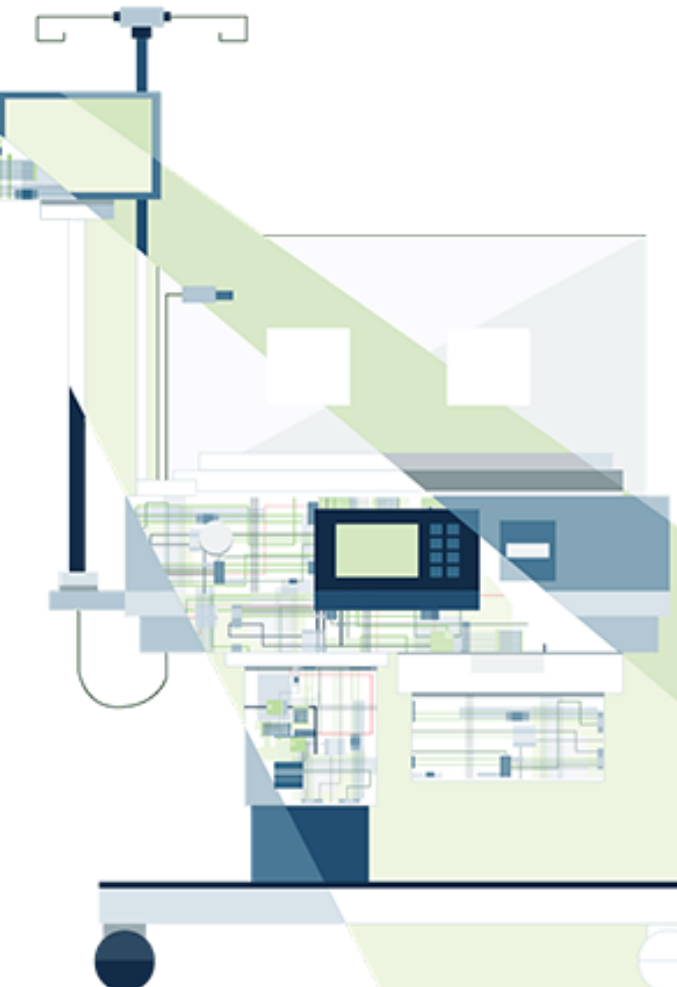
Cynerio



CYNERIO
GETTING STARTED GUIDE

Version 1.2

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

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.

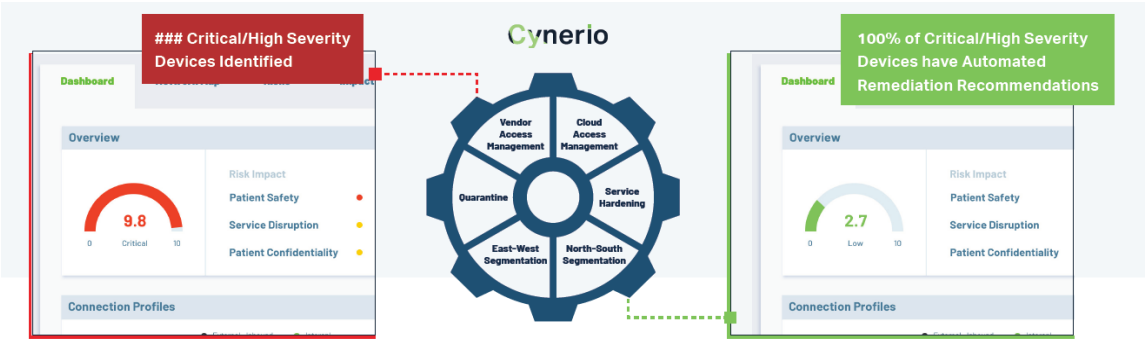
The below guide is intended to quickly introduce you to Cynerio functionality while acting as a long term reference for a variety of day-to-day activities. Throughout this guide you will learn how Cynerio's technology identifies threat vectors and vulnerabilities, and then provides end-to-end risk mitigation 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.

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

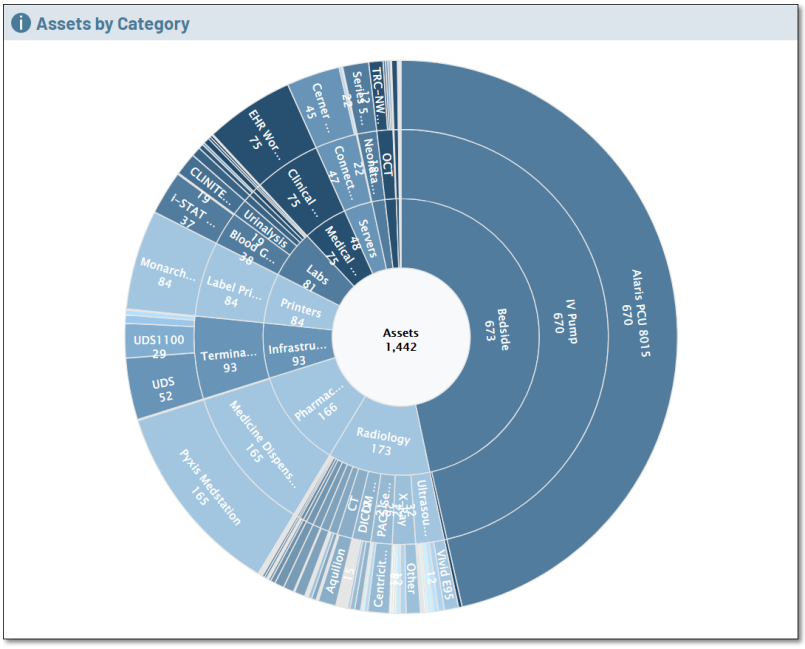
Cynerio classifies assets using the following hierarchy, making it easy to view aggregated data and then drill down to view specific details.

Class (IoT/IoMT) ➔ Category (usage) ➔ Type (function) ➔ Vendor ➔ Model

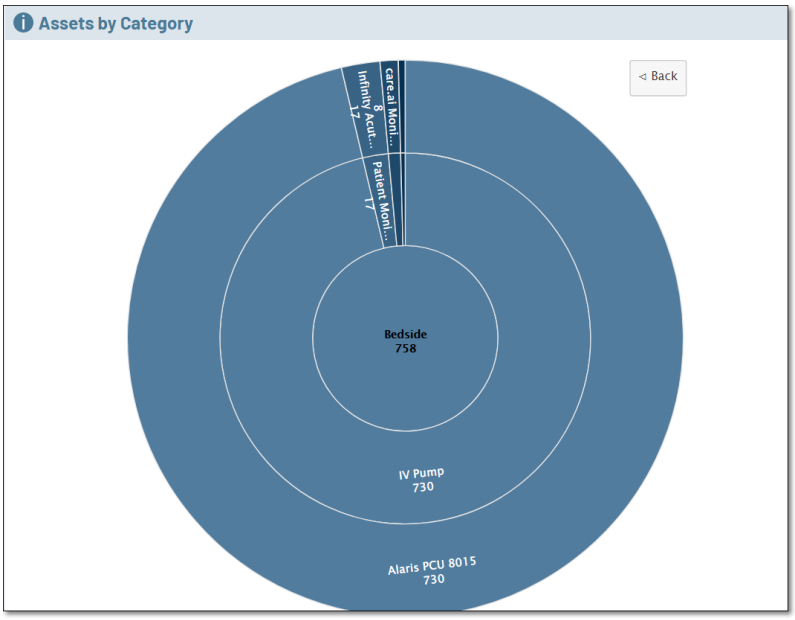
For example, a GE Optima XR220 X-Ray device is categorized as:

IoMT ➔ Radiology ➔ X-Ray ➔ GE ➔ Optima XR220

The breakdown of assets by classification can be viewed on the Dashboard page in the "Assets by Category" sunburst chart.



You can click on an element in the chart to drill-down and show the breakdown of items in that grouping. For example, if you click on "Bedside", the chart shows a breakdown of the assets in that category.



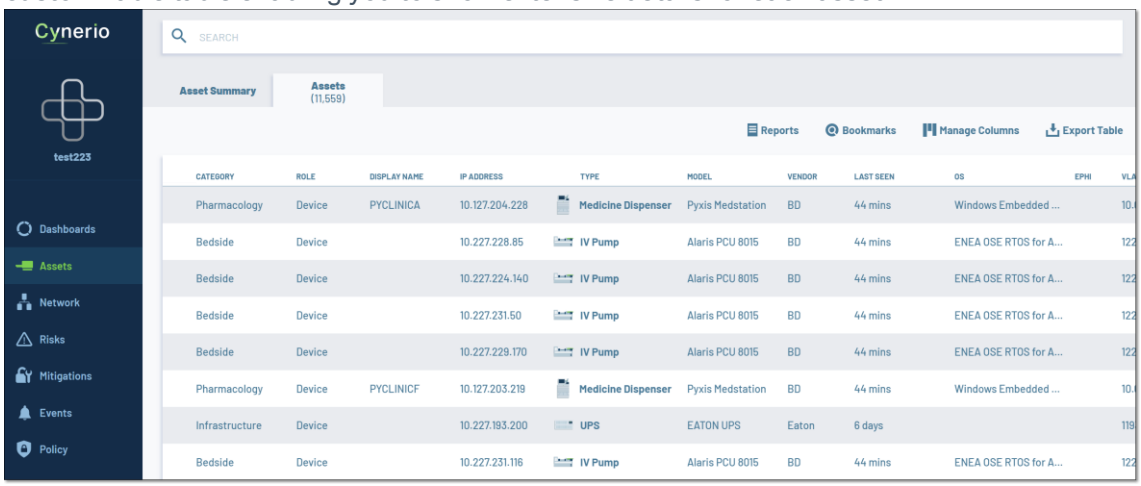
Assets Screen

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

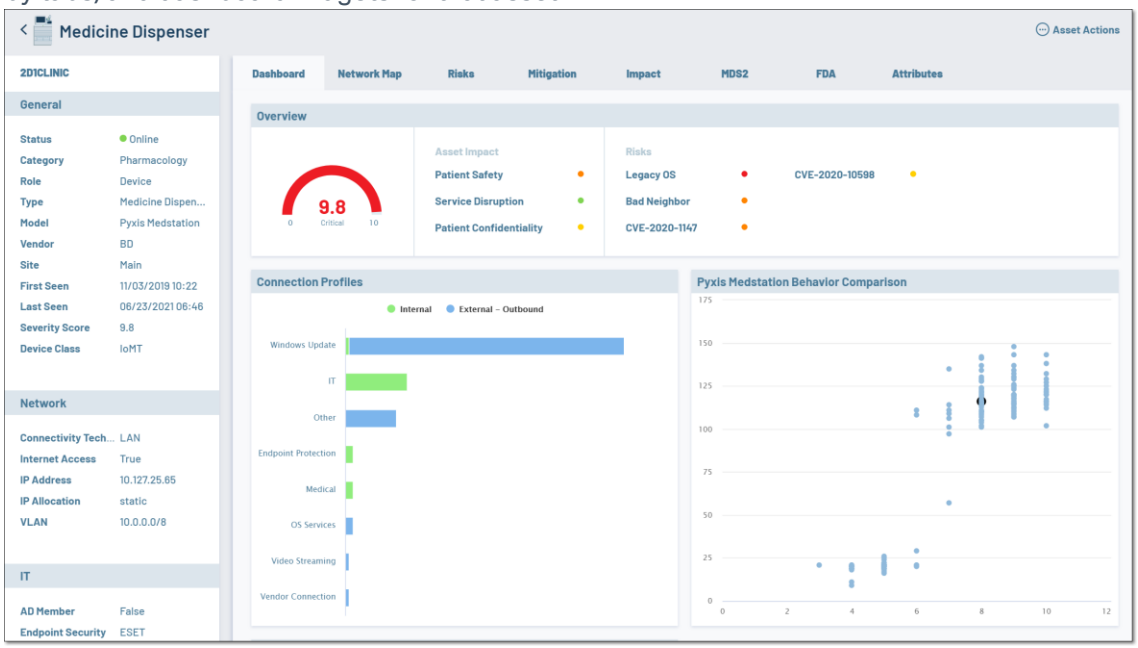
- **Asset Summary** – shows your assets grouped by types. For each type, a tile is shown with a representative icon, the number of assets of that type and a bar graph indicating the risk level of the assets.

