



# Asset Management for Cybersecurity: 10 Essential Questions to Answer



## OVERVIEW

---

In building our cybersecurity asset management platform, we've had conversations with hundreds of security professionals about the challenges they face around seeing and securing all assets. In this post, we'll cover the ten most common questions we've heard, why they are difficult to answer, and how to overcome the obstacles.



## Table of Contents

Asset Management for Cybersecurity: 10 Essential Questions to Answer.....	1
Overview .....	1
Device-Related Questions.....	3
Question 1: Is The Device “Known” and Managed? .....	3
Question 2: Where is the Device? .....	4
Question 3: What is the Device?.....	5
Question 4: Is the Core Software Up-to-Date? .....	5
Question 5: What Additional Software is Installed?.....	6
Question 6: Which of the Devices in My Environment Were Manufactured in a Specific Country?.....	7
User-Related Questions.....	8
Question 7: Which AD-Enabled Users Have Improper Access Configurations?.....	8
Question 8: Do I Have Users with Devices Not Seen in the Past 30 Days?.....	8
Question 9: Do I Have Users that Have Turned Off Their Endpoint Protection Agent?.....	9
Catch-All Policy-Related Question .....	10
Question 10: Do My Devices and Users Adhere to My Security Policy? .....	10
About Axonius .....	11
Support and Questions .....	11
Thank You .....	11



# Device-Related Questions

Whenever we talk to a security professional, we ask the same question: how many devices do you have, and are they secure? We normally hear two answers:

1. I don't know. That's a really hard question to answer.
2. It's a range between 10 and 40,000.

And while we live in a time of incredible innovation from AI to Machine Learning, Deception and Automation, it's still difficult to answer the basics. Let's take a look at some of the foundational questions at the core of any asset management initiative:

## QUESTION 1: IS THE DEVICE "KNOWN" AND MANAGED?

---

In any environment, devices can be split into two distinct categories:

1. **Known/Managed** - Those devices that are known to security and management systems. For example, these are devices:
  - a. That have an EPP/EDR agent installed
  - b. Are being scanned by a VA scanner
  - c. Are part of Active Directory
  - d. Have a device-specific management solution (MDM for mobile, Chef or Puppet, etc.)
2. **Unknown/Unmanaged** - These are devices that are known to the network (Switches and Routers), but do not have any of the agents above installed.

By looking at the devices that are known and managed and those that are only known to the network, we can produce a list of devices that potentially should be managed. In fact, in nearly every case we find devices that were thought to have the right agents installed but did not. Consequently, we also find devices (like smart TVs or Wi-Fi power outlets) that the security teams didn't know existed.



The screenshot displays the Axonius web interface for device management. At the top, there's a search bar with a query: "specific\_data.adapter\_properties != 'Manager' and specific\_data.adapter\_properties != 'Agent'". Below the search bar, a table lists 402 devices. The table has columns for Adapters, Asset Name, Host Name, Network Interfaces: Mac, Network Interfaces: Manufacturer, and Network Interfaces: IPs. The devices listed include various operating systems like Windows, Linux (Ubuntu), and VMware, with different hostnames and network configurations. At the bottom of the table, there's a pagination bar showing "RESULTS PER PAGE: 20 50 100" and a page navigation bar with numbers 1 through 7.

