AEHiA

AEHiS

AEHiT

FALL SUMMIT 2019

Building a Connected Asset Security Program: Lessons From the Field

Rodney Graves, GBMC

Toby Gouker, Carter Groome, First Healthcare Advisory Solutions

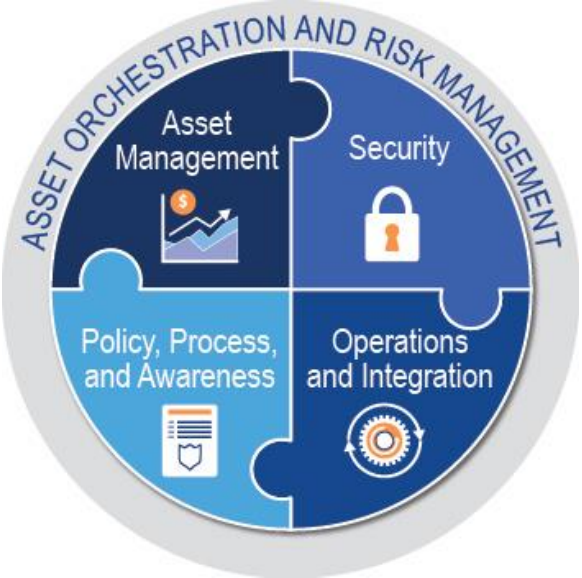
FALL SUMMIT 2019

About GBMC…

- Established in 1965 to combine the best of community and university-level medicine
- 342 bed medical center that that handles more than 23,000 admissions and over 52,000 emergency room visits annually
- GBMC Health Partners in Hunt Manor, Hunt Valley, Owings Mills, Texas Station, Perry Hall, Joppa Road and Jarrettsville
- Gilchrist hospice serves more than 7,600 patients each year

About First…

- Asset Orchestration & Risk Management
- Full Suite Privacy & Security Services
- Clinical and Revenue Cycle HIT


ASSET ORCHESTRATION AND RISK MANAGEMENT
Asset Management
Security
Policy, Process, and Awareness
Operations and Integration