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.



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.



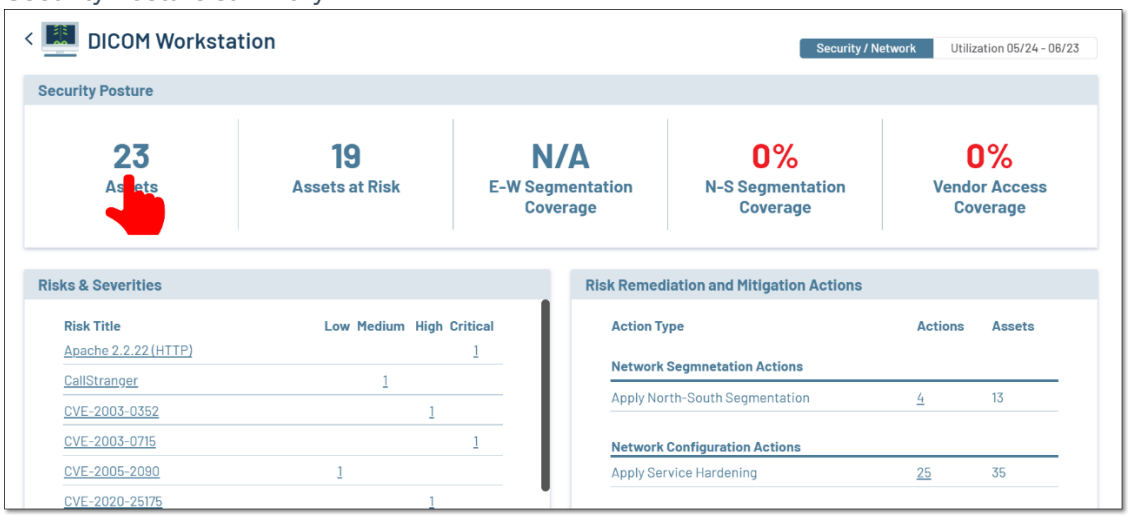
Asset Inventory Use Case 1 – Asset drill-down

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.

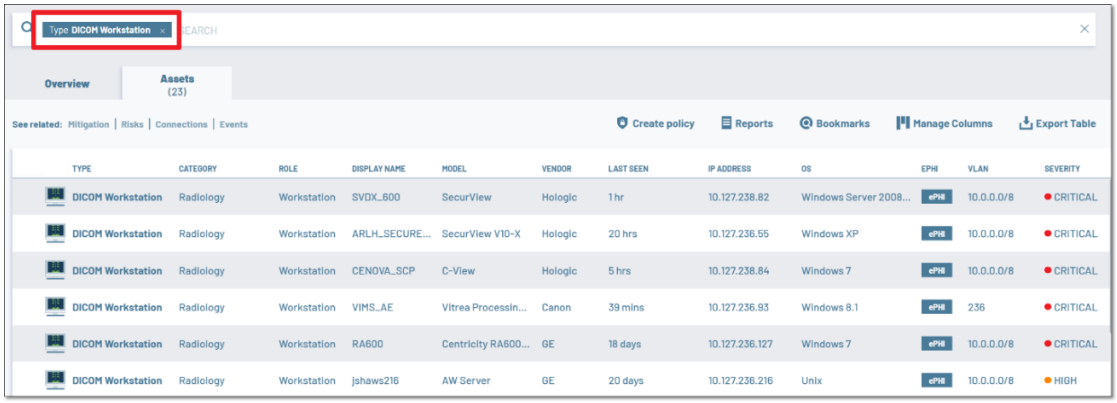
1. Go to the **Assets** > **Asset Summary** screen.
   You can see right away that there is a tile indicating how many DICOM Workstations you have (23).

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.

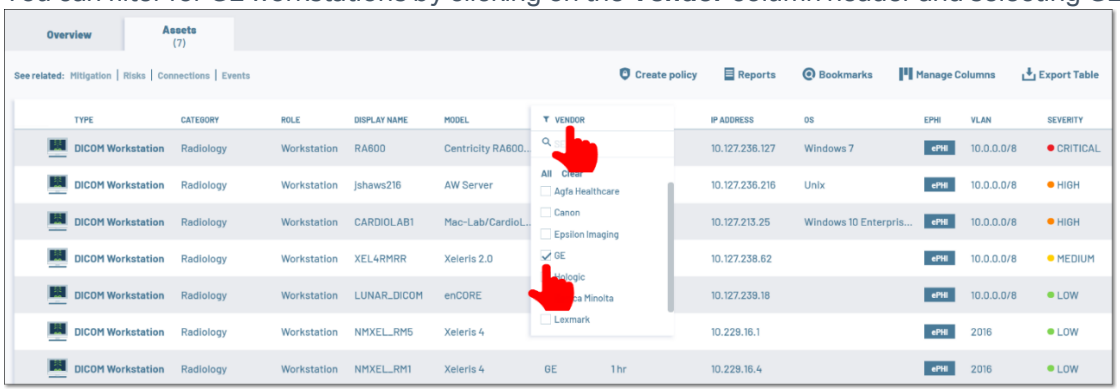
3. To view details about your specific workstations, click on the number of assets in the Security Posture summary.



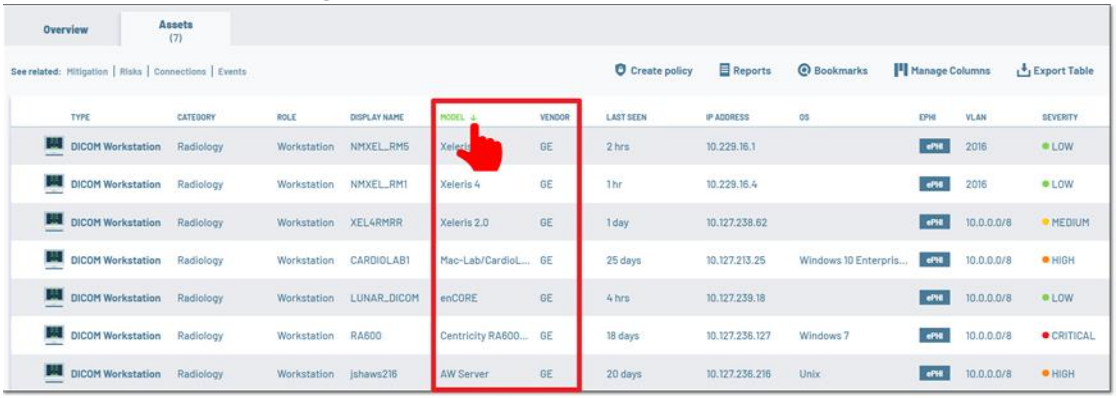
The Assets tab opens with the results automatically filtered to show only DICOM workstations.



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



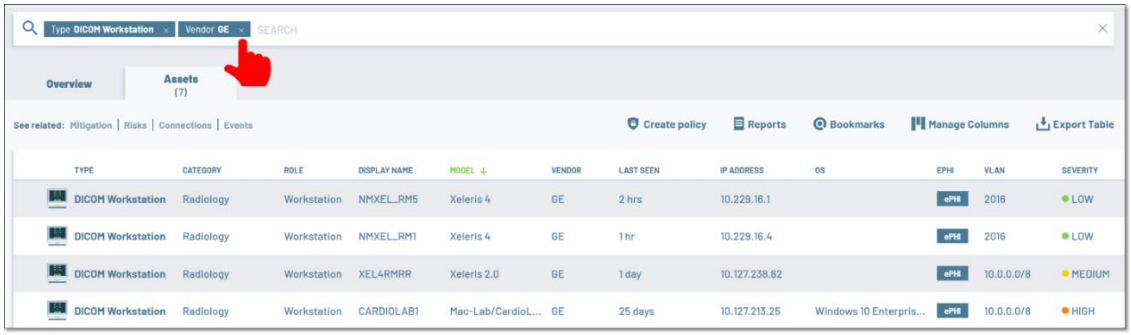
5. Now, only the GE workstations are shown. The Model column shows the Model of each of your GE DICOM workstations. You can sort the display by Model by hovering over the Model column header and clicking on the arrow.



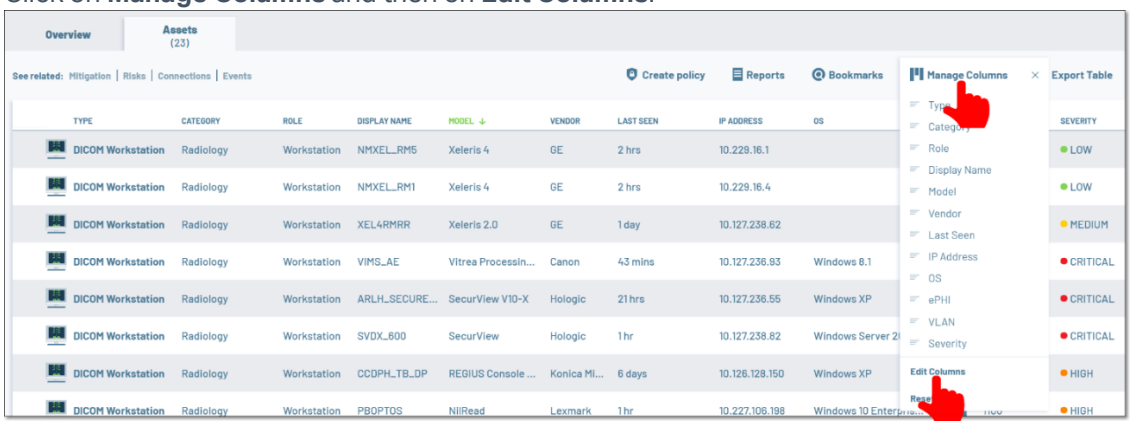
Asset Inventory Use Case 2 – Displaying Additional Columns

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.

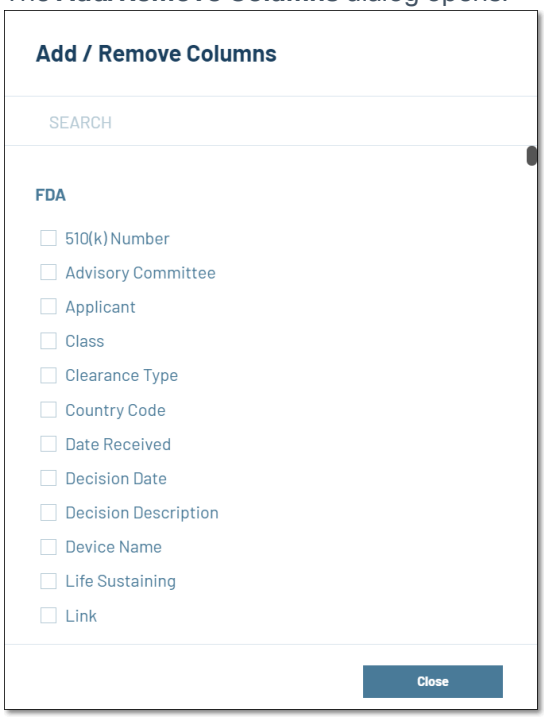
1. First, let's go back to showing all of your DICOM Workstations by clicking the "x" next to the Vendor filter in the Search box.



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

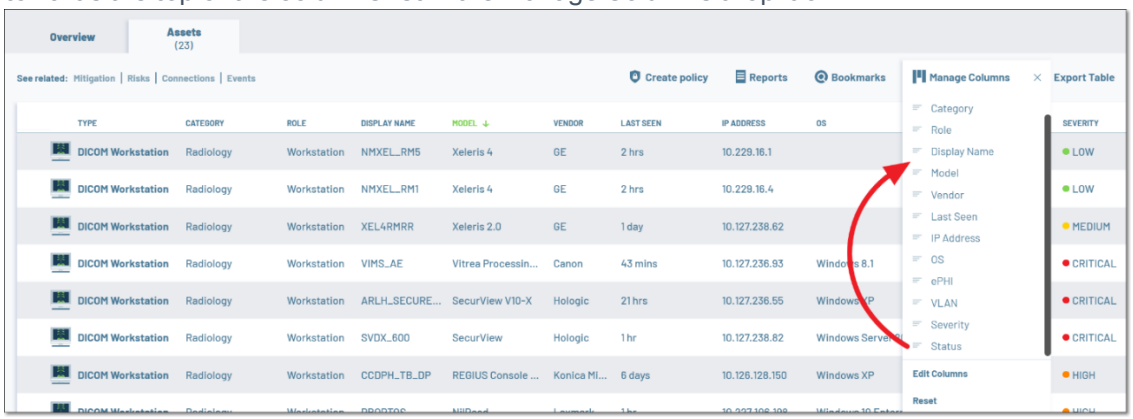


The **Add/Remove Columns** dialog opens.

