Simplify and optimize your hybrid IT infrastructure management with AI- infused IBM Support Insights

Lab Center – Hands-On Lab

Session 2152

Simplify and optimize your hybrid IT infrastructure management with AI-infused IBM Support Insights

Ivan Portilla
AI Architect, IBM TSS
ivanp@us.ibm.com
https://www.linkedin.com/in/ivanportilla/

Speaker 2
Title
speaker@us.ibm.com

Table of Contents

DISCLAIMER

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results like those stated here.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
OpenShift is a trademark of Red Hat, Inc.
UNIX is a registered trademark of The Open Group in the United States and other countries.

© 2020 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

We Value Your Feedback

Don’t forget to submit your Think 2021 session 2152 and speaker feedback! Your feedback is very important to us – we use it to continually improve the conference.

Introduction

Today's IT infrastructures are complex, and your organization cannot afford unplanned downtime. Included with your IBM Technology Support Services maintenance agreement, IBM Support Insights offers actionable indicators for preventive maintenance, helping to improve IT reliability and streamline asset management for IBM and other OEM systems (including Cisco, HP, Oracle, Dell, Juniper, NetApp, EMC and more).

IBM Support Insights helps reduce gaps in support coverage, enabling you to simplify management of your entire IT estate across multiple vendors.

IBM Support Insights helps you proactively manage your inventory, identify contract and security exposures, and avoid downtime to better help manage the device health and growing costs of your IT estate.

IBM Support Insights harness the power of advanced analytics to proactively address risks and exposures that may impact the availability of your hybrid IT infrastructure.

Proposal:

IT managers and admins are invited to join this session to learn how to use advanced analytics & AI to prevent future problems & improve uptime for their hybrid IT infrastructure through critical exposure identifications & prescriptive recommendations. With IBM Support Insights, you can improve your support experience, save time & better maintain the availability of your products to keep business applications available 24x7.

Pre-Requisites

This hands-on lab illustrates how to use some of the enhanced INS capabilities to quantify risk assessment of your IT state. We will show you how to filter and discover security vulnerabilities and check the OS version consistency capabilities based on the OS conformance information

Additionally, please download the box folder to your local machine.

Specifically, we need the following:

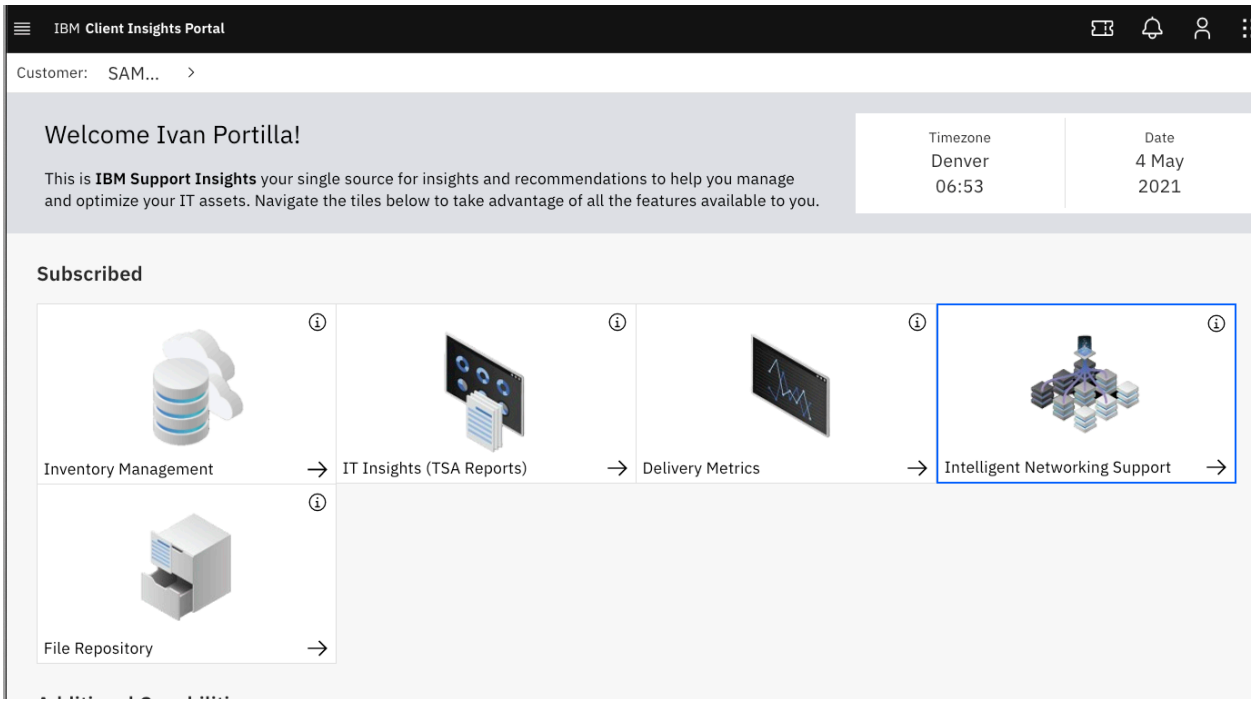
1. Configure Intelligent Networking Support (INS) portal dashboard and check inventory and support coverage status

Start a web browser session and navigate to the IBM Support Insights (CIP) by clicking on the following link:

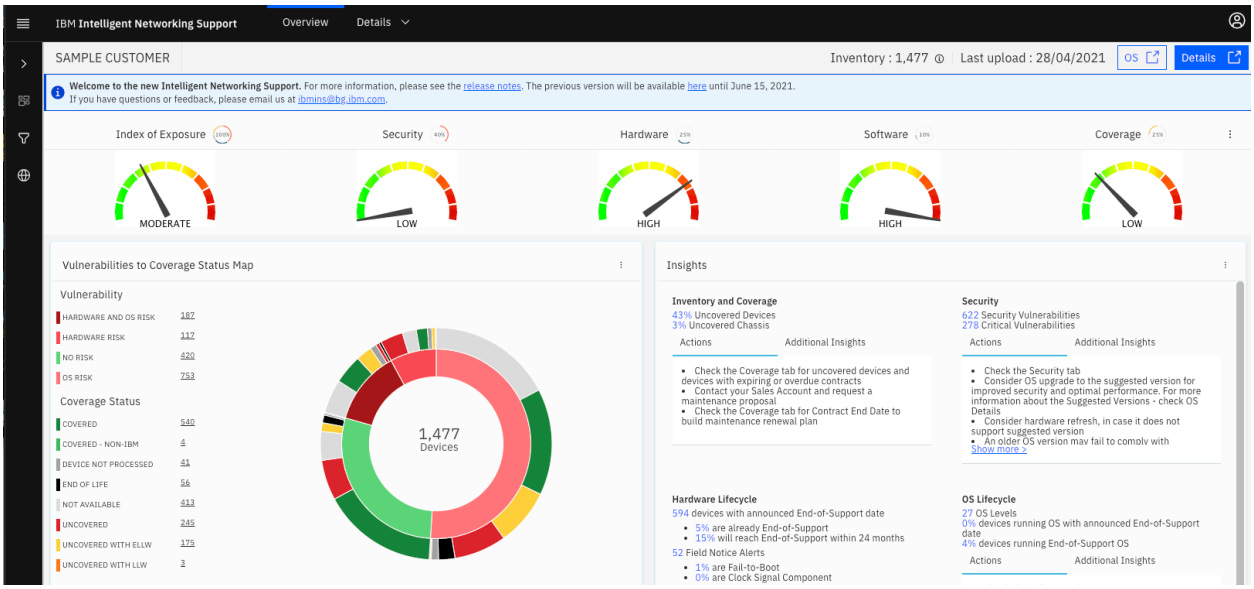
https://clientinsightsportal.ibm.com/cip/#/home/a94bc49f-e34a-4883-82a9-c2da46dd1e04

https://clientinsightsportal.entercoms.com/cip/#/home/96e0975c-183a-4631-9488-eafd9a4d5f92

Click on the Intelligent Networking Support (INS) card



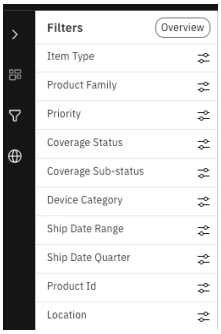
You will see the SAMPLE CUSTOMER data that has been configured for this lab:



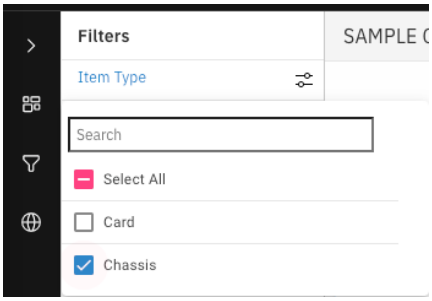
The INS Dashboard is configurable through the global filter functionality available in Left-Hand Navigator (LHN).

For this exercise, let's configure the dashboard to analyze **Network Chassis** for **Location 1**.

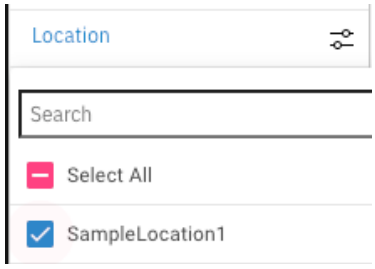
1. Go to Global Filter: On the LHN click on the Filters icon



2. Under **item type** select **chassis**.



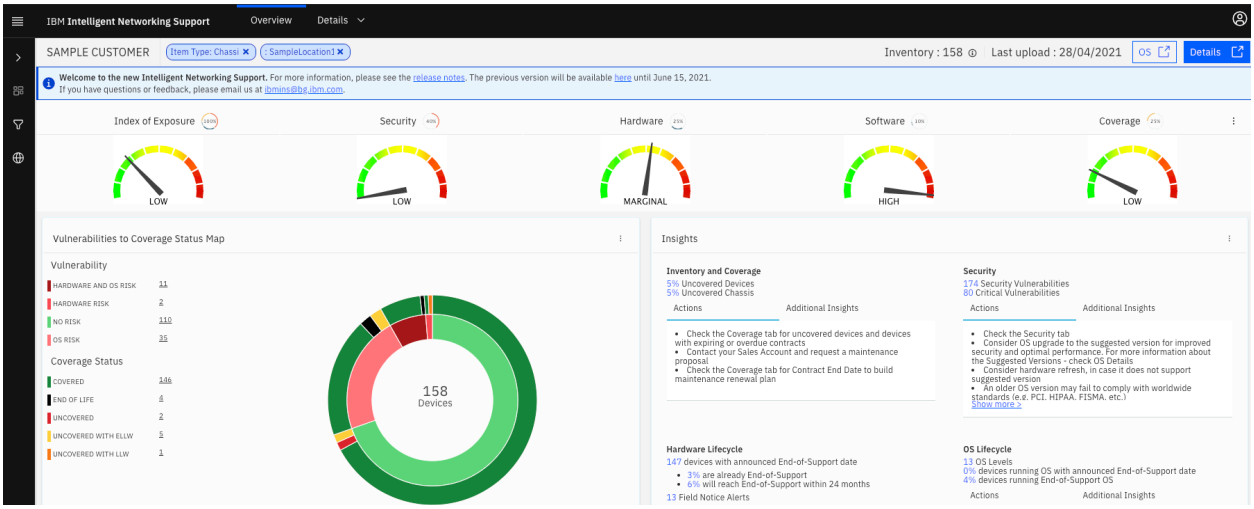
3. Select **SampleLocation1** under the **Location** filter



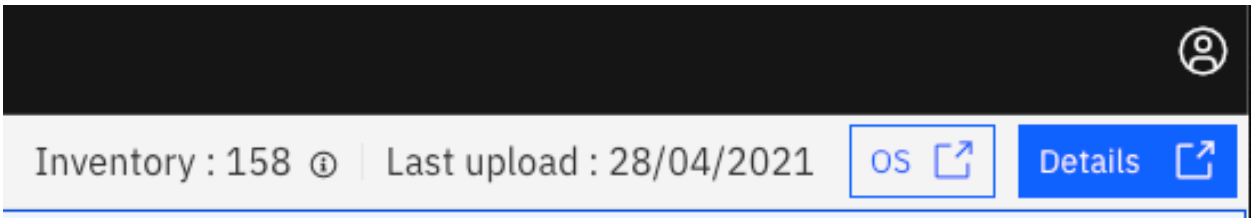
4. Next, click on the Apply Filters blue button at the bottom of the Filters view

5. You will see a full list of all **Network Chassis** devices in **Location 1** along with their current support coverage status (which would help you identify devices with expiring or already expired service contracts and plan for contract renewals)

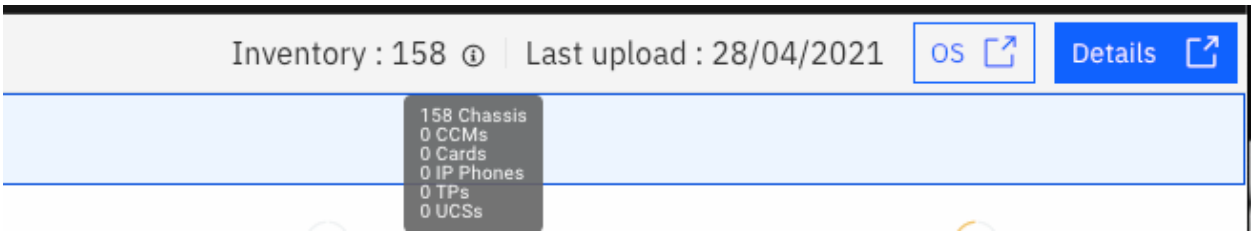
The INS Dashboard also provides a quantifiable risk assessment of the install base through the INS **Index of Exposure.** This index is made up by combining the exposure coming from four focus areas – **Security** Vulnerabilities, **Hardware**, **Software** and Support **Coverage**.



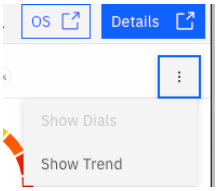
The calculations and analysis are based on the latest data uploaded to the dashboard. In the top right-hand corner, you can see the **Inventory** count and **Last Upload** Date.



Hovering over the ⓘ symbol will display a tooltip with a breakdown of the uploaded inventory by Item type.

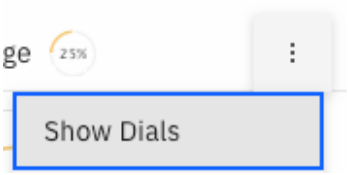


If you would like to see how your network has scored through time, you can go to the **Index of Exposure** menu icon ⋮ and click on **Show Trend**.

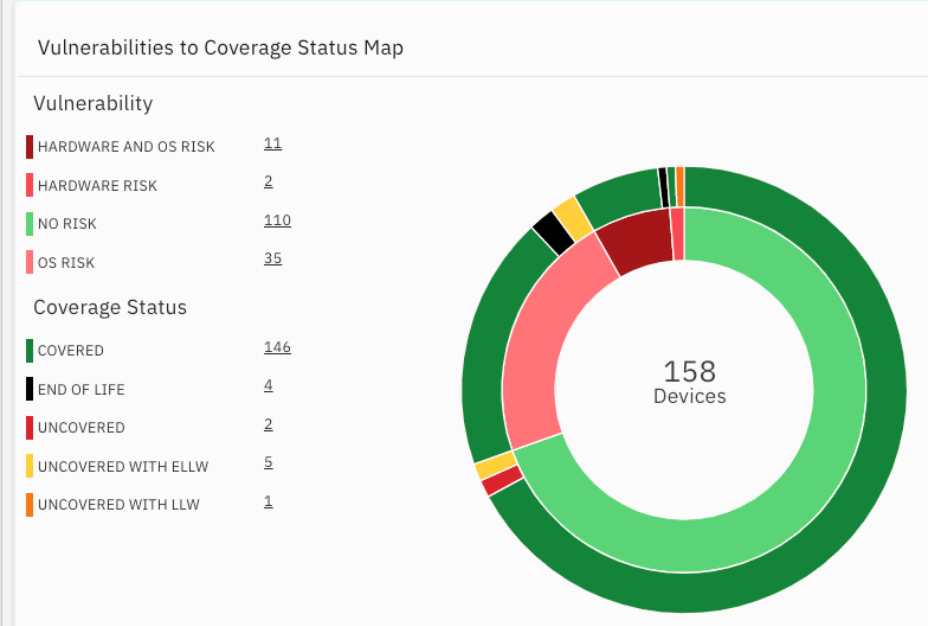


The dials will change to time series analysis as follows:

To see the Sunburst dials, click again on the **Index of Exposure menu** icon an select **Show Dials**



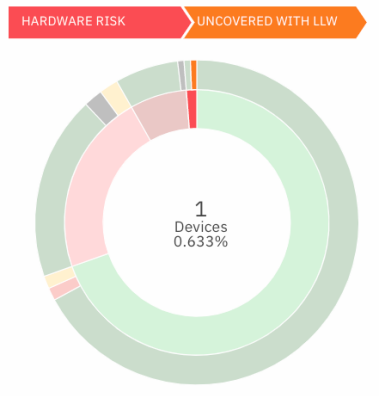
Underneath the dials there is a **sunburst chart** showing the correlation between the Support Coverage status of the install base and the type of risk we have identified in a sunburst chart.