Adapters	Asset Name	Host Name	Network Interfaces: Mac	Network Interfaces: Manufacturer	Network Interfaces: IPs
+6		CiscoEmuRouter	C0:00:07:A5:00:01, C0:00:07:A5:00:00		10.0.0.2 192.168.20.35
+3	Hyper-V_2012_test%20(itay)	WIN-7R88AA776NP	00:50:56:91:7A:6E	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.8
+3	domaincontrol%20and%20dns%20(Avidor)	dcl.axonius.local	00:0C:29:F1:0D:5B	VMware, Inc. (3401 Hillview Avenue Palo Alto CA US 94304 )	192.168.20.4
+3		dhcpc-slow	11:33:33:77:DE:AD		10.0.0.1
+3	test_windows_10_server_2%20(Avidor)	DESKTOP-GOBPIUL	00:50:56:91:CD:30	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.20 fe80::d175:487
+2	RedStone_8.5.2-1995%20(Schwartz)	rsva	00:50:56:91:AC:93	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.42 fe80::250:56ff
+2	storageserver%20(Avidor)	STORAGE	00:0C:29:85:94:F8	VMware, Inc. (3401 Hillview Avenue Palo Alto CA US 94304 )	192.168.20.3
+2	Rapid7VA%20(itay)	nexpose	00:50:56:91:00:66	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.10 fe80::250:56ff
+1	Windows%20Server%202016%20raindcl.RainDomain.test%20(Avidor)	raindcl	00:0C:29:61:DD:22	VMware, Inc. (3401 Hillview Avenue Palo Alto CA US 94304 )	192.168.20.38
+1	Hyper_V_2016_test%20(itay)	WIN-8K0BDJEN2L3	00:50:56:91:58:A0	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.24
+1	Hyper_V_2008R2_test%20(itay)	WIN-OQ5V7ACKHIE	00:50:56:91:E7:EE	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.29
+1	Qualys%20Virtual%20Appliance%20Scanner%20(Off)	localhost.localdomain	00:0C:29:48:5E:64, 00:0C:29:48:5E:6E	VMware, Inc. (3401 Hillview Avenue Palo Alto CA US 94304 )	192.168.20.22
+1	Cisco%20Prime%20(Schwartz)	prime	00:50:56:23:C1:9A	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.34 fe80::250:56ff
+1	cisco%20emulator%20(Schwartz)	cisco-emulator	00:50:56:91:4F:24	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.21 fe80::250:56ff
	Mishka-test_donor_remove	ubuntu	00:50:56:91:81:50, 02:42:E6:54:7B:96 +1	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.43 fe80::250:56ff
	1.4_RC2_export.ova itay test freee multiple update.	ubuntu	00:50:56:91:97:13	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.41
	1_5_export.ova itay Upgrader Test	ubuntu	00:50:56:91:87:92	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.30
	Release-1.5_Mishka_faster_cycle	ubuntu	00:50:56:91:F7:17	VMware, Inc. (3401 Hillview Avenue PALO ALTO CA US 94304 )	192.168.20.15

*A list of unknown and unmanaged devices in the Axonius Cybersecurity Asset Management Platform*

## QUESTION 2: WHERE IS THE DEVICE?

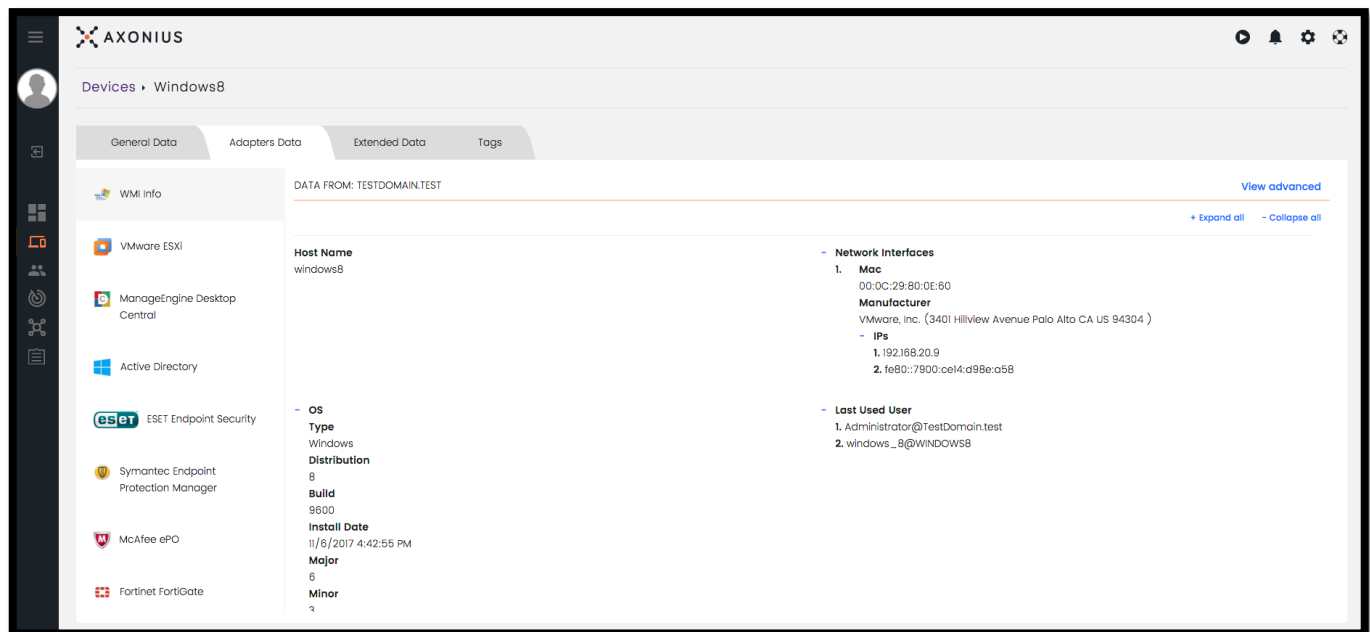
The location of the device can have a few different meanings:

1. Where is it geographically? Is it a laptop in APAC? An IoT device in South America?
2. What network is it on? Many large organizations have many different networks and subnets with nuanced differences in what's allowed on each. For instance, the corporate network will have different policy rules than the R&D environment.
3. What switch or port is it connected to? A device on the guest Wi-Fi has a different meaning and context than a server plugged in to the physical network.



### QUESTION 3: WHAT IS THE DEVICE?

Is the device a corporate-sanctioned laptop running Windows 10? A VM? A smart TV? An IoT device? The type of device is a determining factor in the security implications and the software that manages and performs updates.



*A look at a single device. In this case, a Windows 8 VM.*

### QUESTION 4: IS THE CORE SOFTWARE UP-TO-DATE?

We often hear customers mentioning they want an easy way to see things like:

1. Show me all Windows 10 devices that have not yet installed a published patch.
2. As soon as a new version of OS X is available, give me a list of all devices that need to be updated.



### QUESTION 5: WHAT ADDITIONAL SOFTWARE IS INSTALLED?

Aside from the core software, what else is present? For example:

1. I just saw a news article that there's an exploit in the wild for X software. Show me all devices with that version installed.
2. We're using software from a vendor that was just acquired, and the product is being EOLd. Now that we need to replace that software, show me everywhere it is being used in my environment.

The screenshot displays the Axonius web interface. On the left is a dark sidebar with navigation icons. The main content area is titled 'Devices > Windows8'. Below this, there are tabs for 'General Data', 'Adapters Data', 'Extended Data', and 'Tags'. The 'General Data' tab is active, showing a list of installed software. The list is organized into two columns. Each entry includes a number, a software vendor, the software name, and the software version. The vendors listed include Microsoft Corporation, McAfee, Inc., ESET, spol. s r.o., and VMware, Inc. The software names include 'Microsoft Visual C++ 2015 x64 Minimum Runtime', 'McAfee Agent', 'Microsoft Visual C++ 2008 Redistributable', 'ESET Remote Administrator Agent', and 'VMware Tools'. The software versions are also listed for each item. A 'VMware, Inc.' tag is visible at the bottom right of the list.

Number	Software Vendor	Software Name	Software Version
1.	Microsoft Corporation	Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.24215	14.0.24215
2.	McAfee, Inc.	McAfee Agent	4.8.3002
3.	Microsoft Corporation	Microsoft Visual C++ 2008 Redistributable	8.0.61001
4.	Microsoft Corporation	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	9.0.30729.4148
5.	ESET, spol. s r.o.	ESET Remote Administrator Agent	6.5.522.0
6.	Microsoft Corporation	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	9.0.30729.6161
7.	Microsoft Corporation	Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.24215	14.0.24215
8.	VMware, Inc.	VMware Tools	

*The list of all installed software on a device.*



### QUESTION 6: WHICH OF THE DEVICES IN MY ENVIRONMENT WERE MANUFACTURED IN A SPECIFIC COUNTRY?

One of our customers asked if we could write a query to show them any device that was manufactured in China. By looking at the network interface manufacturer, we were able to produce a list of devices known to have been manufactured there.

The screenshot shows the Axonius web interface. At the top, there's a search bar with the query: `specific_data.data.network_interfaces.manufacturer == regex('CN','I') or specific_data.data.network_interfaces.manufacturer == regex('China','I')`. Below the search bar, there's a table titled "Devices (4)". The table has columns: Adapters, Asset Name, Host Name, Network Interfaces: Mac, Network Interfaces: Manufacturer, and Network Interface. The table contains four rows of data, all representing devices manufactured in China.

