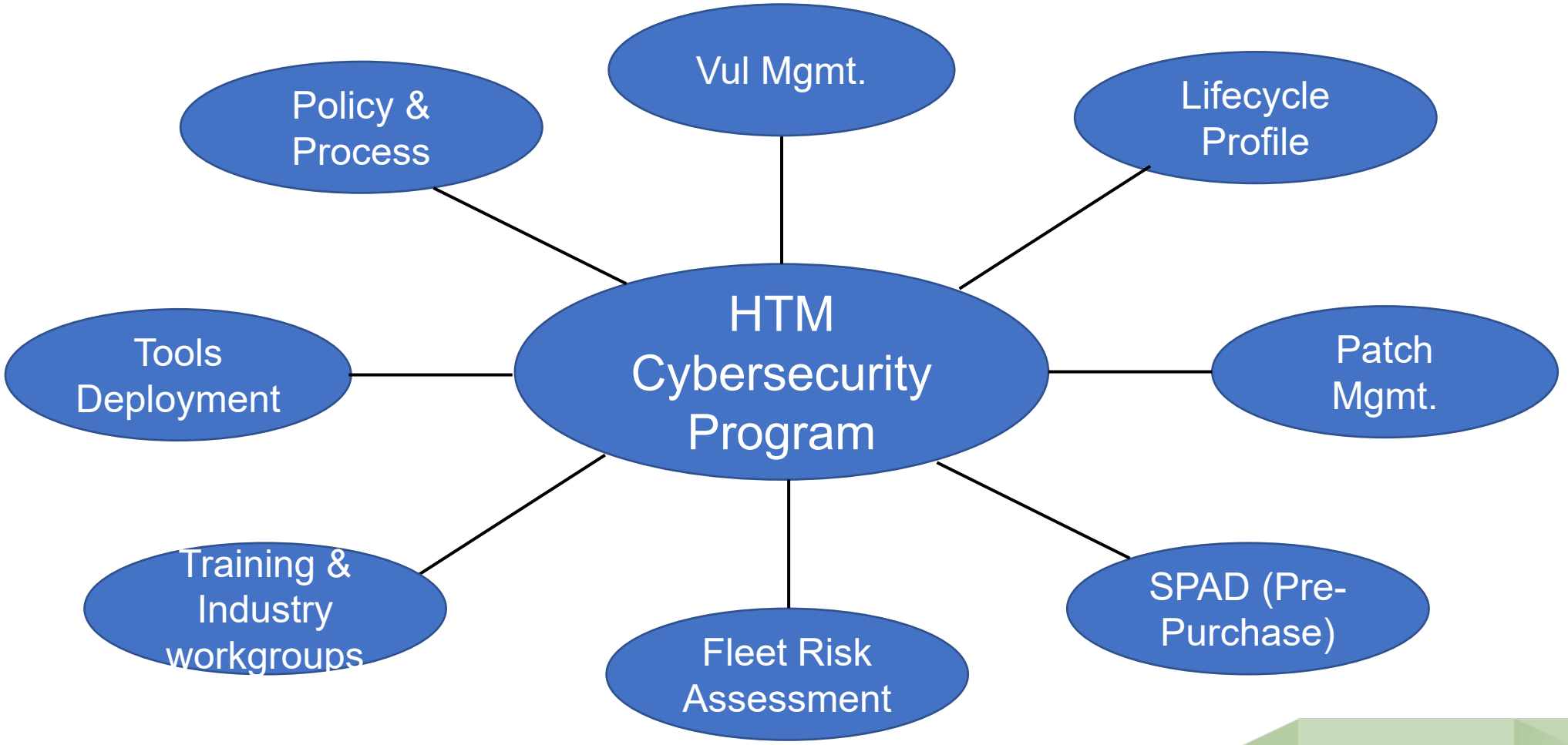
Progress

Two Years…

Program is adding “Security Value”…..

- ✓Significantly Improved Device “**Repeat**” and “**New**” Purchase Turn-around time
- ✓Established an algorithm for **calculating** and determining security risks across the **fleet**.
- ✓Established a mechanism for **tracking** and **applying** security mitigation during device onboarding
- ✓Operationalized the medical device **vulnerability** management program
- ✓Recently launched a medical device patch installation **automation** utility **tool**
- ✓Active participation in the Industry workgroups to contribute to medical device security
- ✓Leveraging Ordr for asset identification and reconciliation, security analysis, VM, and micro-segmentation

Two Years…


Vul Mgmt.
Policy & Process
Lifecycle Profile
HTM Cybersecurity Program
Tools Deployment
Patch Mgmt.
Training & Industry workgroups
Fleet Risk Assessment
SPAD (Pre-Purchase)

About Ordr Inc.

