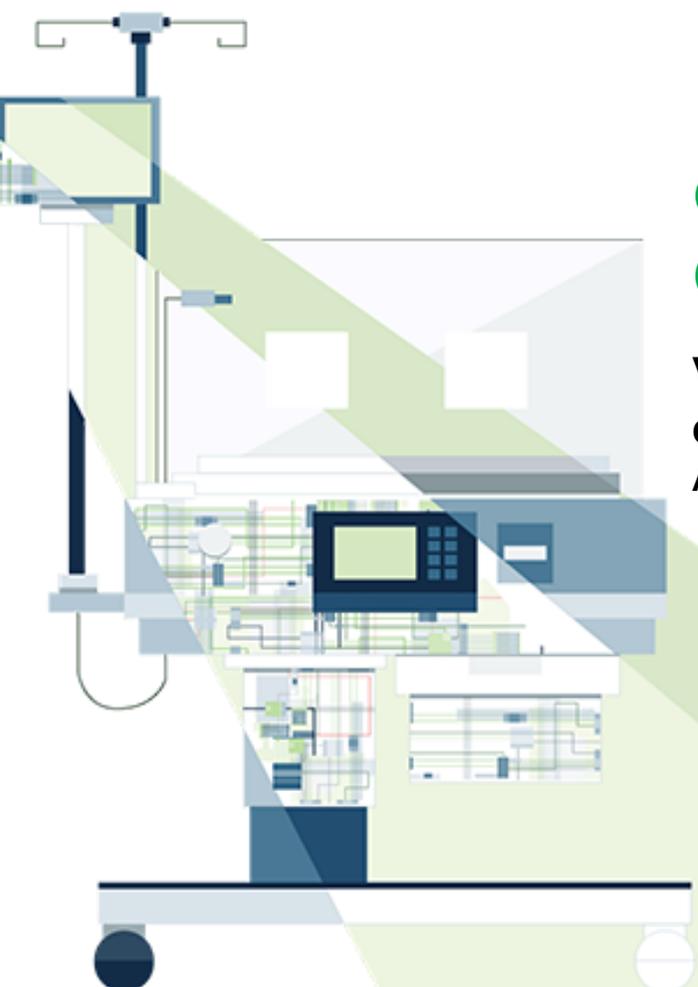


# Cynerio



## **CYNERIO GETTING STARTED GUIDE**

**Version 1.2**

**Copyright © Cynerio 2021**

**All Rights Reserved**

### Revision History

Product version: Cynerio 1.2

Document revision history: 1.0

Document Revision	Date	Description
1.0	13 Oct, 2021	Created first version of Getting Started Guide for Version 1.2



### Table of Contents

Table of Contents .....	3
Introduction .....	5
Main Features .....	5
Key Terms.....	6
Automated Asset Discovery.....	8
Asset Classification.....	8
Assets Screen .....	10
Asset Inventory Use Case 1 – Asset drill-down.....	13
Asset Inventory Use Case 2 – Displaying Additional Columns.....	15
Asset Inventory Use Case 3 – Creating Bookmarks .....	17
Monitoring Network Traffic.....	19
Network Screen.....	19
Network Use Case 1 – Filtering by Profile.....	20
Network Use Case 2 – Drilling down to view Asset communication info.....	20
Risk.....	23
Risk Classification.....	23
Risk Score .....	23
Risk Status.....	24
Risk Screen .....	25
Risk Use Case 1 - Filtering by Risk Type and Generating Reports.....	27
Risk Use Case 2 - Drilling down to analyze Risks – Managing Risk Status.....	28
Dashboards .....	30
Dashboard Screen.....	31



Dashboard Use Case .....	32
Monitoring Events.....	35
Events Screen.....	35
Events Use Case 1 – Creating Notifications .....	36
Events Use Case 2 – Exporting Tables.....	37
Mitigations .....	38
Device Mitigations .....	38
Device Mitigations Use Case .....	38
Network Mitigations .....	39
Service Hardening .....	40
East–West Segmentation.....	44
North-South Segmentation and Vendor Access .....	48



### Introduction

Cynerio's cybersecurity platform has been designed to address the core issues related to IoT security in healthcare - the discovery and reduction of risk throughout hospital environments. We view security through the lens of patient safety, data confidentiality, and avoiding service disruption. Our platform is designed to help healthcare organizations regardless of size and provides customers with real-time insights to identify and manage risk without impacting patient safety.

The below guide is intended to quickly introduce you to Cynerio functionality while acting as a long term reference for a variety of day-to-day activities. Throughout this guide you will learn how Cynerio's technology identifies threat vectors and vulnerabilities, and then provides end-to-end risk mitigation procedures tailored to your network. You will also gain insight into Cynerio's implementation of the NIST Zero Trust framework to create, test and deploy security policies efficiently and safely throughout your environment.

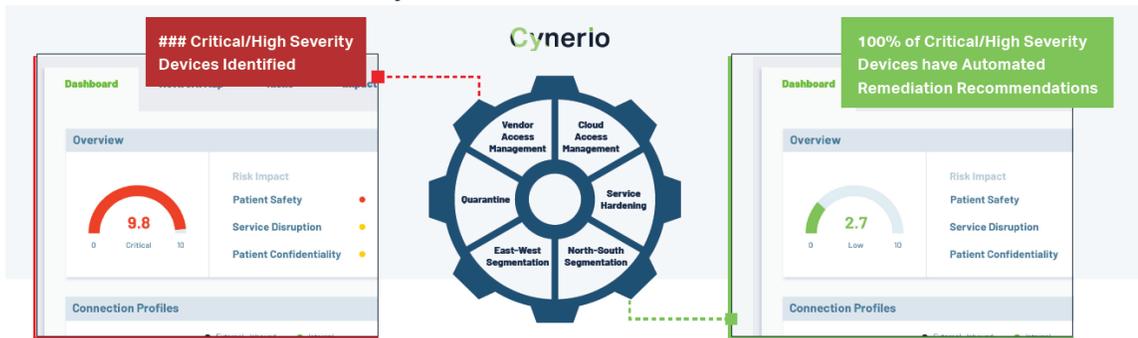
If you have any questions, comments, support needs or update requests, please don't hesitate to contact your Cynerio Customer Success team member or our broader team at [support@cynerio.com](mailto:support@cynerio.com).

### Main Features

- **Risk Detection** – Cynerio automatically detects risks threatening your network. Ranging from insecure device software to device-specific behavioral risk (open ports, insecure authentication, unsafe communication, etc.) our technology identifies weaknesses quickly and efficiently.
- **Automatic Asset Inventory** – Using Deep Packet Inspection (DPI) Cynerio is able to automate continuous end-to-end discovery of assets and track dozens of data points for each item. Beyond just discovering assets, this approach provides the ability to locate and profile the behavior of any IoT, OT or IoMT device in a clinical ecosystem.
- **Risk Ranking and Prioritization** - Each asset in your environment receives a risk score based on the NIST framework for Risk Assessment and Risk Management. Healthcare specific factors are then applied to provide an accurate score relative to your environment. These scores allow for more efficient review and prioritization of risks.



- **Actionable Mitigation Plan** – The Cynerio platform automatically generates operationally-safe Zero Trust security policy and device-level remediation recommendations. These automatically tested plans can then be reviewed, updated and applied to production environments in a safe and timely manner.



- **Interactive Platform** - The Cynerio platform provides insight for all team members focused on risk reduction. From high level summaries to granular device details, data is easily filtered, sorted and made accessible to allow for accurate risk analysis, efficient remediation, and up-to-date insight to progress. Customizable dashboards provide users the ability to tailor data display to their specific needs. The dashboard widgets are clickable, taking you directly to the relevant screens showing related data.

## Key Terms

Cynerio uses industry standard vocabulary whenever possible. The following is a list of key terms and concepts that will benefit readers of this document:

- **Asset** – A device in your network, including IoT, OT and IoMT.
- **Event** – A security related Event that was detected in your network. For each Event details are given about the nature of the Event, the involved assets and the Severity level of the Event.
- **Mitigation** – an action that Cynerio recommends taking in order to mitigate a particular threat. Mitigation actions include actions on individual assets such as changing configurations, updating firmware and service hardening. It also involves segmenting your assets both for E-W traffic and N-S traffic.
- **Network Connections** – Communication involving assets in your network. Conversations with identical characteristics (e.g. source asset, destination asset, protocol etc.) are treated as a single *Network Connection*. In addition, Cynerio uses AI algorithms to determine the purpose of the connection and designates a *Profile* for each connection (e.g. Cloud Services, Data Transfer, Software Update etc.).

- **Policy** – A set of rules governing Network Connections that are blocked for particular assets. Policies can be applied to individual assets (service hardening) or to groups of assets (E-W or N-S segments). Policies are first validated over a period of time and then they are ready to be enforced.
- **Risk** – A security threat that affects an asset in your network. Cynerio identifies three types of Risks:
  - **Behavioral** – improper configuration of an asset (e.g., Default HTTP Credentials, Open SSH Port, Weak Telnet Credentials etc.)
  - **Vulnerability** – a known cybersecurity vulnerability that affects the software/firmware installed on an asset, e.g., CVEs.
  - **Recall** – a device that is subject to factory recall.



### Automated Asset Discovery

Manually documenting, mapping and updating an accurate inventory of medical devices, servers, IT assets and any number of other devices in a healthcare facility is a tedious and error prone task. Cynerio's automated asset discovery functionality integrates seamlessly with your existing infrastructure and uses Deep Packet Inspection (DPI) to automate continuous end-to-end asset discovery, location, and behavior profiling for every connected device in the clinical ecosystem. This approach allows Cynerio technology to continuously identify and update relevant data points for each device including Vendor, Model, Third-party components, AP, OS/firmware, Serial number and hundreds more.

### Asset Classification

Cynerio classifies assets using the following hierarchy, making it easy to view aggregated data and then drill down to view specific details.

Class (IoT/loMT) → Category (usage) → Type (function) → Vendor → Model

For example, a GE Optima XR220 X-Ray device is categorized as:

loMT → Radiology → X-Ray → GE → Optima XR220

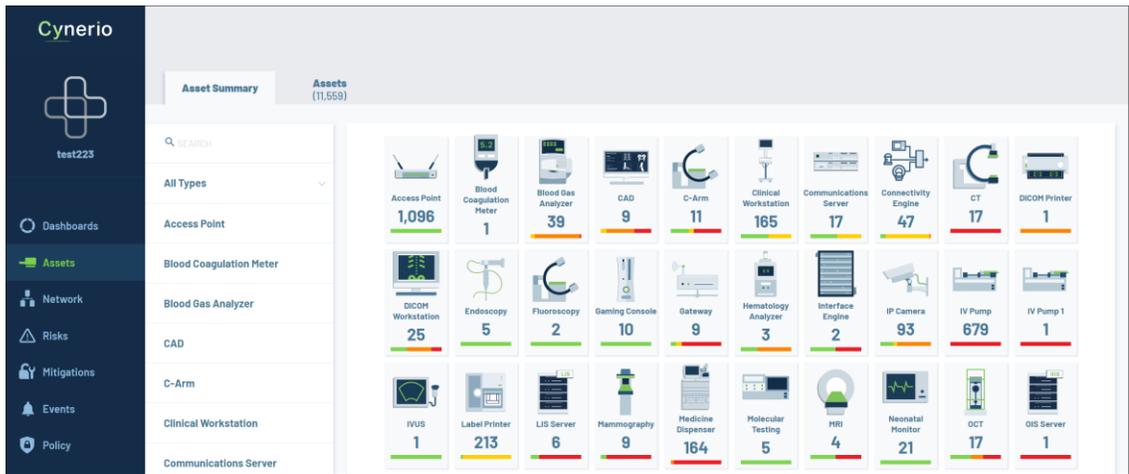




### Assets Screen

The complete automated asset inventory is shown on the Assets screen. The Assets screen has two tabs, *Asset Summary* and *Assets*.

- **Asset Summary** – shows your assets grouped by types. For each type, a tile is shown with a representative icon, the number of assets of that type and a bar graph indicating the risk level of the assets.



You can drill down into a specific type of assets to open a dashboard showing widgets representing the risks and network activity for assets of that type.



- **Assets** – shows a list of all Assets in your network. The Assets are displayed in a fully customizable table enabling you to show extensive details for each asset.

CATEGORY	ROLE	DISPLAY NAME	IP ADDRESS	TYPE	MODEL	VENDOR	LAST SEEN	OS	EPH	VLA
Pharmacology	Device	PYCLINICA	10.127.204.228	Medicine Dispenser	Pyxis Medstation	BD	44 mins	Windows Embedded ...	10.1	10.1
Bedside	Device		10.227.228.85	IV Pump	Alaris PCU 8015	BD	44 mins	ENEAE OSE RTOS for A...	122	122
Bedside	Device		10.227.224.140	IV Pump	Alaris PCU 8015	BD	44 mins	ENEAE OSE RTOS for A...	122	122
Bedside	Device		10.227.231.50	IV Pump	Alaris PCU 8015	BD	44 mins	ENEAE OSE RTOS for A...	122	122
Bedside	Device		10.227.228.170	IV Pump	Alaris PCU 8015	BD	44 mins	ENEAE OSE RTOS for A...	122	122
Pharmacology	Device	PYCLINICF	10.127.203.219	Medicine Dispenser	Pyxis Medstation	BD	44 mins	Windows Embedded ...	10.1	10.1
Infrastructure	Device		10.227.193.200	UPS	EATON UPS	Eaton	6 days		119	119
Bedside	Device		10.227.231.116	IV Pump	Alaris PCU 8015	BD	44 mins	ENEAE OSE RTOS for A...	122	122

You can drill down into a specific asset to open the asset page showing detailed data (divided by tabs) and dashboard widgets for that asset.