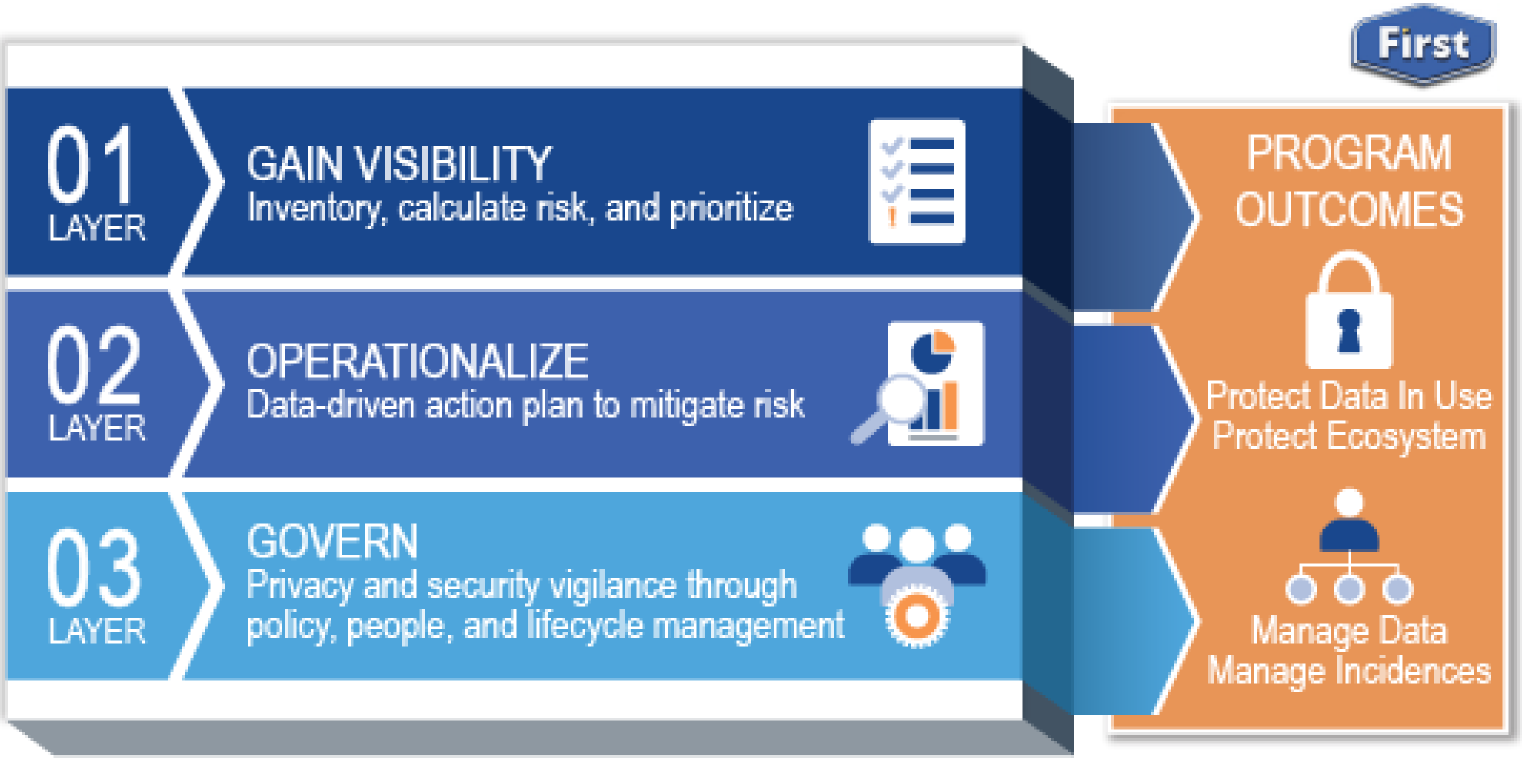
About GBMC Cybersecurity…

- 2016 Medstar, 2017 WannaCry & Not Petya
- Officially began with dedicated staff in 2016
- NIST Framework
- Emerging threat: IOT

Search for a Solution

- Full network visibility
- Internet research, industry colleagues and vendors
- Partnership Healthcare focused IT security

Program, not Product Solution



First

01 LAYER

GAIN VISIBILITY

Inventory, calculate risk, and prioritize

02 LAYER

OPERATIONALIZE

Data-driven action plan to mitigate risk

03 LAYER

GOVERN