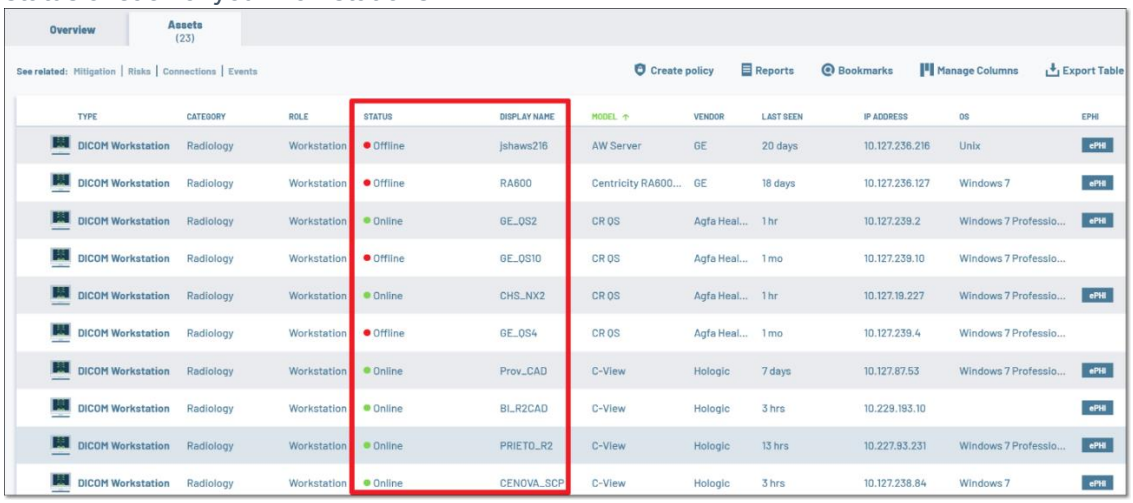


3. In the Search box, type in “status”.
   The status option is shown.
4. Select the checkbox next to “Status” and click **Close**.

5. 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.



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



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**.

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

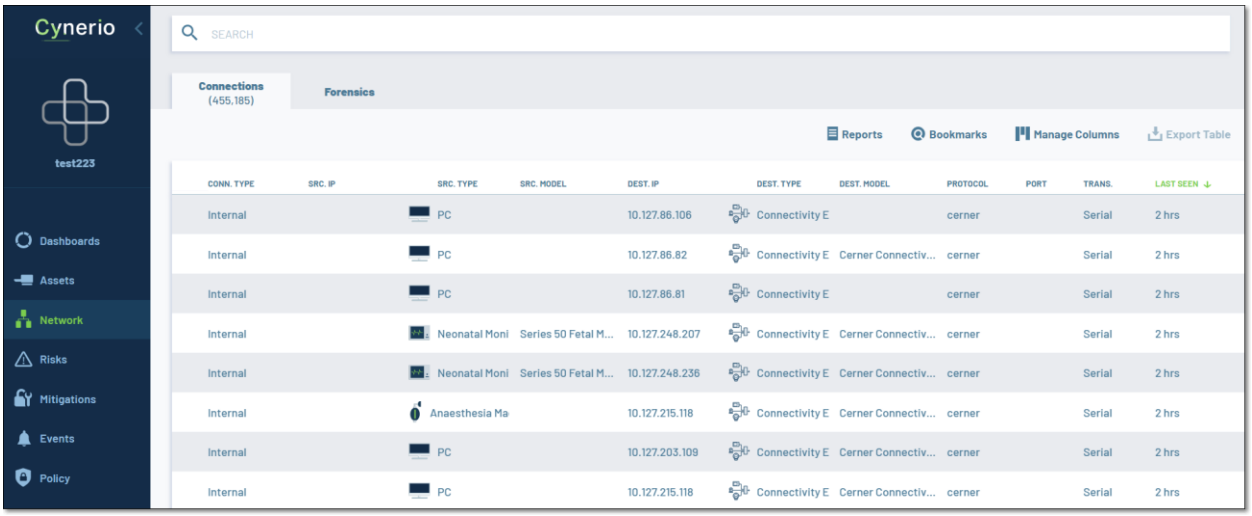
Cynerio integrates with your network through passive Collectors connected to network switches via a SPAN port. This approach provides a copy of network traffic to Cynerio which removes sensitive information such as ePHI while identifying characteristics relevant to the security posture of a device such 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.).

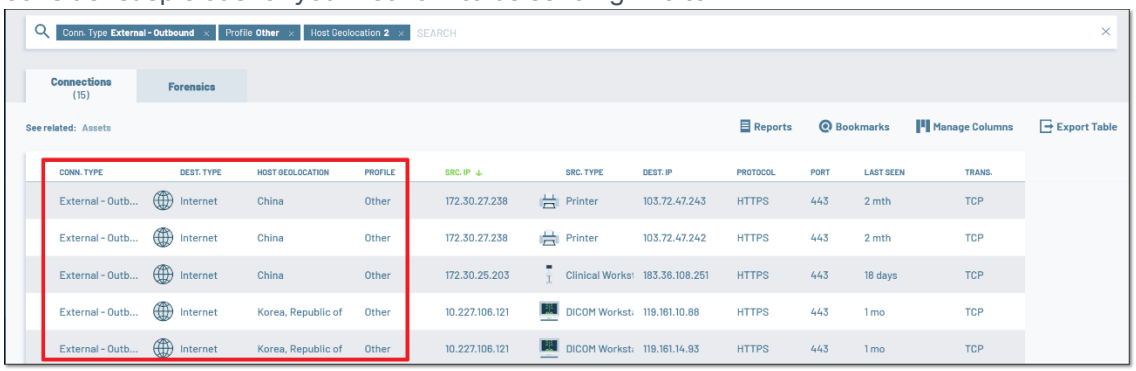
Note: Conversations with identical characteristics (e.g. source asset, destination asset, protocol etc.) are treated as a single Network Connection.



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.

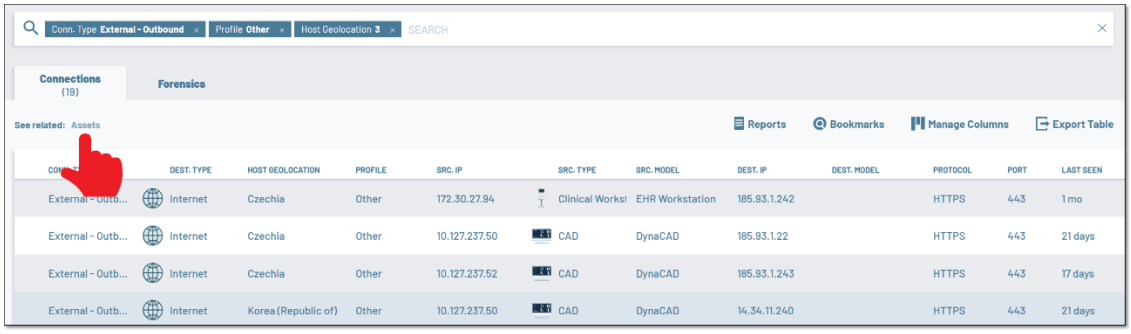
1. Go to the **Network** screen.
2. Click on **Manage Columns** and select **Host Geolocation**.
3. Reposition the columns so that **Conn. type**, **Destination type**, **Profile** and **Host Geolocation** are grouped together.
4. Filter the Conn. type column for **External - Outbound**.
5. Filter the **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.



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

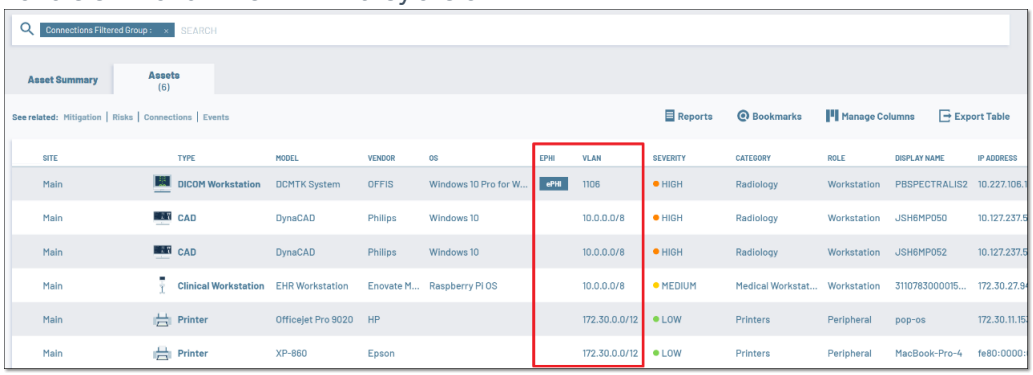
Now, you can drill-down to view more detailed info about the assets that are being used for the risky communications described in the previous use case.

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

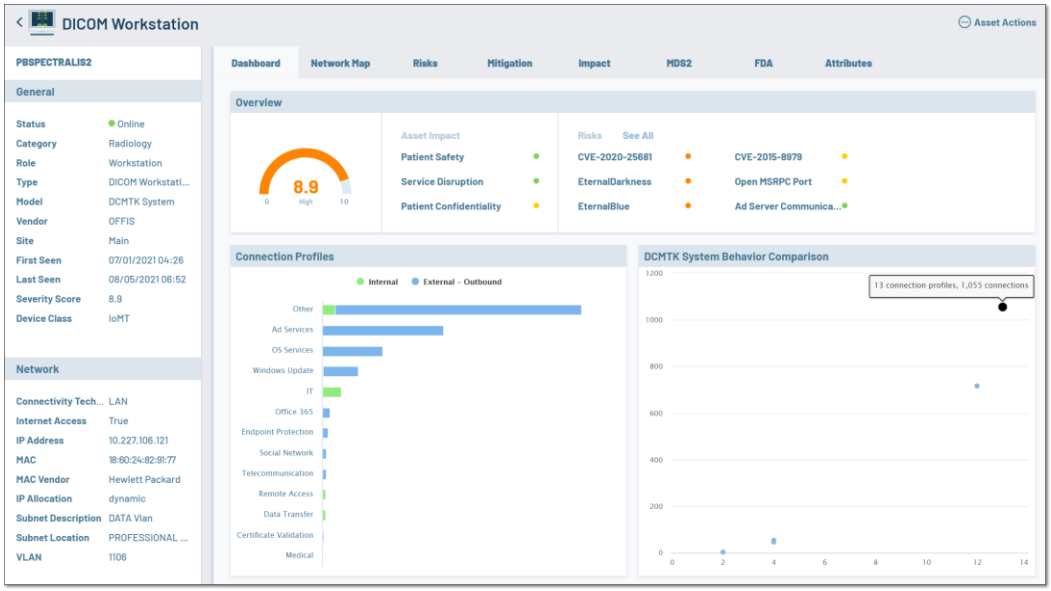


The Assets screen opens, with a customized filter applied to show only the assets that were

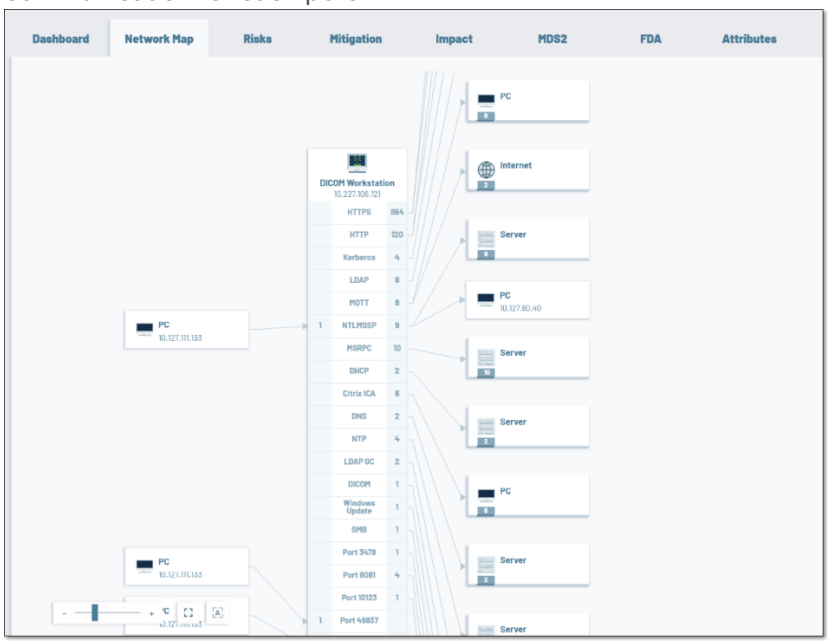
displayed on the Network screen (i.e. External – Outbound, profile "Other", to specified locations). You can see important details about these assets such as, whether or not they handle ePHI and which VLAN they are on.