**Medicine Dispenser**

**Overview**

Asset Impact: Patient Safety (Critical), Service Disruption (High), Patient Confidentiality (Medium)

Risks: Legacy OS (Critical), Bad Neighbor (High), CVE-2020-10598 (High), CVE-2020-1147 (Medium)

Severity Score: 9.8 (Critical)

**Connection Profiles**

Profile	Internal	External - Outbound
Windows Update	High	Low
IT	Medium	Low
Other	Low	Low
Endpoint Protection	Low	Low
Medical	Low	Low
OS Services	Low	Low
Video Streaming	Low	Low
Vendor Connection	Low	Low

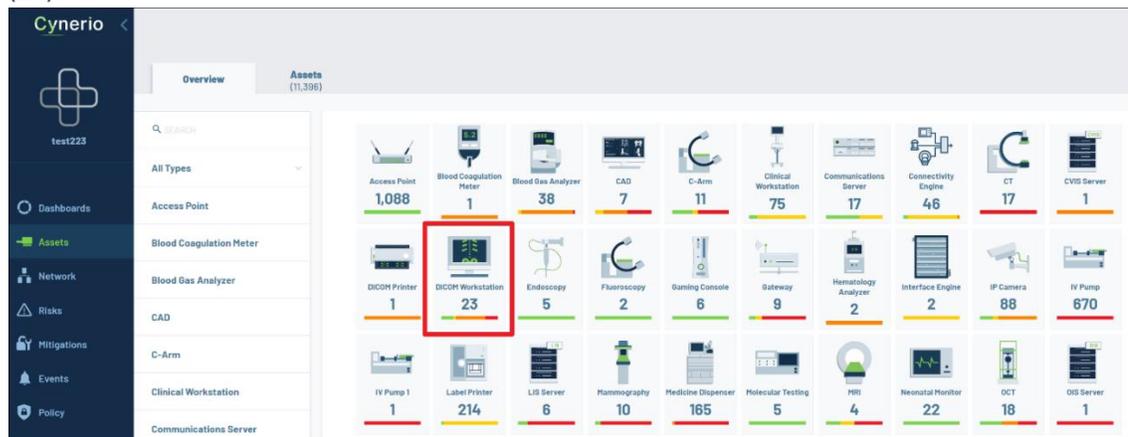
**Pyxis Medstation Behavior Comparison**

Scatter plot showing behavior metrics for various assets, with the selected asset highlighted.

### Asset Inventory Use Case 1 – Asset drill-down

Let's say that you want to find out how many DICOM workstations you have, how many of them are GE, and the models of your GE workstations.

1. Go to the **Assets > Asset Summary** screen.  
You can see right away that there is a tile indicating how many DICOM Workstations you have (23).



2. Click on the tile to show the dashboard for your DICOM workstations. (Alternatively, you could click on "DICOM Workstations" in the selection pane on the left.)  
The DICOM Workstations dashboard opens. The Security Posture summary at the top of the page shows how many of your workstations are at risk (19). Below that, additional widgets give detailed info about the risks affecting you workstations.

- To view details about your specific workstations, click on the number of assets in the Security Posture summary.

**DICOM Workstation** Security / Network Utilization 05/24 - 06/23

**Security Posture**

- 23 Assets
- 19 Assets at Risk
- N/A E-W Segmentation Coverage
- 0% N-S Segmentation Coverage
- 0% Vendor Access Coverage

**Risks & Severities**

Risk Title	Low	Medium	High	Critical
<a href="#">Apache 2.2.22 (HTTP)</a>				1
<a href="#">CallStranger</a>		1		
<a href="#">CVE-2003-0352</a>			1	
<a href="#">CVE-2003-0715</a>				1
<a href="#">CVE-2005-2090</a>		1		
<a href="#">CVE-2020-25175</a>				1

**Risk Remediation and Mitigation Actions**

Action Type	Actions	Assets
<b>Network Segmentation Actions</b>		
Apply North-South Segmentation	4	13
<b>Network Configuration Actions</b>		
Apply Service Hardening	25	35

The Assets tab opens with the results automatically filtered to show only DICOM workstations.

Search: Type: DICOM Workstation SEARCH

Overview Assets (23)

See related: Mitigation | Risks | Connections | Events

Create policy Reports Bookmarks Manage Columns Export Table

TYPE	CATEGORY	ROLE	DISPLAY NAME	MODEL	VENDOR	LAST SEEN	IP ADDRESS	OS	EPH	VLAN	SEVERITY
DICOM Workstation	Radiology	Workstation	SVDX_800	SecurView	Hologic	1 hr	10.127.238.82	Windows Server 2008...	EPH	10.0.0.0/8	CRITICAL
DICOM Workstation	Radiology	Workstation	ARLH_SECURE...	SecurView V10-X	Hologic	20 hrs	10.127.238.55	Windows XP	EPH	10.0.0.0/8	CRITICAL
DICOM Workstation	Radiology	Workstation	CENOVA_SCP	C-View	Hologic	5 hrs	10.127.238.84	Windows 7	EPH	10.0.0.0/8	CRITICAL
DICOM Workstation	Radiology	Workstation	VIMS_AE	Vitrea Processin...	Canon	39 mins	10.127.238.93	Windows 8.1	EPH	236	CRITICAL
DICOM Workstation	Radiology	Workstation	RA600	Centricity RA600...	GE	18 days	10.127.236.127	Windows 7	EPH	10.0.0.0/8	CRITICAL
DICOM Workstation	Radiology	Workstation	jshaws216	AW Server	GE	20 days	10.127.236.216	Unix	EPH	10.0.0.0/8	HIGH

- You can filter for GE workstations by clicking on the Vendor column header and selecting GE.

Overview Assets (7)

See related: Mitigation | Risks | Connections | Events

Create policy Reports Bookmarks Manage Columns Export Table

TYPE	CATEGORY	ROLE	DISPLAY NAME	MODEL	VENDOR	IP ADDRESS	OS	EPH	VLAN	SEVERITY
DICOM Workstation	Radiology	Workstation	RA600	Centricity RA600...	GE	10.127.236.127	Windows 7	EPH	10.0.0.0/8	CRITICAL
DICOM Workstation	Radiology	Workstation	jshaws216	AW Server	GE	10.127.236.216	Unix	EPH	10.0.0.0/8	HIGH
DICOM Workstation	Radiology	Workstation	CARDIOLAB1	Mac-Lab/CardioL...	Canon	10.127.213.25	Windows 10 Enterpris...	EPH	10.0.0.0/8	HIGH
DICOM Workstation	Radiology	Workstation	XEL4RMRR	Xeleris 2.0	Hologic	10.127.238.82		EPH	10.0.0.0/8	MEDIUM
DICOM Workstation	Radiology	Workstation	LUNAR_DICOM	enCORE	Minolta	10.127.239.18		EPH	10.0.0.0/8	LOW
DICOM Workstation	Radiology	Workstation	NMXEL_RMS	Xeleris 4	GE	10.229.16.1		EPH	2016	LOW
DICOM Workstation	Radiology	Workstation	NMXEL_RM1	Xeleris 4	GE	10.229.16.4		EPH	2016	LOW

- Now, only the GE workstations are shown. The Model column shows the Model of each of your GE DICOM workstations. You can sort the display by Model by hovering over the Model column header and clicking on the arrow.

TYPE	CATEGORY	ROLE	DISPLAY NAME	MODEL	VENDOR	LAST SEEN	IP ADDRESS	OS	EPH	VLAN	SEVERITY
DICOM Workstation	Radiology	Workstation	NMXEL_RM5	Xeleris 4	GE	2 hrs	10.229.16.1		ePH	2016	LOW
DICOM Workstation	Radiology	Workstation	NMXEL_RM1	Xeleris 4	GE	1 hr	10.229.16.4		ePH	2016	LOW
DICOM Workstation	Radiology	Workstation	XEL4RMRR	Xeleris 2.0	GE	1 day	10.127.238.62		ePH	10.0.0.0/8	MEDIUM
DICOM Workstation	Radiology	Workstation	CARDIOLAB1	Mac-Lab/CardioL...	GE	25 days	10.127.213.25	Windows 10 Enterpris...	ePH	10.0.0.0/8	HIGH
DICOM Workstation	Radiology	Workstation	LUNAR_DICOM	enCORE	GE	4 hrs	10.127.239.18		ePH	10.0.0.0/8	LOW
DICOM Workstation	Radiology	Workstation	RA600	Centricity RA600...	GE	18 days	10.127.238.127	Windows 7	ePH	10.0.0.0/8	CRITICAL
DICOM Workstation	Radiology	Workstation	jshaws216	AW Server	GE	20 days	10.127.238.216	Unix	ePH	10.0.0.0/8	HIGH

### Asset Inventory Use Case 2 – Displaying Additional Columns

Next, let's say that you want to check how many of your DICOM Workstations are currently online. In the default view, the "Status" (online/offline) column isn't displayed. However, you can customize the column display to show the "Status" column.

- First, let's go back to showing all of your DICOM Workstations by clicking the "x" next to the Vendor filter in the Search box.

TYPE	CATEGORY	ROLE	DISPLAY NAME	MODEL	VENDOR	LAST SEEN	IP ADDRESS	OS	EPH	VLAN	SEVERITY
DICOM Workstation	Radiology	Workstation	NMXEL_RM5	Xeleris 4	GE	2 hrs	10.229.16.1		ePH	2016	LOW
DICOM Workstation	Radiology	Workstation	NMXEL_RM1	Xeleris 4	GE	1 hr	10.229.16.4		ePH	2016	LOW
DICOM Workstation	Radiology	Workstation	XEL4RMRR	Xeleris 2.0	GE	1 day	10.127.238.62		ePH	10.0.0.0/8	MEDIUM
DICOM Workstation	Radiology	Workstation	CARDIOLAB1	Mac-Lab/CardioL...	GE	25 days	10.127.213.25	Windows 10 Enterpris...	ePH	10.0.0.0/8	HIGH

2. Click on **Manage Columns** and then on **Edit Columns**.

TYPE	CATEGORY	ROLE	DISPLAY NAME	MODEL	VENDOR	LAST SEEN	IP ADDRESS	OS	SEVERITY
DICOM Workstation	Radiology	Workstation	NMXEL_RM5	Xeleris 4	GE	2 hrs	10.229.16.1		LOW
DICOM Workstation	Radiology	Workstation	NMXEL_RM1	Xeleris 4	GE	2 hrs	10.229.16.4		LOW
DICOM Workstation	Radiology	Workstation	XEL4RMRR	Xeleris 2.0	GE	1 day	10.127.238.62		MEDIUM
DICOM Workstation	Radiology	Workstation	VIMS_AE	Vitrea Processin...	Canon	43 mins	10.127.236.93	Windows 8.1	CRITICAL
DICOM Workstation	Radiology	Workstation	ARLH_SECURE...	SecurView V10-X	Hologic	21 hrs	10.127.236.55	Windows XP	CRITICAL
DICOM Workstation	Radiology	Workstation	SVDX_600	SecurView	Hologic	1 hr	10.127.238.82	Windows Server 2...	CRITICAL
DICOM Workstation	Radiology	Workstation	CCDPH_TB_DP	REGIUS Console ...	Konica MI...	6 days	10.126.128.150	Windows XP	HIGH
DICOM Workstation	Radiology	Workstation	PBOPTOS	NiiRead	Lexmark	1 hr	10.227.106.198	Windows 10 Enter...	HIGH

The **Add/Remove Columns** dialog opens.

**Add / Remove Columns**

SEARCH

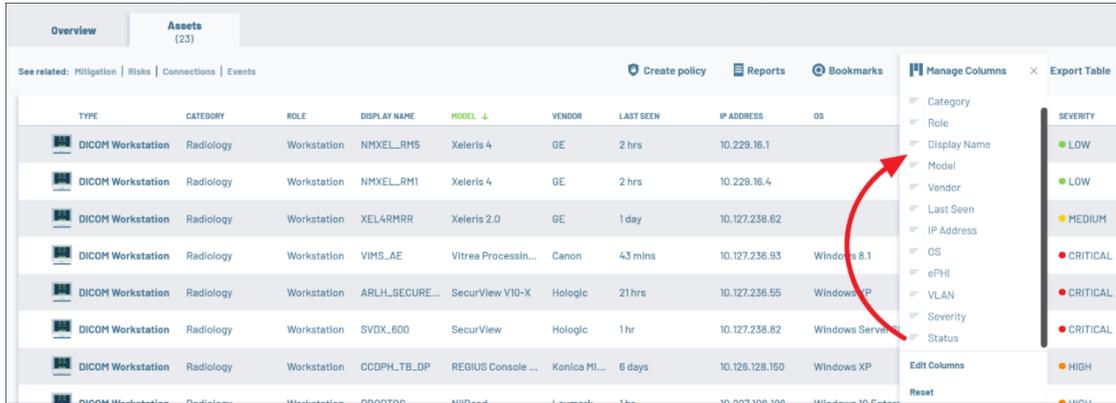
**FDA**

- 510(k)Number
- Advisory Committee
- Applicant
- Class
- Clearance Type
- Country Code
- Date Received
- Decision Date
- Decision Description
- Device Name
- Life Sustaining
- Link

Close

3. In the Search box, type in "status".  
The status option is shown.
4. Select the checkbox next to "Status" and click **Close**.