Privacy and security vigilance through policy, people, and lifecycle management

PROGRAM OUTCOMES

Protect Data In Use
Protect Ecosystem

Manage Data
Manage Incidences

Technical and Organizational Change Solution

Connected asset security is a classic technical risk management issue
With tricky organizational dynamics issues

RISK MANAGEMENT

- Assess
- Detect
- Respond
- Defend/Protect

ORGANIZATIONAL DYNAMICS

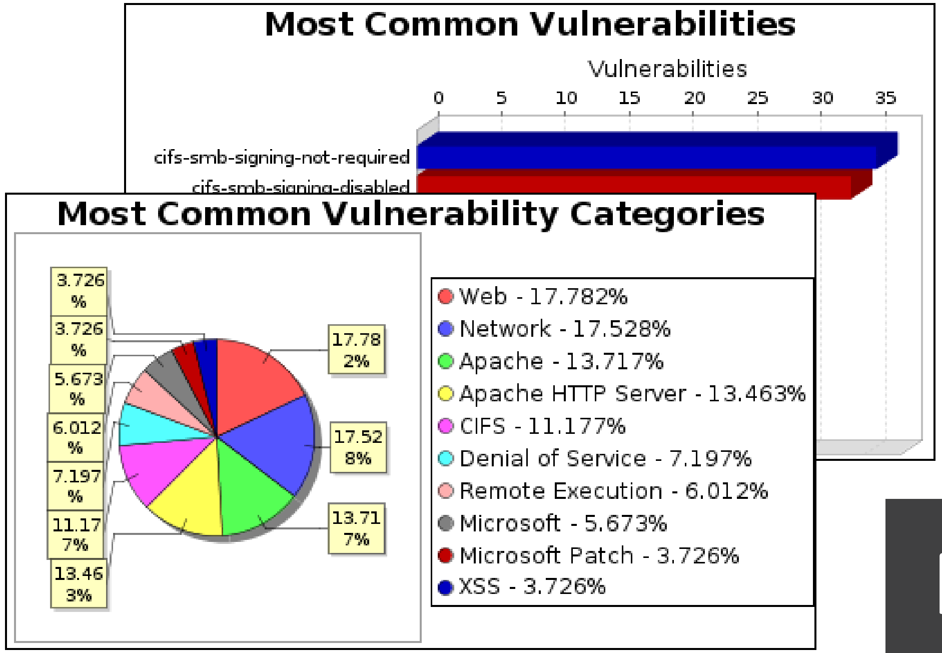
- Attachment to current standard ways/culture
- Resistance to change
- Lack of IoT security education