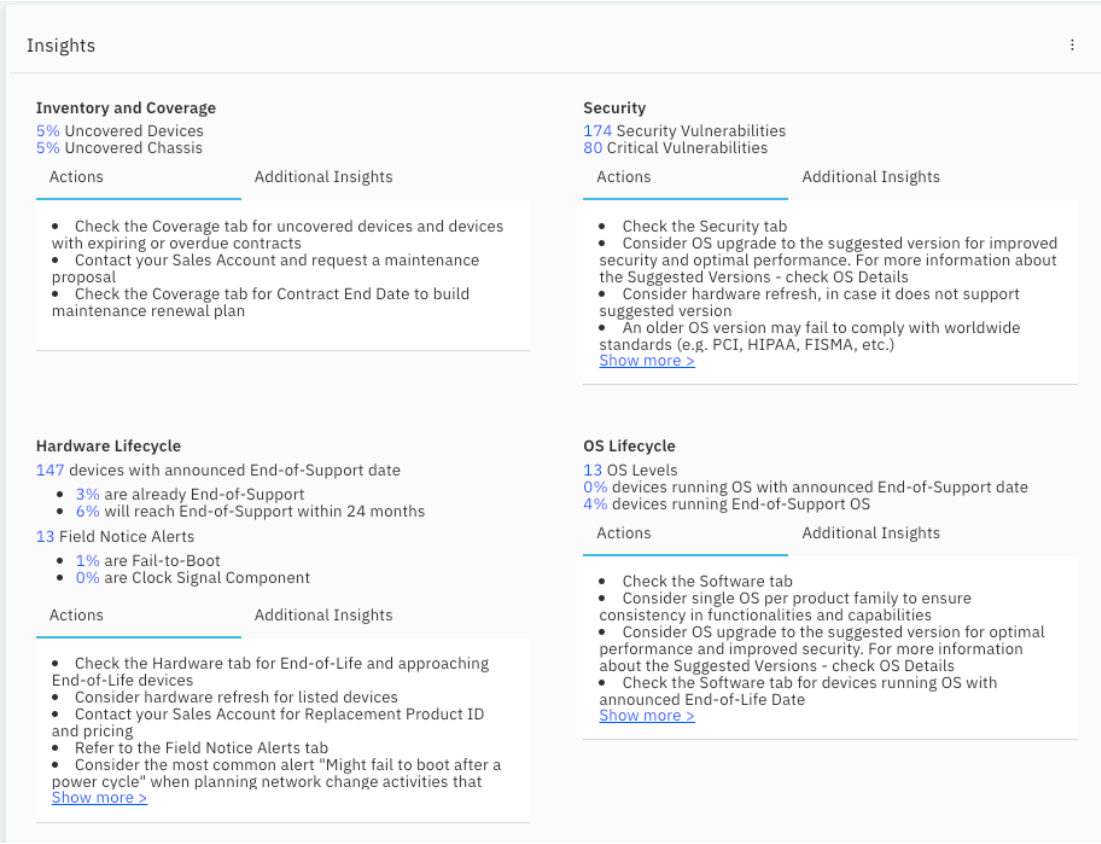
Hardware risk is assigned when a device is already end of life or if there is a product defect (Field Notice alert) matched for it. **OS risk** is assigned when there is either a security vulnerability for a device, or its OS is already end of support.

Support **Coverage status** is assigned following an entitlement check with the OEM.
Devices past their hardware *End of Support* date are labeled as **End of Life**. Devices under active maintenance contract are labeled as **Covered**. Devices without an active contract are labeled as **Uncovered**. Additionally, a distinction is made for devices with an elevated warranty status – in our case, we have **Uncovered** devices with Enhanced Limited Lifetime Warranty (**Uncovered With ELLW**) and Limited Lifetime Warranty (**Uncovered with LLW**).

You can quickly identify devices without active maintenance, which are associated with **Hardware** by hovering over **HW** segment and then **Uncovered with LLW**. Each segment of the sunburst chart as well as the items in the legend to the left are active links to tables containing details for the respective field.

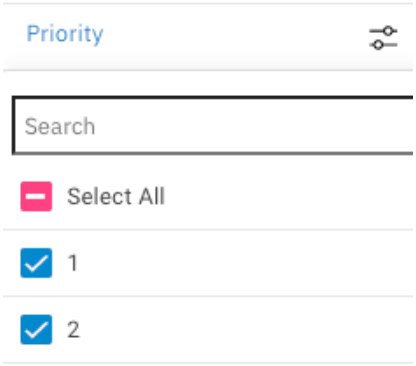


To the right, there is an Insights section with some key **insights** and recommended **actions** for each focus area.



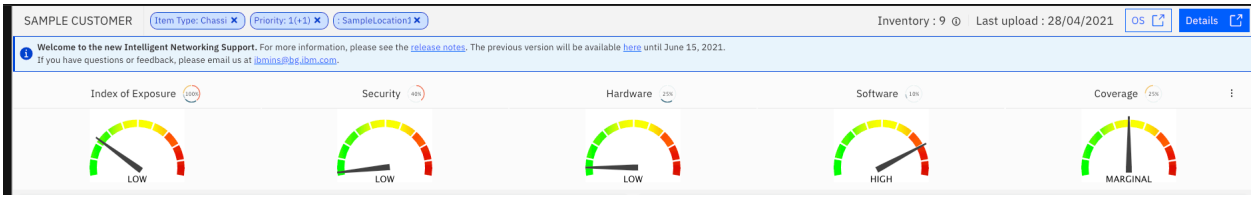
Let's narrow down our query to the top priority items

1. Click on the funnel icon
2. Under **Item Type** verify the Chassis is selected
3. Under **Priority** select 1 and 2



4. Under **Location** verify SampleLocation1 is selected
5. Click the **Apply Filters** bottom

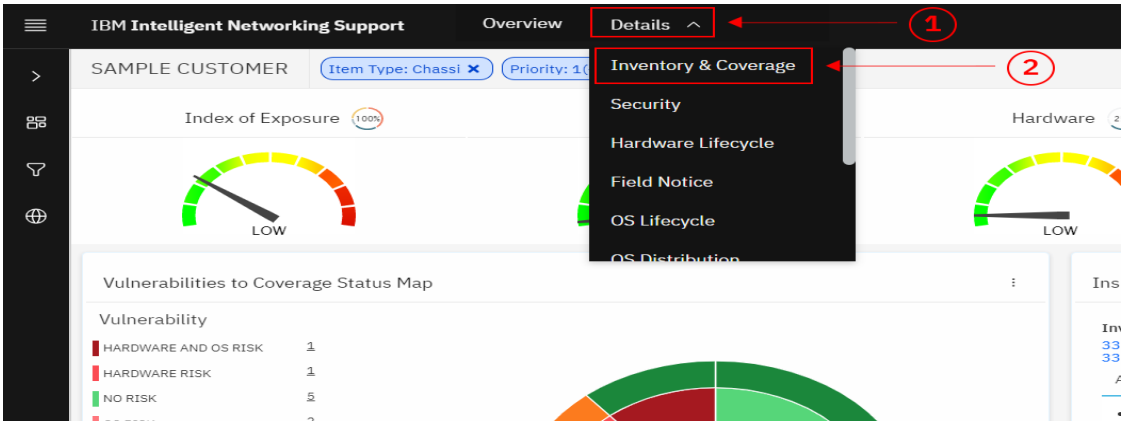
The INS Dashboard will be reconfigured to match your global filter selection. You will notice the Inventory count now shows **9 chassis**; the dials are showing different scores; the sunburst chart and insights sections are updated as well.



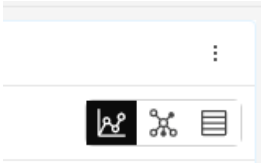
All currently applied global filters are shown as chips at the top of the dashboard.

Please note, any change you make on the dashboard will be saved and carried out between login sessions.

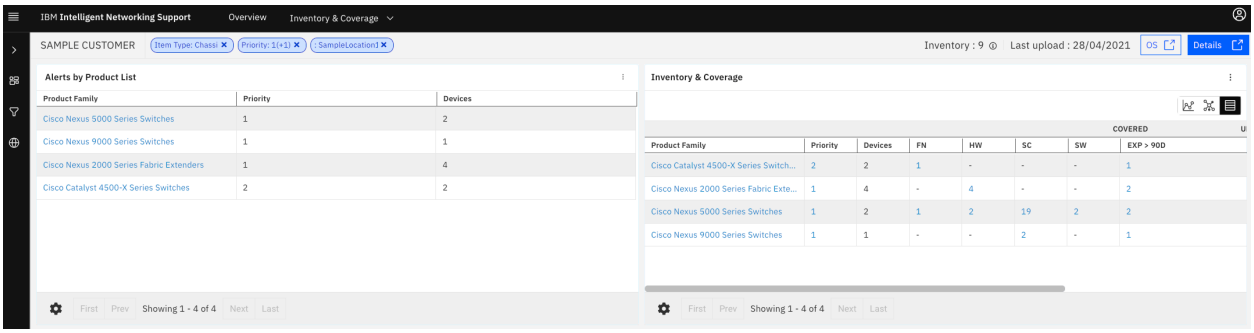
To view the entire support coverage information for the **Chassis** in **Location 1** go to the **Details** dropdown (1) and select **Inventory & Coverage (2)**.



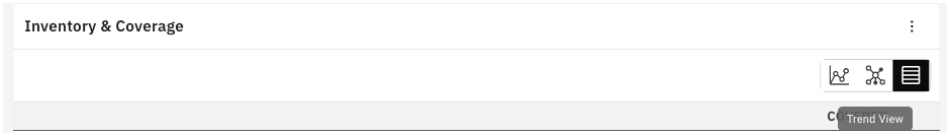
Panels could be resized for better visibility. Additionally, each panel has alternative views buttons available in the top right-hand corner.



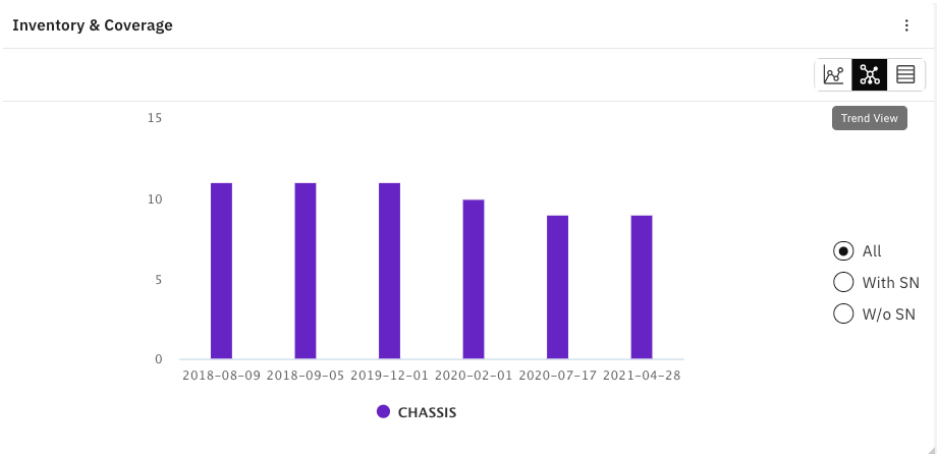
The **Inventory & Coverage** panel displays a chart with breakdown of the coverage status by Product Family by default.



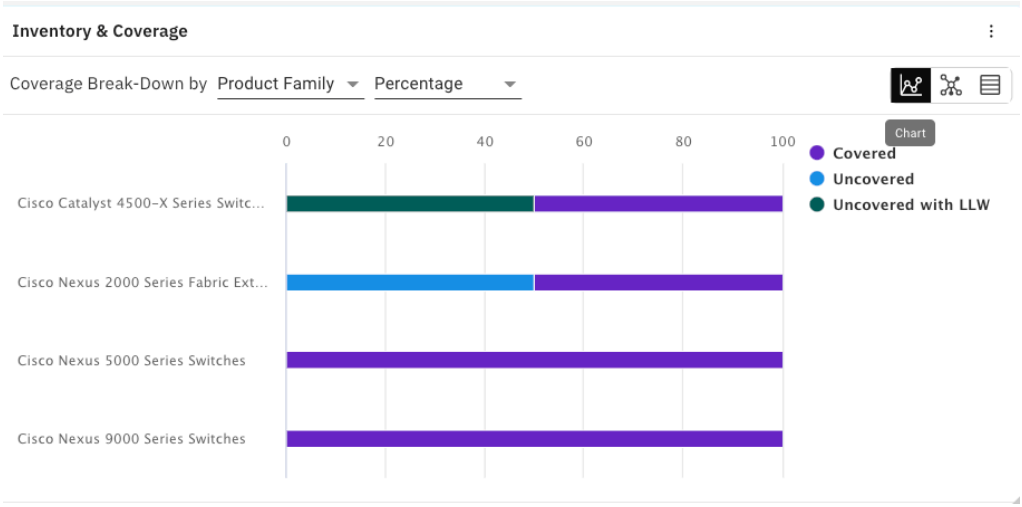
Click on **Trend view** to check how has the number of chassis for this location changed through past uploads.



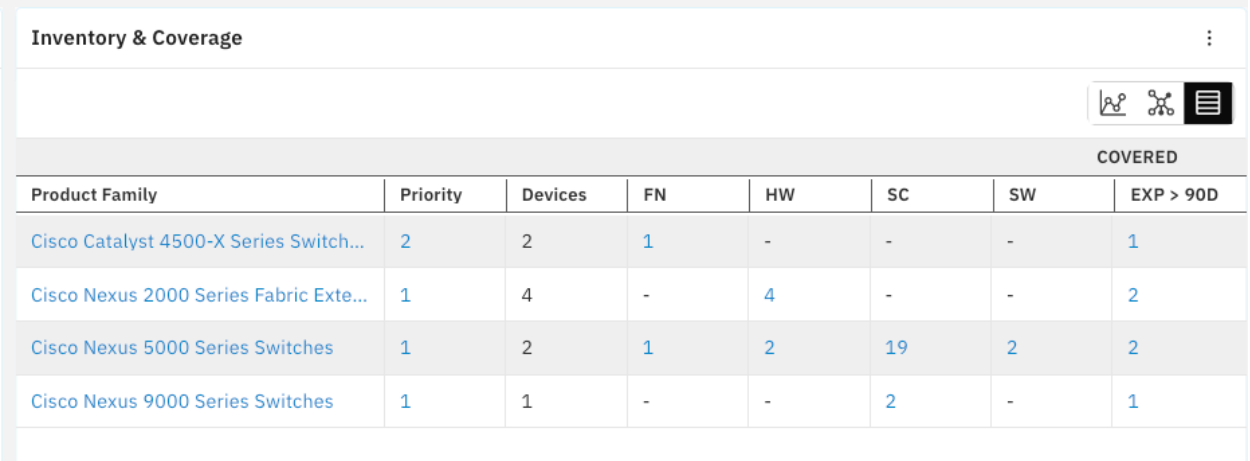
You will see a view like:



The **Chart** view shows additional information on **Coverage** status



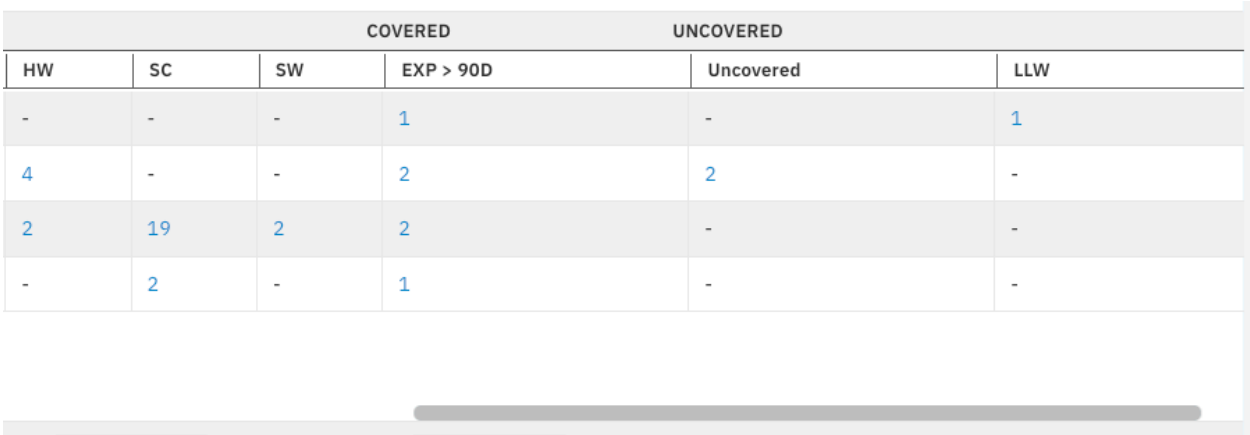
Click on Table view  to have the devices arranged in various support coverage categories as well as information about the various alert types matched for each product family.