- You can now adjust the column position by dragging and dropping the "Status" column towards the top of the columns list in the Manage Columns drop-down.



- The Status columns is now shown next to the Display Name making it easy to see the current status of each of your workstations.

The screenshot shows the 'Assets' page with the 'Status' column moved to the top of the column list. The 'Status' column is highlighted with a red box. The table columns include TYPE, CATEGORY, ROLE, STATUS, DISPLAY NAME, MODEL, VENDOR, LAST SEEN, IP ADDRESS, OS, and EPHI.

TYPE	CATEGORY	ROLE	STATUS	DISPLAY NAME	MODEL	VENDOR	LAST SEEN	IP ADDRESS	OS	EPHI
DICOM Workstation	Radiology	Workstation	Offline	jshaws216	AW Server	GE	20 days	10.127.236.216	Unix	ePHI
DICOM Workstation	Radiology	Workstation	Offline	RA600	Centricity RA600...	GE	18 days	10.127.236.127	Windows 7	ePHI
DICOM Workstation	Radiology	Workstation	Online	GE_OS2	CR OS	Agfa Heal...	1 hr	10.127.239.2	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Offline	GE_OS10	CR OS	Agfa Heal...	1 mo	10.127.239.10	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Online	CHS_NX2	CR OS	Agfa Heal...	1 hr	10.127.19.227	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Offline	GE_OS4	CR OS	Agfa Heal...	1 mo	10.127.239.4	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Online	Prov_CAD	C-View	Hologic	7 days	10.127.87.53	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Online	BILR2CAD	C-View	Hologic	3 hrs	10.229.193.10	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Online	PRIETD_R2	C-View	Hologic	15 hrs	10.227.93.231	Windows 7 Professio...	ePHI
DICOM Workstation	Radiology	Workstation	Online	CENOVA_SCP	C-View	Hologic	3 hrs	10.127.238.84	Windows 7	ePHI

### Asset Inventory Use Case 3 – Creating Bookmarks

You can easily save the current display in order to return to it at a later time. This is done by creating a "Bookmark".

1. Once you have configured the display as desired, click on **Bookmarks** and then on **+ Save Current Search**.

TYPE	CATEGORY	ROLE	STATUS	DISPLAY NAME	MODEL	VENDOR	LAST SEEN		
DICOM Workstation	Radiology	Workstation	Offline	jshaws216	AW Server	GE	20 days		EPH
DICOM Workstation	Radiology	Workstation	Offline	RA600	Centricity RA600...	GE	18 days		EPH
DICOM Workstation	Radiology	Workstation	Online	GE_OS2	CR OS	Agfa Heal...	1 hr		EPH

2. In the dialog that opens, type in a name for the search (e.g. "DICOM Workstations with Status Column"), and then click **Save Search**.  
You can now return to this precise display configuration by clicking on Bookmarks and selecting this item.

### Monitoring Network Traffic

Cynerio integrates with your network through passive Collectors connected to network switches via a SPAN port. This approach provides a copy of network traffic to Cynerio which removes sensitive information such as ePHI while identifying characteristics relevant to the security posture of a device such as destination asset, protocols and ports. Additionally, AI algorithms are implemented to determine the purpose of each communication and designate a "Profile" for each conversation (e.g. Cloud Services, Data Transfer, Software Update, etc.). The result is non-intrusive analysis of network traffic, identification of risky communication patterns, and the foundation for Cynerio to resolve issues through segmentation mappings and customized network polices for each segment.

### Network Screen

This screen shows a list of all Network Connections between assets in your network. For each connection, detailed information is shown about the source and destination asset, protocol used and when the connection was last seen in the network.

Cynerio classifies each connection by the "Connection Type", i.e. Internal, External-Incoming or External-Outgoing. Cynerio also uses AI algorithms to determine the purpose of the communication and designates a "Profile" for each conversation (e.g. Cloud Services, Data Transfer, Software Update etc.).

**NOTE:** Conversations with identical characteristics (e.g. source asset, destination asset, protocol etc.) are treated as a single Network Connection.

CONN. TYPE	SRC. IP	SRC. TYPE	SRC. MODEL	DEST. IP	DEST. TYPE	DEST. MODEL	PROTOCOL	PORT	TRANS.	LAST SEEN ↓
Internal		PC		10.127.86.106	Connectivity E		cerner		Serial	2 hrs
Internal		PC		10.127.86.82	Connectivity E	Cerner Connectiv...	cerner		Serial	2 hrs
Internal		PC		10.127.86.81	Connectivity E		cerner		Serial	2 hrs
Internal		Neonatal Moni	Series 50 Fetal M...	10.127.248.207	Connectivity E	Cerner Connectiv...	cerner		Serial	2 hrs
Internal		Neonatal Moni	Series 50 Fetal M...	10.127.248.236	Connectivity E	Cerner Connectiv...	cerner		Serial	2 hrs
Internal		Anaesthesia Ma		10.127.215.118	Connectivity E	Cerner Connectiv...	cerner		Serial	2 hrs
Internal		PC		10.127.203.109	Connectivity E	Cerner Connectiv...	cerner		Serial	2 hrs
Internal		PC		10.127.215.118	Connectivity E	Cerner Connectiv...	cerner		Serial	2 hrs

### Network Use Case 1 – Filtering by Profile

Let's say that you want to identify which of your assets are sending unidentified types of outbound communications to risky destinations via the internet.

1. Go to the **Network** screen.
2. Click on **Manage Columns** and select **Host Geolocation**.
3. Reposition the columns so that **Conn. type**, **Destination type**, **Profile** and **Host Geolocation** are grouped together.
4. Filter the Conn. type column for **External - Outbound**.
5. Filter the **Profile** column for **Other**.  
You can see all outbound communications for which Cynerio was not able to determine the purpose of the communication.
6. You can now click on the **Host Geolocation** column header and select the countries that you consider suspicious for your network to be sending info to.

CONN. TYPE	DEST. TYPE	HOST GEOLOCATION	PROFILE	SRC. IP	SRC. TYPE	DEST. IP	PROTOCOL	PORT	LAST SEEN	TRANS.
External - Outb...	Internet	China	Other	172.30.27.238	Printer	103.72.47.243	HTTPS	443	2 mth	TCP
External - Outb...	Internet	China	Other	172.30.27.238	Printer	103.72.47.242	HTTPS	443	2 mth	TCP
External - Outb...	Internet	China	Other	172.30.25.203	Clinical Works...	183.38.108.251	HTTPS	443	18 days	TCP
External - Outb...	Internet	Korea, Republic of	Other	10.227.106.121	DICOM Workst...	119.161.10.88	HTTPS	443	1 mo	TCP
External - Outb...	Internet	Korea, Republic of	Other	10.227.106.121	DICOM Workst...	119.161.14.93	HTTPS	443	1 mo	TCP

### Network Use Case 2 – Drilling down to view Asset communication info

Now, you can drill-down to view more detailed info about the assets that are being used for the risky communications described in the previous use case.

1. In the **See related** section, click on **Assets**.

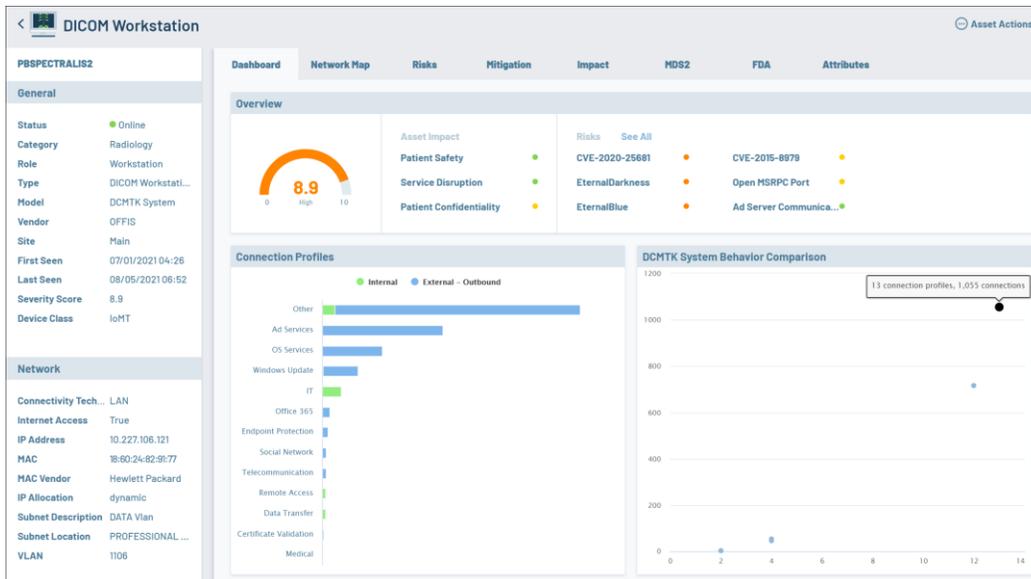
CONN. TYPE	DEST. TYPE	HOST GEOLOCATION	PROFILE	SRC. IP	SRC. TYPE	SRC. MODEL	DEST. IP	DEST. MODEL	PROTOCOL	PORT	LAST SEEN
External - Outb...	Internet	Czechia	Other	172.30.27.94	Clinical Works...	EHR Workstation	185.93.1.242		HTTPS	443	1 mo
External - Outb...	Internet	Czechia	Other	10.127.237.50	CAD	DynaCAD	185.93.1.22		HTTPS	443	21 days
External - Outb...	Internet	Czechia	Other	10.127.237.52	CAD	DynaCAD	185.93.1.243		HTTPS	443	17 days
External - Outb...	Internet	Korea (Republic of)	Other	10.127.237.50	CAD	DynaCAD	14.34.11.240		HTTPS	443	21 days

The Assets screen opens, with a customized filter applied to show only the assets that were

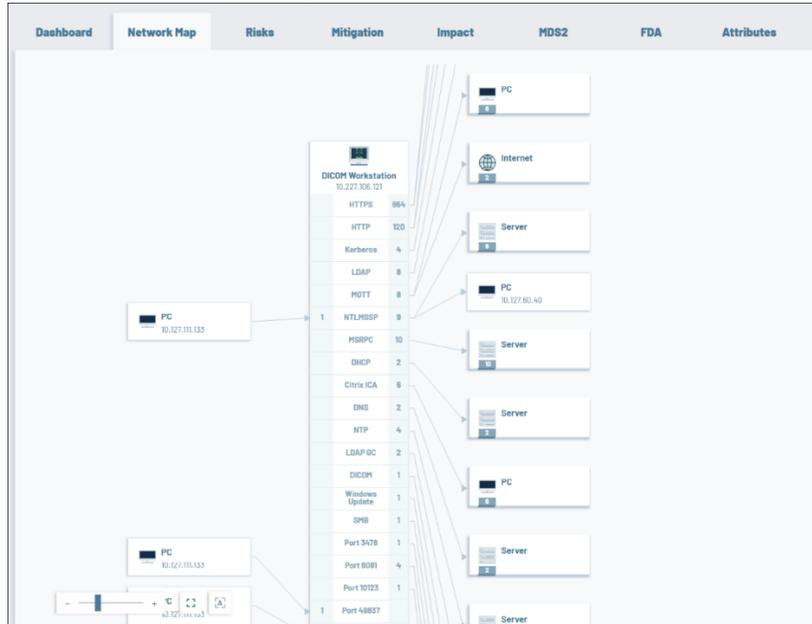
displayed on the Network screen (i.e. External – Outbound, profile “Other”, to specified locations). You can see important details about these assets such as, whether or not they handle ePHI and which VLAN they are on.

SITE	TYPE	MODEL	VENDOR	OS	ePHI	VLAN	SEVERITY	CATEGORY	ROLE	DISPLAY NAME	IP ADDRESS
Main	DICOM Workstation	DCHTK System	OFFIS	Windows 10 Pro for W...	Y	1106	HIGH	Radiology	Workstation	PBSPECTRALIS2	10.227.106.1
Main	CAD	DynaCAD	Phillips	Windows 10		10.0.0.0/8	HIGH	Radiology	Workstation	JSH6MP050	10.127.237.5
Main	CAD	DynaCAD	Phillips	Windows 10		10.0.0.0/8	HIGH	Radiology	Workstation	JSH6MP052	10.127.237.5
Main	Clinical Workstation	EHR Workstation	Enovate M...	Raspberry PI OS		10.0.0.0/8	MEDIUM	Medical Workstat...	Workstation	3110783000015...	172.30.27.9
Main	Printer	Officejet Pro 8020	HP			172.30.0.0/12	LOW	Printers	Peripheral	pop-os	172.30.11.15
Main	Printer	XP-880	Epson			172.30.0.0/12	LOW	Printers	Peripheral	MacBook-Pro-4	fe80-0000:

2. Click on an asset row to drill-down to see additional info about that asset. The Dashboard shows important info about the asset, such as the overall Risk status and the Connection Profiles that it was involved in.