- Founded in 2015 by **Cisco and Aruba Networks** veterans
- **$50M** raised from top investors
- Customers in **North America, Europe and APJ**
- **95%+** customer retention rate
- **Ordr is IoT device security made simple….**
  - Zero agents, zero touch provisioning
  - One comprehensive platform to
    - secure all unmanaged devices (IoT, IoMT, OT)
    - enable the entire device security workflow
    - address the needs of security, networking and device owners

Venture Partners

WiNG · BV Battery Ventures · TENELEVEN · UNUSUAL VENTURES

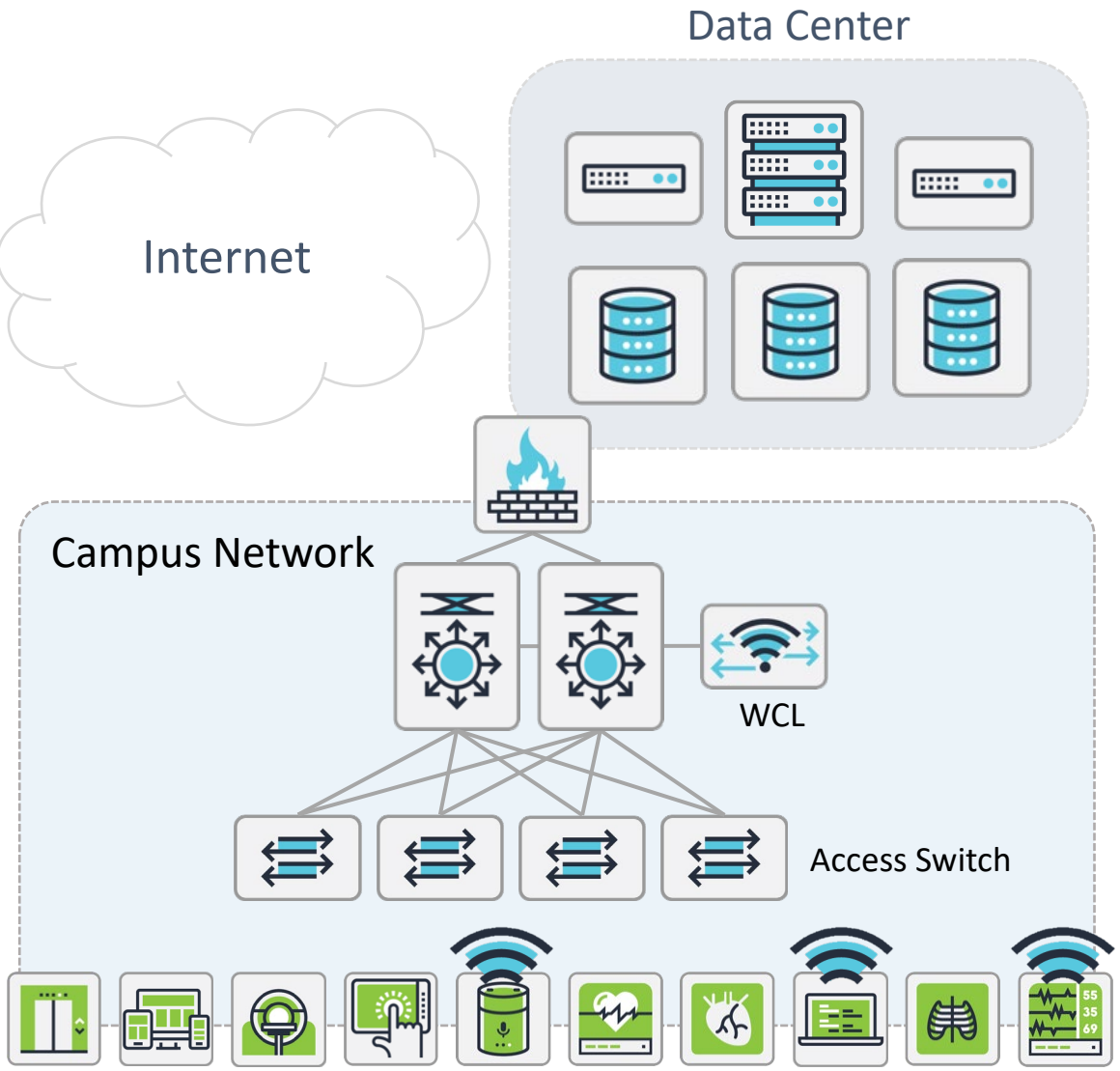
Kaiser Permanente Ventures and Mayo Clinic Invest in Ordr

Additional Series B funding comes as Ordr expands to meet growing demand from all industries for their enterprise IoT and unmanaged device security technology