Inventory & Coverage

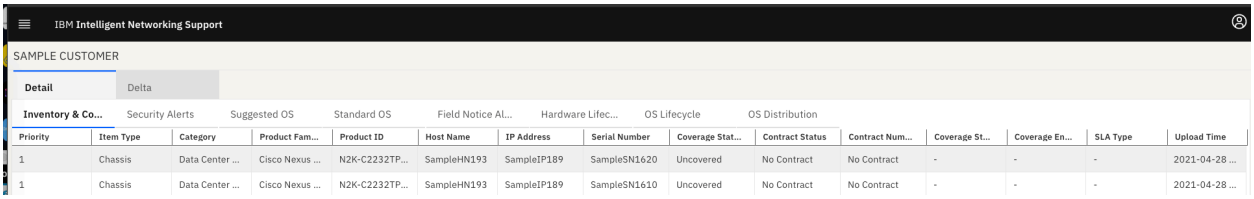
			COVERED				
Product Family	Priority	Devices	FN	HW	SC	SW	EXP > 90D
Cisco Catalyst 4500-X Series Switch...	2	2	1	-	-	-	1
Cisco Nexus 2000 Series Fabric Exte...	1	4	-	4	-	-	2
Cisco Nexus 5000 Series Switches	1	2	1	2	19	2	2
Cisco Nexus 9000 Series Switches	1	1	-	-	2	-	1

Next, scroll to the right and Click on any number link under the **Uncovered** column:

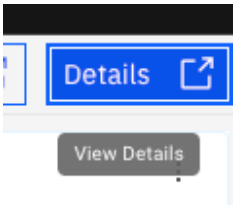


			COVERED	UNCOVERED	
HW	SC	SW	EXP > 90D	Uncovered	LLW
-	-	-	1	-	1
4	-	-	2	2	-
2	19	2	2	-	-
-	2	-	1	-	-

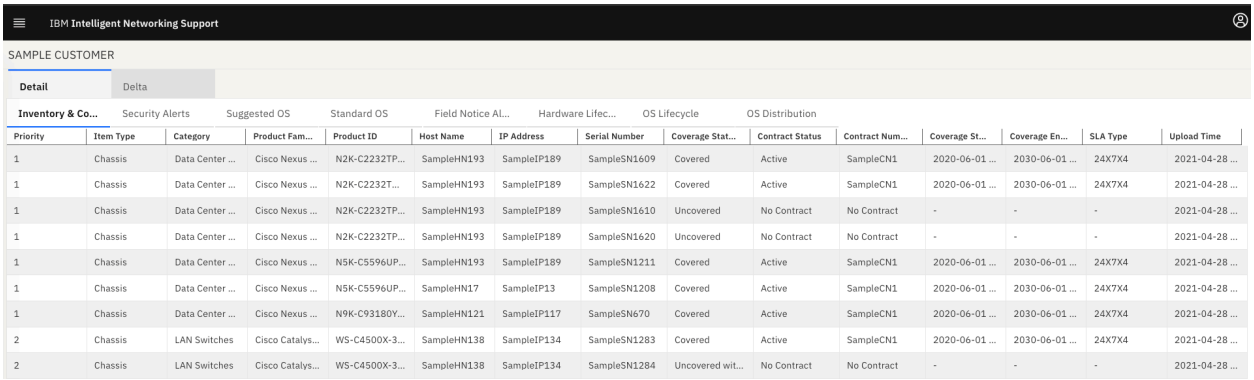
A **detailed view** will load on a new browser session with the uncovered device(s), along with data to help you identify the device on your network.



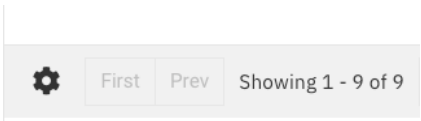
Alternatively, you could get support coverage information for all **Chassis** in **Location 1** by clicking on **Details** link from the top right-hand side of the dashboard.



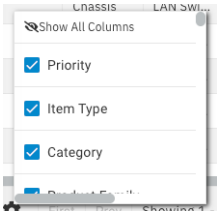
There are several columns added to a detailed view by default, however, you can add more detail columns



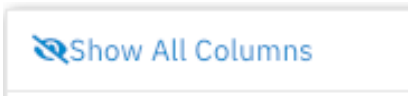
Click on the **cogwheel menu** at the lower left-hand side of the detailed view



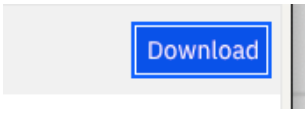
and review the details available.



Click on **Show all Columns** to enable all data options in your detail view.

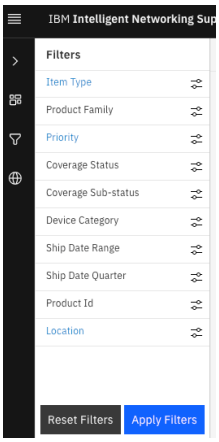


Click on Download in the lower right-hand side of the detail view to download a spreadsheet with all the data from your screen.



Close this browser tab to go back to the original browser session

Click on the global Filter and then on the **Reset Filters** bottom to reset the INS Dashboard before the next scenario.



2. ISS INS Security

In this section, we will review the security exposure analysis capabilities based on the report alerts. We will show how to:

1- Display all security alerts reported per device

2- Perform security exposure analysis based on the reported alerts

3- Perform a what-if analysis demonstrating how the security exposure will change (improve) if we migrate to Cisco's suggested OS versions

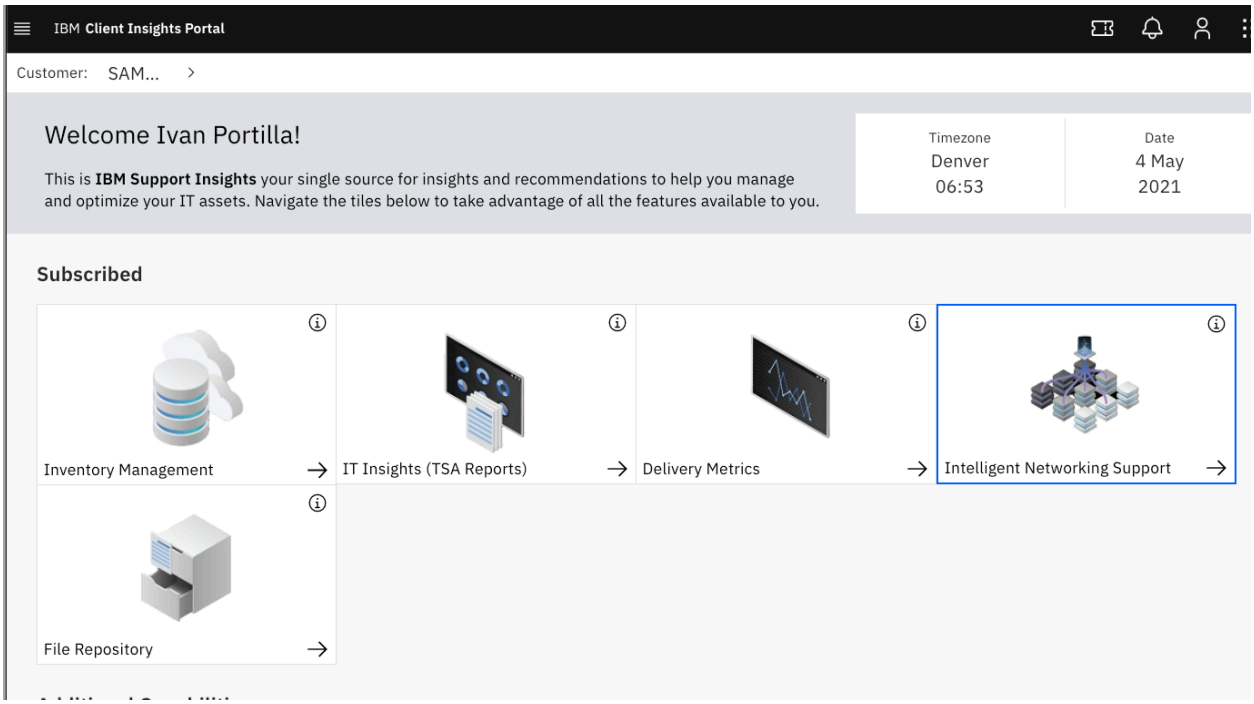
4- Validate the level of OS conformance status by comparing the current OS versions against company OS standards

As shown in section 1, start a web browser session and navigate to the IBM Support Insights (CIP) by clicking on the following link:

https://clientinsightsportal.ibm.com/cip/#/home/a94bc49f-e34a-4883-82a9-c2da46dd1e04

https://clientinsightsportal.entercoms.com/cip/#/home/96e0975c-183a-4631-9488-eafd9a4d5f92

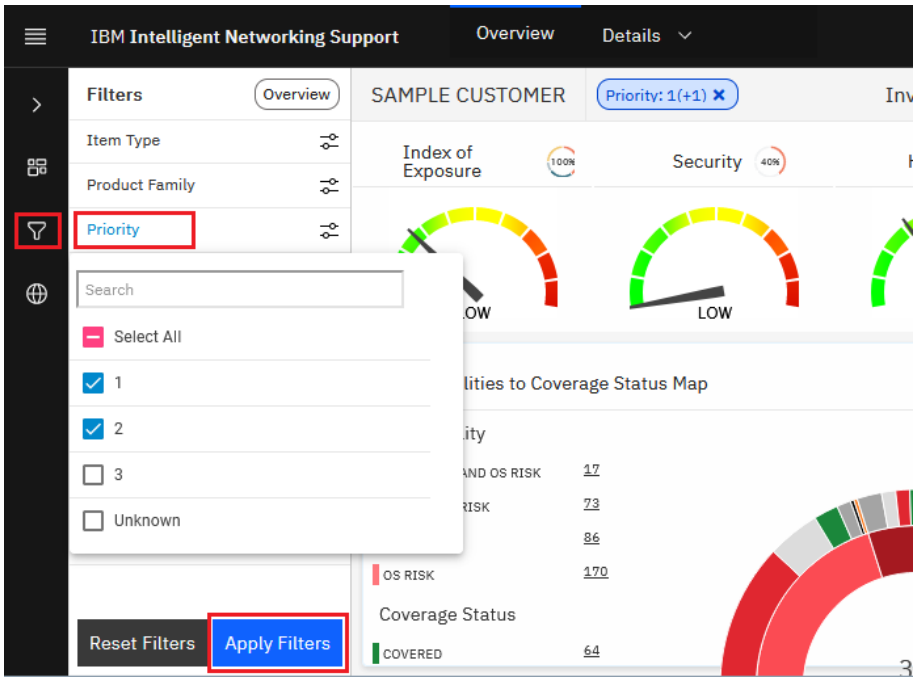
Click on the Intelligent Networking Support (INS) card



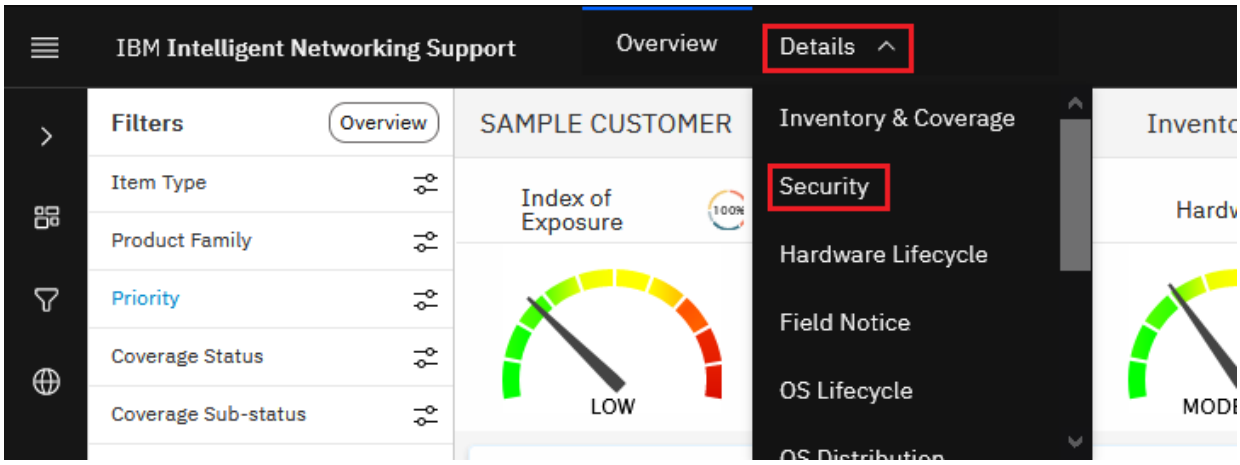
You will see the SAMPLE CUSTOMER data that has been configured for this lab:

Instructions:

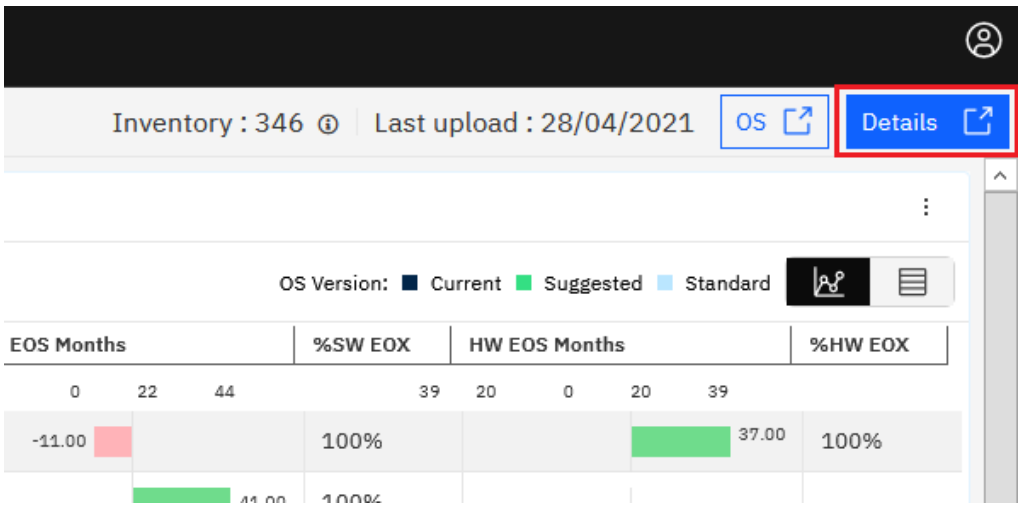
1. Limit the scope of the analysis to **priority 1** and **2** devices by making the appropriate selection in the **Global filters**. (Remember to click on **Apply Filters** blue button)



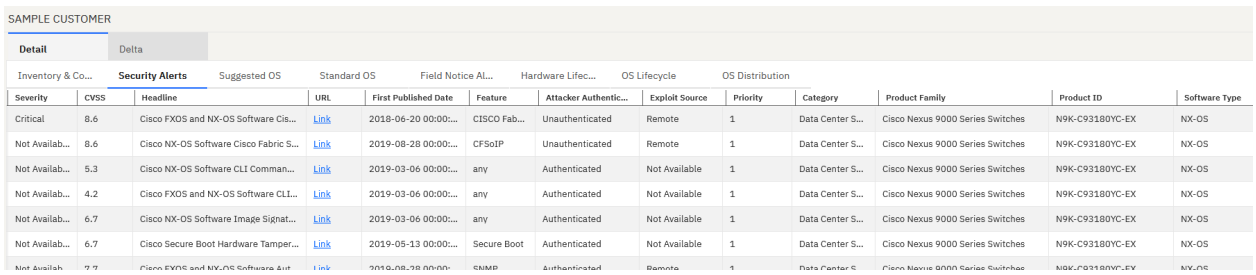
2. In the dashboard, from the **Details** drop-down menu at the top, select **Security**:



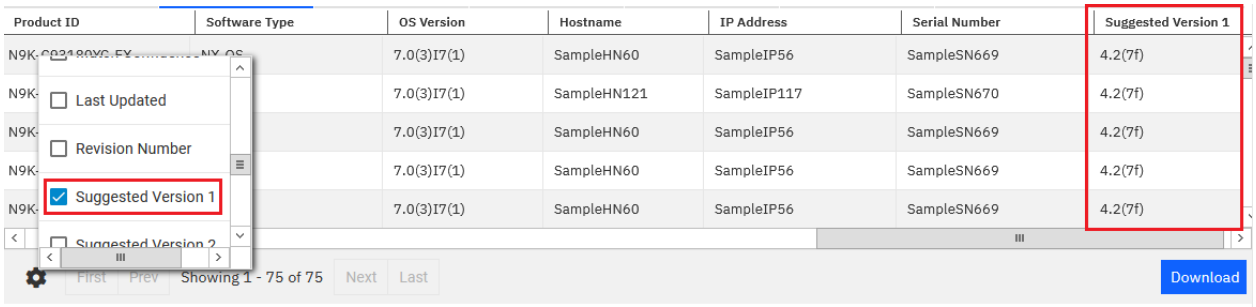
3. Next, the **Details** button in the top right corner will open a new browser tab with all identified security alerts:



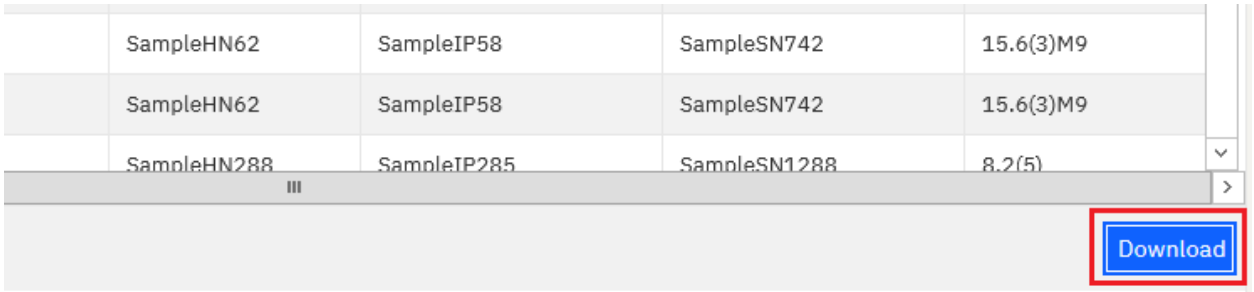
Each row of data represents a security advisory affecting a particular device in the inventory. The first few columns have the details of the PSIRT (headline, URL, CVSS, severity, affected feature etc.), whereas the remaining fields show the attributes of the device (hostname, IP address, OS level, etc.):