3. Click on the **Network Map** tab to show a map of the ports on the asset and the communication for each port.



## Risk

Cynerio automatically identifies and detects risks affecting the devices in your network. Our wide ranging detection capabilities include vulnerabilities affecting the software running on your devices as well as behavioral risks due to insecure practices such as improper authentication, open ports, unsafe communication etc.

A "Risk" in Cynerio refers to a specific instance of a particular Risk that affects a specific asset in your network.

## Risk Classification

Cynerio classifies Risks using a hierarchical system. The main Risk Types are:

- Behavioral – the asset was not configured in a secure manner, for example, the default password is still in use.
- Vulnerability – the software or firmware running on the asset is affected by a known cyber security vulnerability, for example, a CVE.
- Recall – the asset is subject to a manufacturer recall.

The Risk classification is broken down further using the following hierarchy:

Risk Type → Risk Group → Risk Title → Risk Instance

For example, if you have a DICOM Workstation that has weak HTTP credentials, it is classified as:

Behavioral → Misconfigurations → Weak HTTP Credentials → Weak HTTP Credentials on DICOM Workstation at IP 10.127.236.83

## Risk Score

Accurately managing and prioritizing risk in clinical environments is inaccurate without accounting for the clinical impact of each device. Therefore, for each Risk, Cynerio first determines the "Base Score" (0-10) based on the NIST framework for Risk Assessment and Risk Management. Then, Cynerio factors in the healthcare specific factors of impact on confidentiality, patient safety and service disruption, in order to determine the specialized healthcare "Risk Score" (0-10).

### Risk Status

A Risk Status is assigned to each individual Risk instance, making it easy to prioritize and manage the required mitigation procedures. The following is a description of the various statuses:

- **Identified** – the Risk was identified by Cynerio, with a high degree of certainty
- **Suspected** – the Risk was identified by Cynerio, but there is some degree doubt
- **Accepted** – a user marked the Risk as “Accepted”, indicating that they are not concerned about the threat posed by this Risk
- **Mitigated** – the Risk has been mitigated. This may have been automatically detected by Cynerio or it may have been manually marked by a user.
- **Inactive** – the Risk hasn’t been identified by the system for an extended period of time

When a Risk is first identified, it is designated either as Identified, or Suspected (depending on the degree of certainty). You can then assess the relevance to your deployment and mark it as Accepted, if you feel that it does not require attention. If you take steps to mitigate the Risk, you can then manually mark it as Mitigated or you can wait for the system to automatically identify the mitigation.

You can change the status of a Risk on the **Asset** page > **Risks** tab, by clicking on the status box at the top of the Risk pane.

The screenshot shows the Cynerio interface for a specific risk instance. The top navigation bar includes tabs for Dashboard, Network Map, Risks, Mitigation, Impact, Utilization, MDS2, FDA, and Attributes. The 'Risks' tab is active. The main content area displays the risk details for CVE-2010-5310, which is categorized as 'Default Password CVEs'. A red hand icon points to the 'IDENTIFIED' status box in the top right corner of the risk pane. The risk score is 10, indicated by a red gauge. The interface also shows a table of impact categories and a description of the vulnerability.

Impact (environmental score)	Base Score
Confidentiality: Medium	10
Patient Safety: High	
Service Disruption: Medium	

Confidentiality	Integrity	Availability
Complete	Complete	Complete

Type	Vendor	CVE	CWE	Publish Date
Vulnerability	GE	CVE-2010-5310	Credentials Management...	08/04/2015

Alternatively, you can right click on a row in the **Risks** screen > **Risks** tab, and select **Change status**.

### Risk Screen

All Risks that affect the assets in your network are shown on the Risks screen. The Risks screen has two tabs, *Risk Summary* and *Risks*.

- **Risk Summary** – shows a list of all of the Risk Titles that were identified in your network. For each Risk Title, details about the nature of the threat are shown as well as the number of assets affected by the Risk, broken down by status. You can click on a number to view all of the instances of that Risk with a particular status in the Risks tab. You can also filter the display by Risk Type by clicking on the filter buttons at the top of the tab.

NAME	RISK GROUP	IDENTIFIED	MITIGATED	CVE	CWE	BASE SCORE
Web Services Discovery In Use	Vuln. Bcast/Mcast	14	0			
Weak Telnet Credentials	Misconfigurations	5	0			
Weak SNMP Credentials	Misconfigurations	0	0			
Weak HTTP Credentials	Misconfigurations	25	0			
Weak FTP Credentials	Misconfigurations	10	0			
Vulnerable Service Lighttpd: 1.4.23	Vuln. Services	16	0	CVE-2013-4659	Permissions, Privileges, and ...	7.6
vsFTPd 2.2.2	Vuln. Services	0	0	CVE-2015-1419	Vulnerable FTP Service	5
vsFTPd 2.1.0	Vuln. Services	1	0	CVE-2015-1419	Vulnerable FTP Service	5

You can drill down to see additional info about the characteristics of the Risk by clicking on a row to expand the view.

NAME	RISK GROUP	IDENTIFIED	MITIGATED	CVE	CWE	BASE SCORE
Web Services Discovery In Use	Vuln. Bcast/Mcast	14	0			
CONNECTIONS: 474,952    EVENTS (Last 7d): N/A    LAST EVENT DATE: N/A						
<b>DETAILS</b> Since UDP is a stateless protocol, requests to the WSD service can be spoofed. This ultimately causes the impacted server, or service, to send responses to the intended victim, consuming large amounts of the target's bandwidth.						
Weak Telnet Credentials	Misconfigurations	5	0			
Weak SNMP Credentials	Misconfigurations	0	0			

- Risks** – shows a list of each specific instance of the Risks in your network. For each Risk, detailed info is shown about the affected asset as well as info about the severity of the Risk and its status.

RISK TYPE	ASSET TYPE	IP	DISPLAY NAME	IMPACT CONFIDENTIALITY	IMPACT PATIENT SAFETY	IMPACT SERVICE DISRUPTION	RISK SCORE	STATUS
Behavioral	Printer	172.30.30.24	DEV03B21F.local	Low	Low	Low	1.8	Accepted
Behavioral	Printer	172.30.4.42	HP860E39	Low	Low	Low	1.8	Identified
Behavioral	CAD	10.127.238.125	JSHRW125	Medium	Low	Medium	2.9	Identified
Behavioral	Printer	10.127.180.130	ET788C77A077A3	Low	Low	Low	1.8	Identified
Behavioral	Printer	10.127.177.151	HP8ADE0A	Low	Low	Low	1.8	Inactive
Behavioral	Printer	172.30.19.12	HP8F2241	Low	Low	Low	1.8	Inactive
Behavioral	Printer	172.30.11.210	ET788C77F4AAE3	Low	Low	Low	1.8	Inactive
Behavioral	Mammography	10.127.239.21	DIM_2422	Medium	High	Medium	2.9	Identified

You can click on a row to drill down to see detailed info about the nature of the threat and suggested mitigation procedures. This info is shown in the Risks tab on the Asset page for the affected asset.

Name **Apache 2.2.27 (HTTP)** Risk Group **Vuln. Services** IDENTIFIED

**9.8**  
Critical

Impact (environmental score)		Base Score	
Confidentiality	Medium	Confidentiality	High
Patient Safety	High	Integrity	High
Service Disruption	Medium	Availability	High

Type	Vulnerability
Vendor	Apache
CVE	CVE-2017-3167
CWE	Improper Authentication
Publish Date	06/19/2017

**Description**  
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap\_get\_basic\_auth\_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

**Mitigation**  
1. Apply Service Hardening: Apply service hardening for vulnerable service.

**More Details**  
[CVE-2014-0231\(NVD\)](#), [CVE-2014-0231\(MITRE\)](#), [CVE-2016-4975\(NVD\)](#), [CVE-2016-4975\(MITRE\)](#), [CVE-2016-8612\(NVD\)](#), [CVE-2016-8612\(MITRE\)](#), [CVE-2017-3167\(NVD\)](#), [CVE-2017-3167\(MITRE\)](#), [CVE-2017-3169\(NVD\)](#), [CVE-2017-3169\(MITRE\)](#), [CVE-2017-7668\(NVD\)](#), [CVE-2017-7668\(MITRE\)](#), [CVE-2017-7679\(NVD\)](#), [CVE-2017-7679\(MITRE\)](#), [CVE-2018-1312\(NVD\)](#), [CVE-2018-1312\(MITRE\)](#)

### Risk Use Case 1 - Filtering by Risk Type and Generating Reports

Let's say that you want to find out about devices subject to manufacturer recall, and you want to provide the operations manager of a specific facility with an up to date list of all devices at his site that are subject to manufacturer recall.

1. Go to the **Risks** screen > **Risks** tab.
2. Click on **Manage Columns** and select **Risk Type**, **Site**, **Vendor** and **Model**. Reposition the columns so that they are grouped together.
3. Filter the **Risk Type** column for **Recall**.
4. Filter the **Site** column for the desired site (e.g. Main).  
The screen now shows a list of all Risks related to manufacturer recalls at the specified site, as well as details about the affected assets and the impact of the Risk.

RISK TITLE	RISK GROUP	RISK TYPE	MODEL	SITE	ASSET TYPE	IP	IMPACT CONFIDENTIALITY	IMPACT PA
Recall Z-274i-2020	Device Recall Notice	Recall	Alaris PCU 8015	Main	IV Pump	10.227.231.67	Medium	High
Recall Z-274i-2020	Device Recall Notice	Recall	Alaris PCU 8015	Main	IV Pump	10.227.227.101	Medium	High
Recall Z-274i-2020	Device Recall Notice	Recall	Alaris PCU 8015	Main	IV Pump	10.227.224.160	Medium	High
Recall Z-274i-2020	Device Recall Notice	Recall	Alaris PCU 8015	Main	IV Pump	10.227.231.160	Medium	High
Recall Z-274i-2020	Device Recall Notice	Recall	Alaris PCU 8015	Main	IV Pump	10.227.224.28	Medium	High

5. You can now generate a report to be sent to the operations manager, as follows:
  - a. Click on **Reports** > **Create Report**.  
The **Create Report** dialog opens.

**Create Report**

**Device Names**

Report Title: Medical device list

Schedule:  Daily  Weekly  Monthly

**Email Content**

Subject: Medical device list - a scheduled report by Cynerio

Recipients: \_\_\_\_\_

- b. You can edit the **Report Title** and **Subject line** by typing in a description of the report (e.g. Manufacturer Recalls at Main Site).
- c. Select the radio button for the desired schedule (frequency).
- d. In the **Recipients** field, enter the email of the operations manager.
- e. Click **Save Report**.  
Reports will be sent periodically with up to date information about recall Risks at the specified site.

## Risk Use Case 2 - Drilling down to analyze Risks – Managing Risk Status

Let's say that you want to assess the most critical cyber security vulnerabilities (e.g. CVEs) that effect patient confidentiality at your healthcare facility.

1. Go to the **Risks** screen > **Risks** tab and clear all existing filters but leave the column configuration.
  2. Click on **Manage Columns** and select **Risk Type**.
  3. Filter the **Risk Type** column by **Vulnerabilities**.
  4. Filter the **Impact Confidentiality** column by **High**.
  5. Filter the **Status** column by **Identified**.
  6. Sort by **Risk Score** (from high to low).
- The results now show a list of vulnerabilities that have high impact on confidentiality, sorted from the most severe to the least.

RISK TITLE	RISK GROUP	RISK TYPE	ASSET TYPE	IP	IMPACT CONFIDENTIALITY	IMPACT PATIENT SAFETY	IMPACT SERVICE DISRUPTION	RISK SCORE
Apache 2.4.27 (HTTP)	Vuln. Services	Vulnerability	LIS Server	10.127.62.42	High	Low	High	10
DejaBlue	RDP CVEs	Vulnerability	LIS Server	10.127.60.27	High	Low	High	10
DejaBlue	RDP CVEs	Vulnerability	LIS Server	10.127.60.27	High	Low	High	10
Legacy OS	End of Life OS	Vulnerability	PACS Server	10.127.62.114	High	Low	High	10
Legacy OS	End of Life OS	Vulnerability	LIS Server	10.127.60.27	High	Low	High	10
Legacy OS	End of Life OS	Vulnerability	LIS Server	10.127.60.249	High	Low	High	10
Legacy OS	End of Life OS	Vulnerability	LIS Server	10.127.193.232	High	Low	High	10

- Click on the top item in the list to view additional details and mitigation recommendations. Details about the vulnerability are shown in the Risks tab for the affected asset.

The screenshot displays the 'Risks' tab for the asset 'Apache 2.4.27 (HTTP)'. The risk is categorized as 'Vuln. Services' and is currently 'IDENTIFIED'. A gauge shows a score of 10, labeled as 'Critical'. Key attributes include Confidentiality (High), Integrity (High), and Availability (High). The description states: 'In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.' Mitigation steps include 'Apply Service Hardening: Apply service hardening for vulnerable service.' A list of 'More Details' includes various CVEs such as CVE-2017-15710, CVE-2018-1283, and CVE-2019-10098.

- If you would like to change the Status of this Risk, for example if you have taken mitigation steps or have determined that it does not pose a threat in the context of your facility. Do the following:

- Click on the status box at the top right of the Risk pane (IDENTIFIED). The Risk Settings dialog opens.