Adapters	Asset Name	Host Name	Network Interfaces: Mac	Network Interfaces: Manufacturer	Network Interface
<input type="checkbox"/>	DESKTOP-FBSUUE7		00:23:24:F1:0D:FA	G-PRO COMPUTER (first arrange C, Yinghu Industrial estate DongGuan City Guangdong Province CN 523648 )	192.168.10.4
<input type="checkbox"/>	RVCMS32W0200A/DA28170000004101		E0:50:8B:9B:F4:A7	Zhejiang Dahua Technology Co., Ltd. (No.1199,Waterfront Road Hangzhou Zhejiang CN 310053 )	192.168.10.12
<input type="checkbox"/>	MI5s-MIPhone		C4:0B:C8:85:55:61	Xiaomi Communications Co Ltd (The Rainbow City of China Resources NO.68, Qinghe Middle Street Haidian District, Beijing CN 100085 )	192.168.254.8
<input type="checkbox"/>	HUAWEI_P9_Plus		A4:CA:A0:1E:AB:BF	HUAWEI TECHNOLOGIES CO.,LTD (No.2 Xin Cheng Road, Room R6,Songshan Lake Technology Park Dongguan CN 523808 )	192.168.254.11

*The results of the query: show me all devices manufactured in China.*



# User-Related Questions

By correlating user information with devices, we can ask questions that get to the intersection of users, devices, and software.

## QUESTION 7: WHICH AD-ENABLED USERS HAVE IMPROPER ACCESS CONFIGURATIONS?

In many large organizations, keeping track of user permissions in AD can be difficult. A few examples:

1. Show me users with AD Account Disabled.
2. Let me see any user account with AD Password Not Required.
3. I want to see all users with their AD Password set to Never Expire.
4. Do I have user accounts with no pre-authentication required?

<input type="checkbox"/>	User Name	Domain	Last Seen In Domain	<input type="checkbox"/> AD Account Disabled	<input type="checkbox"/> AD Password Not Required	<input type="checkbox"/> AD Password Never Expires	<input type="checkbox"/> AD No Pre Authentication Required
<input type="checkbox"/>	RAINDOMAINS\$	TestDomain.test		x	✓	x	x
<input type="checkbox"/>	WEST\$	TestDomain.test		x	✓	x	x

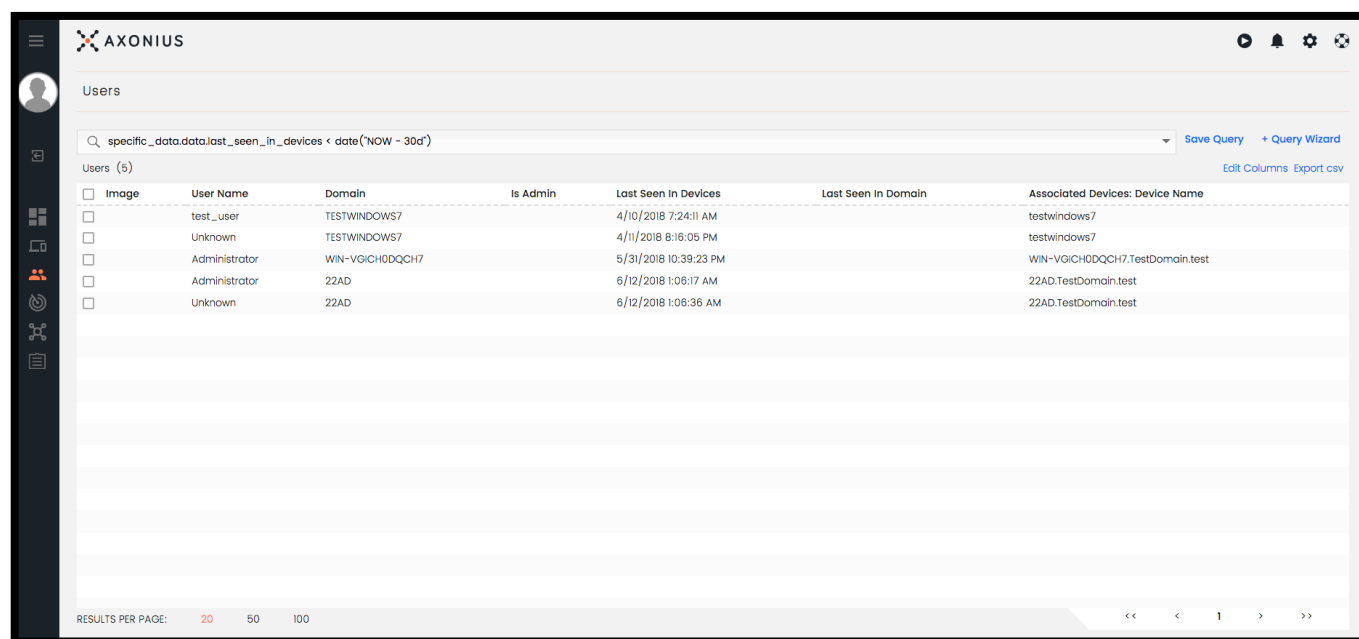
*AD-Enabled Users with Bad Configurations.*





### QUESTION 8: DO I HAVE USERS WITH DEVICES NOT SEEN IN THE PAST 30 DAYS?

Given a specific timeframe, show me users that have devices that have seemingly disappeared. This could mean a device has been stolen, dropped into a pool, or something completely benign. Either way, customers want to understand more.