Ordr Proven In Large Networks, Many Verticals

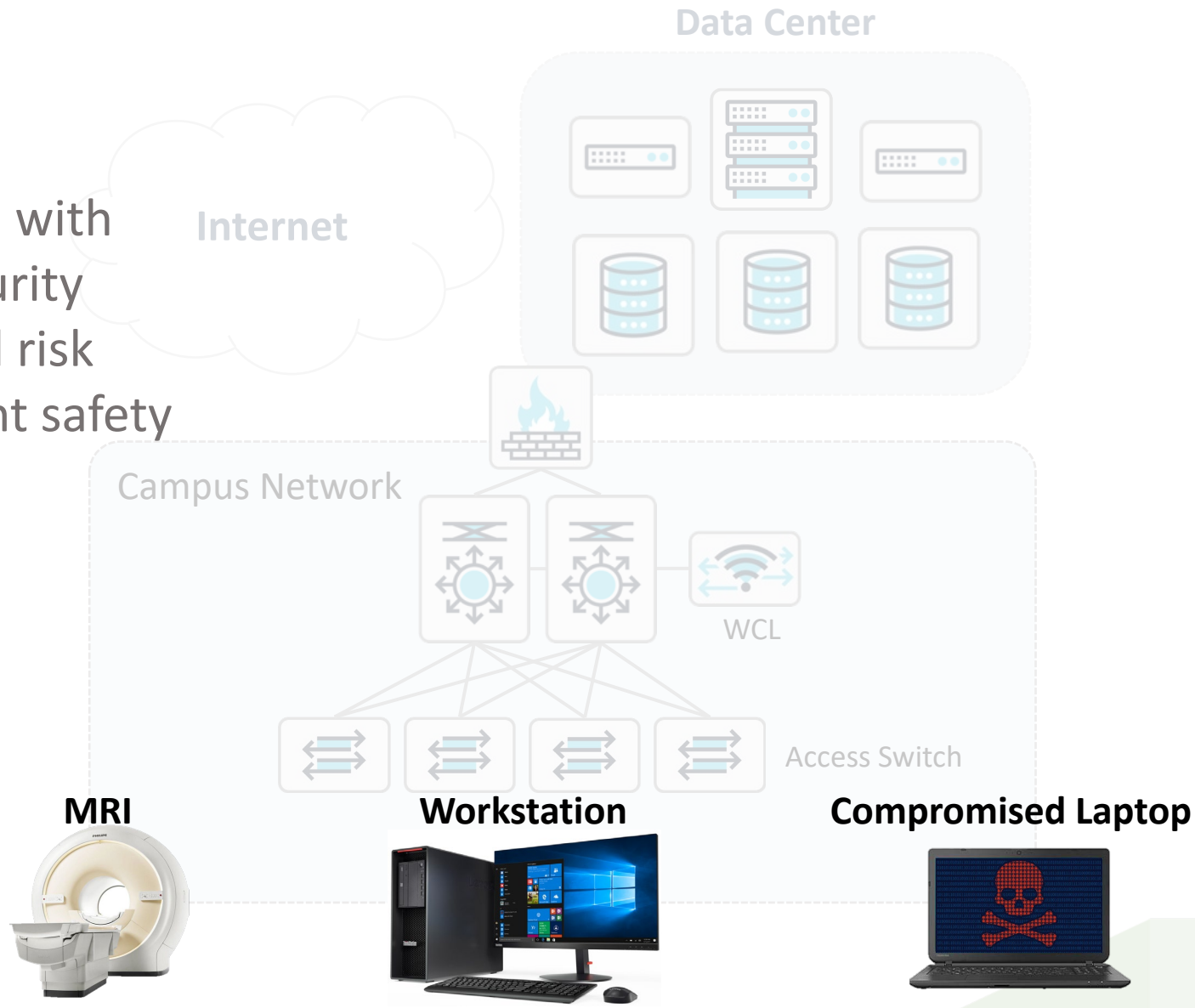
- Mayo Clinic
- Cleveland Clinic
- Ginkgo Bioworks
- Sephora
- Nat'l Institute of Health
- RTC Las Vegas

One Network One Team



360 Degree Enforcement – Complete Accurate Inventory

Inventory augmented with vulnerability and security threats to do detailed risk assessment for patient safety



Foundation - Detailed Info on Med Devices

Data Center

Internet

DEVICE INFORMATION

Mac Address :	7C:94:B2:7B:73:D3
Device Description :	MRI
Manufacturer :	Philips
Model Name/No. :	Ingenia
Serial No. :	PH38700562
OS Type :	RTOS
OS Version :	BSP
SW Version :	DCX R3.1
FQDN :	sflab.philips.643481555.ordr.net
DHCP Hostname :	sflab.philips.643481555
Has PHI :	Yes
DICOM AE Title :	PMRI-14

Asset Detail

FIELD SET 1		FIELD SET 2	
Mac Address :	00:0B:AB:CF:A5:72	Category Description :	Ultrasound System
Asset ID :	1000057831	SubCategory Code :	22757
Segment ID :	4	SubCategory Desc :	Radiography
Asset Number :	64835	Support Status :	
Cost Basis :	45000	Type :	Equipment
Date Accepted :	6/18/08 0:00	Orig Manufacturer Name :	GE HEALTHCARE
Date Created :	6/18/08 12:45	TMS Vendor Code :	102109
Date Purchased :	6/20/08 0:00	TMS Vendor Name :	GE HEALTHCARE
Date Received :	7/20/08 0:00	Warranty Vendor Code :	456354
Date Retired :		Warranty Vendor Name :	GE HEALTHCARE
Description :	ULTRASOUND SYSTEM	Priority :	Need CE/Vendor to come to device
Extended Description :		Item Identifier :	
First Month :		Life Expectancy :	10
Cost Center Code :	RADIO	Location Description :	RADIOLOGY DEPT
Cost Center Desc :	RADIOLOGY DEPT	Serial Number :	203393US6
Building Name :	ABC HEALTHCARE	Model Number :	LOGIQE9
HIPAA - Contains PHI :	Yes	Network Device :	
Location Code :	RADIOLOGY	Options :	
Location Code Desc :	RADIOLOGY DEPT	Original Cost :	
Physical Condition :		Other Number :	
Shop :	Imaging CH	Owner :	
Skill :	Imaging Service Techs	Replacement Cost :	400.0
Status :	Active	Service Manual Loc :	
Category Code :	1773		