The 'Risk Settings' dialog box is shown with a close button (X) in the top right corner. The 'Status' is currently set to 'Identified' with a dropdown arrow. Below it is a text area for a 'Comment' with an asterisk indicating it is mandatory. At the bottom, there are 'Cancel' and 'Confirm' buttons.

- Click on the **Status** field and select from the dropdown list the Status that you would like to assign to this Risk (Mitigated or Accepted).
  - In the **Comment** field, add a comment describing the reasons for the change of Status. (Mandatory)
  - Click **Confirm**.
- When you finish analyzing this vulnerability, you can navigate back to the Risks screen to view the next item in the list.

### Dashboards

Cynerio dashboards provide centralized information that enables stakeholders to gain important insights at a glance. Cynerio provides standardized dashboards with each deployment that consist of a series of widgets showing key data and visualizations. These widgets are interactive and allow users to navigate to relevant information with one click. In addition to the standard dashboards supplied by Cynerio, individual users can prepare specialized dashboards and share them with other users. There are two types of dashboards:

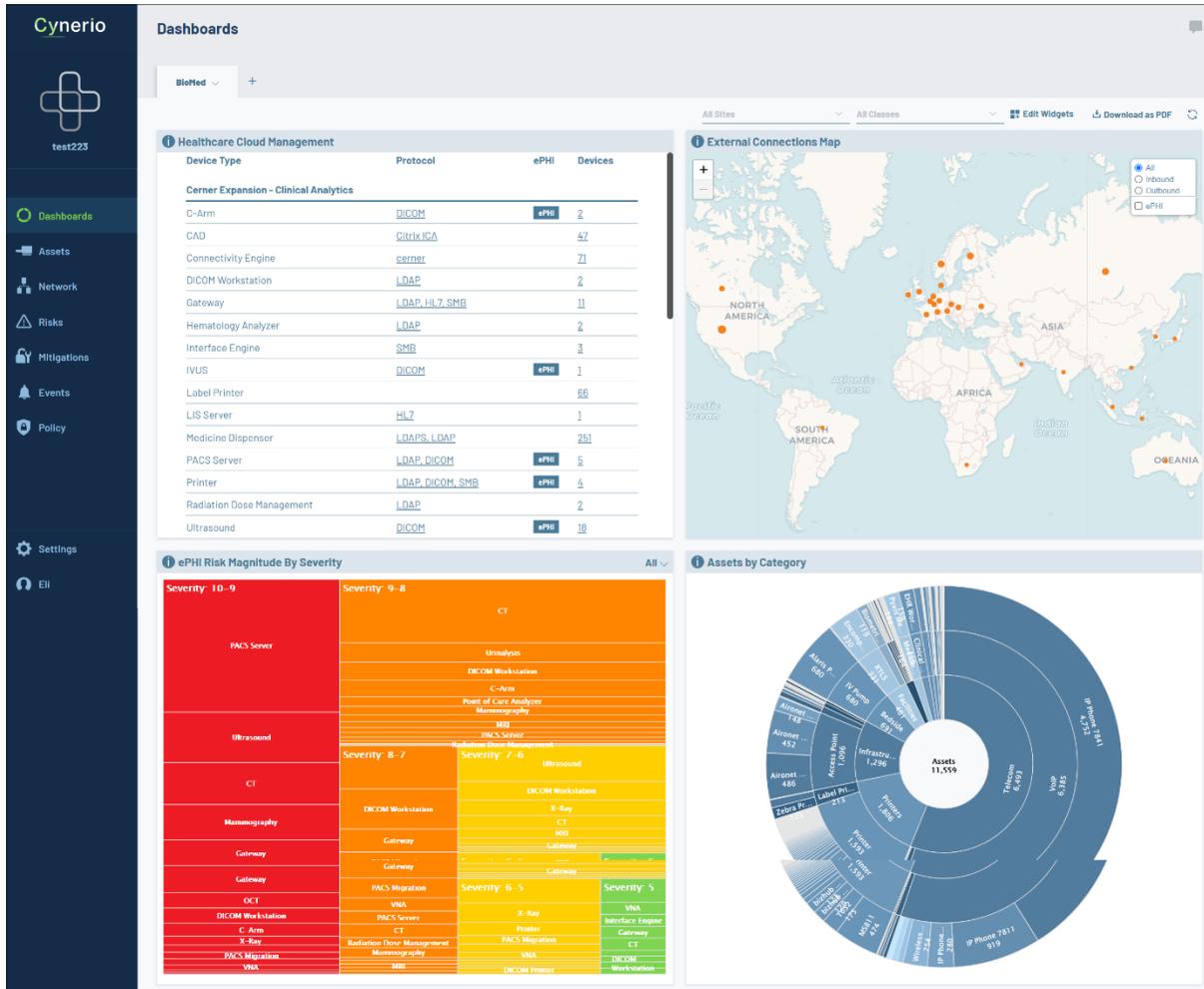
- Private – viewable only to the user who creates the dashboard.
- Public - viewable for all users.

All you need to do to create a customized dashboard is select the widgets that you want to include (from dozens of pre-configured widgets) and adjust their positions on the page.



### Dashboard Screen

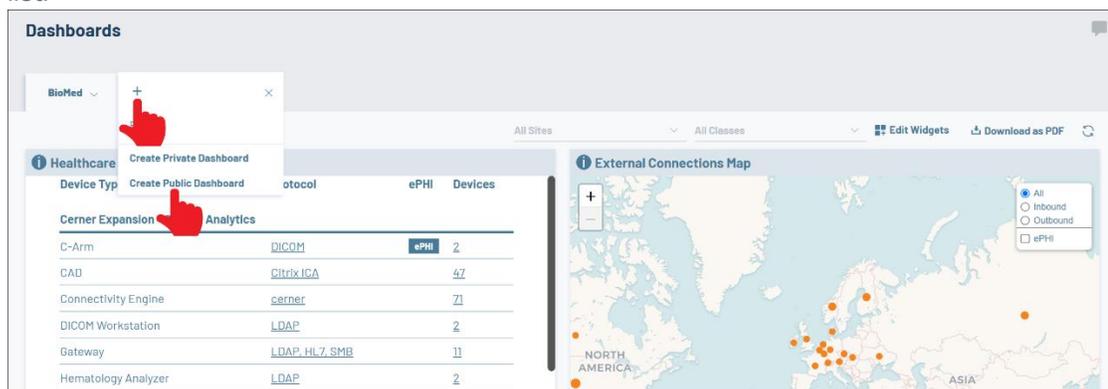
The Dashboards tab shows each of your Dashboards in a separate tab. You can filter the display by Site and by Asset Class. Click on a data element to drill-down into that element.



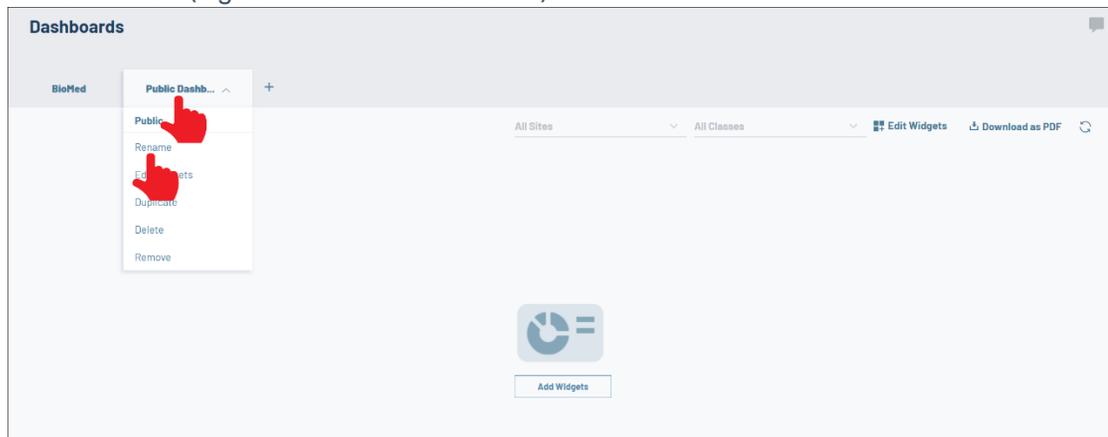
### Dashboard Use Case

Let's say that you want to create a public dashboard that enables your security department to monitor outbound internet access from the IoMT devices in your network.

1. Go to the **Dashboards** screen.
2. Click on "+" in the tabs selection and select **Create Public Dashboard** from the dropdown list.



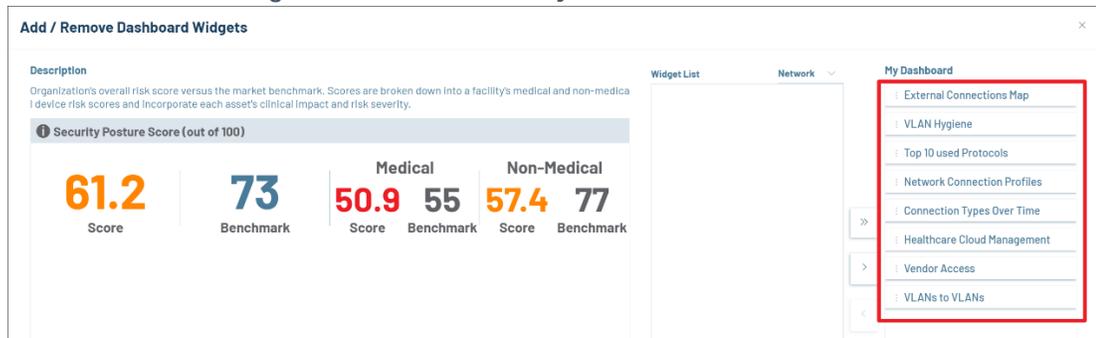
3. Click on the **Public Dashboard** tab and select **Rename**. Then, enter a descriptive name for the dashboard (e.g. External Communication).



- Click on **Add Widgets** (either in the middle of the screen or in the header bar). The **Add/Remove Dashboard Widgets** window is shown.

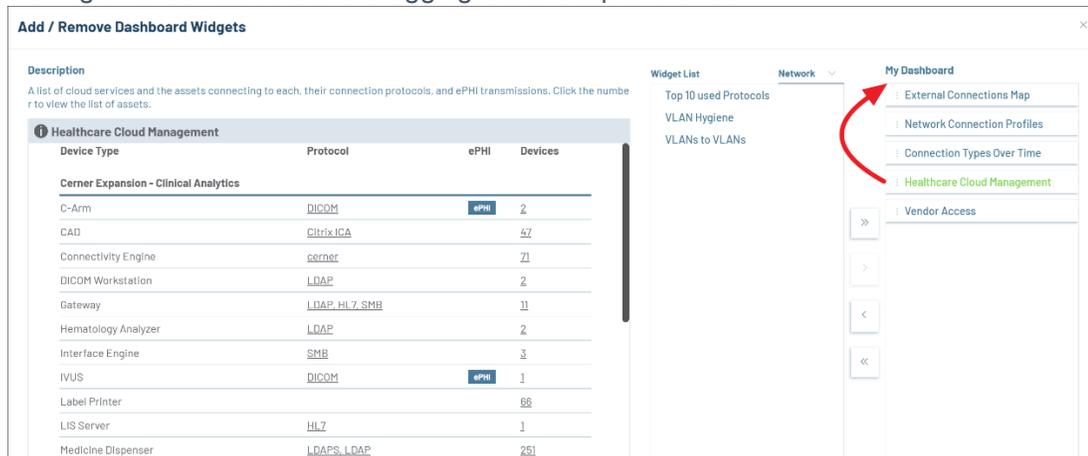


- For our use case we want to focus on network widgets, so click on the widget filter (All) and select **Network**.
- Bulk add all Network widgets by clicking on the  button. All of the Network widgets are added to the **My Dashboard** column.



- For our dashboard, the "VLAN Hygiene", "Top 10 used Protocols" and "VLANs to VLANs" widgets are less interesting. So, we will select each one and click on the  button to remove it from the dashboard.
- Click on the "Healthcare Cloud Management" widget to show a preview in the left pane. We see that this is very useful information, so you can promote it to the top of the display by

clicking on the three dots and dragging it to the top of the list.



9. Click **Save** at the bottom of the screen.  
Your new dashboard is created.

### Monitoring Events

Cynerio detects a broad range of Events that occur in your Network that may require your attention. The Events screen shows a log of all of the Events that are detected. You can also create notification profiles in order to receive email notifications when particular Events occur.

The following Event Types (Modules) are detected:

- **Assets** – Events that relate to the automated Asset Inventory, for example, a new asset was detected in the Network.
- **Healthcare Protocols** – An error was detected in the use of a healthcare protocol.
- **Intrusion Detection System (IDS)** – An insecure communication pattern was detected. This includes both actual exploitation attempts as well as use of insecure protocols (Telnet, RDP etc.) which are susceptible to attacks.
- **Policy Violation** – Once you have configured security Policies in your system (which define allowed and not allowed traffic for particular assets based on E-W, N-S segmentation etc.) any traffic which violates a Policy generates an Event.  
**NOTE:** Policy violations are only logged while the Policy is in “Validation” status. Once a Policy has been enforced on the network no further Events are detected by Cynerio.
- **Risk** – A new Risk was detected on one of the assets in your network, or the status of an existing Risk changed (e.g. a Risk became Inactive or returned to being Active). See **RISK**.