01 LAYER

GAIN VISIBILITY

Inventory, calculate risk, and prioritize

- Develop relationship between IT, Security and HTM teams
- Coordinated active sample scan
- Discovery of any significant issues
- Initiate system wide passive scanning
- Conduct a risk-based assessment
- Set critical alert mitigation priorities



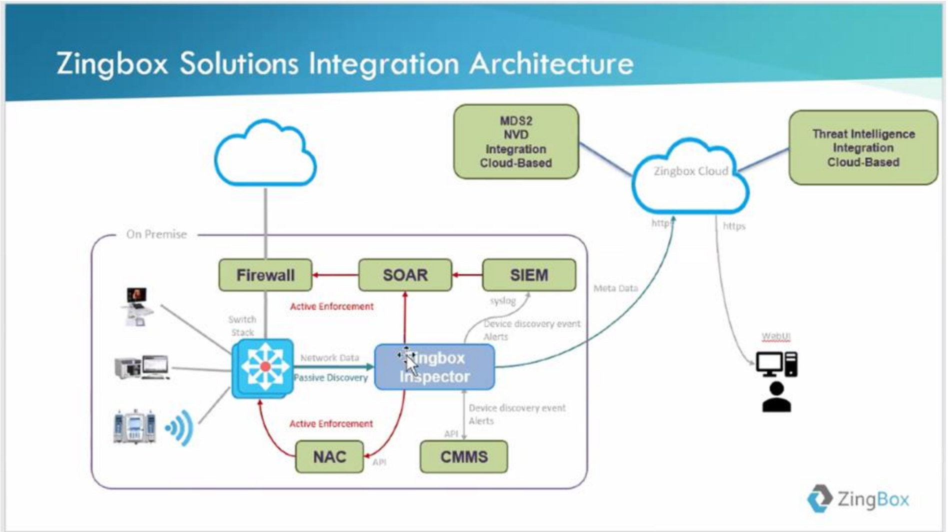
01 LAYER

GAIN VISIBILITY

Inventory, calculate risk, and prioritize

Platform initiation

- Manage installation, testing and operation
- Inventory connected assets within assigned network
- Develop a prioritized list of issues and vulnerabilities
- Prioritize for FY 2020 short-term plan and budget to address mission critical remediations



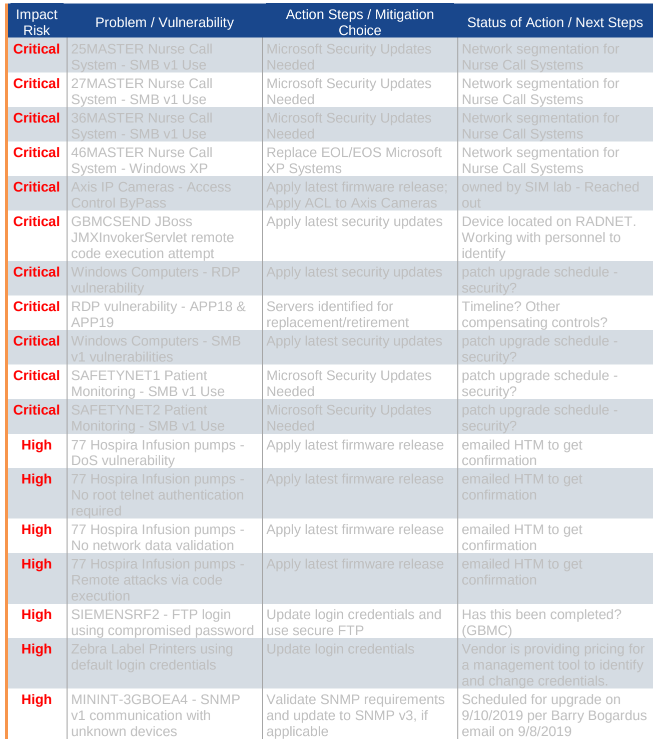
Zingbox Solutions Integration Architecture