Classification / Risk

CONNECTIVITY

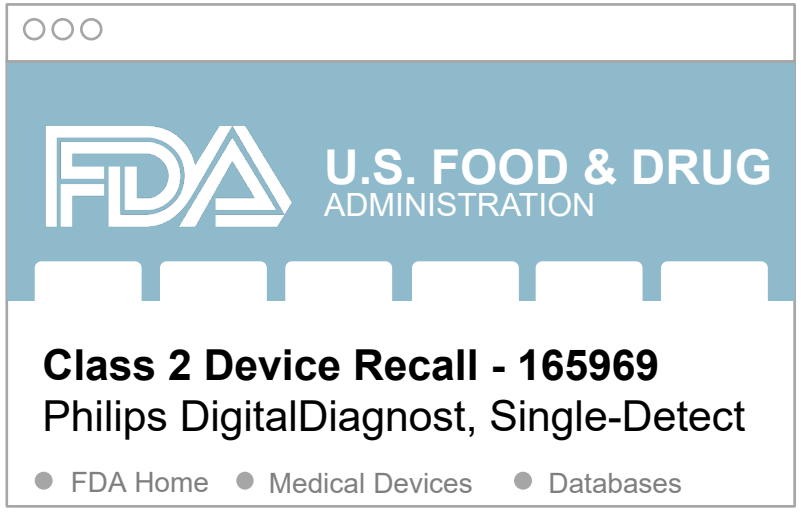
Ordr Sensor :	abc-cpnanalytics-engine
IP Address :	Offline (last IP = 10.20.80.16)
Subnet :	10.20.80.0/21
VLAN :	Vlan(2102)
Access Type :	WIRED
Network Device :	10.172.7.1 (accsw-f01-6)
Access Interface :	GigabitEthernet1/0/4
First Seen :	4/11/2018 9:13:47 AM
Last Seen :	6/18/2018 11:05:03 AM
Location :	Fremont

Network Connectivity

36

Assess Vulnerabilities - Patches, Hotfixes, AV Updates

Criticality: LEVEL_1
Alarm Count: 5
Risk Score: 93
Vulnerability: normal



25 vulnerabilities

ordr take control.

ID	Description
FDA-165969	DigitalDiagnost, Single-Detect (stitching Patient Support) 712062…

Operating System Patches/Updates (10)

No.	Hotfix Id	Description
1	KB4100347	Update

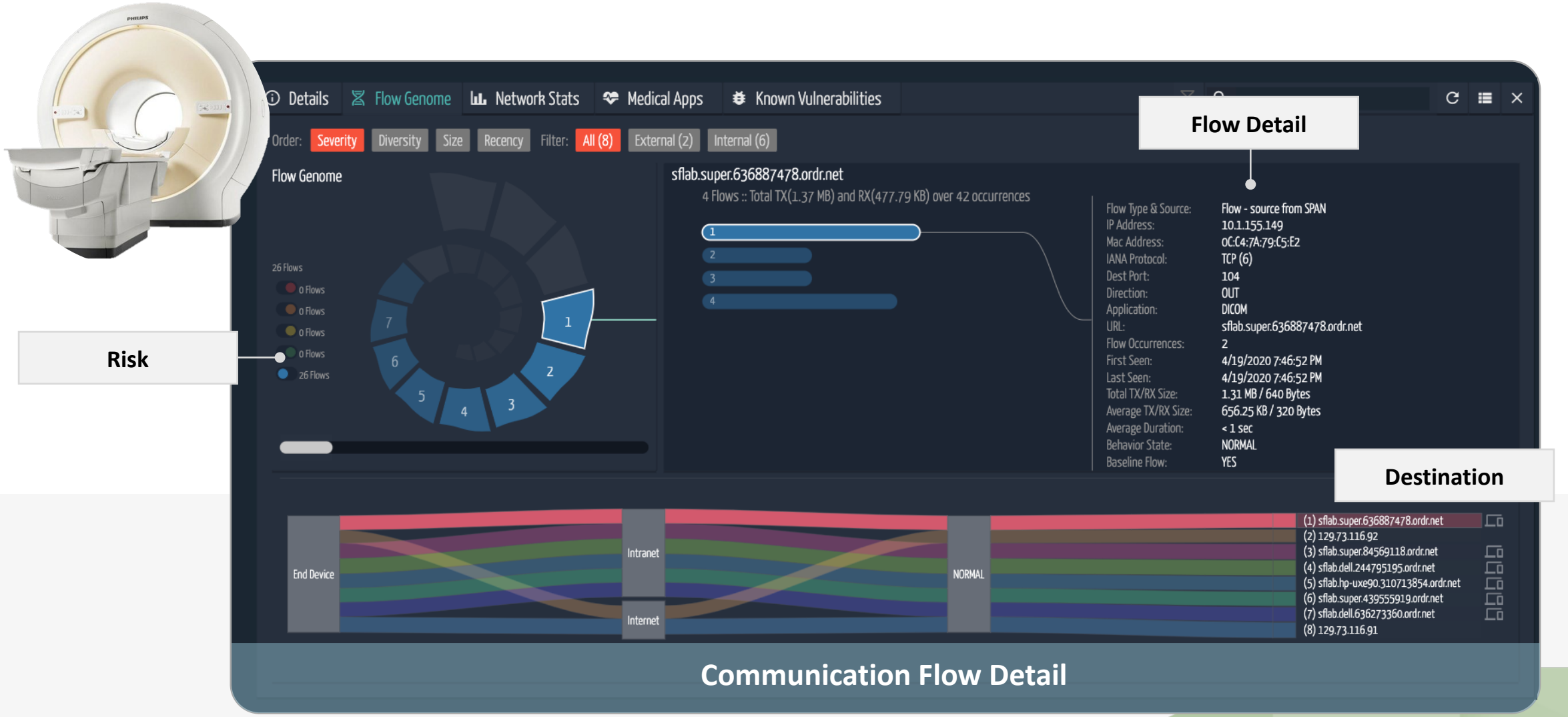
Third Party Software (7)