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).

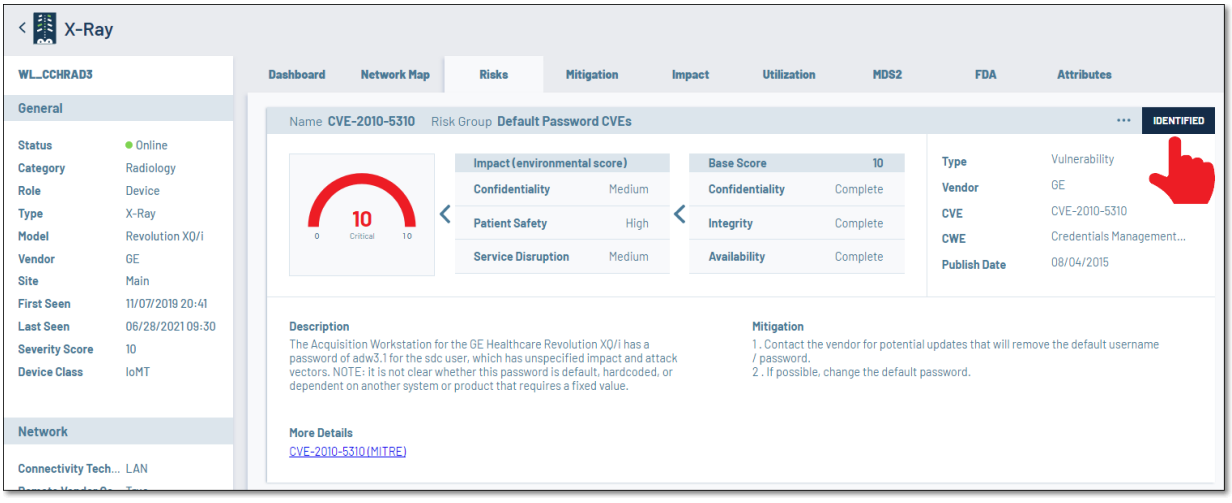
Risk Status

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.

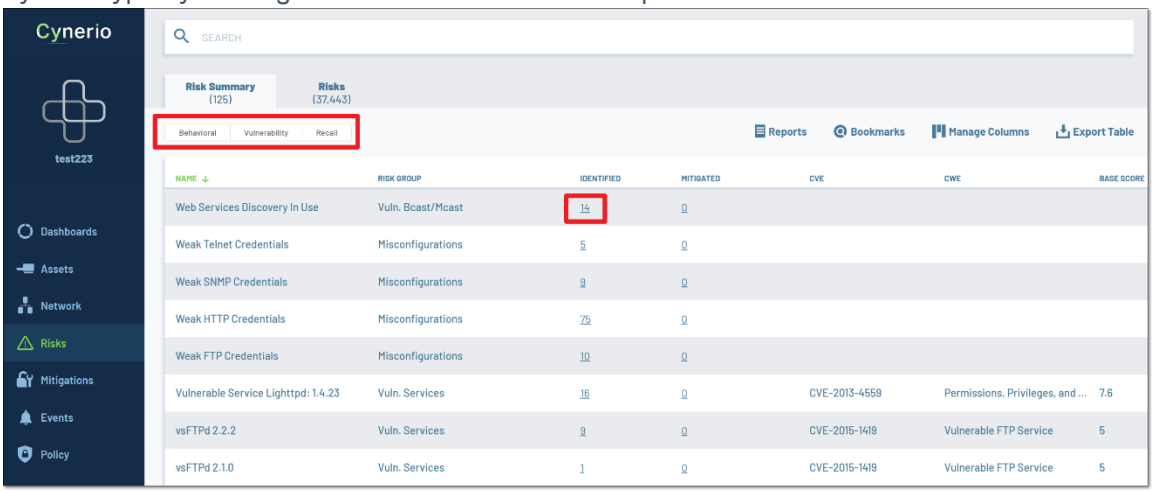


Alternatively, you can right click on a row in the **Risks** screen > **Risks** tab, and select **Change status**.

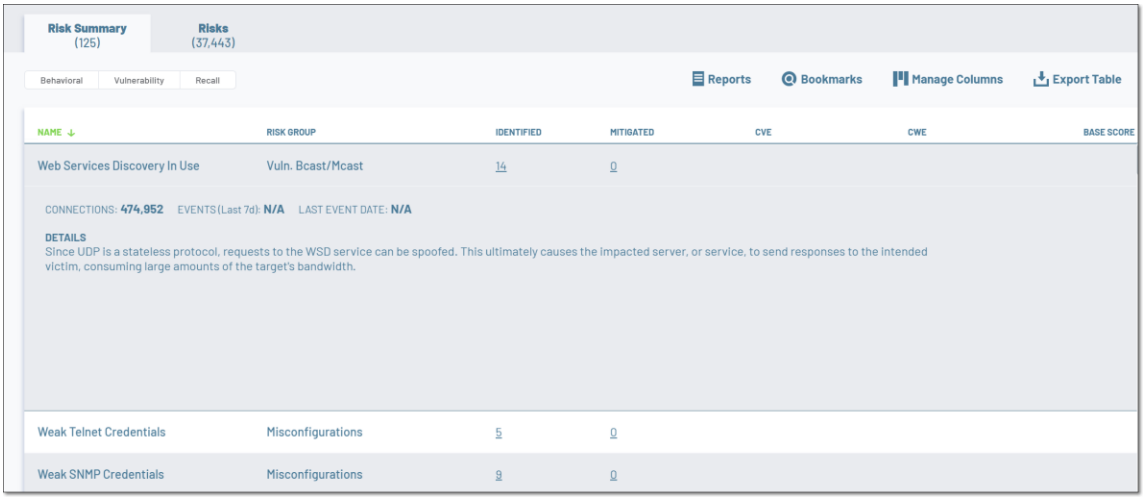
Risk Screen

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*.

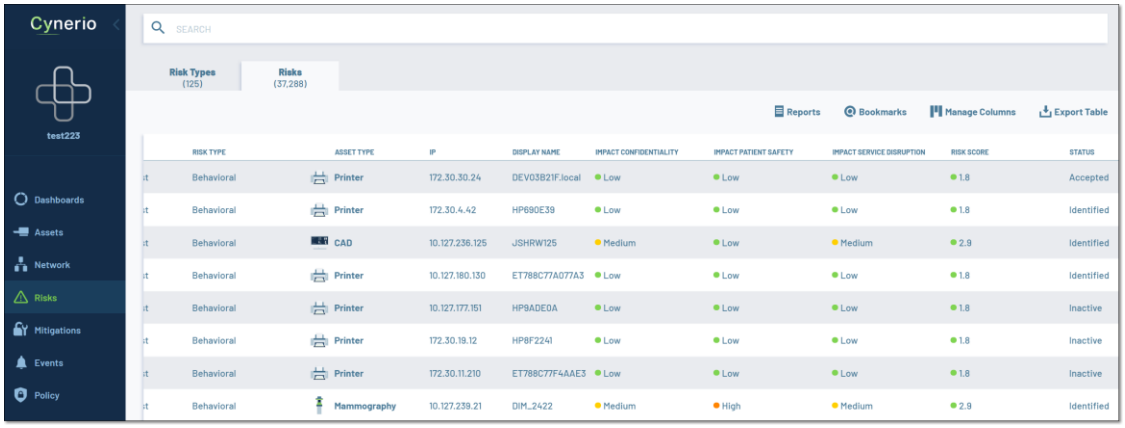
- **Risk Summary** – shows a list of all of the Risk Titles that were identified in your network. For each Risk Title, details about the nature of the threat are shown as well as the number of assets affected by the Risk, broken down by status. You can click on a number to view all of the instances of 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.



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



- **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.

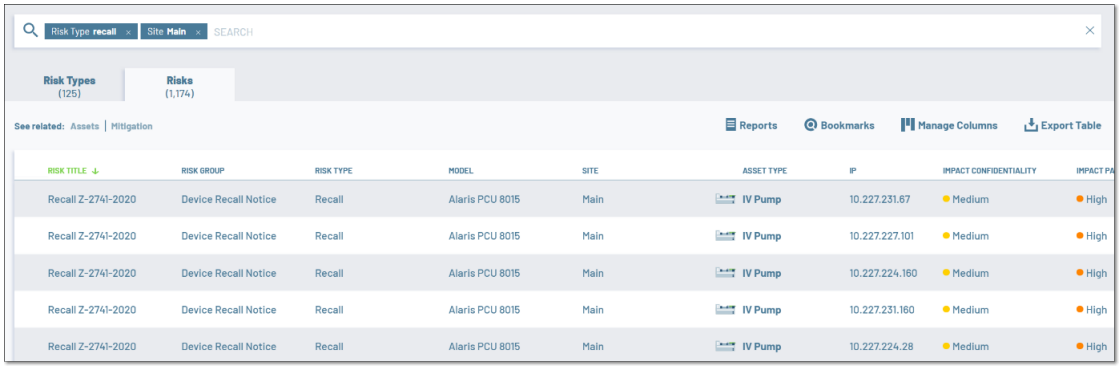


You can click on a row to drill down to see detailed info about the nature of the threat and suggested mitigation procedures. This info is shown in the Risks tab on the Asset page for the affected asset.

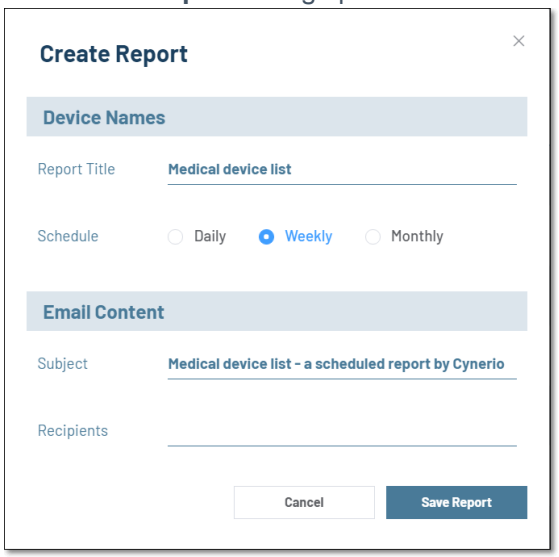
Risk Use Case 1 - Filtering by Risk Type and Generating Reports

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.



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.