### Events Screen

This screen shows a list of all Events that occurred in your network. Each Event is categorized by the general type of Event (Module) and the specific Event that occurred. Detailed info is given about the affected asset as well as a description of the Event.

The screenshot shows the Cynerio interface with a sidebar on the left containing navigation options: Dashboards, Assets, Network, Risks, Mitigations, Events (highlighted), and Policy. The main content area has a search bar and two tabs: 'Security Events (345,096)' and 'Audit Log (...)'. Below the tabs are icons for Reports, Bookmarks, Manage Columns, and Export Table. The table below lists events with columns for Time, Module, Event, Details, Device Type, Device IP, and Severity.

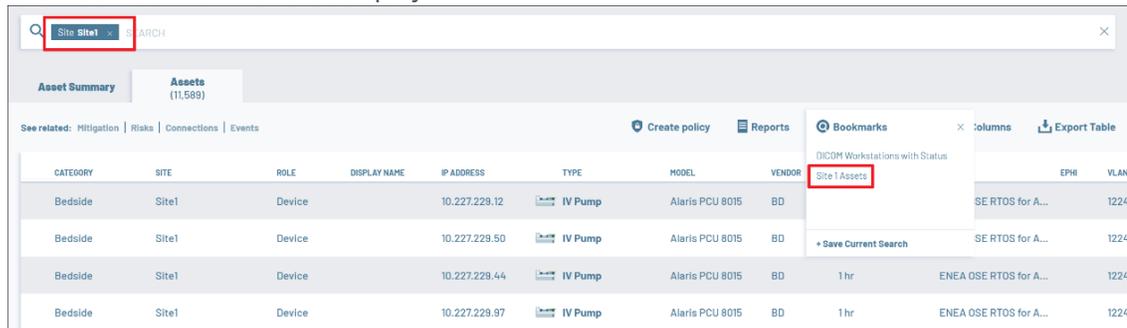
TIME	MODULE	EVENT ↓	DETAILS	DEVICE TYPE	DEVICE IP	SEVERITY
12/11/2020 08:29:24	IDS	Weak Password	Service: HTTP, User Name: admin, Source IP: 10.127.60.166	UPS	10.127.221.250	MEDIUM
12/11/2020 15:36:23	IDS	Weak Password	Service: HTTP, User Name: logclient, Source IP: 10.127.236.84	DICOM Workstation	10.127.236.93	MEDIUM
12/10/2020 10:06:04	IDS	Weak Password	Service: HTTP, User Name: logclient, Source IP: 10.127.236.84	DICOM Workstation	10.127.236.93	MEDIUM
12/11/2020 08:26:37	IDS	Weak Password	Service: HTTP, User Name: logclient, Source IP: 10.127.236.84	DICOM Workstation	10.127.236.93	MEDIUM
12/14/2020 16:30:48	IDS	Weak Password	Service: HTTP, User Name: admin, Source IP: 10.127.60.166	UPS	10.127.221.250	MEDIUM
12/11/2020 15:27:35	IDS	Weak Password	Service: HTTP, User Name: root_admin, Source IP: 10.127.82.40	PACS Server	10.127.58.229	MEDIUM
12/09/2020 16:06:58	IDS	Weak Password	Service: FTP, User Name: gpooperator, Source IP: 10.127.63.215	MRI	10.127.239.138	MEDIUM
12/10/2020 00:08:24	IDS	Weak Password	Service: FTP, User Name: kingbird, Source IP: 10.127.63.215	CT	10.127.239.125	MEDIUM



### Events Use Case 1 – Creating Notifications

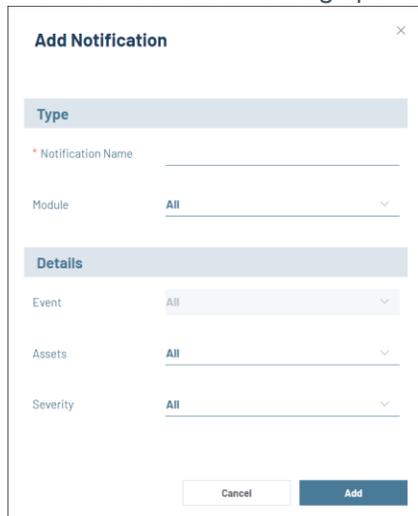
Let's say that you are responsible for IT security at one of your organization's facilities. You can create a Bookmark for all assets at your site. You can then set up notifications for cyber threats affecting those assets to be sent to you.

1. On the **Assets** screen, filter for a specific Site (you may need to first add the "Site" column using Manage Columns).
2. Create a Bookmark for that display.



CATEGORY	SITE	ROLE	DISPLAY NAME	IP ADDRESS	TYPE	MODEL	VENDOR	EPH	VLAN
Bedside	Site1	Device		10.227.229.12	IV Pump	Alaris PCU 8015	BD		1224
Bedside	Site1	Device		10.227.229.50	IV Pump	Alaris PCU 8015	BD		1224
Bedside	Site1	Device		10.227.229.44	IV Pump	Alaris PCU 8015	BD	1 hr	1224
Bedside	Site1	Device		10.227.229.97	IV Pump	Alaris PCU 8015	BD	1 hr	1224

3. Click on your user name at the bottom of the main navigation.
4. In the Notifications tab (default) click **Add Notification**.  
The Add Notification dialog opens.



**Add Notification**

Type

\* Notification Name

Module: All

Details

Event: All

Assets: All

Severity: All

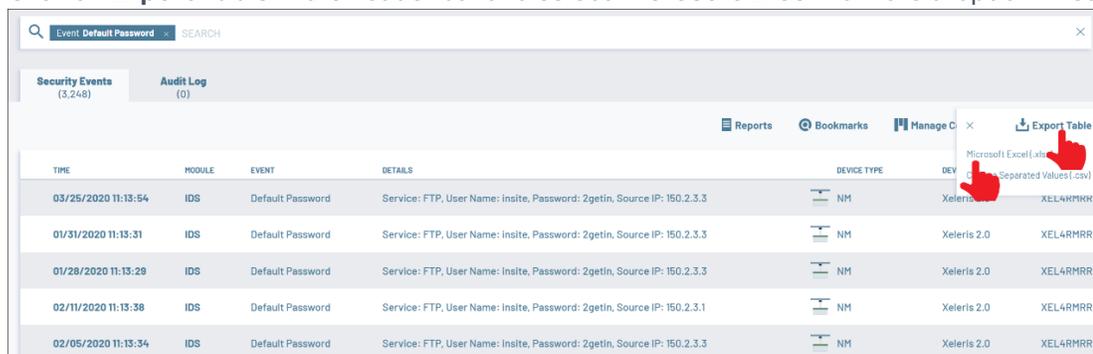
Cancel Add

5. Enter a name for the notification, then select **IDS** for the Module
6. In the Details section, for **Event** select **Exploitation Attempt**. For **Assets**, select **Site 1 Assets** (referring to the Bookmark that you created in step 2).
7. Click **Add**.  
You will receive email notification whenever an Exploitation Attempt is detected at Site 1.

### Events Use Case 2 – Exporting Tables

Let's say that you were assigned the responsibility to ensure that no assets in your facility are using default passwords.

1. On the **Events** screen, filter the **Module** column for "IDS".
2. Filter the **Event** column for "Default Password".
3. Sort the table by the **Device Name** column.  
You now have a comprehensive list of Events involving use of default passwords, sorted by the devices on which they occurred. For each Event, the default User Name and Password are shown.
4. Click on **Export Table** in the header bar and select **Microsoft Excel** from the dropdown list.



TIME	MODULE	EVENT	DETAILS	DEVICE TYPE	DEV	EXPORT
03/25/2020 11:13:54	IDS	Default Password	Service: FTP, User Name: insite, Password: 2getin, Source IP: 150.2.3.3	NM	Xeleris	XEL4RMRR
01/31/2020 11:13:31	IDS	Default Password	Service: FTP, User Name: insite, Password: 2getin, Source IP: 150.2.3.3	NM	Xeleris 2.0	XEL4RMRR
01/28/2020 11:13:29	IDS	Default Password	Service: FTP, User Name: insite, Password: 2getin, Source IP: 150.2.3.3	NM	Xeleris 2.0	XEL4RMRR
02/11/2020 11:13:38	IDS	Default Password	Service: FTP, User Name: insite, Password: 2getin, Source IP: 150.2.3.1	NM	Xeleris 2.0	XEL4RMRR
02/05/2020 11:13:34	IDS	Default Password	Service: FTP, User Name: insite, Password: 2getin, Source IP: 150.2.3.3	NM	Xeleris 2.0	XEL4RMRR

5. In the dialog that opens, enter a **File Name** for the file and click **Export**.
6. You can now print out this file and use it to identify each device that needs to have the credentials updated. Then, use the default Username and Password to log in and set the new credentials.
7. You can keep up to date if new Events occur of assets using default passwords. This is done by can creating a Report that is generated at scheduled intervals (e.g. daily, weekly) and sent to designated email recipients. See the procedure described in the **GENERATING REPORTS** use case.

## Mitigations

In addition to the automated discovery of assets and risks, Cynerio automatically generates mitigation recommendations in order to quickly and efficiently address any identified issues. Mitigations can relate to individual assets or they can involve segmenting groups of assets both for East-West traffic and North-South traffic. There are two types of Mitigation actions:

- **Device mitigations** – Cynerio identifies the actions that need to be taken on specific device, such as changing passwords, changing configurations or updating firmware.
- **Network mitigations** – Cynerio automatically generates recommended Policies, which comprise a series of rules defining allowed traffic for the assets in your network. These Policies can relate to individual assets (service hardening) or to a group of assets that are treated as a virtual segment. Separate segmentation Policies are applied to E-W and N-S traffic.

**NOTE:** Device mitigations are generally intended to remove the vulnerability entirely, as opposed to Network mitigations which focus on limiting the risk posed by existing vulnerabilities by reducing the exposed attack surface.

## Device Mitigations

For risks that relate to the configuration of the devices themselves (and not to their network traffic), Cynerio gives recommendations for reconfiguring the specified devices in a manner that makes them less vulnerable to risks.

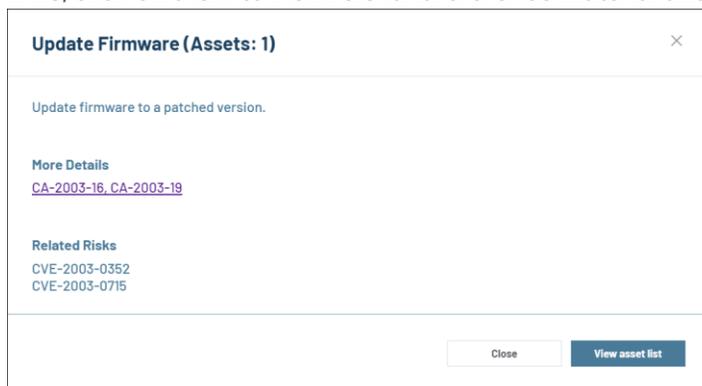
**NOTE:** After implementing a Mitigation you can manually change the status of the related Risk to "Mitigated". However, this is generally unnecessary as the system automatically marks Risks as "Mitigated" when it detects that effective mitigation steps have been taken.

## Device Mitigations Use Case

*Let's say that you want to protect your network from risks caused by outdated firmware on your IP Cameras.*

1. On the **Mitigations** screen, filter the **Action** column for **Update Firmware**.
2. Filter the **Type** column for **IP Camera**.
3. For each Mitigation, take the following steps:

- a. Click on a row to view additional info about that Mitigation. If there are "More Details" links, click on them to view relevant reference material and then close the dialog.



- b. Click on the number in the **Asset Count** column.  
The Assets screen opens, filtered to show only assets that require this Mitigation.
  - c. Identify the relevant devices by their IPs and/or Display Names.  
**NOTE:** If you have integrated Cynerio with your asset management system, then the device location will also be shown.
  - d. Upgrade the firmware on each of the relevant devices.
4. Navigate back to the list of "Update Firmware" Mitigations for "IP Cameras" and repeat the above procedure for each Mitigation.