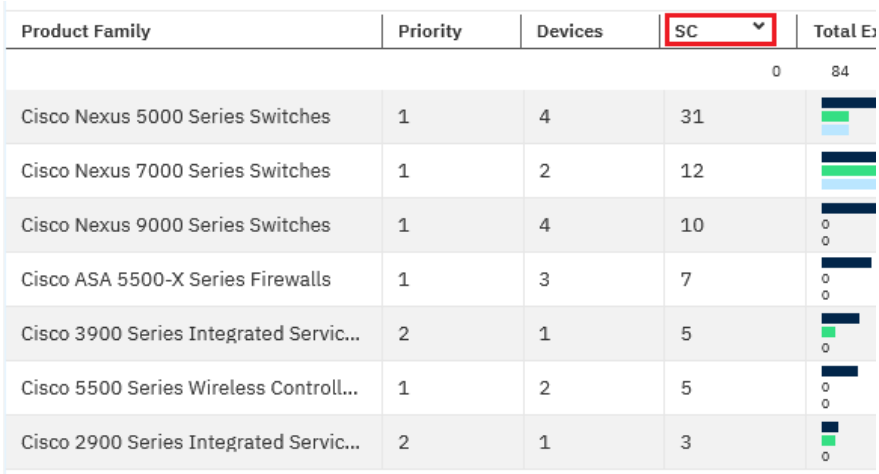
By default, only a subset of the available columns is displayed. Click on the **cogwheel** icon in the bottom left corner to reveal the list of all available data fields. Enable **Suggested Version 1** and scroll to the right end of the table to check the suggested versions:



Click on the **Download** button to generate and save locally a spreadsheet with the data in the table:



4. Go back to the tab with **Security**. It shows an **Alerts by Product List** view aggregated at the product family level of the condition of the inventory with respect to security. The three columns following the family names show the **Priority**, the number of devices (**Devices**) and the number of identified security vulnerabilities affecting the devices (**SC**) in the family. Click on the **SC column** to sort by the number of alerts:

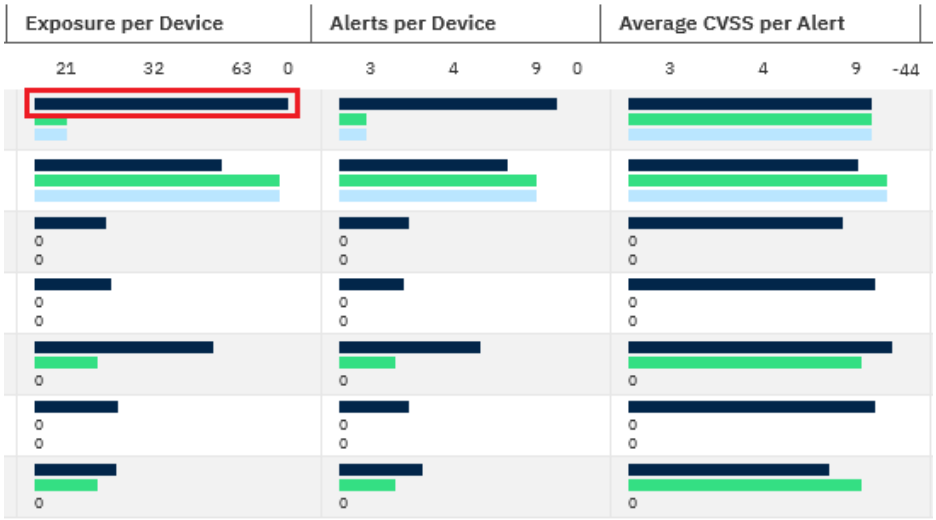


Product Family	Priority	Devices	SC	Total Ex
			0	84
Cisco Nexus 5000 Series Switches	1	4	31	
Cisco Nexus 7000 Series Switches	1	2	12	
Cisco Nexus 9000 Series Switches	1	4	10	
Cisco ASA 5500-X Series Firewalls	1	3	7	
Cisco 3900 Series Integrated Servic...	2	1	5	
Cisco 5500 Series Wireless Controll...	1	2	5	
Cisco 2900 Series Integrated Servic...	2	1	3	

The charts next to the numbers visualize the various dimensions of the security exposure. **Total Exposure** is the sum of the CVSS score of all vulnerabilities affecting all devices of the same product family. By summing the CVSS scores, instead of counting alerts, we weigh the vulnerabilities and take into account their severity. Clicking on the header of the column will push to the top the family contributing the most to the exposure, in this case - the Nexus 5K switches. An upgrade across this family or mitigation of the affecting vulnerabilities will have the greatest impact on the overall level of exposure.

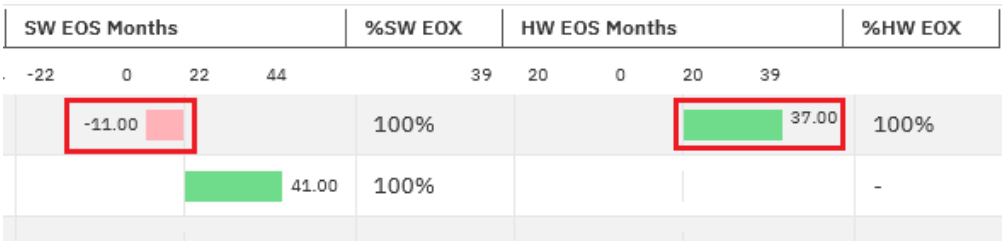
Product Family	Priority	Devices	SC	Total Exposure	Exposure per Device	Alerts per Device
				0 84 126 251 0	21 32 63 0	3 4 9 0
Cisco Nexus 5000 Series Switches	1	4	31			
Cisco Nexus 7000 Series Switches	1	2	12			
Cisco Nexus 9000 Series Switches	1	4	10			
Cisco ASA 5500-X Series Firewalls	1	3	7			
Cisco 3900 Series Integrated Servic...	2	1	5			
Cisco 5500 Series Wireless Controll...	1	2	5			
Cisco 2900 Series Integrated Servic...	2	1	3			

The next three charts show the average **Exposure per device**, the average number of **Alerts per device**, and the **Average CVSS per alert**. These additional dimensions help refine your decision which family or type of device should be tackled first. Instead of going for the family with the highest total exposure, you might decide to turn your attention first to the family where the individual exposure is the highest. In our example, it is again the Nexus 5Ks:



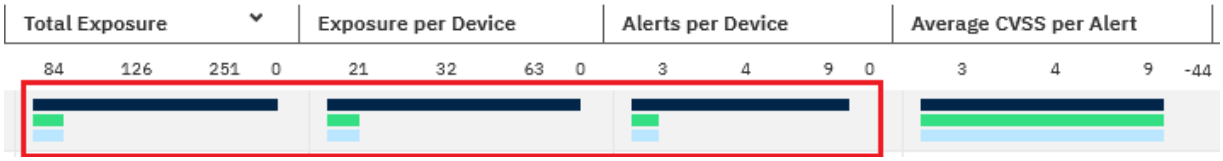
You could also factor in the **Hardware** and **Software EoL** statistics. They show, on average, in how many months the hardware or the currently installed OS levels will reach End-of-

Support. A negative value of **SW EoL** means that the OS is past the End-of-Support date and could only reaffirm your decision to initiate upgrades. A negative score of **HW EoL** means that the devices themselves are already end-of-support and you would be better advised to refresh the hardware instead of spending resources on performing OS upgrades. It should be noted that those statistics are calculated only for that part of the family for which the vendor has already announced an EoL schedule. The **percentages** next to the charts reflect this fact:



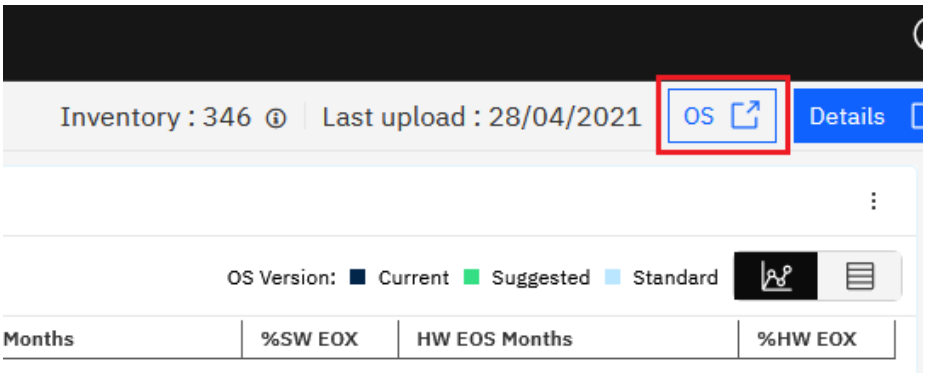
The Nexus 5Ks have 37 months until they reach their last day of support, but the currently installed OS is already end-of-support. Upgrading the OS is the way to go in such a situation.

The green and light blue bars in the exposure charts visualize the expected change, if all devices within the product family are migrated to a Cisco suggested version (green bar) or respectively to the company standard version (light blue bar). The change is not always positive, because Cisco's suggestions are not based on the applicable security vulnerabilities alone. The decision to recommend a version could be influenced by its longevity and adoption rate. Bug-free versions, where all known vulnerabilities are patched, are usually quite new. Consequently, a long-lived version, with multitude of deployments among the existing Cisco customers could still be recommended, although it is not free from any defects and vulnerabilities.



For the Nexus 5Ks the benefit of upgrading to the standard or suggested version – in terms of overall exposure, exposure per device, and alerts per device – is clearly visible.

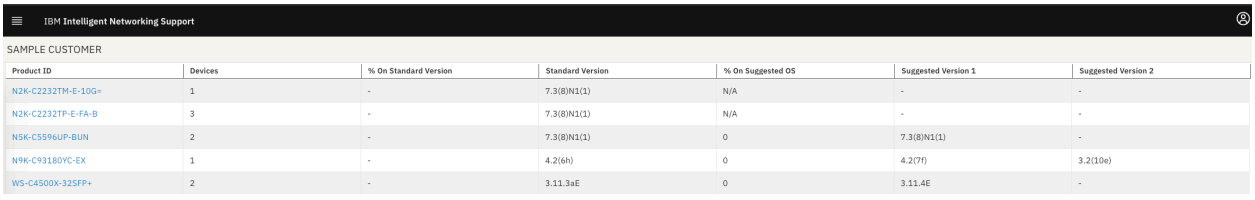
5. Click on the OS button in the top right corner. The OS Conformance report will open a new browser tab:



Verify that current OS conformance for the Nexus 5000s is 0%. An OS upgrade to the company standard level could remedy this violation of company policy:

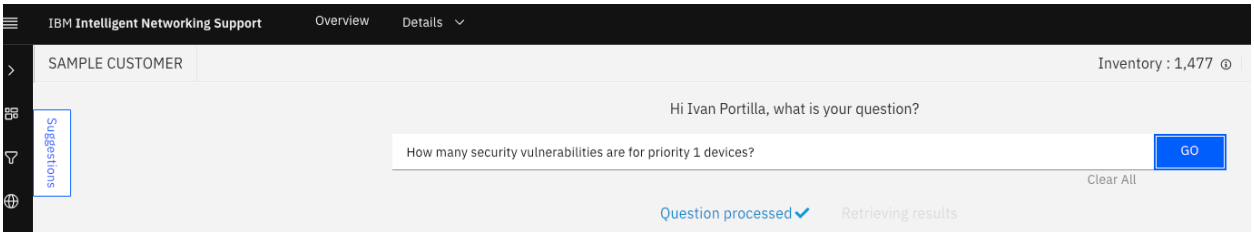
SAMPLE CUSTOMER

Product ID	Devices	% On Standard Version	Standard Version	% On Suggested OS	Suggested Version 1
CISCO2901-SEC/K9	1	-	15.7(3)M8	0	15.6(3)M9
CISCO3925E-SEC/K9	1	-	15.7(3)M8	0	15.6(3)M9
N2K-C2232TM-E-10G=	2	-	7.3(8)N1(1)	N/A	-
N2K-C2232TP-E-FA-B	20	-	7.3(8)N1(1)	N/A	-
N5K-C5596UP-BUN	4	-	7.3(8)N1(1)	0	7.3(8)N1(1)
N7K-C7004-S2E	2	-	8.2(5)	0	8.2(5)
N9K-C93180YC-EX	4	-	4.2(6h)	0	4.2(7f)
WS-C4500X-32SFP+	2	-	3.11.3aE	0	3.11.3aE



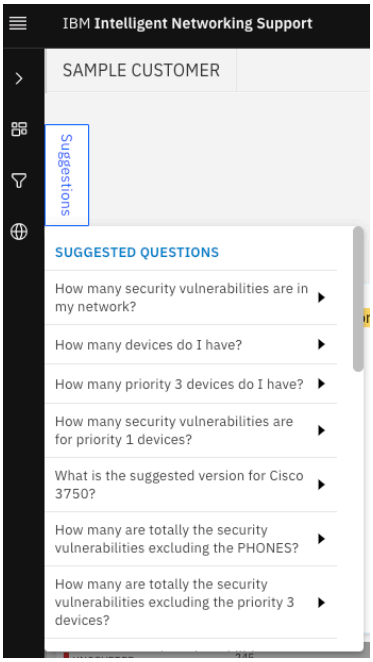
Preview: Coming soon INS chatbot

Click on INS assistant icon on the Left-Hand Navigator, ask a question like: **How many security vulnerabilities are for priority 1 devices?**

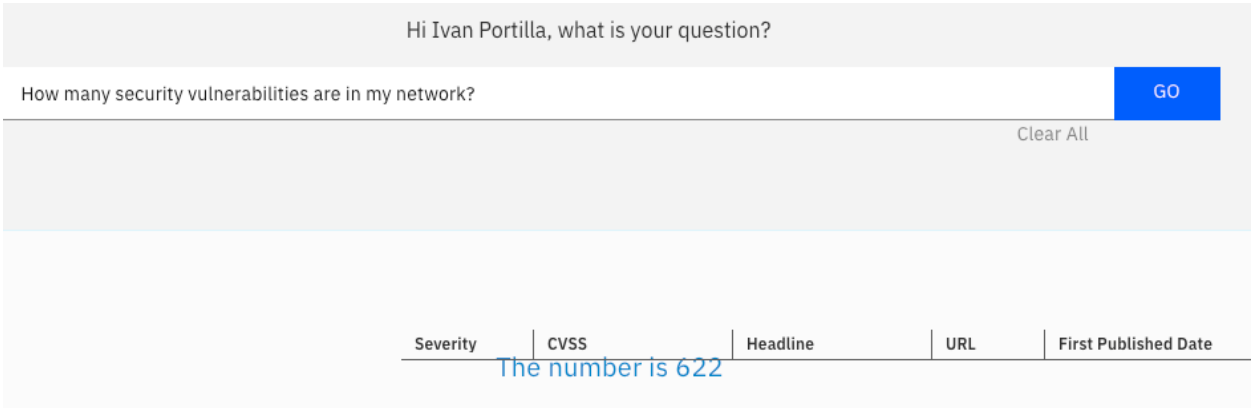


Review or download the query results by clicking on the Download button

Review other suggested questions by clicking on the Suggestions box on the LHN



For example, ask **How many security vulnerabilities are in my network?**


Hi Ivan Portilla, what is your question?
How many security vulnerabilities are in my network?
GO
Clear All
Severity
CVSS
Headline
URL
First Published Date
The number is 622

3. TSS INS OS distribution

In this section, we will review The OS level consistency across a given product family, where low level of consistency equals higher risk exposure.

Start a web browser session and navigate to the IBM Support Insights (CIP) by clicking on the following link:

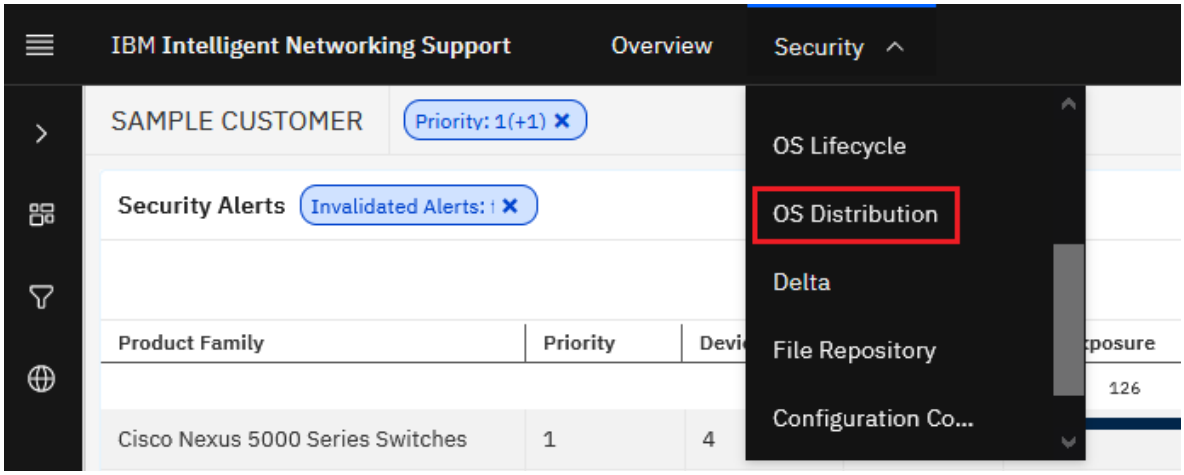
https://clientinsightsportal.ibm.com/cip/#/home/a94bc49f-e34a-4883-82a9-c2da46dd1e04

https://clientinsightsportal.entercoms.com/cip/#/home/96e0975c-183a-4631-9488-eafd9a4d5f92

As before, click on the Intelligent Networking Support (INS) card, and set the global filter to Priority 1 and 2.