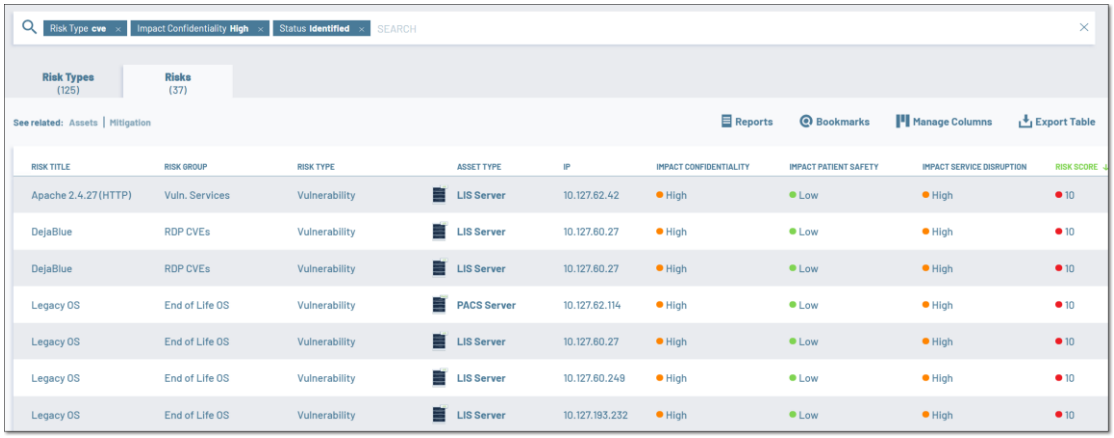


b. You can edit the **Report Title** and **Subject line** by typing in a description of the report (e.g. Manufacturer Recalls at Main Site).
c. Select the radio button for the desired schedule (frequency).
d. In the **Recipients** field, enter the email of the operations manager.
e. Click **Save Report**.
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

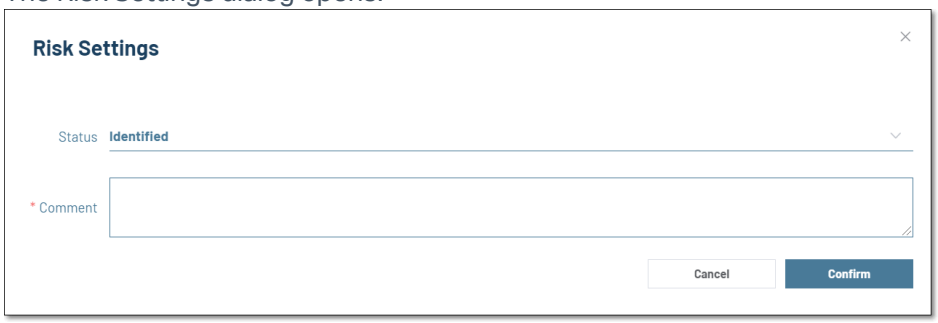
Let's say that you want to assess the most critical cyber security vulnerabilities (e.g. CVEs) that effect patient confidentiality at your healthcare facility.

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.



7. 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.

8. 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:
   a. Click on the status box at the top right of the Risk pane (IDENTIFIED).
      The Risk Settings dialog opens.



   b. 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).
   c. In the **Comment** field, add a comment describing the reasons for the change of Status. (Mandatory)
   d. Click **Confirm**.
9. When you finish analyzing this vulnerability, you can navigate back to the Risks screen to view the next item in the list.

Dashboards

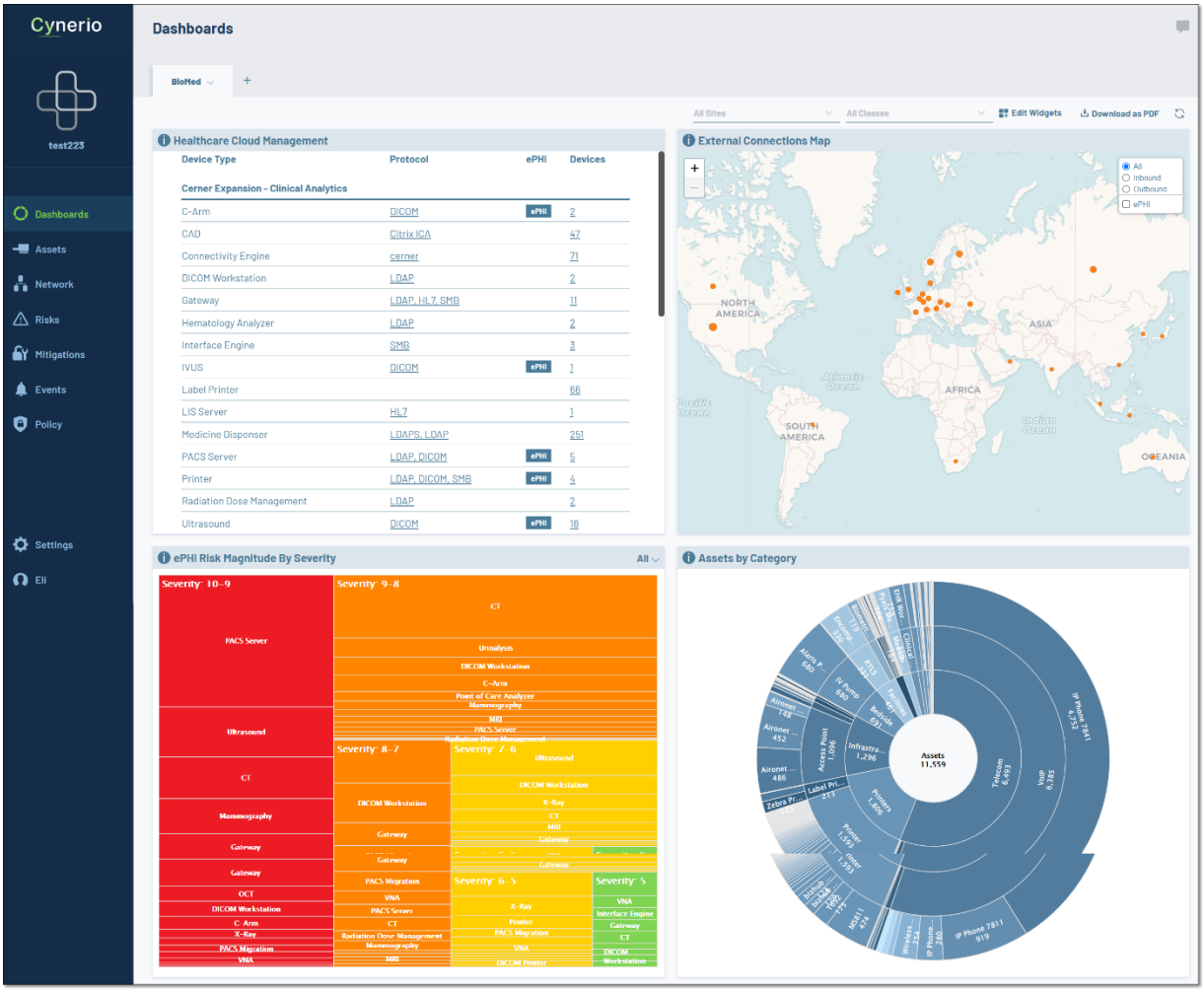
Cynerio dashboards provide centralized information that enables stakeholders to gain important insights at a glance. Cynerio provides standardized dashboards with each deployment that consist of a series of widgets showing key data and visualizations. These widgets are interactive and allow users to 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

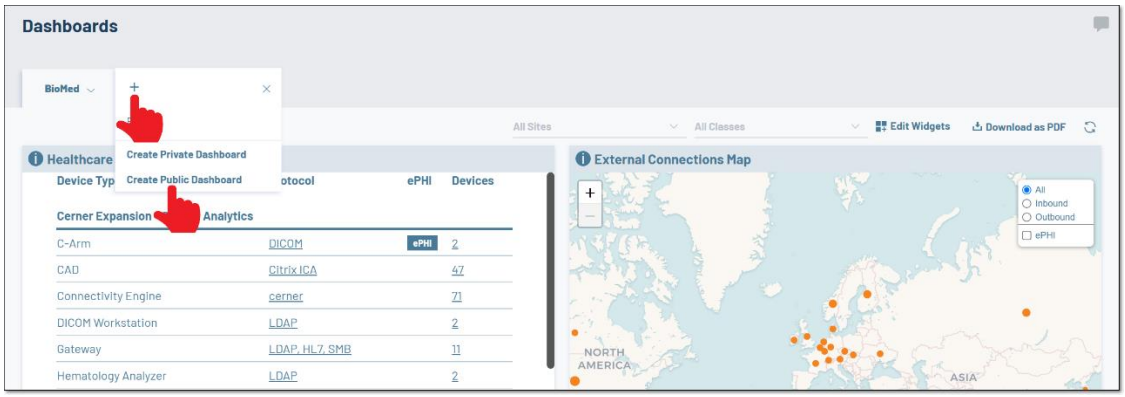
The Dashboards tab shows each of your Dashboards in a separate tab. You can filter the display by Site and by Asset Class. Click on a data element to drill-down into that element.



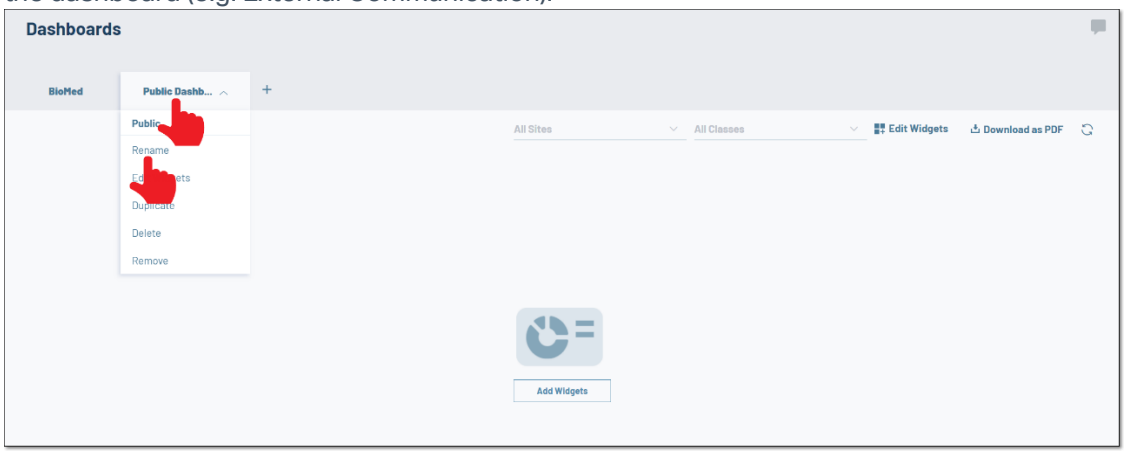
Dashboard Use Case

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.

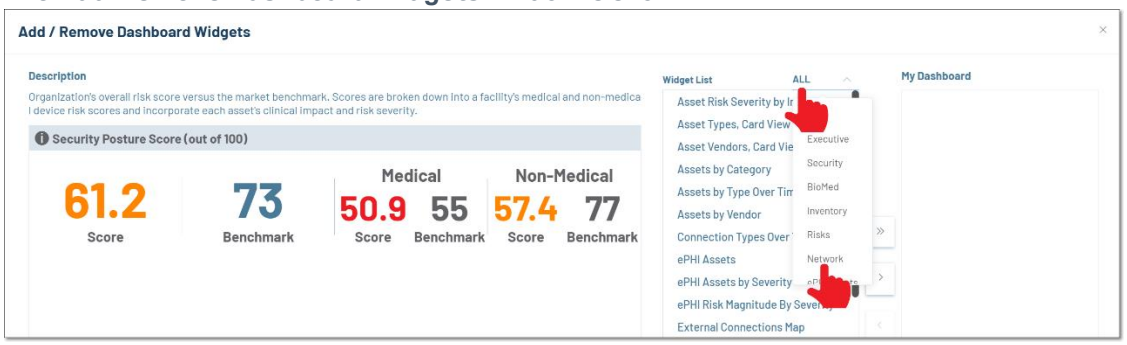
1. Go to the **Dashboards** screen.
2. Click on "**+**:" in the tabs selection and select **Create Public Dashboard** from the dropdown list.



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

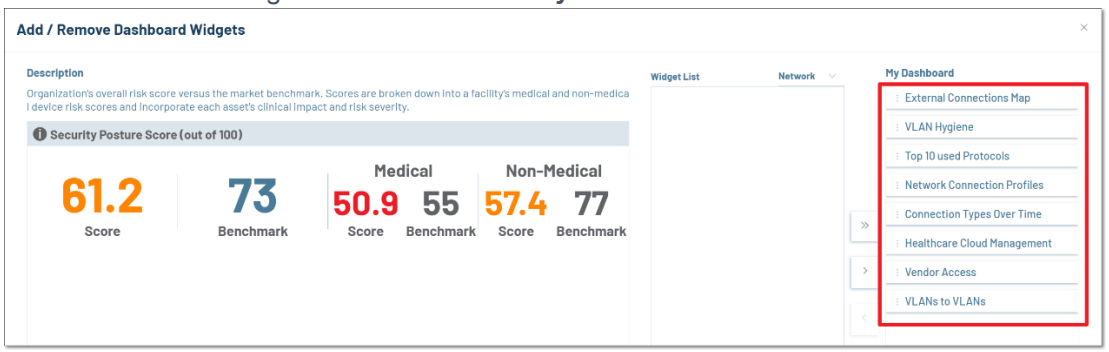


4. Click on **Add Widgets** (either in the middle of the screen or in the header bar).
   The **Add/Remove Dashboard Widgets** window is shown.