No.	Name
1	AVG AntiVirus FREE

Anti-Virus Software (2)

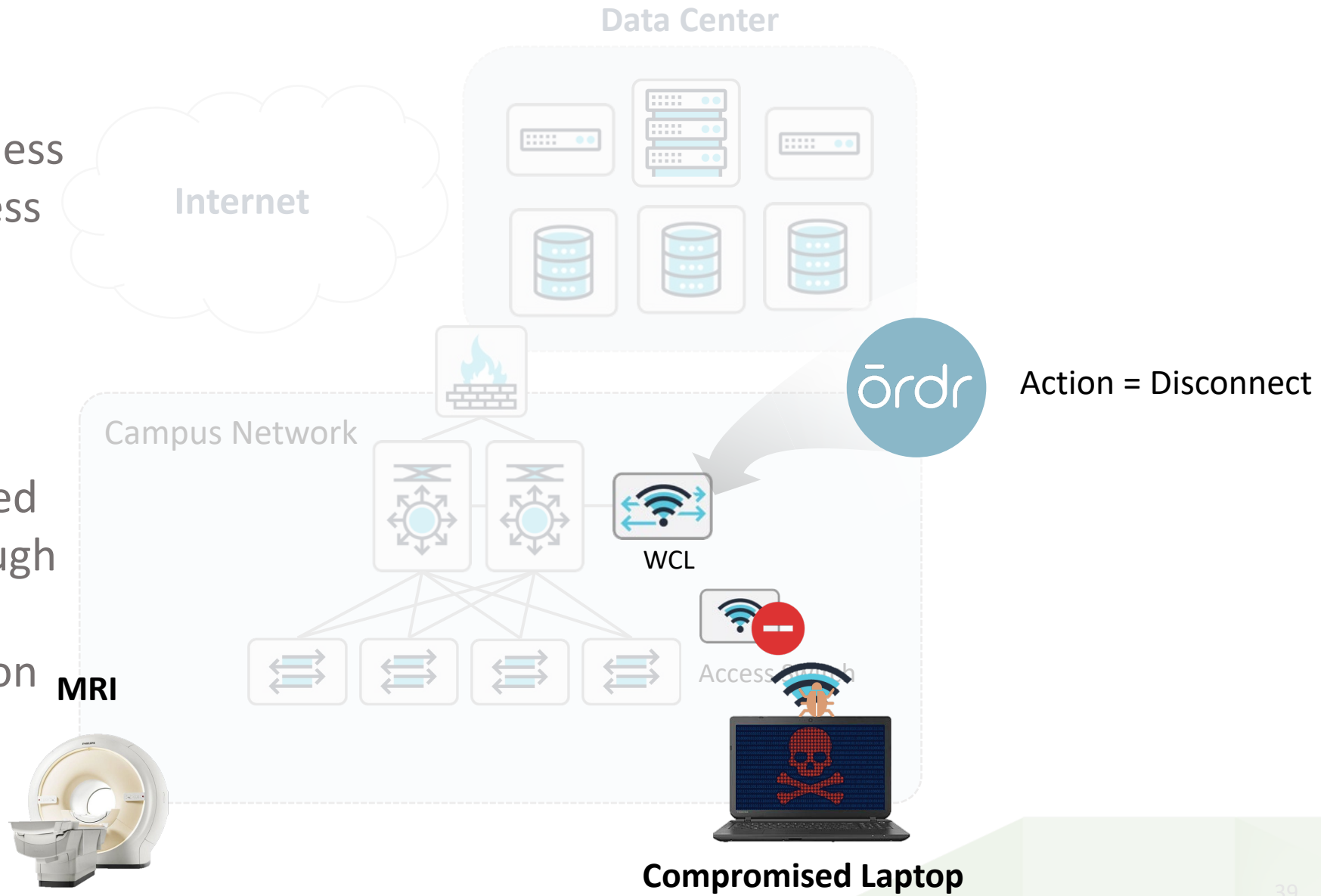
No.	Name	Up-to-date	Last Updated	Protection State	Path
1	Windows Defender	Yes	Mon June 3rd 2019	Inactive	windowsdefender://