02 LAYER

OPERATIONALIZE

Data-driven action plan to mitigate risk

- Inventory and Vulnerability verification
- Dashboard and report design and customization
- Mitigation prioritization and planning
- Roadmap and budget plan for connected asset program



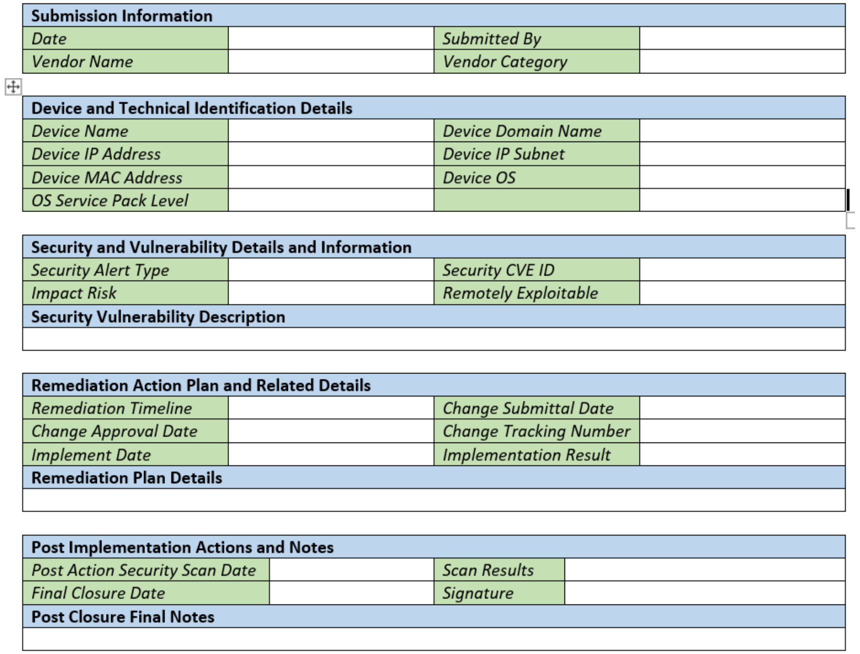
Impact Risk	Problem / Vulnerability	Action Steps / Mitigation Choice	Status of Action / Next Steps
Critical	25MASTER Nurse Call System - SMB v1 Use	Microsoft Security Updates Needed	Network segmentation for Nurse Call Systems
Critical	27MASTER Nurse Call System - SMB v1 Use	Microsoft Security Updates Needed	Network segmentation for Nurse Call Systems
Critical	36MASTER Nurse Call System - SMB v1 Use	Microsoft Security Updates Needed	Network segmentation for Nurse Call Systems
Critical	46MASTER Nurse Call System - Windows XP	Replace EOL/EOS Microsoft XP Systems	Network segmentation for Nurse Call Systems
Critical	Axis IP Cameras - Access Control ByPass	Apply latest firmware release; Apply ACL to Axis Cameras	owned by SIM lab - Reached out
Critical	GBMCSEND JBoss JMXInvokerServlet remote code execution attempt	Apply latest security updates	Device located on RADNET. Working with personnel to identify
Critical	Windows Computers - RDP vulnerability	Apply latest security updates	patch upgrade schedule - security?
Critical	RDP vulnerability - APP18 & APP19	Servers identified for replacement/retirement	Timeline? Other compensating controls?
Critical	Windows Computers - SMB v1 vulnerabilities	Apply latest security updates	patch upgrade schedule - security?
Critical	SAFETYNET1 Patient Monitoring - SMB v1 Use	Microsoft Security Updates Needed	patch upgrade schedule - security?
Critical	SAFETYNET2 Patient Monitoring - SMB v1 Use	Microsoft Security Updates Needed	patch upgrade schedule - security?
High	77 Hospira Infusion pumps - DoS vulnerability	Apply latest firmware release	emailed HTM to get confirmation
High	77 Hospira Infusion pumps - No root telnet authentication required	Apply latest firmware release	emailed HTM to get confirmation
High	77 Hospira Infusion pumps - No network data validation	Apply latest firmware release	emailed HTM to get confirmation
High	77 Hospira Infusion pumps - Remote attacks via code execution	Apply latest firmware release	emailed HTM to get confirmation
High	SIEMENSRF2 - FTP login using compromised password	Update login credentials and use secure FTP	Has this been completed? (GBMC)
High	Zebra Label Printers using default login credentials	Update login credentials	Vendor is providing pricing for a management tool to identify and change credentials.
High	MININT-3GBOEA4 - SNMP v1 communication with unknown devices	Validate SNMP requirements and update to SNMP v3, if applicable	Scheduled for upgrade on 9/10/2019 per Barry Bogardus email on 9/8/2019