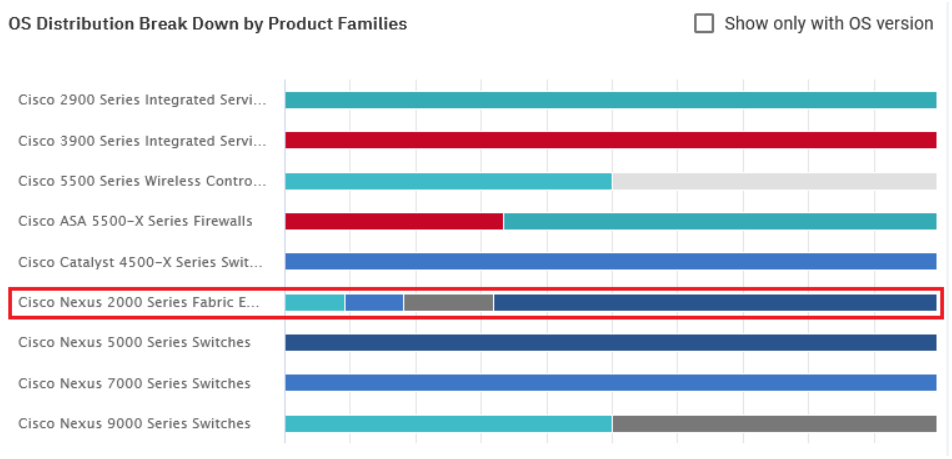
Instructions:

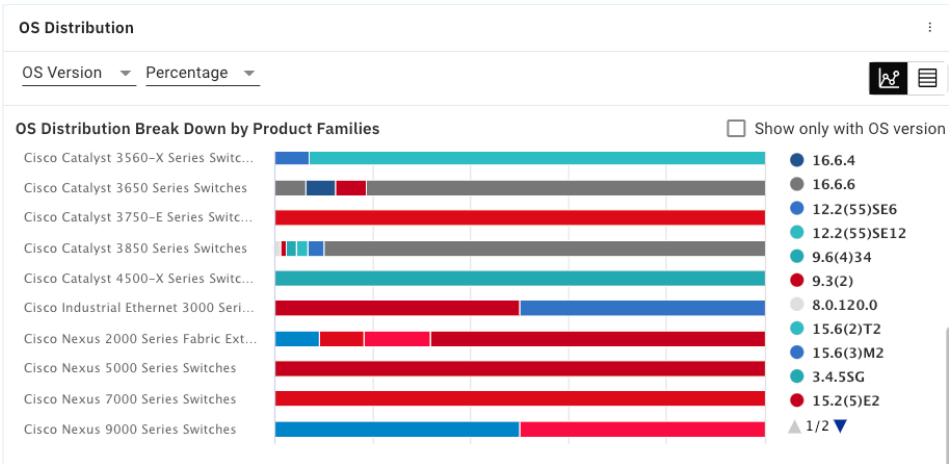
1. A positive side effect of upgrading to a single OS level across all devices within a product family is that this process also reduces the fragmentation of the OS distribution. Select **OS Distribution** from the drop-down menu at the top of the dashboard:



The level of OS fragmentation could quickly be identified by the number of colors in the bar corresponding to a product family, e.g., the Nexus 2K FEXes have 4 different OS levels. (Scroll down to see the full list). Multiple OS versions increase the complexity of managing

those devices, e.g., a bug scrub must be performed for each version separately. On the other hand, uniformity in the OS distribution equates to parity in features and functionalities:





4. Hardware Lifecycle

Start a web browser session and navigate to the IBM Support Insights (CIP) by clicking on the following link:

https://clientinsightsportal.ibm.com/cip/#/home/a94bc49f-e34a-4883-82a9-c2da46dd1e04

https://clientinsightsportal.entercoms.com/cip/#/home/96e0975c-183a-4631-9488-eafd9a4d5f92

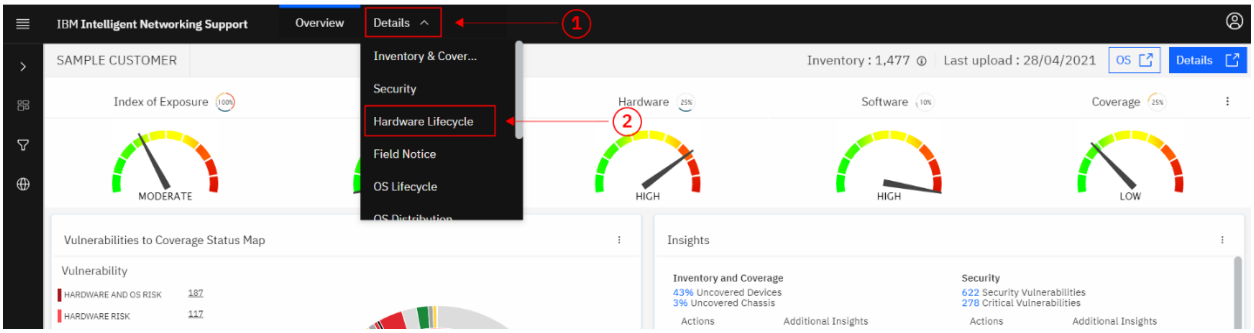
As before, click on the Intelligent Networking Support (INS) card.

In this section we will…

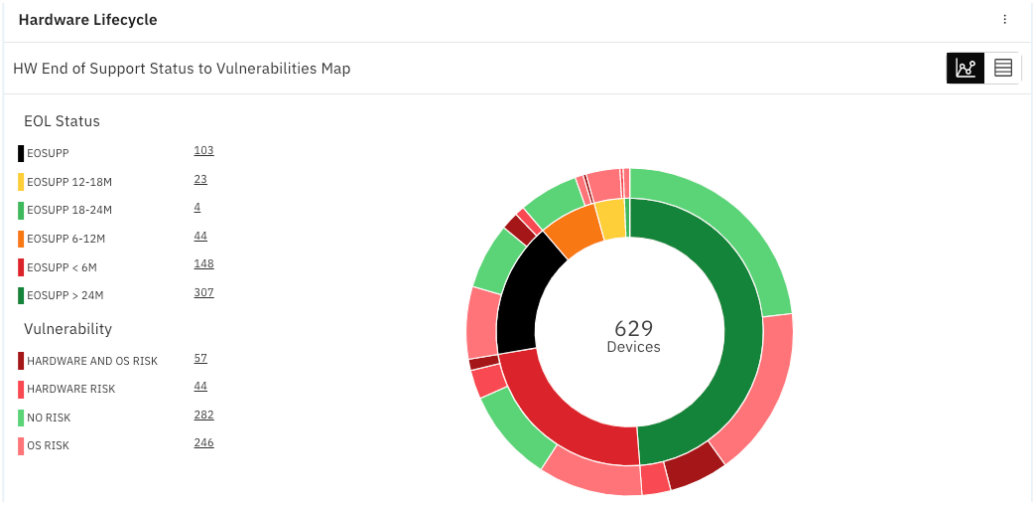
1. Review Hardware lifecycle information, including current products milestones, estimated time (in months) till End of Support, suggested replacement products, and list prices in the local currency (if available)
2. Plan Hardware refresh and forecast budget accordingly or plan extended support (post EoL)

Instructions:

1. To navigate to the **Hardware Lifecycle** section of the INS Portal, go to the **Details** drop-down menu at the top (1) and select **Hardware Lifecycle** (2):



The **Hardware Lifecycle** panel allows you to see all devices with published **End of Support** notice and their current hardware lifecycle milestone and hardware lifecycle status. Additionally, all hardware lifecycle milestone dates (e.g., **End of Sale** Date, **End of routine Failure Analysis** Date, etc.) are available as well as **suggested replacement product** and the **replacement product price**.



2. Review of **HW End of Support Status to Vulnerabilities Map** and understanding the **End of Support statuses and Vulnerabilities**

   The **HW End of Support Status to Vulnerabilities Map** allows you to see the correlation between End of Support Status and device vulnerabilities.

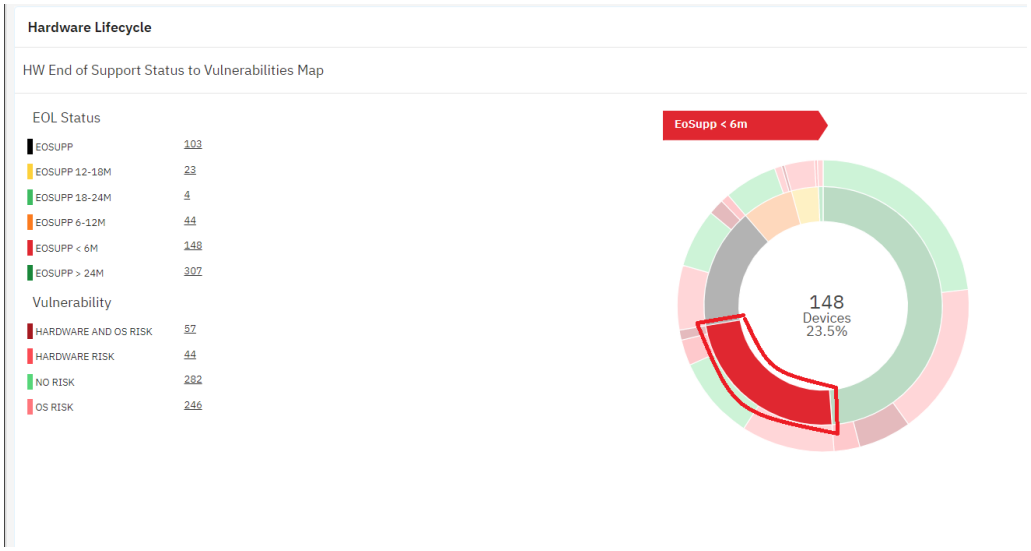
   Hardware Lifecycle statuses include:

   - **End of Support** – devices past the last day of support. These devices are no longer supported by the vendor
   - **End of Support in 6 months** - devices whose last day of support is within 6 months
   - **End of Support 6 - 12 months** - devices whose last day of support is between 6 and 12 months
   - **End of Support 12 - 18 months** - devices whose last day of support is between 12 and 18 months
   - **End of Support 18 - 24 months** - devices whose last day of support is between 18 and 24 months
   - **End of Support in more than 24 months** - Devices whose last day of support is in more than 24 months

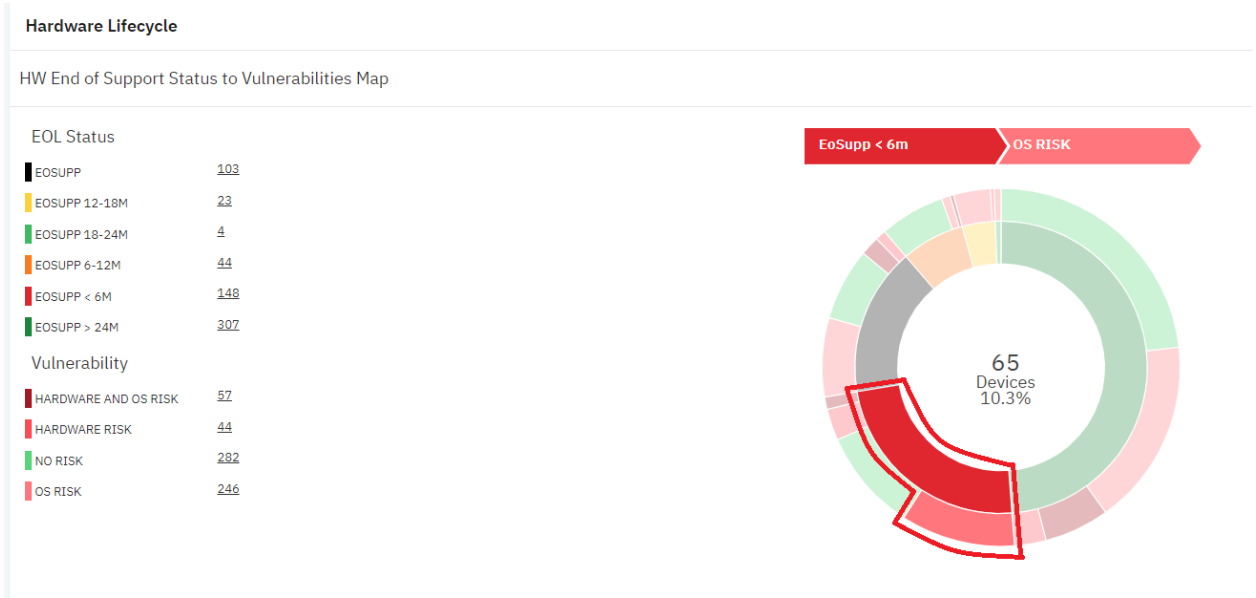
   Vulnerability statuses include:

   - **Hardware risk** – the device is either affected by a Field Notice alert(s) or has reached End of Support
   - **OS risk** – the device is either affected by a Security Vulnerability(s) or its OS has reached End of Support

The **sunburst chart** has 2 circles – inner and outer. To start, hover your mouse over a portion of the inner circle. Each portion represents a different hardware lifecycle status. The number in the center shows the number of devices with that status and % of the total:



To continue, hover your cursor over a portion of the outer circle. The outer circle correlates vulnerabilities to the selected hardware lifecycle status (from the inner circle):



In the example, there are 65 devices (10.3%) that are going to reach **End of Support in 6 months** and are associated with **OS risk**.

Clicking on the section, will show the respective devices details:

SAMPLE CUSTOMER -

Product Family	Host Name	IP Address	Item Type	Serial Number	FN Vulnerability Status	Hardware Lifecycle Status
Catalyst 2K/3K Series Modules	SampleHN40	SampleIP36	Card	SampleSN522	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN40	SampleIP36	Card	SampleSN1533	Not Vulnerable	EoSupp < 6m
Cisco Catalyst 3560-X Series Switch...	SampleHN40	SampleIP36	Chassis	SampleSN651	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Fans	SampleHN40	SampleIP36	Card	n/a	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Fans	SampleHN40	SampleIP36	Card	n/a	Not Vulnerable	EoSupp < 6m
Cisco Catalyst 3560-X Series Switch...	SampleHN230	SampleIP226	Chassis	SampleSN530	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN29	SampleIP25	Card	SampleSN1489	Not Vulnerable	EoSupp < 6m
Cisco Catalyst 3560-X Series Switch...	SampleHN29	SampleIP25	Chassis	SampleSN512	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Fans	SampleHN230	SampleIP226	Card	n/a	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Fans	SampleHN296	SampleIP296	Card	n/a	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Fans	SampleHN202	SampleIP198	Card	n/a	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN245	SampleIP241	Card	SampleSN1327	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN296	SampleIP296	Card	SampleSN1337	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN234	SampleIP230	Card	SampleSN1369	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN202	SampleIP198	Card	SampleSN1300	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Fans	SampleHN202	SampleIP198	Card	n/a	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN202	SampleIP198	Card	SampleSN1343	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Modules	SampleHN296	SampleIP296	Card	SampleSN528	Not Vulnerable	EoSupp < 6m
Catalyst 2K/3K Series Power Supplies	SampleHN296	SampleIP296	Card	SampleSN249	Not Vulnerable	EoSupp < 6m

First Prev Showing 1 - 65 of 65 Next Last Download

3. Review the **table view**

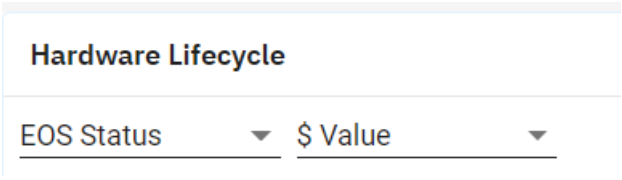
   To switch to the table view, use the button on the top right-hand side 

   You can choose how to group the devices. By:

   - **Hardware Lifecycle Status** – End of Support, End of Support in 6 months, End of Support 6 – 12 months, etc.
   - **Hardware Milestone** – End of Support, End of Service Contract Renewal, End of Software Maintenance, End of Sale, etc.
   - **End of Support year** – Devices going End of Support in 2025, 2024, 2023, etc.

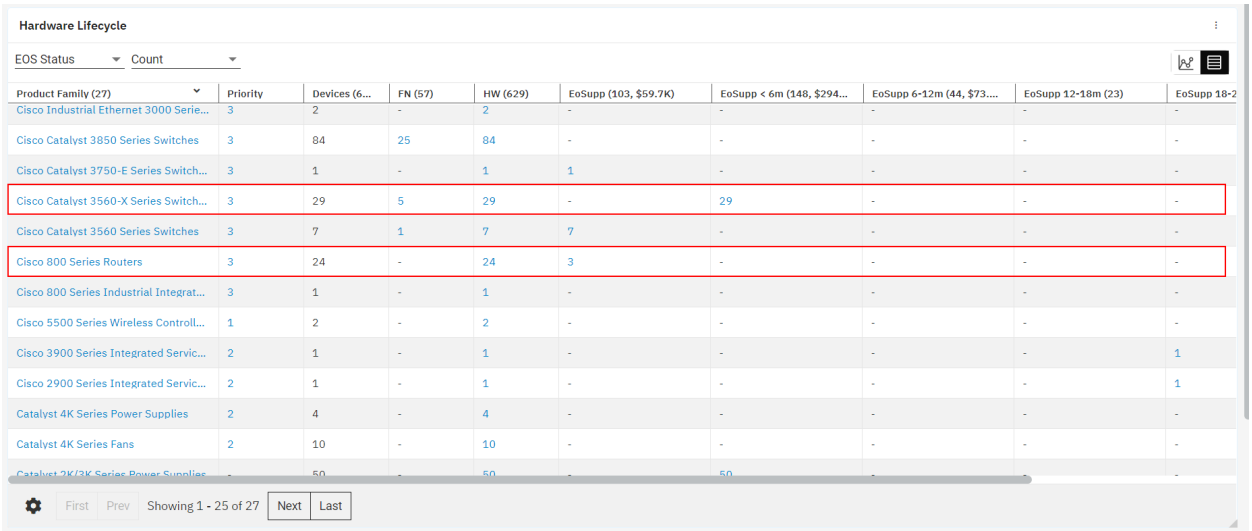
   You can also choose whether the data points show the device count or the estimated replacement value.