Medical Device Behavior Monitoring and Analytics



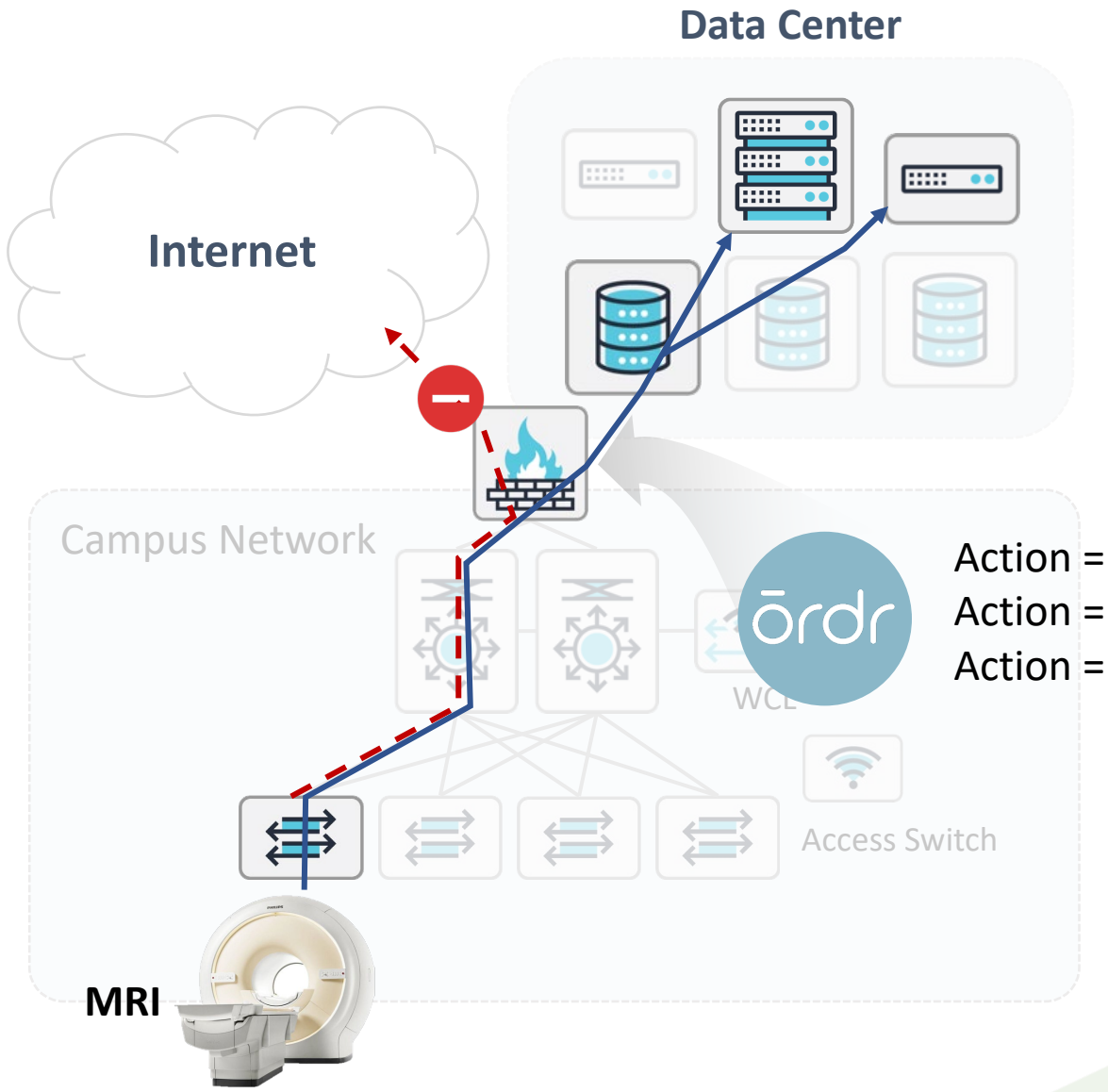
360 Degree Enforcement – Disconnect Attackers

- Non-compliant wireless laptop trying to access to the network, spreading malware laterally.
- Indicator of compromise observed in the network through this laptop and immediate prevention needed