02 LAYER

OPERATIONALIZE

Data-driven action plan to mitigate risk

- Mitigation Program Activities
  - Network segmentation
  - Subnet reassignments
  - Patches
  - Equipment retirement
  - System hardening
  - Compensating Controls…



Submission Information			
Date		*Submitted By*	
Vendor Name		*Vendor Category*	

Device and Technical Identification Details			
Device Name		*Device Domain Name*	
Device IP Address		*Device IP Subnet*	
Device MAC Address		*Device OS*	
OS Service Pack Level			

Security and Vulnerability Details and Information			
Security Alert Type		*Security CVE ID*	
Impact Risk		*Remotely Exploitable*	
Security Vulnerability Description			

Remediation Action Plan and Related Details			
Remediation Timeline		*Change Submittal Date*	
Change Approval Date		*Change Tracking Number*	
Implement Date		*Implementation Result*	
Remediation Plan Details			

Post Implementation Actions and Notes			
Post Action Security Scan Date		*Scan Results*	
Final Closure Date		*Signature*	
Post Closure Final Notes			

03 LAYER

GOVERN

Security vigilance through policy, people, and lifecycle management

Communication to C-suite

Policies for new purchases

Committee to handle change management

Monitor regulatory changes & manufacturer alerts

Business operation changes

Closed-loop equipment lifecycle management

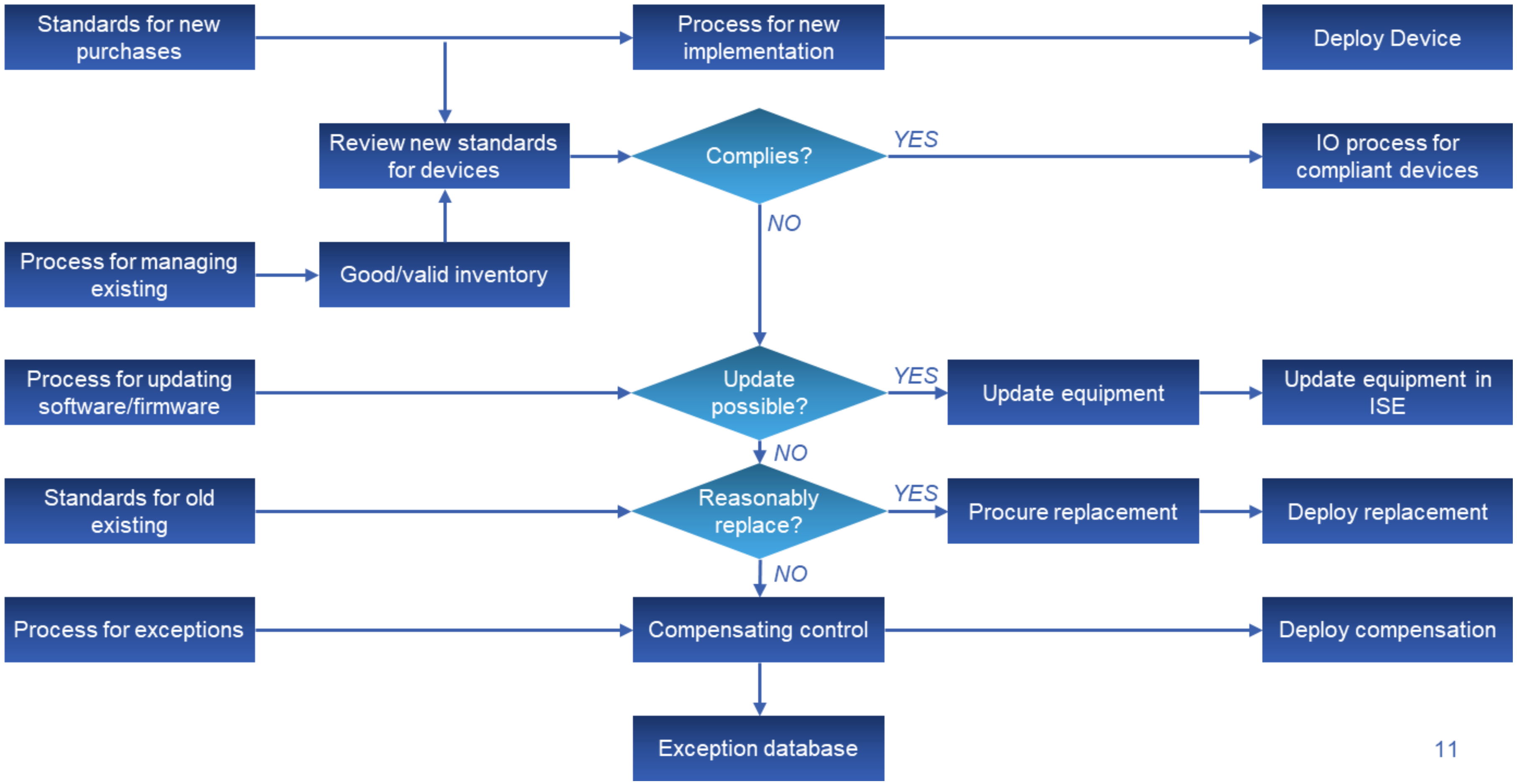
Continuous monitoring

Organizational Cyber Health Maturity Level Attainment Objectives	Weighted %
Visibility, inventory, workforce education and awareness	15%
24x7 monitoring and alerting	10%
Full system integration (CMMS, SIEM, NAC, vulnerability scanners, firewalls, SOAR, Network management, wireless LAN, managed security services)	10%
Complete mitigation of critical and high vulnerabilities	25%
Mitigation of remaining issues to attain risk appetite	15%
Fully established governance program – • Data driven operationalization of policies and processes • Enhanced inventory capabilities for utilization metrics, device load leveling, and maintenance	25%
Total	**100%**

03 LAYER

GOVERN

Security vigilance through policy, people, and lifecycle management



Standards for new purchases

Process for new implementation

Deploy Device

Review new standards for devices

Complies?

YES

IO process for compliant devices

NO

Process for managing existing

Good/valid inventory

Process for updating software/firmware

Update possible?

YES

Update equipment

Update equipment in ISE

NO

Standards for old existing

Reasonably replace?