   Use the dropdown menus at the top left-had side to make your selection:



   The table shows a list of product families within which there are devices with End of Support notices, the product priority (**Priority**), the number of devices (**Devices**), and all available End of Support statuses.

   To illustrate how to read the table, we will look at 2 examples:



The **Cisco Catalyst 3560-X Series Switches** are **priority 3**. There are **29 devices** for which End of Support notice is published. All of them will become **End of Support in less than 6 months**.

The **Cisco 800 Series Routers** are **priority 3**. There are **24 devices** for which End of Support notice is published. **3** of them are already passed last date of support (i.e., **End of Support**) and the rest - **21** devices will reach **End of Support in more than 24 months**.

To view the details for any point of interest you can click on it.

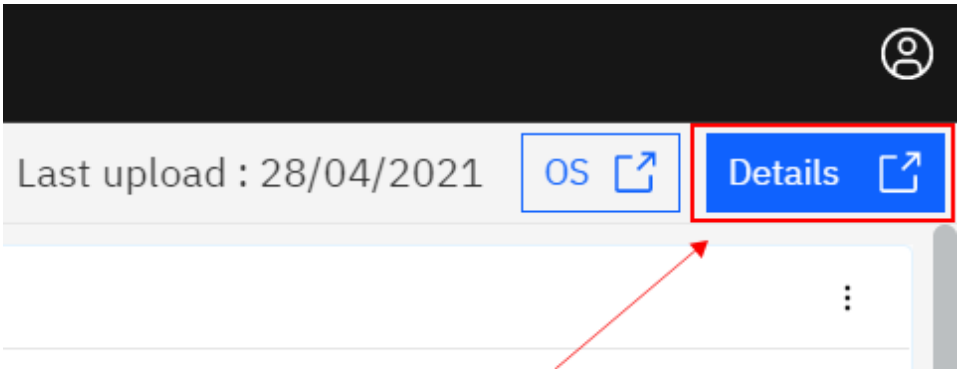
For example, to view the details for the 3 Cisco 800 Series Routers, which are already End of Support, click on the number 3 under column **EoSupp**.

To view the hardware lifecycle details for all Cisco 800 Series Routers, click on the product family name.

4. Review the **Details**

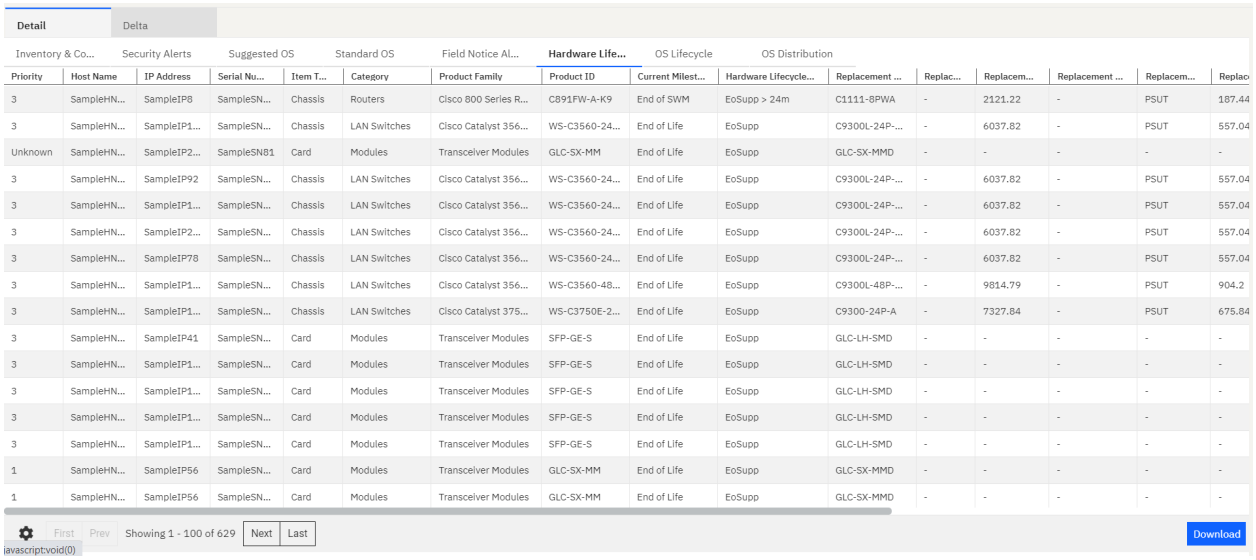
Click on a point of interest and you will see the hardware lifecycle details for the selected devices (e.g., particular product family, section from the sunburst chart, etc.)

To view the hardware lifecycle details for the entire inventory, click on the **Details** button at the top right-hand side of the dashboard:



In the details only devices with End of Support notices are shown, i.e. if there are devices for which the vendor is yet to publish End of Support notice, they will not be shown here.

The details contain device information such as device hostname, IP address, serial number, product ID, product priority, etc.

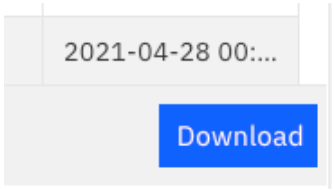


Additionally, you can find all hardware lifecycle milestone dates (e.g., **End of Sale** date, **End of Software Maintenance** date, **End of Support** date, etc.), the **current milestone**, the **hardware lifecycle status**, the **suggested replacement product**, **replacement product price**, **replacement product service price**, etc.

The prices are based on the vendor's current local list price. The prices are estimated and can be used to forecast your budget for hardware refresh. The currency is either the local currency or USD (depending on the region). For example, for Canadian customers the prices are in CAD.

Optional columns can be added to or removed from the details from the **cogwheel menu**.

The details can be exported to an Excel spreadsheet using the **Download** button.



5. OS Lifecycle

Start a web browser session and navigate to the IBM Support Insights (CIP) by clicking on the following link:

https://clientinsightsportal.ibm.com/cip/#/home/a94bc49f-e34a-4883-82a9-c2da46dd1e04

https://clientinsightsportal.entercoms.com/cip/#/home/96e0975c-183a-4631-9488-eafd9a4d5f92

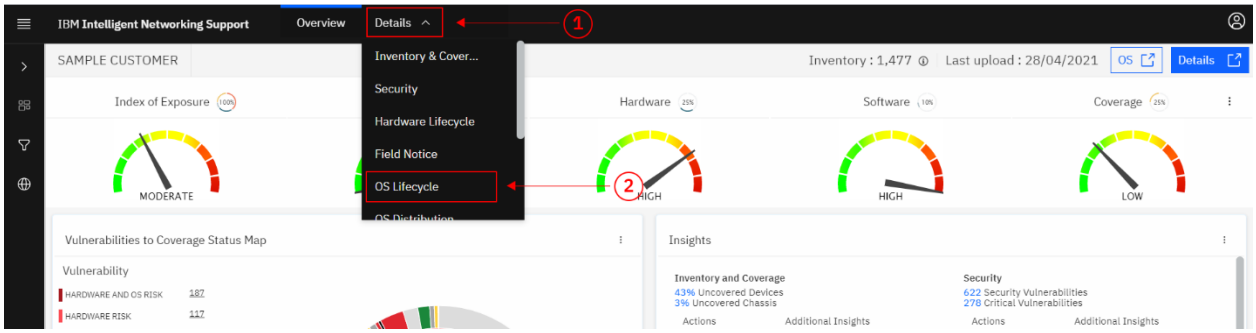
As before, click on the Intelligent Networking Support (INS) card.

In this section we will…

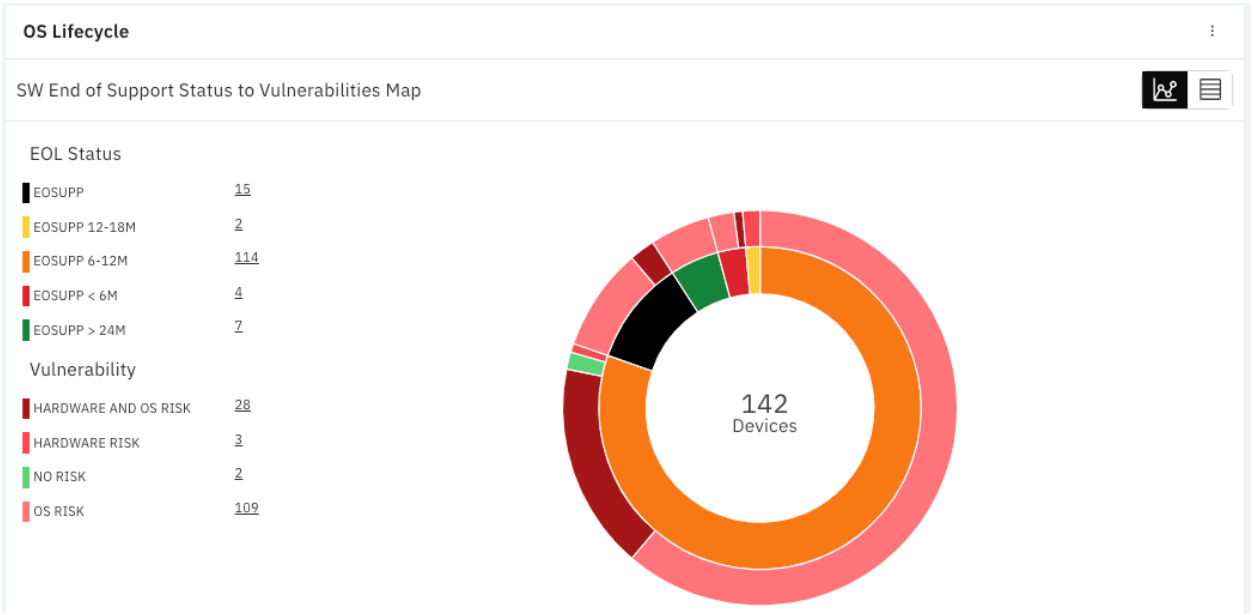
1. Review OS lifecycle information including current milestone, estimated time (in months) till End of Support
2. Plan OS upgrade based on provided suggested version

Instructions:

1. To navigate to the OS Lifecycle section of the INS Portal, go to the **Details** drop-down menu at the top (1) and select **OS Lifecycle** (2):



The **OS Lifecycle** panel allows you to see all devices with OS for which there is published End of Support notice and their **current OS lifecycle milestone** and **OS lifecycle status**. Additionally, all OS lifecycle milestone dates (e.g., **End of Sale** Date, **End of Engineering** Date, etc.) are available as well as up to 3 vendor suggested versions.



2. Review of **OS End of Support Status to Vulnerabilities Map** and understanding the **End of Support statuses** and **Vulnerabilities**

   The **OS End of Support Status to Vulnerabilities Map** allows you to see the correlation between OS End of Support Status and device vulnerabilities.

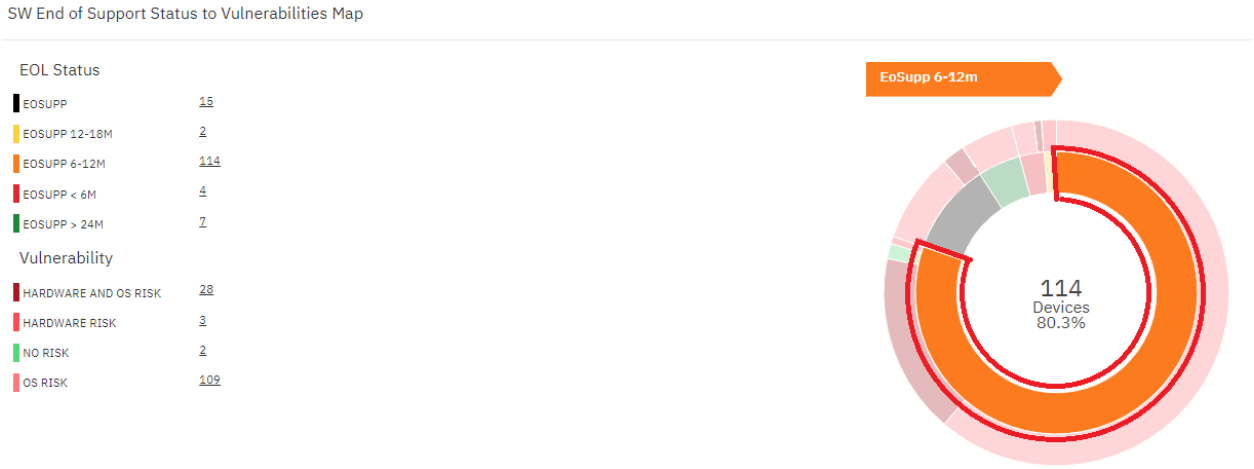
   OS Lifecycle statuses include:

   - **End of Support** – devices whose OS is past the last day of support. These OS versions are no longer supported by the vendor
   - **End of Support in 6 months** - devices whose OS last day of support is within 6 months
   - **End of Support 6 - 12 months** - devices whose OS last day of support is between 6 and 12 months
   - **End of Support 12 - 18 months** - devices whose OS last day of support is between 12 and 18 months
   - **End of Support 18 - 24 months** - devices whose OS last day of support is between 18 and 24 months
   - **End of Support in more than 24 months** - devices whose OS last day of support is in more than 24 months

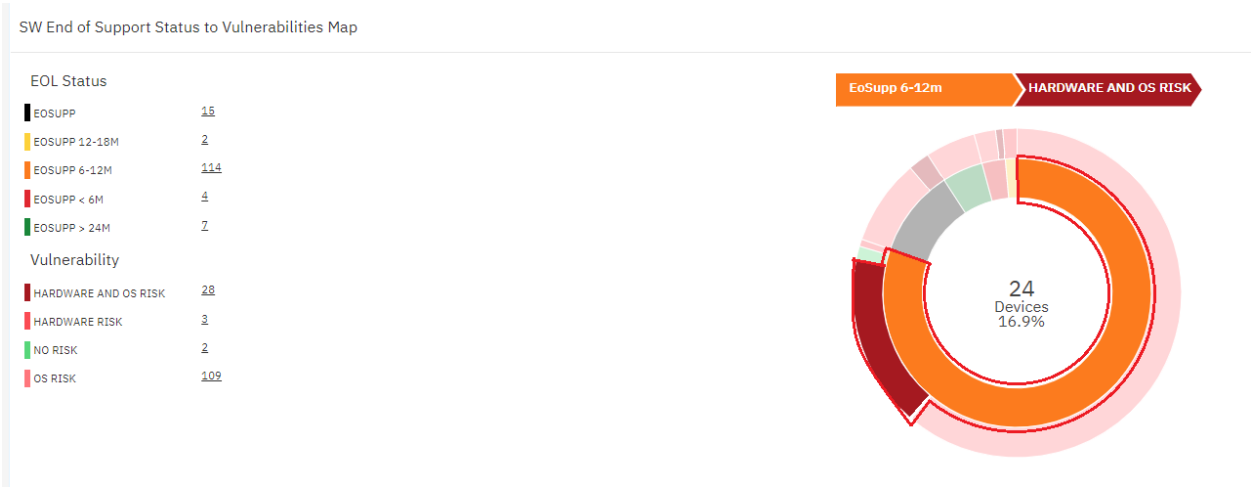
   Vulnerability statuses include:

   - **Hardware risk** – the device is either affected by Field Notice alert(s) or is End of Support
   - **OS risk** – the device is either affected by Security Vulnerability(s) or its OS is End of Support

The sunburst chart has 2 circles – inner and outer. To start, hover your mouse over a portion of the inner circle. Each segment represents a different OS lifecycle status. The number in the center shows the number of devices with that status and % of the total:

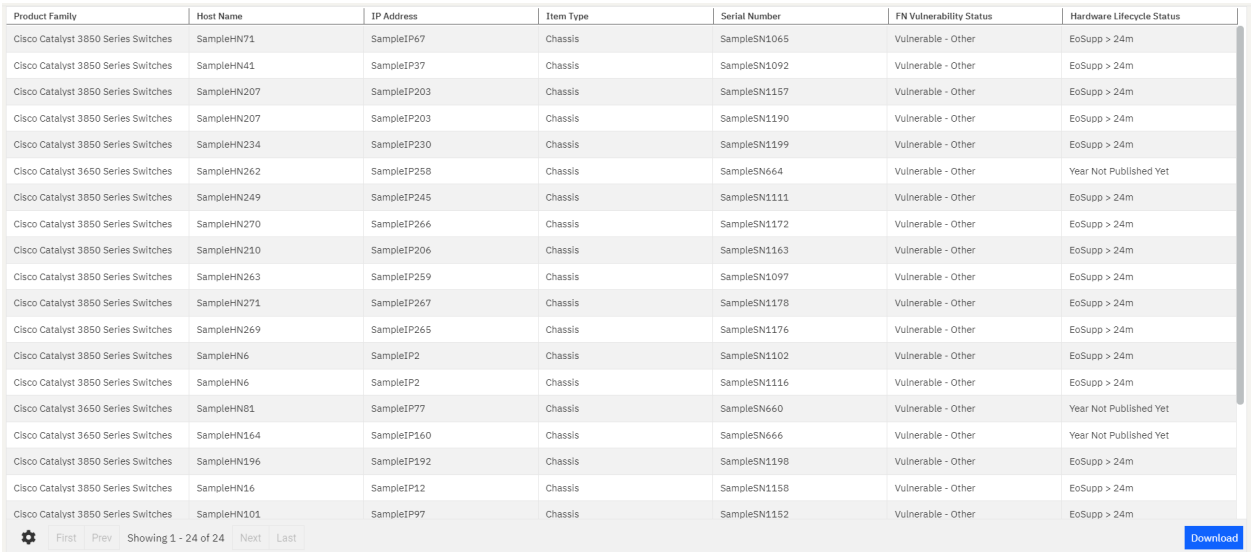


To continue, hover your cursor over a segment of the outer circle. The outer circle correlates vulnerabilities to the selected OS lifecycle status (from the inner circle):



In the example, there are 24 devices (16.9%) whose OS is going to be **End of Support within 6 to 12 months** and have **Hardware and OS risk**.