360 Degree Enforcement – Regulate Internet Traffic

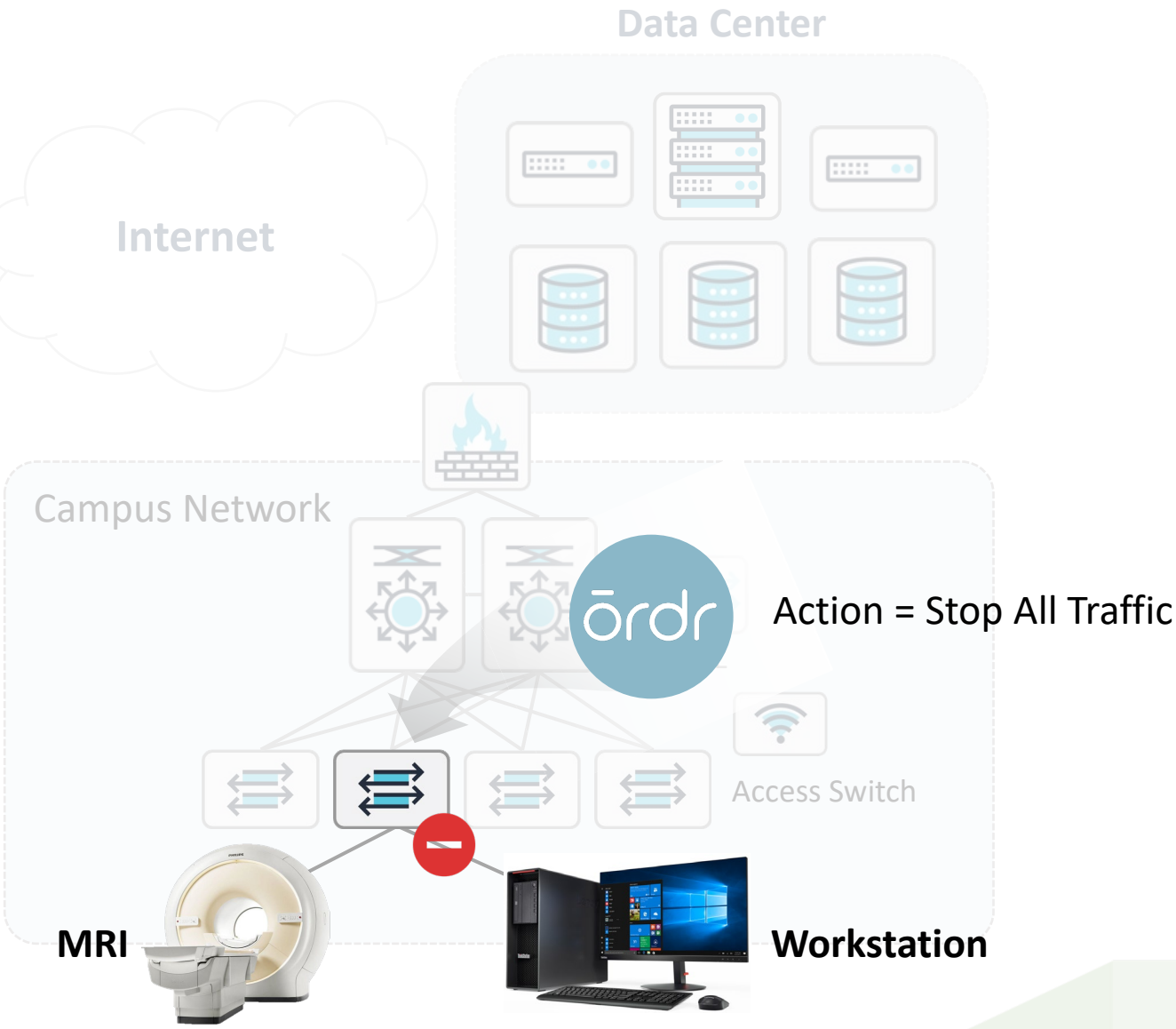
- Firewall allowing specific site and operation based on device type
- Disallow usage of MRI to browse internet for bitcoin mining, and allow legitimate traffic to imaging servers in the data center using firewall



Action = Drop HTTPS to Internet
Action = Allow DICOM to PAC
Action = Drop NetBIOS to AD