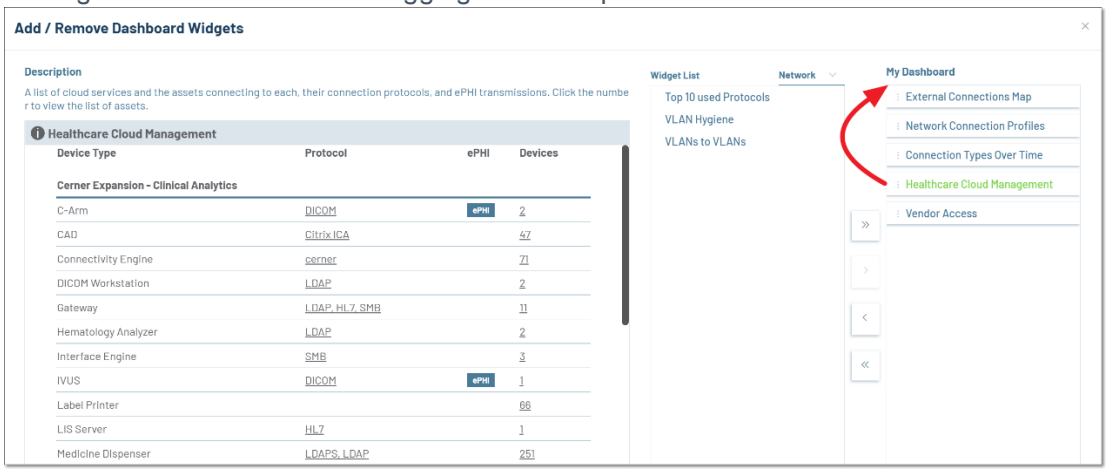
5. For our use case we want to focus on network widgets, so click on the widget filter (All) and select **Network**.

6. Bulk add all Network widgets by clicking on the » button.
   All of the Network widgets are added to the **My Dashboard** column.



7. For our dashboard, the "VLAN Hygiene", "Top 10 used Protocols" and "VLAN to VLANs" widgets are less interesting. So, we will select each one and click on the ‹ button to remove it from the dashboard.
8. 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

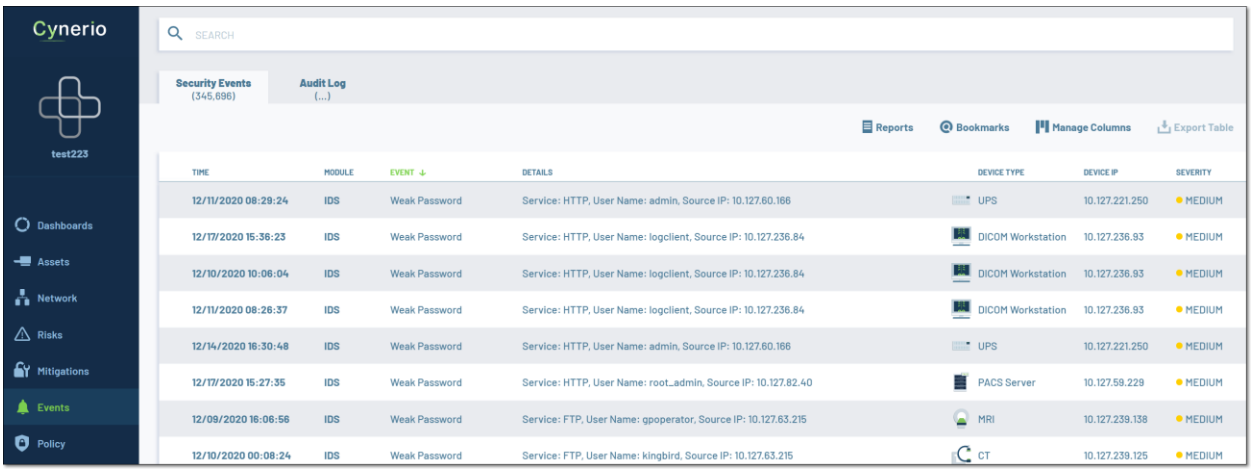
Cynerio detects a broad range of Events that occur in your Network that may require your attention. The Events screen shows a log of all of the Events that are detected. You can also create notification profiles in order to receive email notifications when particular Events occur.

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

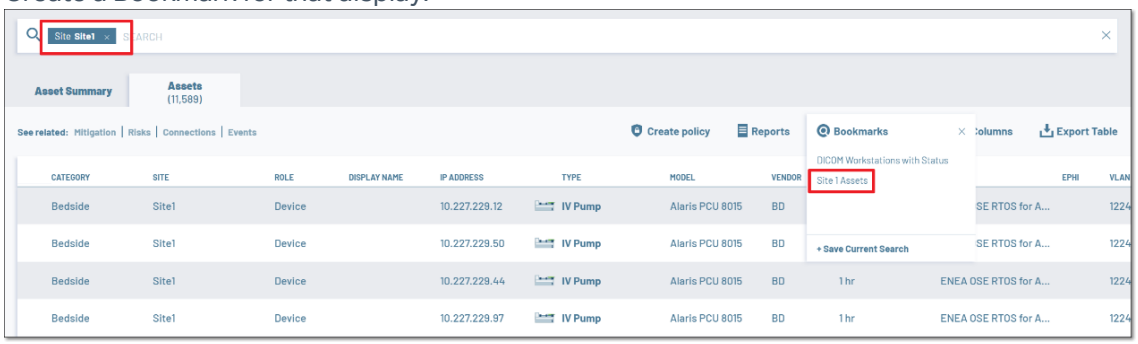
This screen shows a list of all Events that occurred in your network. Each Event is categorized by the general type of Event (Module) and the specific Event that occurred. Detailed info is given about the affected asset as well as a description of the Event.



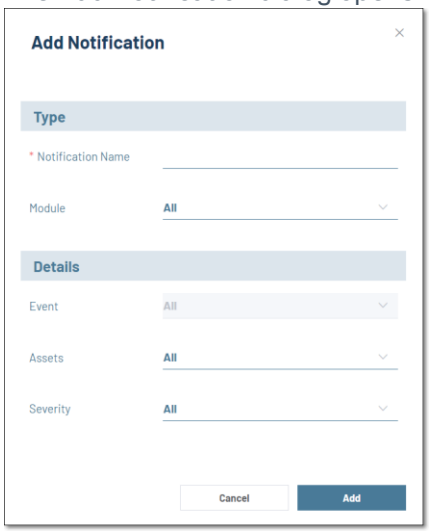
Events Use Case 1 – Creating Notifications

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.



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.

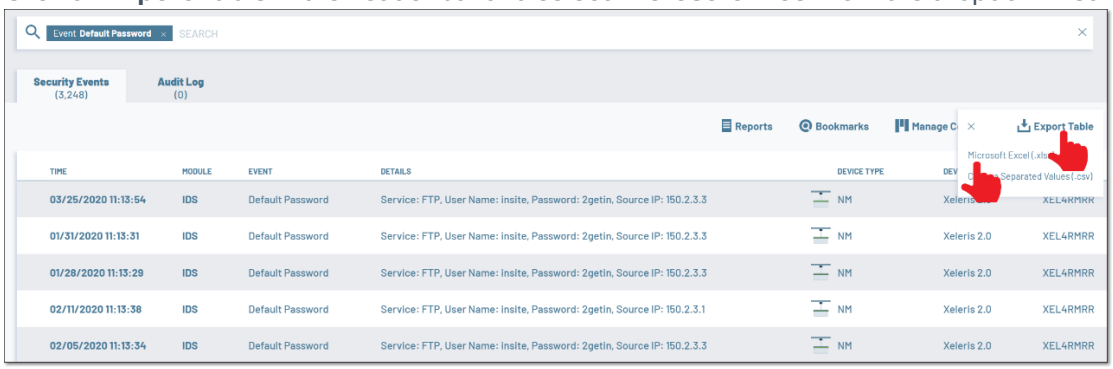


5. Enter a name for the notification, then select **IDS** for the Module
6. In the Details section, for **Event** select **Exploitation Attempt**. For **Assets**, select **Site 1 Assets** (referring to the Bookmark that you created in step 2).
7. Click **Add**.
   You will receive email notification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



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

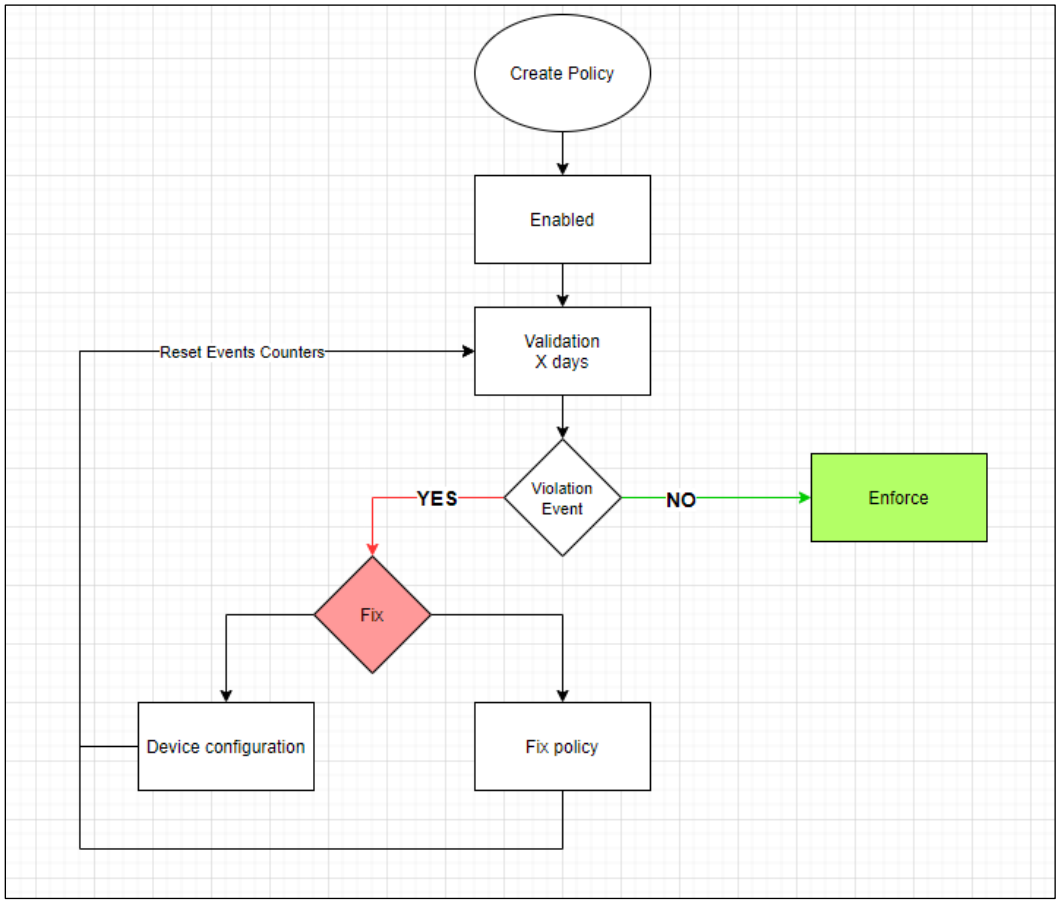
Network Mitigations are some of the most effective ways to quickly reduce a wide variety of risks. Through Network Mitigations you are able to limit the types of communication that are allowed for the assets in your network. These Mitigations can apply to specific ports/services on a particular asset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

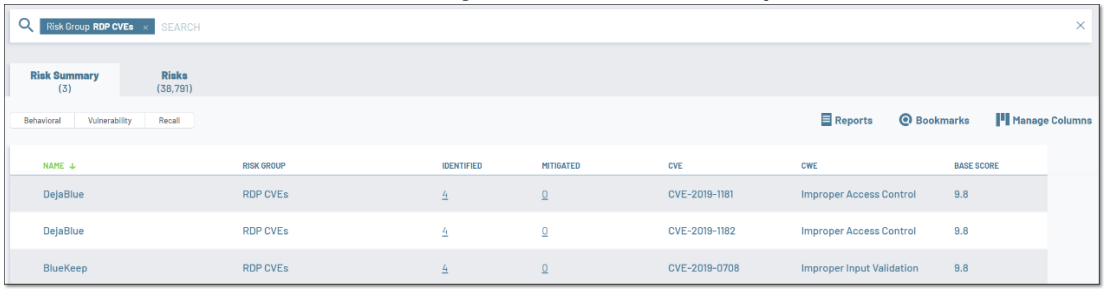
NOTE: If several ports/services on the same asset require service hardening, a separate Policy is created for each port.