## Network Mitigations

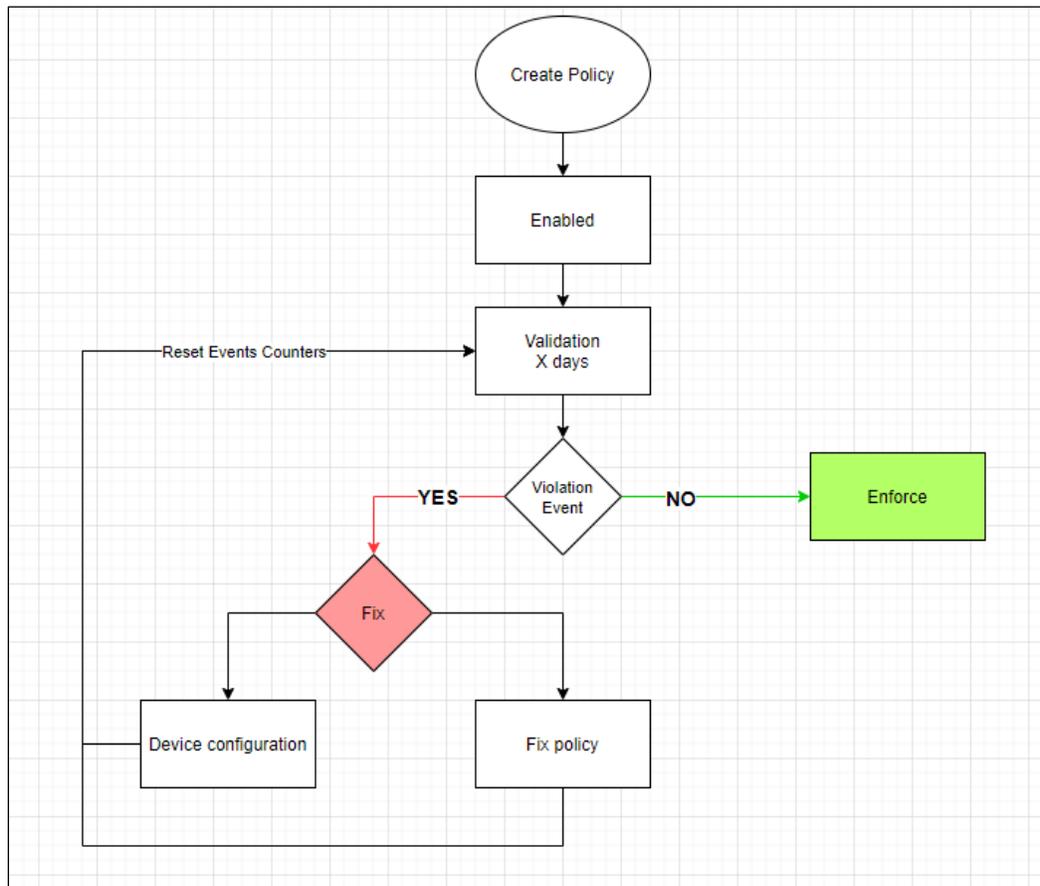
Network Mitigations are some of the most effective ways to quickly reduce a wide variety of risks. Through Network Mitigations you are able to limit the types of communication that are allowed for the assets in your network. These Mitigations can apply to specific ports/services on a particular asset or to an entire segment.

Cynerio enables you to apply the following types of network mitigations:

- **SERVICE HARDENING** - for a specific device.
- **EAST-WEST SEGMENTATION** - for assets with similar E-W communication patterns.
- **NORTH-SOUTH SEGMENTATION AND VENDOR ACCESS** - for assets with similar N-S communication patterns.

For each type of Mitigation, Cynerio automatically generates recommended Policies, which comprise a series of rules defining allowed traffic. First, you enable a policy and begin the *validation* period, during which Policy violations generate warning Events in the system. Then, you have the opportunity to tweak the rules before starting to enforce the Policy on your NAC/firewalls.

The following diagram shows the workflow for implementing Policies:



### Service Hardening

Service hardening involves reducing the attack surface of a device by limiting the entities with which it is allowed to communicate. Cynerio analyzes your baseline network communication patterns and automatically generates customized service hardening Policy recommendations for your assets. All you need to do is enable the Policy, monitor the system during the *validation* period, tweak the rules as needed and then go ahead and *enforce* the Policy in your network.

This is done on asset by asset basis, making it easier to implement than segmentation.

**NOTE:** If several ports/services on the same asset require service hardening, a separate Policy is created for each port.

### Service Hardening Use Case

Let's say you'd like to monitor RDP based vulnerabilities on critical medical devices and limit that type of access on them.

**NOTE:** RDP (Remote Desktop Protocol) is known to be a highly vulnerable protocol, which is susceptible to various types of Ransomware and Malware. Therefore, when dealing with critical medical devices you should try to limit RDP communications to only required services (e.g. maintenance technicians).

1. On the **Risks** screen > **Risks Summary** tab, filter the **Risk Group** column for "RDP CVEs".

The screenshot shows the 'Risks Summary' tab in the Cynerio interface. A search bar at the top contains the text 'Risk Group: RDP CVEs'. Below the search bar, there are two tabs: 'Risk Summary (3)' and 'Risks (38,791)'. The 'Risk Summary' tab is active. Below the tabs, there are three filter buttons: 'Behavioral', 'Vulnerability', and 'Recall'. To the right, there are icons for 'Reports', 'Bookmarks', and 'Manage Columns'. The main table has the following columns: NAME, RISK GROUP, IDENTIFIED, MITIGATED, CVE, CWE, and BASE SCORE. The table contains three rows of data:

NAME	RISK GROUP	IDENTIFIED	MITIGATED	CVE	CWE	BASE SCORE
DejaBlue	RDP CVEs	1	0	CVE-2019-1181	Improper Access Control	9.8
DejaBlue	RDP CVEs	1	0	CVE-2019-1182	Improper Access Control	9.8
BlueKeep	RDP CVEs	1	0	CVE-2019-0708	Improper Input Validation	9.8

2. Click on the number shown in the **Identified** column for a particular Risk row. This shows a list of the instances of that Risk that were identified.

The screenshot shows the 'Risks Summary' tab in the Cynerio interface. A search bar at the top contains the text 'Risk Group: RDP CVEs'. Below the search bar, there are two tabs: 'Risk Summary (3)' and 'Risks (8)'. The 'Risks' tab is active. Below the tabs, there are two filter buttons: 'Assets' and 'Mitigation'. To the right, there are icons for 'Reports', 'Bookmarks', 'Manage Columns', and 'Export Table'. The main table has the following columns: RISK TITLE, RISK GROUP, ASSET TYPE, IP, IMPACT CONFIDENTIALITY, IMPACT PATIENT SAFETY, IMPACT SERVICE DISRUPTION, RISK SCORE, and STATUS. The table contains four rows of data:

RISK TITLE	RISK GROUP	ASSET TYPE	IP	IMPACT CONFIDENTIALITY	IMPACT PATIENT SAFETY	IMPACT SERVICE DISRUPTION	RISK SCORE	STATUS
DejaBlue	RDP CVEs	LIS Server	10.127.60.27	High	Low	High	10	Identified
DejaBlue	RDP CVEs	LIS Server	10.127.193.232	High	Low	High	10	Identified
DejaBlue	RDP CVEs	PACS Server	10.127.62.114	High	Low	High	10	Identified
DejaBlue	RDP CVEs	DICOM Workstation	10.127.19.227	Medium	Low	Low	8.9	Identified

3. Select a critical Risk instance based on the Asset Type and Risk Score, for example, a LIS Server. Click on the row of that Risk to open the Risks tab for the affected asset.
4. Identify an RDP CVEs Risk for which "service hardening" is a suggested Mitigation action.

- Click on the "Apply Service Hardening" step in the Mitigation section.

The screenshot displays the details for a vulnerability named 'DejaBlue' with a risk group of 'RDP CVEs'. A red hand icon points to the 'Apply Service Hardening' step in the mitigation section.

Impact (environmental score)		Base Score	
Confidentiality	High	Confidentiality	High
Patient Safety	Low	Integrity	High
Service Disruption	High	Availability	High

**Type:** Vulnerability  
**Vendor:** Microsoft  
**CVE:** CVE-2019-1182  
**CWE:** Improper Access Control  
**Publish Date:** 08/14/2019

**Description:** A remote code execution vulnerability exists in Remote Desktop Services - formerly known as Terminal Services - when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka Remote Desktop Services Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2019-1181, CVE-2019-1222, CVE-2019-1226.

**Mitigation:** 1. Apply Service Hardening: Apply service hardening for vulnerable service. 2. Change Configuration: Configure Network Level Authentication for Remote Desktop Services connections, there is partial mitigation on affected systems that have Network Level Authentication (NLA) enabled. The affected systems are mitigated against 'wormable' malware or advanced malware threats that could exploit the vulnerability, as NLA requires authentication before the vulnerability can be triggered. However, affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

- The Mitigation tab opens showing the Mitigation recommendations for the specified asset.

The screenshot shows the 'Mitigation' tab for the 'DejaBlue' vulnerability. A red hand icon points to the 'Create policy' button.

Name	Risk	Score
Apply Service Hardening	DejaBlue	10
	DejaBlue	10

**Description:** Apply service hardening for vulnerable service.  
**More Details:** [Microsoft Security Response Center](#)

**Name:** Change Configuration  
**Description:** Configure Network Level Authentication for Remote Desktop Services connections, there is partial mitigation on affected systems that have Network Level Authentication (NLA) enabled. The affected systems are mitigated against 'wormable' malware or advanced malware threats that could exploit the vulnerability, as NLA requires authentication before the vulnerability can be triggered. However, affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.  
**More Details:** [Configure Network Level Authentication for RDP](#)

- Click **Create Policy**.

- A dialog opens showing the suggested Policy for this asset.

### Service Hardening Policy ×

---

#### RDP

Asset Type Created  
■ LIS Server Fri, 06 Aug 2021 10:54:11

Asset IP Address Modified  
10.127.60.27 Fri, 06 Aug 2021 10:54:11

Deny access to port 3389/TCP except from the following IPs

IP	NOTE
10.227.135.92	
10.127.178.215	
10.227.135.58	
10.227.135.68	

Add IP
Cancel
Save

- You can add or remove IPs to the whitelist as needed.
- When the Policy is ready, click **Save**.

The **Policies** screen > **Service Hardening** tab opens showing the newly created Policy.

E-W Segmentation (8)	N-S Segmentation (8)	Vendor Access (1)	Service Hardening (6)	Cloud Services (5)	Quarantine (0)																																																															
<table border="1" style="width: 100%; border-collapse: collapse; text-align: left;"> <thead> <tr> <th>DEVICE TYPE</th> <th>DEVICE IP</th> <th>PORT</th> <th>CONNECTIONS</th> <th>UNPROFILE CONNECTIONS</th> <th>VIOLATIONS</th> <th>LAST VIOLATION EVENT</th> <th>STATUS</th> <th>STATE</th> </tr> </thead> <tbody> <tr> <td>UPS</td> <td>10.227.195.188</td> <td>80</td> <td>0</td> <td>0</td> <td>0</td> <td></td> <td>●</td> <td>ON</td> </tr> <tr> <td>Printer</td> <td>10.127.16.87</td> <td>139</td> <td>2</td> <td>0</td> <td>0</td> <td></td> <td>●</td> <td>ON</td> </tr> <tr> <td>Printer</td> <td>10.127.16.87</td> <td>21</td> <td>1</td> <td>0</td> <td>0</td> <td></td> <td>●</td> <td>ON</td> </tr> <tr> <td>Printer</td> <td>10.127.16.87</td> <td>445</td> <td>2</td> <td>0</td> <td>0</td> <td></td> <td>●</td> <td>ON</td> </tr> <tr> <td>Printer</td> <td>10.127.233.238</td> <td>21</td> <td>1</td> <td>0</td> <td>0</td> <td></td> <td>●</td> <td>ON</td> </tr> <tr style="border: 2px solid red;"> <td>LIS Server</td> <td>10.127.60.27</td> <td>3389</td> <td>4</td> <td>0</td> <td>0</td> <td></td> <td>●</td> <td>OFF</td> </tr> </tbody> </table>						DEVICE TYPE	DEVICE IP	PORT	CONNECTIONS	UNPROFILE CONNECTIONS	VIOLATIONS	LAST VIOLATION EVENT	STATUS	STATE	UPS	10.227.195.188	80	0	0	0		●	ON	Printer	10.127.16.87	139	2	0	0		●	ON	Printer	10.127.16.87	21	1	0	0		●	ON	Printer	10.127.16.87	445	2	0	0		●	ON	Printer	10.127.233.238	21	1	0	0		●	ON	LIS Server	10.127.60.27	3389	4	0	0		●	OFF
DEVICE TYPE	DEVICE IP	PORT	CONNECTIONS	UNPROFILE CONNECTIONS	VIOLATIONS	LAST VIOLATION EVENT	STATUS	STATE																																																												
UPS	10.227.195.188	80	0	0	0		●	ON																																																												
Printer	10.127.16.87	139	2	0	0		●	ON																																																												
Printer	10.127.16.87	21	1	0	0		●	ON																																																												
Printer	10.127.16.87	445	2	0	0		●	ON																																																												
Printer	10.127.233.238	21	1	0	0		●	ON																																																												
LIS Server	10.127.60.27	3389	4	0	0		●	OFF																																																												

- Toggle the **State** switch to **ON**.
- Navigate back to the list of RDP CVE Risks and repeat the above procedure for each Policy that you would like to create.

### East–West Segmentation

East-West (E-W) segmentation enables you to implement a zero-trust policy in your network. This is done by first dividing your network into logical units which share similar patterns for E-W communication (i.e. lateral traffic between assets inside your network). Then, you can apply unique security policies to each segment, defining what types of E-W communication are allowed. This is essential for isolating threats that have penetrated your network and preventing them from compromising the entire network.

Cynerio enables you to easily apply virtual E-W segmentation to your network. We automate the process of identifying logical segments of assets based on their network communication patterns and generating the rules that define the baseline acceptable communication patterns for each segment. All you need to do is apply our suggested segmentation policies, monitor the segment during the *Validation* period, tweak the rules as needed and then go ahead and *enforce* the Policy in your network.

### East-West Segmentation Use Case

Cynerio monitors the communication between assets in your network and automatically maps out the virtual segmentation of your network, based on shared communication patterns, and generates a recommended policy for each segment.