Clicking on a section of the **sunburst chart**, will yield the respective devices details:



Product Family	Host Name	IP Address	Item Type	Serial Number	FN Vulnerability Status	Hardware Lifecycle Status
Cisco Catalyst 3850 Series Switches	SampleHN71	SampleIP67	Chassis	SampleSN1065	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN41	SampleIP37	Chassis	SampleSN1092	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN207	SampleIP203	Chassis	SampleSN1157	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN207	SampleIP203	Chassis	SampleSN1190	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN234	SampleIP230	Chassis	SampleSN1199	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3650 Series Switches	SampleHN262	SampleIP258	Chassis	SampleSN664	Vulnerable - Other	Year Not Published Yet
Cisco Catalyst 3850 Series Switches	SampleHN249	SampleIP245	Chassis	SampleSN1111	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN270	SampleIP266	Chassis	SampleSN1172	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN210	SampleIP206	Chassis	SampleSN1163	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN263	SampleIP259	Chassis	SampleSN1097	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN271	SampleIP267	Chassis	SampleSN1178	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN269	SampleIP265	Chassis	SampleSN1176	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN6	SampleIP2	Chassis	SampleSN1102	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN6	SampleIP2	Chassis	SampleSN1116	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3650 Series Switches	SampleHN81	SampleIP77	Chassis	SampleSN660	Vulnerable - Other	Year Not Published Yet
Cisco Catalyst 3650 Series Switches	SampleHN164	SampleIP160	Chassis	SampleSN666	Vulnerable - Other	Year Not Published Yet
Cisco Catalyst 3850 Series Switches	SampleHN196	SampleIP192	Chassis	SampleSN1198	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN16	SampleIP12	Chassis	SampleSN1158	Vulnerable - Other	EoSupp > 24m
Cisco Catalyst 3850 Series Switches	SampleHN101	SampleIP97	Chassis	SampleSN1152	Vulnerable - Other	EoSupp > 24m

First Prev Showing 1 - 24 of 24 Next Last Download

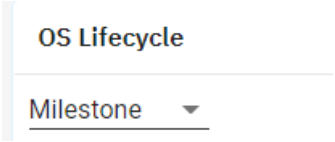
3. Review the **table view**

To switch to the table view, use the button on the top right-hand side  .

You can choose how to group the devices. By:

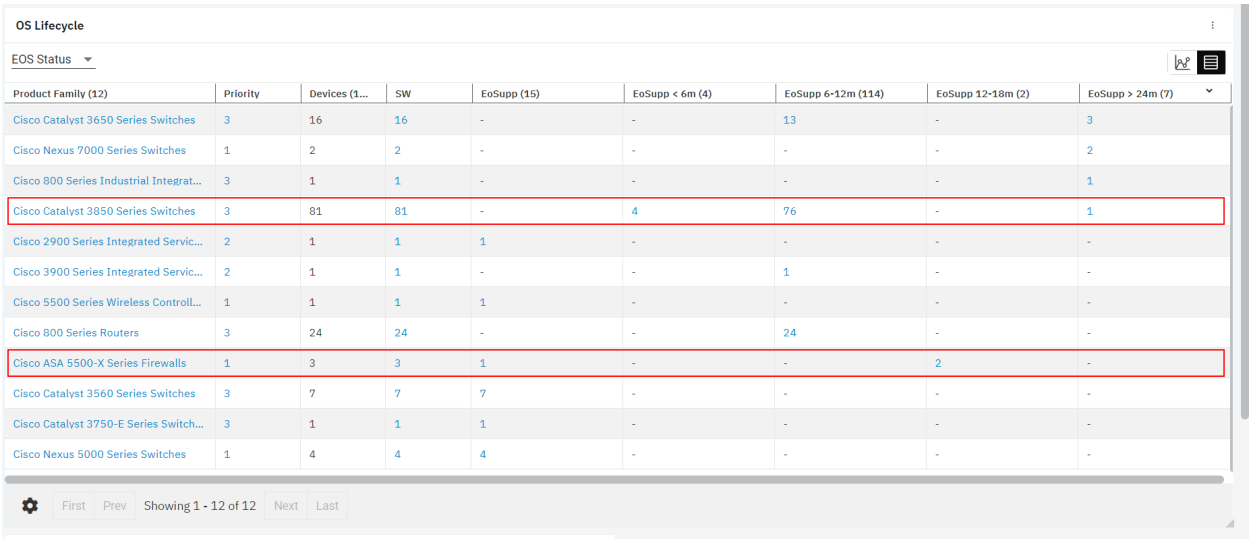
- **OS Lifecycle Status** – End of Support, End of Support in 6 months, End of Support 6 – 12 months, etc.
- **OS Milestone** – End of Support, End of Engineering, End of Vulnerability Support, End of Sale, etc.
- **End of Support year** – devices whose OS is going End of Support in 2025, 2024, 2023, etc.

Use the drop-down menu from the top left-had side to make your selection:



The table shows a list with product families within which there are devices with OS End of Support notices, the product priority (**Priority**), the number of devices (**Devices**), and all available End of Support statuses.

To illustrate how to read the table, we will look at 2 examples:



The **Cisco Catalyst 3850 Series Switches** are **priority 3**. There are **81 devices** with OS for which End of Support notice is published. **4** of them will reach **End of Support within 6 months**, **76** will reach **End of Support in 6 to 12 months** and the other **1** will reach **End of Support in more than 24 months**.

The **Cisco ASA 5500-X Series Firewalls** are **priority 1**. There are **3 devices** with OS for which End of Support notice is published. **1** is already **End of Support** and **2** will become **End of Support in 12 to 18 months**.

To view the details for any point of interest you can click on it.

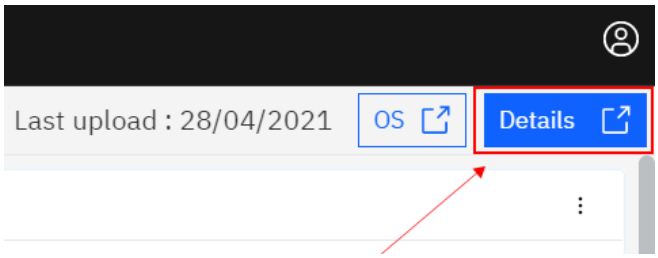
For example, to view the details for the 1 Cisco ASA 5500-X Series Firewall whose OS is already End of Support, click on the number 1 under column **EoSupp**.

To view the OS lifecycle details for all Cisco ASA 5500-X Series Firewalls, click on the product family name.

4. Review the **Details**

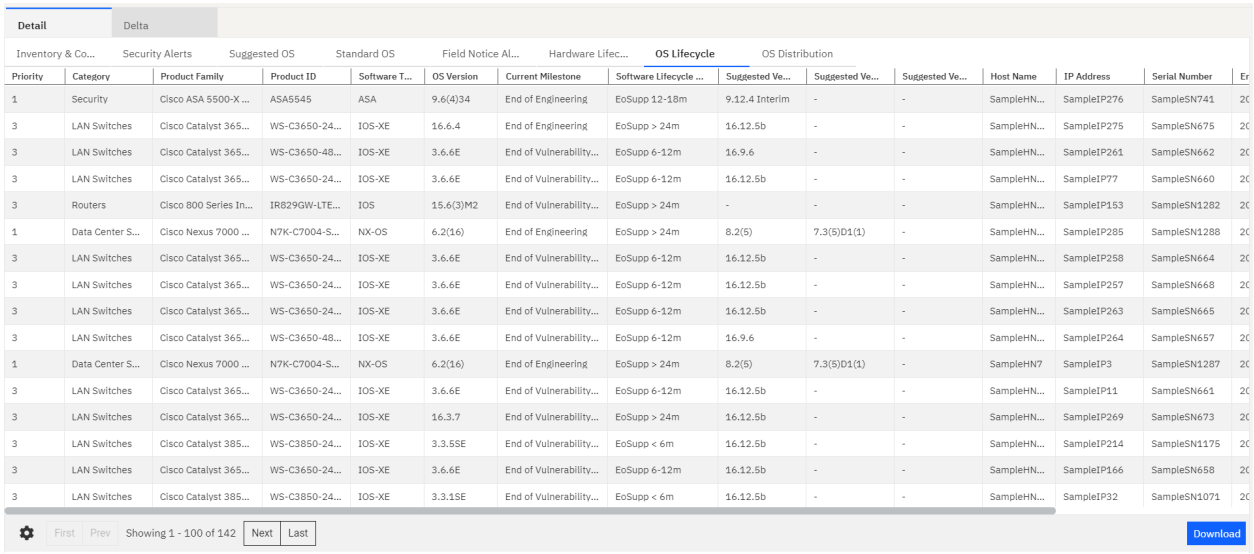
Click on a point of interest and you will see the **OS lifecycle details** for the selected devices (e.g., particular product family, section from the sunburst chart, etc.)

To view the OS lifecycle details for the entire inventory, click on the **Details** button at the top right-hand side:



In the **Details** only devices with OS End of Support notices are shown, i.e. if there are devices running OS for which the vendor is yet to publish End of Support notice, they will not be shown here.

The **Details** contain device information such as device hostname, IP address, serial number, product ID, product priority, OS type, OS version, etc.



Additionally, you can find all OS lifecycle milestone dates (e.g. **End of Sale** date, **End of Engineering** date, **End of Support** date, etc.), the **current OS milestone**, the **OS lifecycle status** and up to **3 suggested OS versions**.

The suggested versions are provided by the vendor and are based primarily on stability, longevity, and adoption rate.

Optional columns can be added to or removed from the details from the **cogwheel menu**.

The details can be exported to an Excel spreadsheet using the **Download** button.

6. Delta

Start a web browser session and navigate to the IBM Support Insights (CIP) by clicking on the following link:

https://clientinsightsportal.ibm.com/cip/#/home/a94bc49f-e34a-4883-82a9-c2da46dd1e04

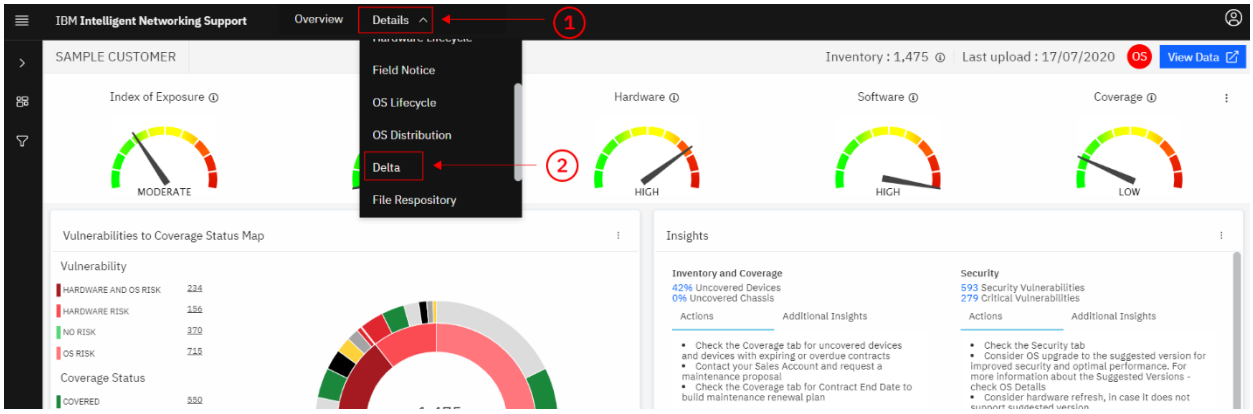
https://clientinsightsportal.entercoms.com/cip/#/home/96e0975c-183a-4631-9488-eafd9a4d5f92

In this section we will:

1. Check for **Added** / **Removed** devices (for example: after product refresh/replacement, new/closed office location, etc.)
2. Check for support coverage changes between two data collections (for example, after adding new assets to the network)
3. Check for security vulnerabilities introduced to / removed from the network after OS upgrades

Instructions:

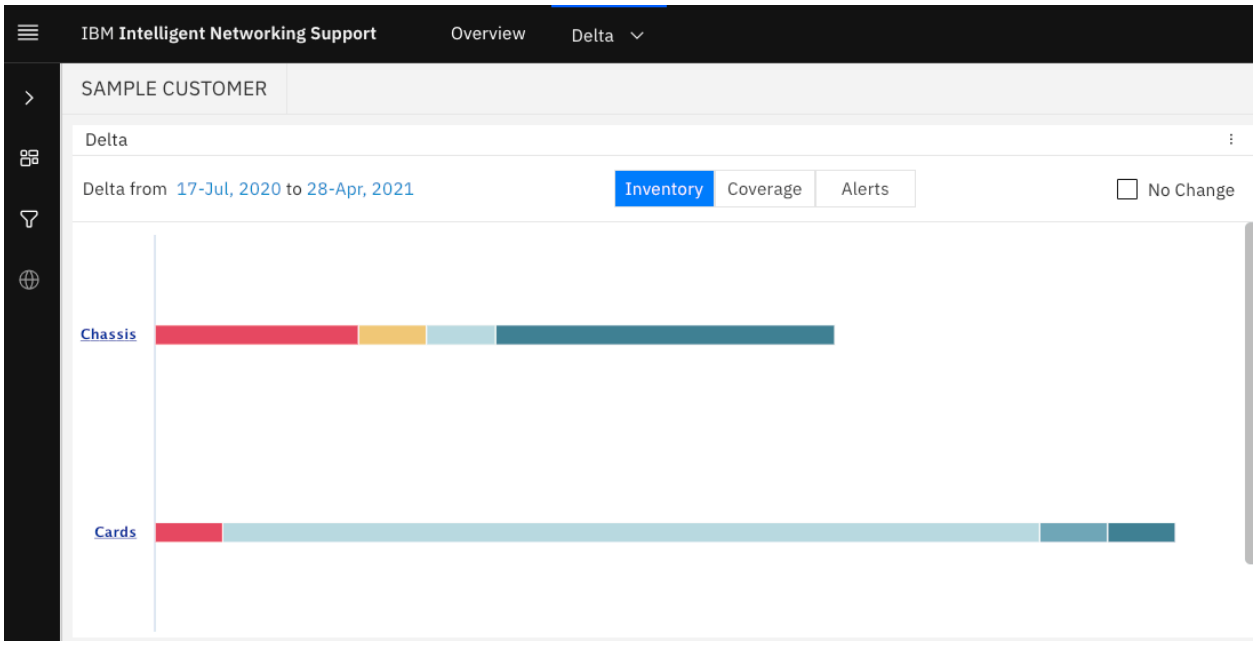
1. To navigate to the **Delta** section of the INS Portal, go to the **Details** drop-down menu at the top (1) and select **Delta** (2).



2. Review of **Inventory Delta** and understanding the different **inventory delta statuses**

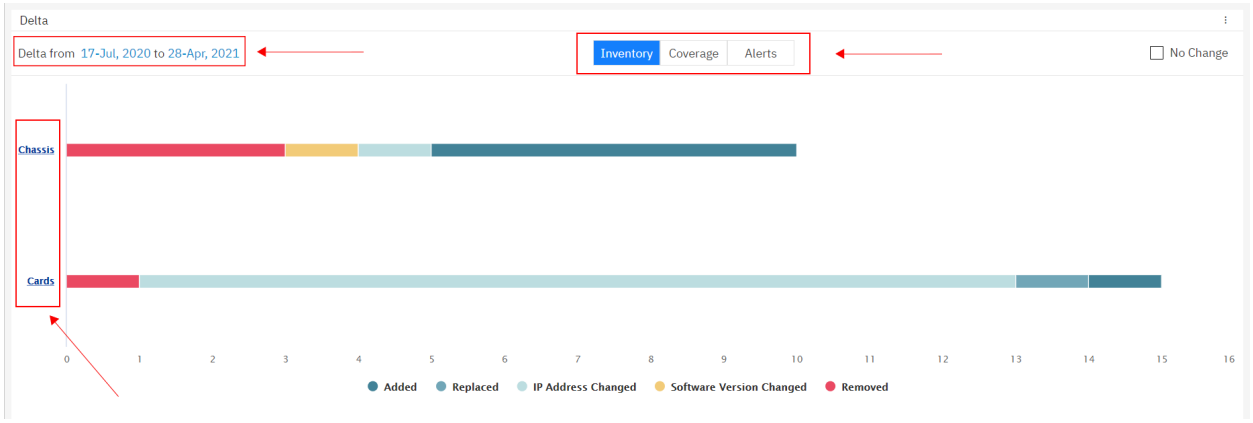
   The **Delta** allows you to see inventory, support coverage and alert changes which have occurred between two data collections (by default – the last and second to last data

collections). The exact time period is shown at the top (Delta from **date** to **date**). The information is presented in a chart format with drill-down functionalities. By using the 3 buttons at the top, you can switch between the different charts (i.e., **Inventory** delta chart, Support **Coverage** delta chart and **Alerts** delta chart).