Service Hardening Use Case

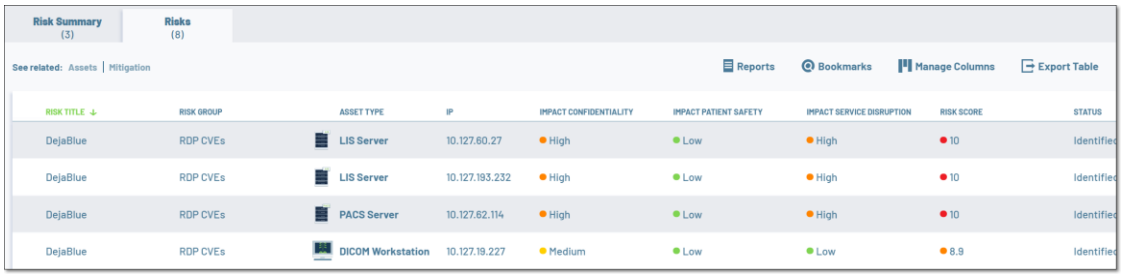
Let's say you'd like to monitor RDP based vulnerabilities on critical medical devices and limit that type of access on them.

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".

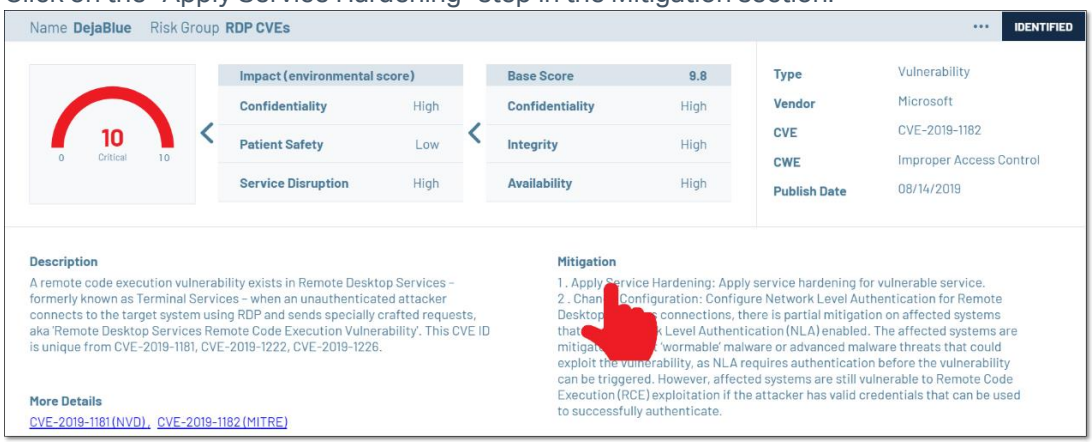


2. Click on the number shown in the **Identified** column for a particular Risk row. This shows a list of the instances of that Risk that were identified.

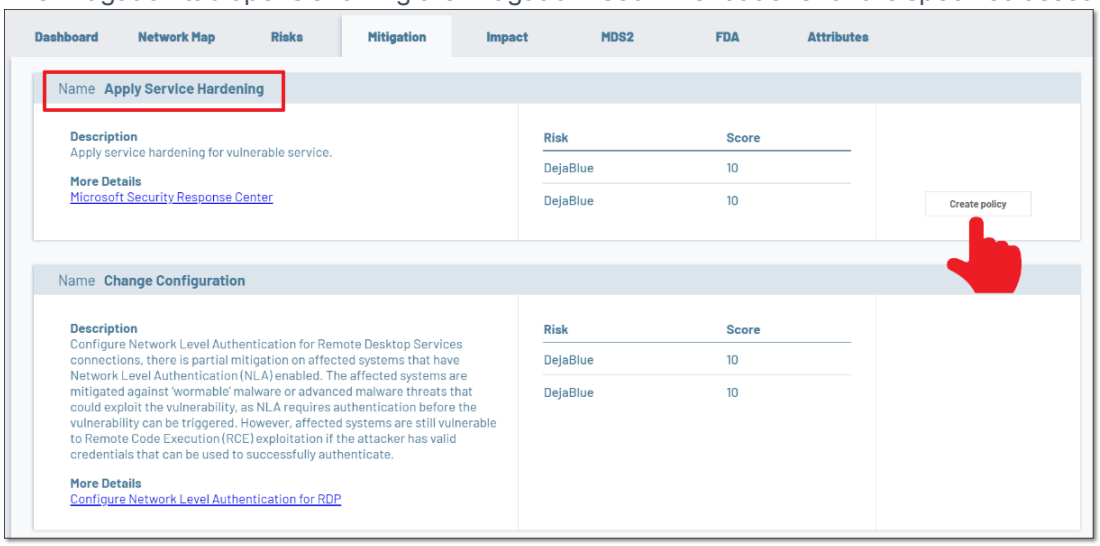


3. Select a critical Risk instance based on the Asset Type and Risk Score, for example, a LIS Server. Click on the row of that Risk to open the Risks tab for the affected asset.
4. Identify an RDP CVEs Risk for which "service hardening" is a suggested Mitigation action.

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

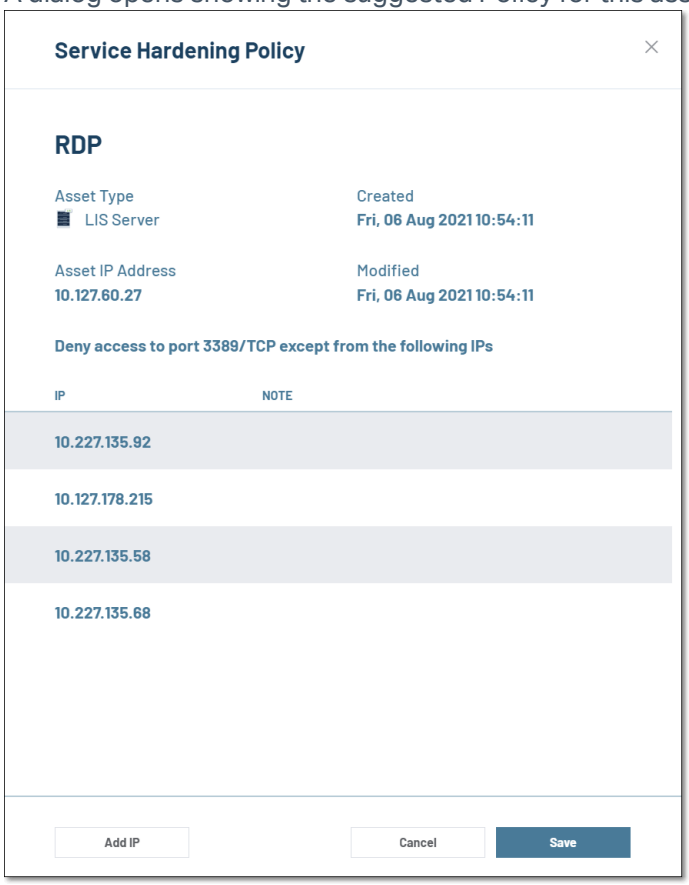


6. The Mitigation tab opens showing the Mitigation recommendations for the specified asset.

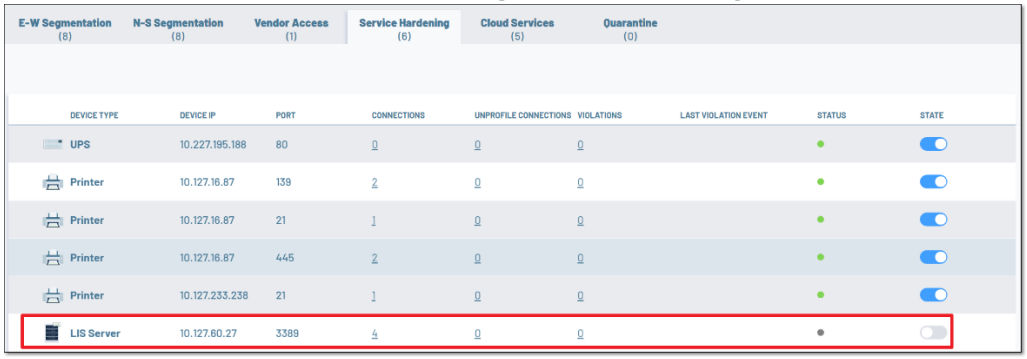


7. Click **Create Policy**.

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



9. You can add or remove IPs to the whitelist as needed.
10. When the Policy is ready, click **Save**.
    The **Policies** screen > **Service Hardening** tab opens showing the newly created Policy.



11. Toggle the **State** switch to **ON**.
12. 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.

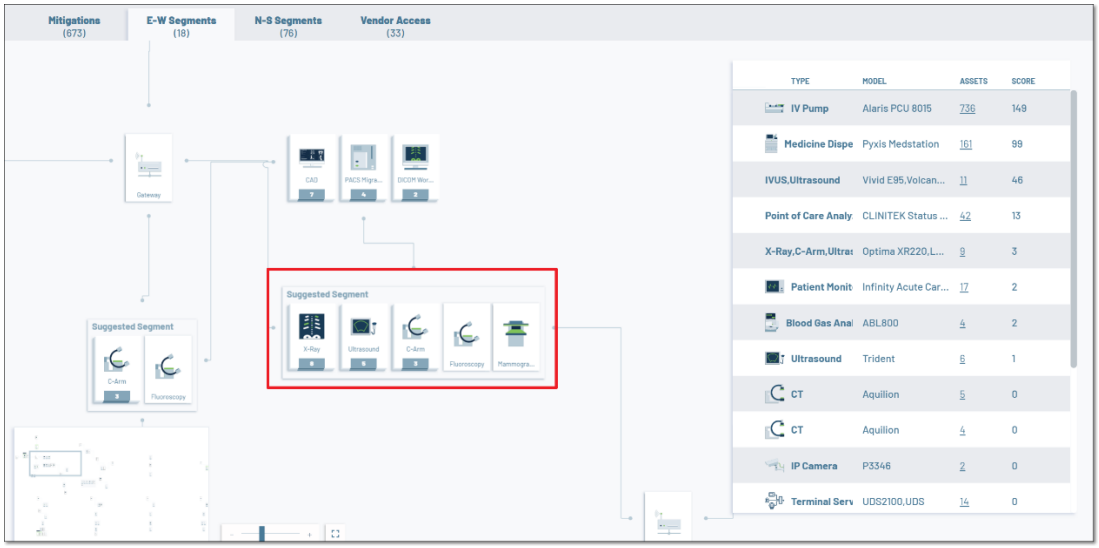
Cynerio enables you to easily apply virtual E-W segmentation to your network. We automate the process of identifying logical segments of assets based on their network communication patterns and generating the rules that define the baseline acceptable communication patterns for each segment. All you need 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

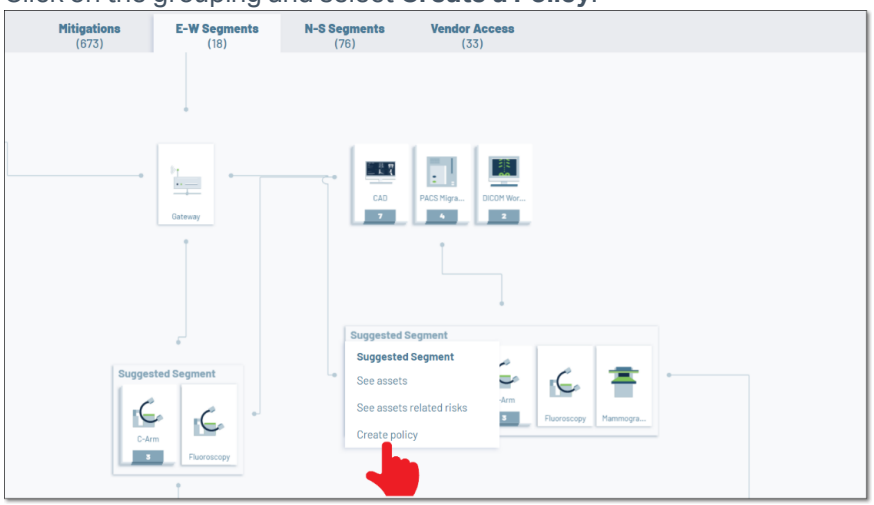
Cynerio monitors the communication between assets in your network and automatically maps out the virtual segmentation of your network, based on shared communication patterns, and generates a recommended policy for each segment.