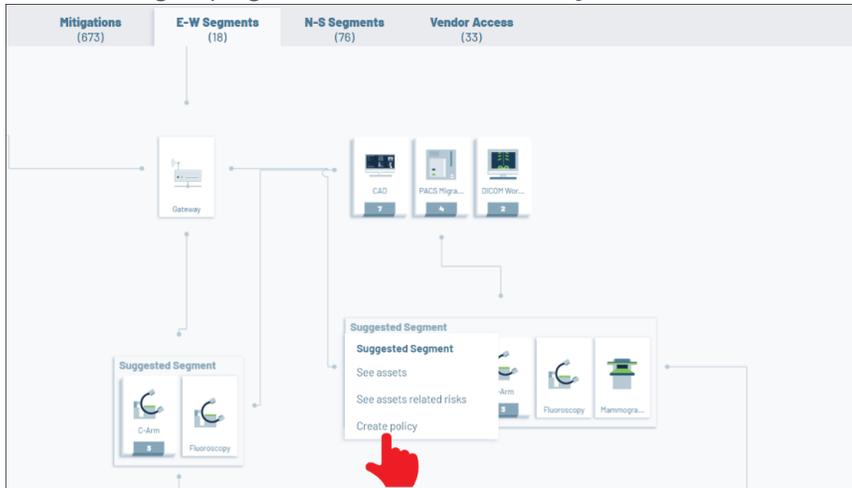
*For each segment, you can use the following procedure to create a policy that limits the allowed communication for the assets in that segment.*

1. On the **Mitigation** screen > **E-W Mitigation** tab, choose a suggested segment for which you would like to create a policy.

The screenshot displays the Cynerio E-W Mitigation interface. At the top, there are four tabs: Mitigations (673), E-W Segments (18), N-S Segments (76), and Vendor Access (53). The main area shows a network diagram with a 'Gateway' node and several device icons. A 'Suggested Segment' box is highlighted in red, containing icons for X-Ray, Ultrasound, C-Arm, Fluoroscopy, and Mammography. To the right, a table lists suggested segments with columns for TYPE, MODEL, ASSETS, and SCORE.

TYPE	MODEL	ASSETS	SCORE
IV Pump	Alaris PCU 8015	738	149
Medicine Disp	Pyxis Medstation	161	89
IVUS,Ultrasound	Vivid E95,Volcan...	11	46
Point of Care Analy	CLINITEK Status ...	42	13
X-Ray,C-Arm,Ultra	Optima XR220,L...	9	3
Patient Monit	Infinity Acute Car...	17	2
Blood Gas Ana	ABL800	4	2
Ultrasound	Trident	5	1
CT	Aquilion	5	0
CT	Aquilion	4	0
IP Camera	P3346	2	0
Terminal Serv	UDS2100,UDS	14	0

- Click on the grouping and select **Create a Policy**.



The Segmentation Summary dialog opens, showing a summary of the policy configuration.

Segmentation Summary				
NAME	TYPE	ASSETS ADDED	NETWORK RULES	UNPROFILED ASSETS
Surgery, Radiology devices (1)	Static	18	117	0

Buttons: Cancel, Create policy

- Click **Create policy**.

The policy is implemented and you are redirected to the **Policy** screen > **E-W Segmentation** tab.

- Enable the Policy by toggling the switch to the right (on).

E-W Segmentation (6)	N-S Segmentation (8)	Vendor Access (1)	Service Hardening (6)	Cloud Services (5)	Quarantine (0)		
<a href="#">Create policy</a> <a href="#">Manage Columns</a>							
NAME	ASSETS	CONNECTIONS	UNPROFILED	VIOLATIONS	LAST VIOLATION EVENTS	STATUS	ENABLED
Surgery, Radiology devices (1)	18	211	0	0		●	<input checked="" type="checkbox"/>
Pharmacology devices (1)	101	3,120	4	65	08/09/2021 14:19:53	●	<input type="checkbox"/>
Infrastructure devices (1)	4	8	0	2	08/07/2021 13:48:37	●	<input type="checkbox"/>
Radiology devices (1)	5	34	3	10	08/09/2021 09:00:43	●	<input type="checkbox"/>
UDS1100 (10.127.200.153)	1	6	0	1	08/08/2021 03:47:25	●	<input type="checkbox"/>
INTENSIVE CARE	5	17	0	19	08/09/2021 10:06:40	●	<input type="checkbox"/>



- If you would like to view and edit the rules for the Policy, you can open the **Rules** tab. This tab shows a list of the rules that define the allowed communications for this segment. On this screen you can **Add**, **Delete** or **Edit** a Policy. (There is also a **Map** tab which shows a map of the assets in the segment.)

IP ADDRESS	DIRECTION	PORT	TRANS.	PROTOCOL	ASSETS	PROFILE
10.0.0.11	outbound	161	UDP	SNMP	1	IT
10.127.111.130	inbound	161	UDP	SNMP	13	IT
10.127.111.97	inbound	161	UDP	SNMP	8	IT
10.127.111.97	inbound	5353	UDP	Multicast DNS	9	IT
10.127.236.103	outbound	3320	TCP	DICOM	18	Medical
10.127.236.111	outbound	161	UDP	SNMP	1	IT

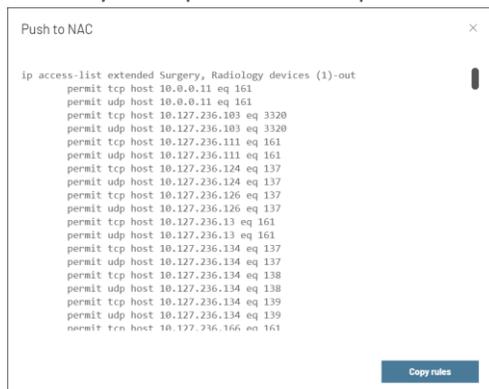
- If you would like to monitor and manage the Policy violations, you can open the **Unresolved violation events** tab. A list of communications that violated the Policy is shown.

TIME	DETAILS	DEVICE TYPE	DEVICE IP	SEVERITY
08/12/2021 11:31:23	Segment violated: Pharmacology devices (1). Source IP: 10.127.82.19, Destination IP: 10.127.62.47, Transport: UDP, Port: 137	Medicine Dispenser	10.127.82.19	LOW
08/09/2021 13:49:40	Segment violated: Pharmacology devices (1). Source IP: 10.133.65.30, Destination IP: 10.127.25.61, Transport: UDP, Port: 53	Medicine Dispenser	10.127.25.61	LOW
08/09/2021 13:49:40	Segment violated: Pharmacology devices (1). Source IP: 10.133.65.30, Destination IP: 10.127.25.58, Transport: UDP, Port: 53	Medicine Dispenser	10.127.25.58	LOW
08/09/2021 13:49:40	Segment violated: Pharmacology devices (1). Source IP: 10.133.65.30, Destination IP: 10.127.24.192, Transport: UDP, Port: 53	Medicine Dispenser	10.127.24.192	LOW
08/09/2021 13:49:40	Segment violated: Pharmacology devices (1). Source IP: 10.133.65.30, Destination IP: 10.127.25.68, Transport: UDP, Port: 137	Medicine Dispenser	10.127.25.68	LOW
08/09/2021 13:49:30	Segment violated: Pharmacology devices (1). Source IP: 10.133.65.30, Destination IP: 10.127.25.72, Transport: UDP, Port: 53	Medicine Dispenser	10.127.25.72	LOW

- If you would like to allow a communication for this segment, right-click on the row of that communication and select **Add to policy**.
  - If you determine that a device needs to be reconfigured to prevent future violations then take the necessary steps.
- Once you have resolved all of the violations, you can click **Reset Events Counter** in order to ensure that you are no longer getting violations.
  - Once the validation period is completed, if you are satisfied with the Policy configuration you can begin enforcing the Policy.
    - If Cynerio is integrated with your NAC/firewall application, then all you need to do is click **Enforce Now** on the Dashboard. The required VLANs are automatically created and all unauthorized communication is blocked by the NAC/firewall.

Policy Validation/Enforcement Status			
Status Enabled	Enabled 08/12/2021	Validation 0 days no violations logged	Enforcement Ready To enforce

- If Cynerio is not integrated with your NAC/firewall, then you can enforce the Policy manually by right-clicking on the Policy and selecting Push To NAC. You can then copy the rules to your clipboard and implement them on your NAC/firewall.



```
ip access-list extended Surgery, Radiology devices (1)-out
  permit tcp host 10.0.0.11 eq 161
  permit udp host 10.0.0.11 eq 161
  permit tcp host 10.127.236.103 eq 3320
  permit udp host 10.127.236.103 eq 3320
  permit tcp host 10.127.236.111 eq 161
  permit udp host 10.127.236.111 eq 161
  permit tcp host 10.127.236.124 eq 137
  permit udp host 10.127.236.124 eq 137
  permit tcp host 10.127.236.126 eq 137
  permit udp host 10.127.236.126 eq 137
  permit tcp host 10.127.236.13 eq 161
  permit udp host 10.127.236.13 eq 161
  permit tcp host 10.127.236.134 eq 137
  permit udp host 10.127.236.134 eq 137
  permit tcp host 10.127.236.134 eq 138
  permit udp host 10.127.236.134 eq 138
  permit tcp host 10.127.236.134 eq 139
  permit udp host 10.127.236.134 eq 139
  permit tcp host 10.127.236.166 eq 161
```

### North-South Segmentation and Vendor Access

North-South (N-S) segmentation refers to the ability to limit external asset communication to only authorized entities. This is an essential practice when protecting your network from cyber threats. Virtual North-South segmentation is based on the assumption that similar devices should have similar N-S communication patterns. Cynerio includes all assets that are of the same “type” (e.g. DICOM Workstation, IV Pump etc.) and from the same vendor in the same N-S segment. Cynerio automatically generates a series of rules that define acceptable communication for both inbound and outbound connections for each segment. The rules are based on identifying which services (e.g. Windows update, OS services, certificate validation etc.) the segment needs to access and whitelisting only communication that relates to those services. All you need to do is apply our suggested segmentation Policies, monitor the segment during the Validation period, tweak the rules as needed and then go ahead and Enforce the Policy.

*Vendor Access Policies* are a specialized type of N-S Policies that relate specifically to services provided by the asset vendor.

**Note:** If Cynerio is integrated with your firewall application, then once a Policy is enforced, all unauthorized communication is blocked by the firewall. If you are applying the Policy manually, then you can copy the list of connections related to each service included in the Policy and add them to the whitelist on your firewall for the relevant assets.

Mitigations (665)	E-W Segments (15)	N-S Segments (66)	Vendor Access (31)																																				
<table border="1"> <thead> <tr> <th>DEVICE TYPE ↓</th> <th>VENDOR</th> <th># OF SERVICES</th> <th># OF ASSETS</th> </tr> </thead> <tbody> <tr> <td> Blood Gas Analyzer</td> <td>Abbott</td> <td>1</td> <td>41</td> </tr> <tr> <td> C-Arm</td> <td>Philips</td> <td>1</td> <td>4</td> </tr> <tr> <td> C-Arm</td> <td>GE</td> <td>1</td> <td>6</td> </tr> <tr> <td> C-Arm</td> <td>Siemens</td> <td>2</td> <td>1</td> </tr> <tr> <td> CAD</td> <td>Philips</td> <td>29</td> <td>12</td> </tr> <tr> <td> Clinical Workstation</td> <td>Enovate Medical</td> <td>31</td> <td>171</td> </tr> <tr> <td> Clinical Workstation</td> <td>Stryker</td> <td>15</td> <td>3</td> </tr> <tr> <td> Clinical Workstation</td> <td>Raspberry Pi Foundation</td> <td>1</td> <td>1</td> </tr> </tbody> </table>				DEVICE TYPE ↓	VENDOR	# OF SERVICES	# OF ASSETS	Blood Gas Analyzer	Abbott	1	41	C-Arm	Philips	1	4	C-Arm	GE	1	6	C-Arm	Siemens	2	1	CAD	Philips	29	12	Clinical Workstation	Enovate Medical	31	171	Clinical Workstation	Stryker	15	3	Clinical Workstation	Raspberry Pi Foundation	1	1
DEVICE TYPE ↓	VENDOR	# OF SERVICES	# OF ASSETS																																				
Blood Gas Analyzer	Abbott	1	41																																				
C-Arm	Philips	1	4																																				
C-Arm	GE	1	6																																				
C-Arm	Siemens	2	1																																				
CAD	Philips	29	12																																				
Clinical Workstation	Enovate Medical	31	171																																				
Clinical Workstation	Stryker	15	3																																				
Clinical Workstation	Raspberry Pi Foundation	1	1																																				

The following is a brief description of the workflow for applying N-S segmentation Policies:

1. Cynerio assigns each of your assets to a virtual N-S segment based on shared asset type and vendor.
2. On the **Mitigation** screen > **N-S Mitigation** tab, select a segment and select the **Create a Policy** option.
3. Cynerio creates the automatically configured Policy.
4. You can edit the Policy rules according to your needs, and enable/disable the policy separately for inbound and outbound traffic.
5. Cynerio validates the Policy over a period of time. During this time, you are alerted for any Policy violations that occur. For each violation you can either exclude that communication from the Policy (i.e. allow it) or you can maintain the Policy so that that communication will be blocked by the Policy.
6. When you are satisfied with the integrity of the Policy, you can "Enforce" the Policy.
7. Once the Policy is enforced, your firewall will block all communication that violates the Policy for that segment.