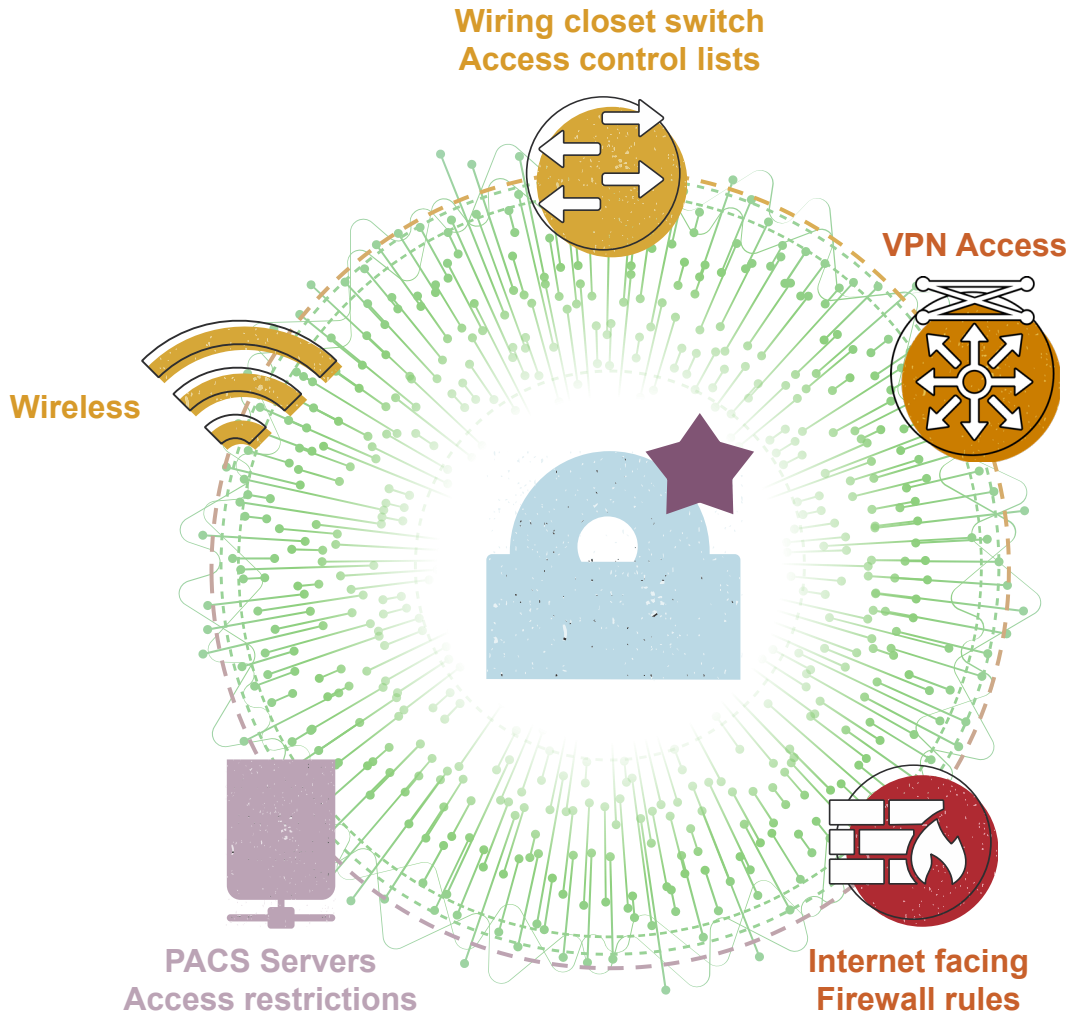
360 Degree Enforcement - MicroSegment Med Devices

- Prevent traffic going in and out of MRI – only legitimate devices can communicate with MRI
- Microsegentation policy to permit specific action to protect line of business and its critical devices



41

360 Degree Enforcement – Close the Loop



Proactive Protection Methods

Border Gateway – Firewall rules

Wireless Controllers - Role Based Access

Wired switches – Access Control Lists

Server Access control – VMware/NSX

Remote user access control - VPN

Application tracking - Load Balancers

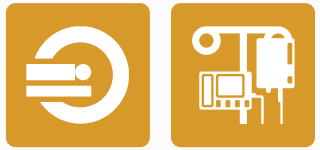
User Tracking - Active Directory/local users

Endpoint agent not possible

Medical Device Protection: Best Practices

DEVICE INVENTORY, UPDATES & ALLOWLISTING

- Allowlist medical devices reconciling with CMDB/CMMS
- Patch(OS/AV) vulnerable medical Devices; Identify older OS like XP
- Identify facility devices – elevator, phones to understand the interactions
- Update password, close open ports, vulnerability scan if possible



GROUP BY DEV MODEL AND SEGMENTATION

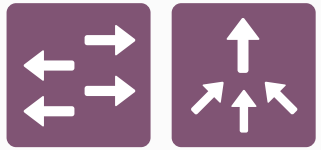
- Create network segments for medical vs facilities vs contractor vs ER vs pharmacy vs guest
- Selectively allow group-to-group access

HYGIENE ON NETWORK ENVIRONMENT

- Plug open ethernet ports on the walls, Patient waiting areas
- Disconnect rogue APs
- Prevent devices from guest network accessing clinical resources
- Identify and remove move outlier devices from wrong segments

SWITCH/WIRELESS POLICY FOR MICROSEGMENTATION

- Stop Malware spreads - Restrict internal traffic from devices in the same segment reaching out to medical or facility devices
- AllowList internal flows for medical devices with for imaging and EMR/HER servers



FIREWALL POLICY FOR EXT. COMMUNICATION

- Block any device reaching out to bad IP/URL to prevent phishing attacks
- Block unwanted users accessing medical devices – zero trust model with admin access
- Ransomware - Prevent Medical workstations used to reach social sites

ACCE Membership

Apply Now!

https://accenet.org/Membership/Pages/ApplicationForms.aspx

Benefits

- Bi-monthly ACCE newsletter with timely updates and articles
- Complimentary ACCE receptions
- Volunteer opportunities
- Complimentary educational webinar

Discounts

- AAMI, HIMSS, IFMBE conference registration
- JCE Journal
- ACCE educational content
- Free access to IFMBE/Springer publications

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

MAYO CLINIC ordr

Q & A

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Keith Whitby
Section Head of Healthcare Technology Management
Cybersecurity and Operations
Mayo Clinic

MAYO CLINIC

Pandian Gnanaprakasam
Chief Product Officer
Ordr Inc.

ordr
take control.

Please complete the online survey at https://www.surveymonkey.com/r/8-27-2020