YES

Procure replacement

Deploy replacement

NO

Process for exceptions

Compensating control

Deploy compensation

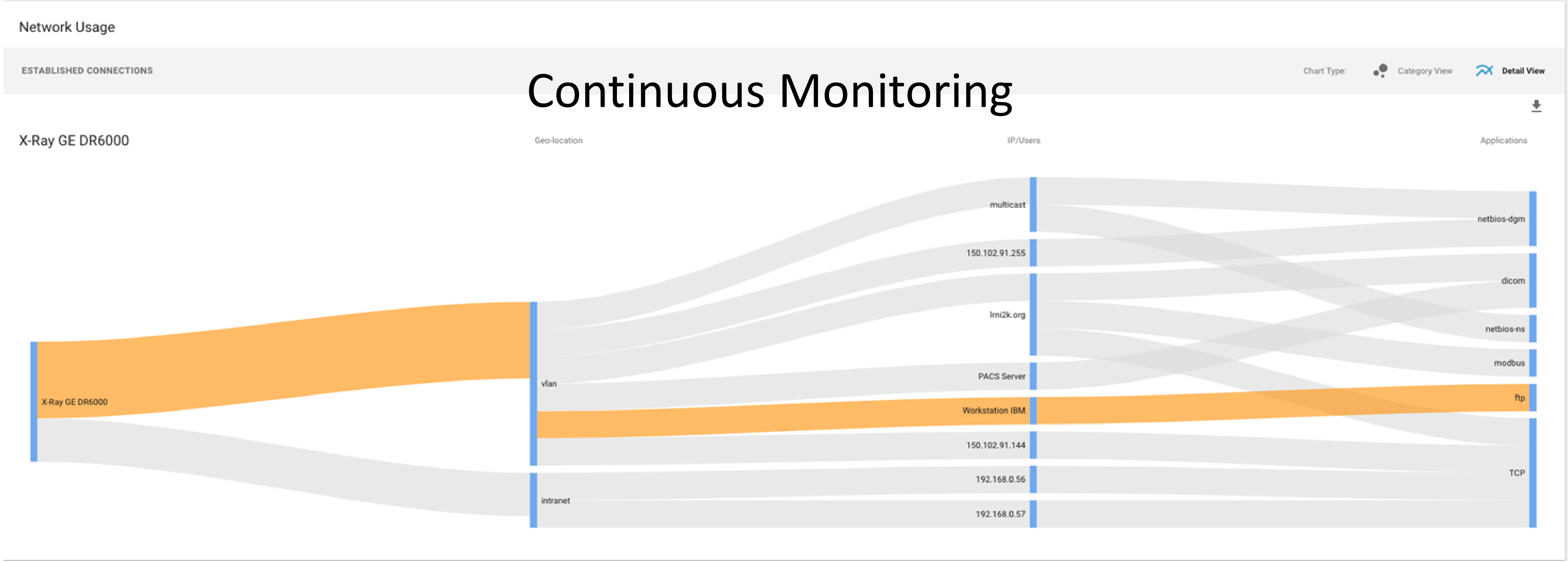
Exception database

03 LAYER

GOVERN

Security vigilance through policy, people, and lifecycle management

Continuous Monitoring



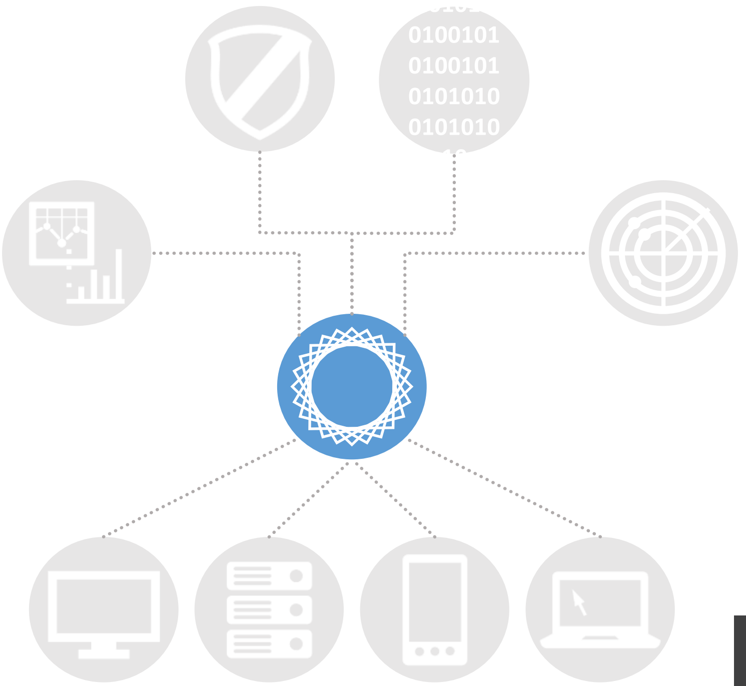
FALL SUMMIT 2019

03
LAYER

GOVERN
Security vigilance through policy, people, and lifecycle management

Continuous Monitoring Bonuses

- Capacity utilization metrics for new purchase justification
- Device load leveling to avoid new purchases
- Maintenance based on use, not time passed
- Abnormalities as indication of pending failures
- Performance improvement coaching
- Redirect of patient to available capacity



Questions & Answers

Now, or later….

rgraves@gbmc.org

tgouker@fcp.com

cgroome@fcp.com