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

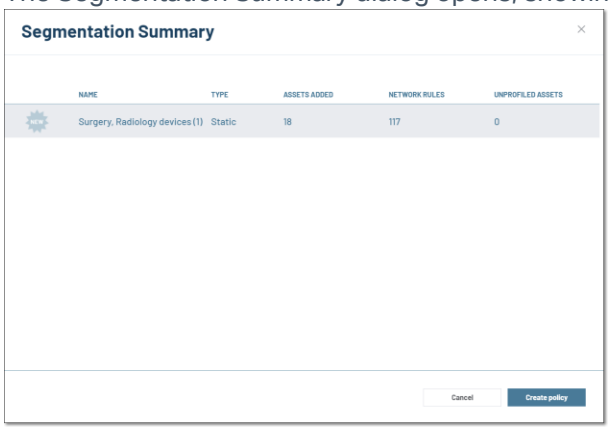
1. On the **Mitigation** screen > **E-W Mitigation** tab, choose a suggested segment for which you would like to create a policy.



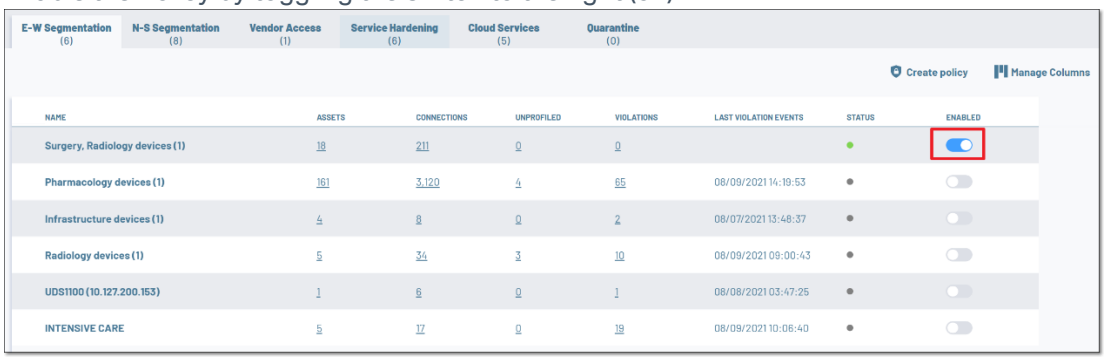
2. Click on the grouping and select **Create a Policy**.



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

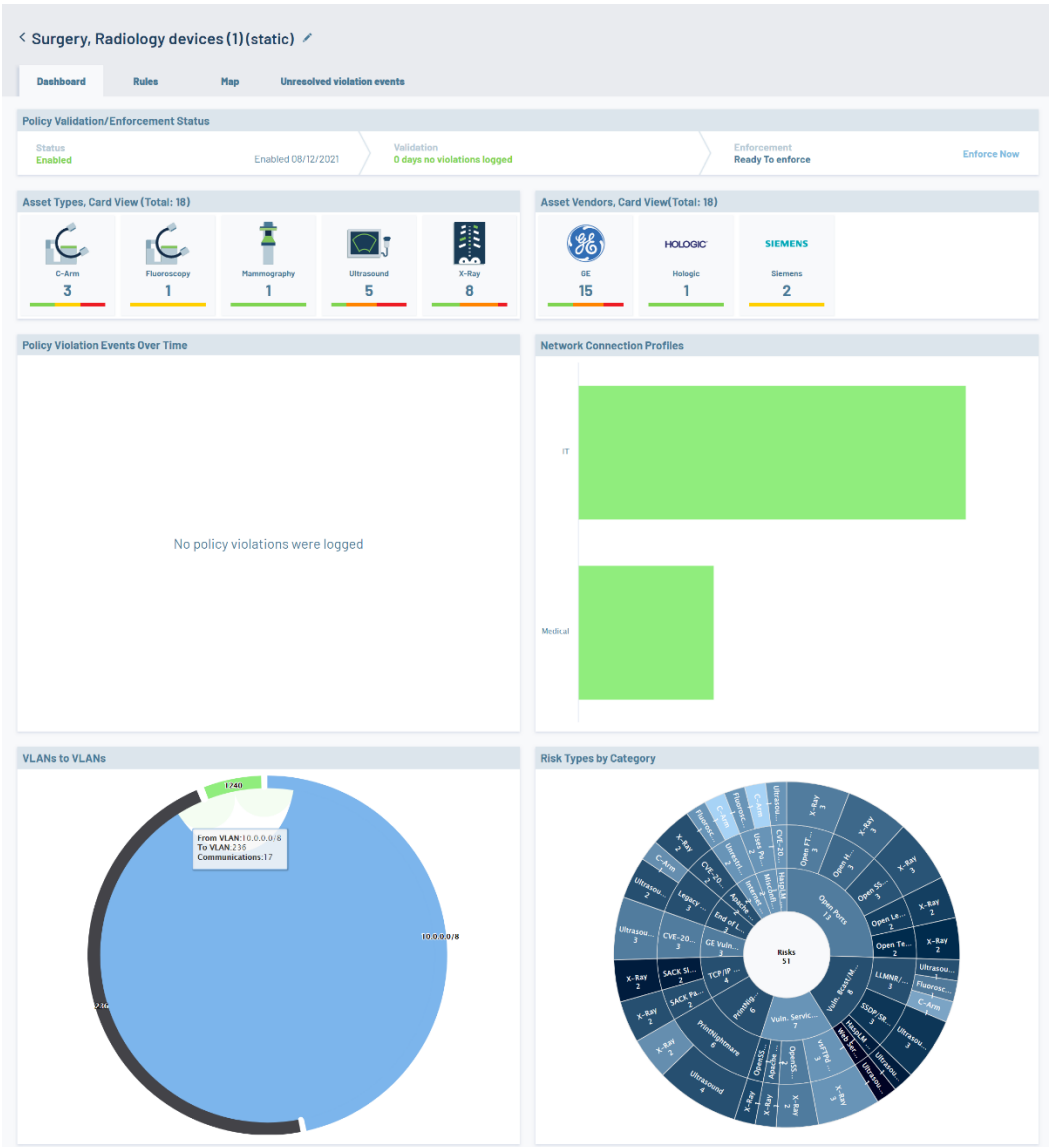


3. Click **Create policy**.
   The policy is implemented and you are redirected to the **Policy** screen > **E-W Segmentation** tab.
4. Enable the Policy by toggling the switch to the right (on).

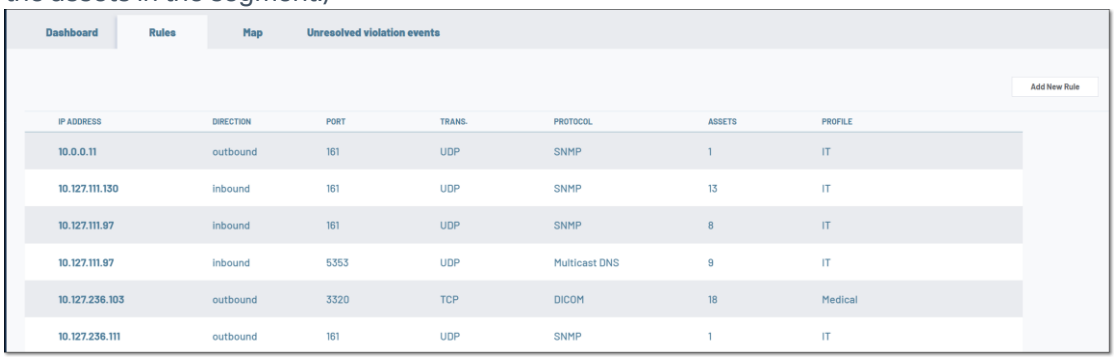


The segmentation Policy is activated in "Validation" mode. During the validation period, Cynerio logs all violations of the Policy. This enables you to fine tune the Policy before you start enforcing it.

5. Click on the row of the Policy to view the **Dashboard** with a series of widgets showing detailed info about the Policy: timeline and status, Assets involved, policy violations over time, network connection profiles, VLANs and Risks involved.

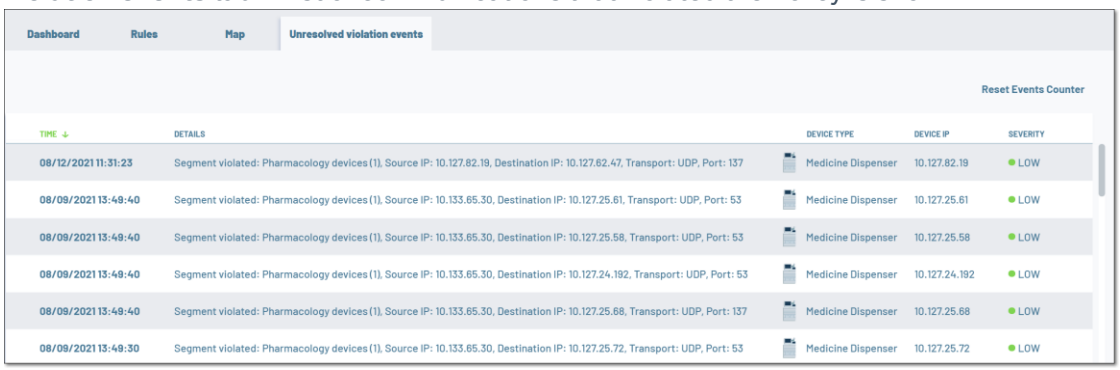


6. If you would like to view and edit the rules for the Policy, you can open the **Rules** tab. This tab shows a list of the rules that define the allowed communications for this segment. On this screen you can **Add**, **Delete** or **Edit** a Policy. (There is also a **Map** tab which shows a map of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

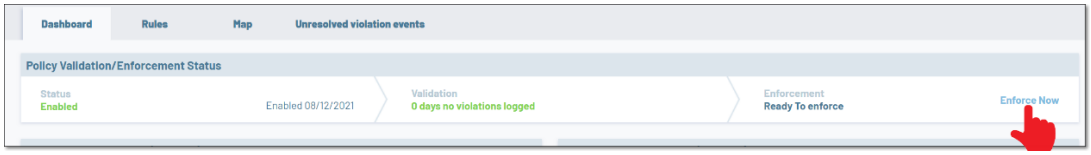
7. If you would like to monitor and manage the Policy violations, you can open the **Unresolved violation events** tab. A list of communications that violated the Policy is shown.



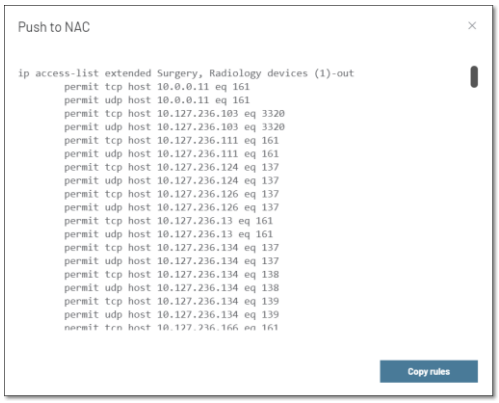
TIME	DETAILS	DEVICE TYPE	DEVICE IP	SEVERITY
08/12/2021 11:31:23	Segment violated: Pharmacology devices (1), Source IP: 10.127.82.19, Destination IP: 10.127.62.47, Transport: UDP, Port: 137	Medicine Dispenser	10.127.82.19	LOW
08/09/2021 13:49:40	Segment violated: Pharmacology devices (1), Source IP: 10.133.65.30,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

   a. If you would like to allow a communication for this segment, right-click on the row of that communication and select **Add to policy**.
   b. If you determine that a device needs to be reconfigured to prevent future violations then take the necessary steps.

8. 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.
9. 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.



- 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.



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 Polic*ies 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.

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.