<input type="checkbox"/>	Image	User Name	Domain	Is Admin	Last Seen In Devices	Last Seen In Domain	Associated Devices: Device Name
<input type="checkbox"/>		test_user	TESTWINDOWS7		4/10/2018 7:24:11 AM		testwindows7
<input type="checkbox"/>		Unknown	TESTWINDOWS7		4/11/2018 8:16:05 PM		testwindows7
<input type="checkbox"/>		Administrator	WIN-VGICH0DQCH7		5/31/2018 10:39:23 PM		WIN-VGICH0DQCH7.TestDomain.test
<input type="checkbox"/>		Administrator	22AD		6/12/2018 1:08:17 AM		22AD.TestDomain.test
<input type="checkbox"/>		Unknown	22AD		6/12/2018 1:08:36 AM		22AD.TestDomain.test

*Users with Devices Not Seen in 30 Days.*

### QUESTION 9: DO I HAVE USERS THAT HAVE TURNED OFF THEIR ENDPOINT PROTECTION AGENT?

This is one that we've seen several times, and it's interesting. In organizations that give users local admin rights on their devices, we've heard the following: "We know that every device has our EPP product installed, but we have a suspicion that people are turning it off. By logging in to our EPP admin interface, we see that the software is installed, but we can't tell whether it's running."

By comparing the EPP agent's "last seen" time with the last time the user's device has checked in with Active Directory, we can see a list of suspects that may have turned off their endpoint agent. We say suspects, as something malicious could have killed the process or it could have simply crashed.



# Catch-All Policy-Related Question

## QUESTION 10: DO MY DEVICES AND USERS ADHERE TO MY SECURITY POLICY?

Admittedly, this is a question that is bigger and more complicated than the rest above. However, it's the question at the core of cybersecurity asset management: how can I be sure that my security policies are being adhered to continuously?

While this question varies widely by organization, some examples of the similarities we often see:

1. We've decided on x as our endpoint security agent, and every laptop, desktop, and VM should have that agent installed. Send me an alert any time a relevant device is found without that agent.
2. All devices must be scanned weekly by our chosen vulnerability assessment tool. Any time a new device is found that is unknown to my scanner, add it to the next scheduled scan.
3. Let me know any time there's an available security patch and create a ticket automatically in ServiceNow.

The screenshot displays the Axonius web interface for creating a new alert. The sidebar on the left contains various navigation icons. The main content area is titled 'Alerts > New Alert'. It includes a text input for 'Alert Name', a dropdown for 'Select Saved Query' (currently showing 'OS Available Security Patches Information'), and sections for 'Alert Trigger' (with checkboxes for 'Increased', 'Decrease', and 'Not Changed'), 'Alert Severity' (with radio buttons for 'Info', 'Warning', and 'Error'), and 'Action' (with checkboxes for 'Push a system notification', 'Create ServiceNow Incident', 'Create ServiceNow Computer', 'Notify Syslog', and 'Send an Email'). At the bottom right, there are 'Cancel' and 'Save' buttons.

*All queries can be saved, and any query can be turned into an alert.*



AXONIUS

ASSET MANAGEMENT FOR CYBERSECURITY

## About Axonius

For organizations that see opportunity in today's always-on and always-connected reality, Axonius is the Cyber Security Asset Management (CSAM) platform that lets IT and Security teams see devices for what they are in order to manage and secure all. By easily integrating with customers' existing management and security technologies and using an extensible plugin infrastructure to add custom logic, customers are able to get a unified view of all devices - both known and unknown. Axonius aims to be IT's favorite Security tool and Security's favorite IT tool. For more information and to see what's possible with a universal view of all devices, visit [Axonius.com](https://Axonius.com).

## Support and Questions

We are committed to helping our customers deploy, configure, and start seeing value immediately. The POC deployment process will be hands-on, with any and all support services available to get up and running. Should you have any questions, concerns, or product feedback, please do not hesitate to contact your Axonius account representative at any time.

## Thank You

Finally, we want to thank you for considering working with Axonius. As IT and Security professionals ourselves, we understand the time and effort it takes to consider a new product. Thank you for trusting us to help you.

Try It Now.