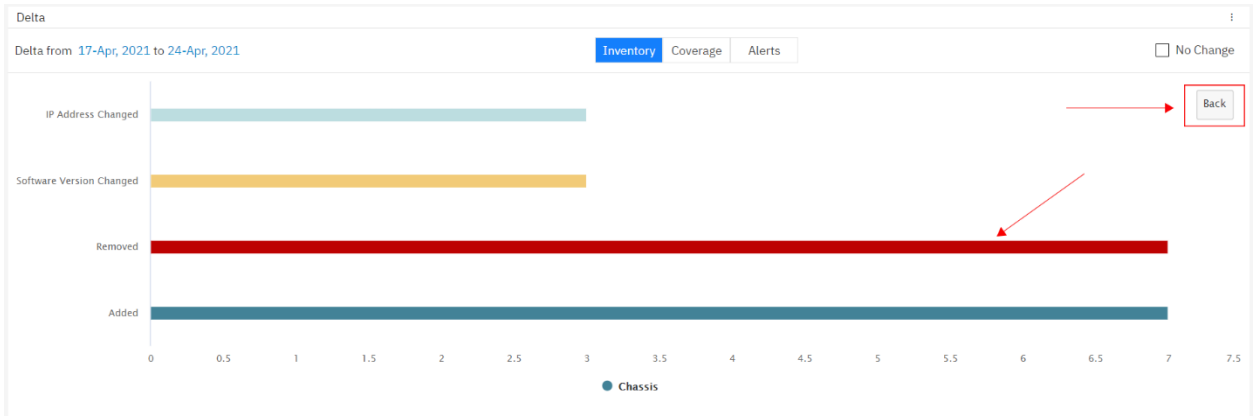


Inventory changes, captured by INS, include:

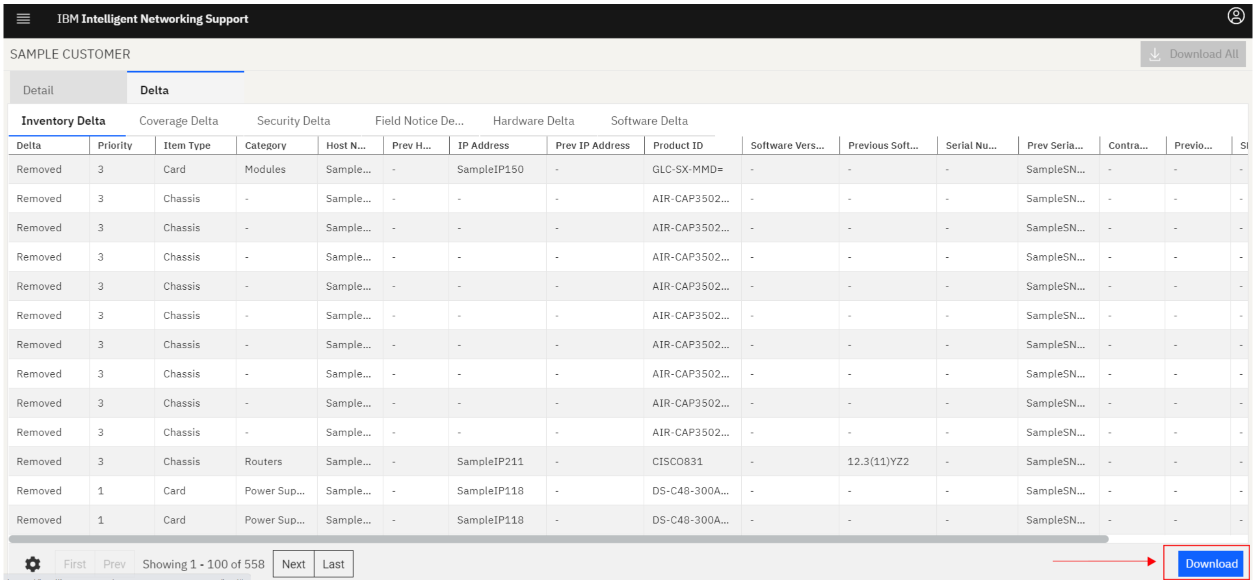
- Additions to inventory (**Added**) – these are new devices added to the network which were not present in the previous data collection
- Replacements (**Replaced**) - a device is considered Replaced when it has the same Product ID, IP address and hostname, but appears with two different serial numbers in the two data collections
- IP address changes (**IP address changed**) – in the latest data collection the IP address of the device is different from the one captured in the previous data collection
- OS version changes (**SW version changed**) - the software version of the device has changed in the latest data collection
- IP address + OS version changes on the same asset (**IP address and software version changed**) – both the IP address and the software version of the device have been changed
- Removal of assets from the environment (**Removed**) - the device has been removed from the collected inventory (i.e., the serial number was not found in the latest data collection). The item might have been removed from the network or not accessible during the inventory collection.



The axis labels on the left (Chassis, Cards) are active links, allowing you to drill down into more details. For example, if you'd like to focus only on a specific item type, click on the respective label, e.g. **Chassis**. This will zoom in on chassis only. You can use the **Back** button on the right-hand side to return to the previous chart:



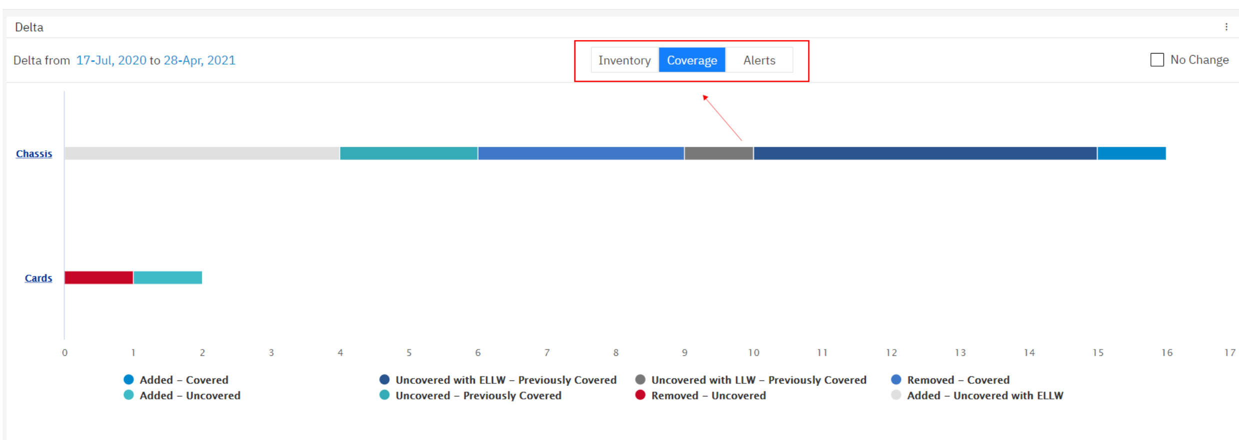
To identify all recently removed assets and validate their status (i.e., check whether they were permanently removed or just were not accessible during the data collection), click on the **Removed** bar. This will open up a view (in a new browser tab) which contains various device details, such as serial number, IP address, host name, product ID, category, location information, etc. You can use the **Download** button to export this information to an Excel spreadsheet.



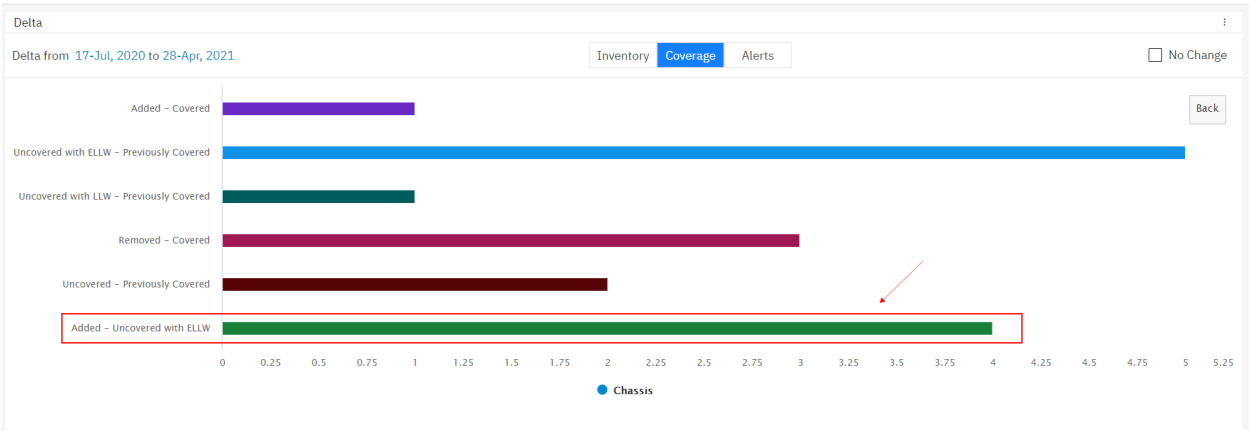
Delta	Priority	Item Type	Category	Host N...	Prev H...	IP Address	Prev IP Address	Product ID	Software Vers...	Previous Soft...	Serial Nu...	Prev Seria...	Contra...	Previo...	Sl
Removed	3	Card	Modules	Sample...	-	SampleIP150	-	GLC-SX-MMD=	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	-	Sample...	-	-	-	AIR-CAP3502...	-	-	-	SampleSN...	-	-	-
Removed	3	Chassis	Routers	Sample...	-	SampleIP211	-	CISCO831	-	12.3(11)YZ2	-	SampleSN...	-	-	-
Removed	1	Card	Power Sup...	Sample...	-	SampleIP118	-	DS-C48-300A...	-	-	-	SampleSN...	-	-	-
Removed	1	Card	Power Sup...	Sample...	-	SampleIP118	-	DS-C48-300A...	-	-	-	SampleSN...	-	-	-

3. Review of **Coverage Delta** and understanding the different **coverage delta statuses.**

   Use the **Coverage** button above the chart to switch to **Coverage delta**.



The **coverage delta** captures not only how the support coverage status of the devices on the network has changed over time, but also shows the coverage status of all newly added, recently removed and replaced assets. For example, to see which of the added chassis do not have maintenance contract, zoom in on **Chassis** (by clicking on the **Chassis** axis label) and then click on the **Added – Uncovered ELLW** bar:



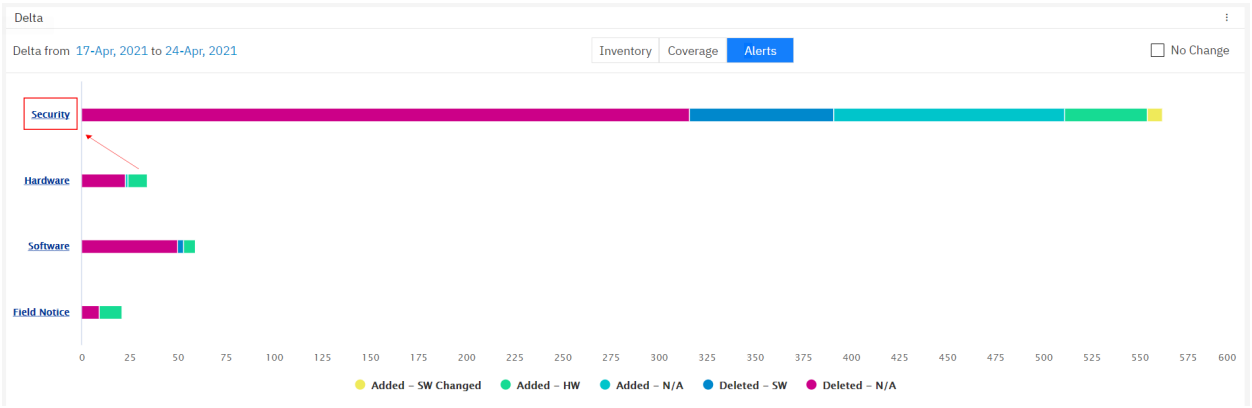
Again, you can save the details to Excel by using the **Download** button.

4. Review of **Alerts Delta** and understanding the different **alerts delta statuses**

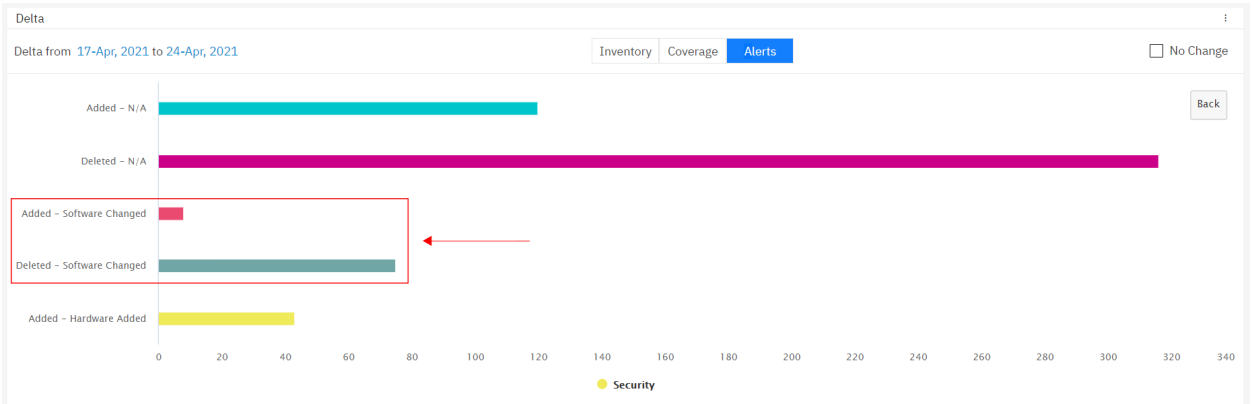
   The alerts delta shows changes in terms of Security, Field Notice, Hardware and Software alerts.

   The changes encompass (all the items below refer to the delta count of assets with alerts):

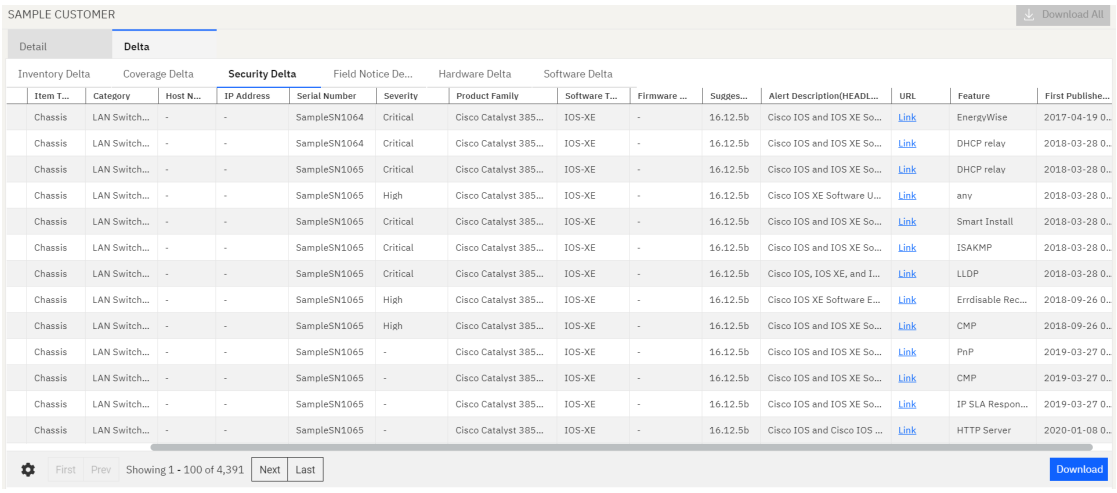
   - **Added net-new** - alerts which were not present in the older data collection but are present in the latest one. These are newly introduced alerts/publications by Cisco.
   - **Added – SW changed** - alerts which were not present in the older data collection but are present in the latest one, as the device's software has changed
   - **Added – HW added** - alerts which were not present in the older data collection but are present in the latest one, as a new device has been installed on the network
   - **Added – N/A** - alerts which were not present in the older data collection but are present in the latest one for unknown reason
   - **Deleted – HW removed** - alerts which were present in the older data collection, but are not present in the latest one, as the device has been removed from the network
   - **Deleted – SW changed** - alerts which were present in the older data collection, but are not present in the latest one, as the device's software has changed
   - **Deleted – N/A** - alerts which were present in the older data collection but are not present in the latest one for unknown reason



Consider the following scenario – you performed OS upgrades and now you'd like to see how this has reflected on the number of reported security vulnerabilities. By looking at the security alerts delta chart, you can quickly and easily determine how many security alerts were removed (i.e., are no longer applicable to your devices) and how many were introduced with the SW upgrades. To deep dive into more details click on **Security**, and then click on the **Deleted – SW changed** and **Added – SW changed** bars.



You will be redirected to the respective details which include alert description (headline), publication URL, severity, CVSS score, affected feature, etc.



7. Conclusion

In this lab, we illustrated how to use some of the enhanced INS capabilities to quantify risk assessment of your IT state. We showed you how to filter and discover security vulnerabilities and check the OS version consistency capabilities based on the OS conformance information.

Security vulnerabilities, down-level systems, devices and software lapses in support contracts and varying product lifecycles across vendors can lead to service disruptions. With IBM Support Insights, you can consolidate data from multiple vendor contracts into a security-rich, cloud-based portal to better manage, maintain and optimize the health of your IT environment. Turn to IBM Technology Support Services to find out how you can gain this level of visibility and control into all your support contracts so you can increase the availability of your infrastructure and keep your business up and running.

For more information

To learn more about IBM Support Insights please contact your IBM representative or IBM Business Partner or

Visit http://www.ibm.com/products/support-insights