What Security Teams Discover When They Automate Cybersecurity Asset Management

OVERVIEW

After working with hundreds of security professionals and covering over 1 million assets at some of the world's most innovative brands, the team at Axonius has identified 5 things that security teams discover when they automate cybersecurity asset management. In this short paper, we'll review each of these findings, discuss their security implications, and show how automating asset management can both find and resolve these challenges.

Table of Contents

Assets Missing an Endpoint Agent

WHAT IT MEANS

Most security teams purchase a multitude of security and management tools to protect assets like laptops, desktops, servers, VMs, mobile devices. Cloud instances, and IoT devices. Despite purchasing and deploying multiple agents, organizations often struggle to answer questions like:

1. Which assets are missing the relevant EPP/EDR agent defined by my security policy?
2. Which assets have the right agent installed, but have disabled its functionality?
3. Which assets have an old version of the right agent installed?

Each of these questions speak to the notion of agent health and cyber hygiene: understanding which assets are missing the proper security tool coverage and which are missing the tools' functionality.

By the Numbers

Axonius customers find that between 16% and 24% of assets are missing an endpoint agent, or have an agent installed that is not functioning correctly.

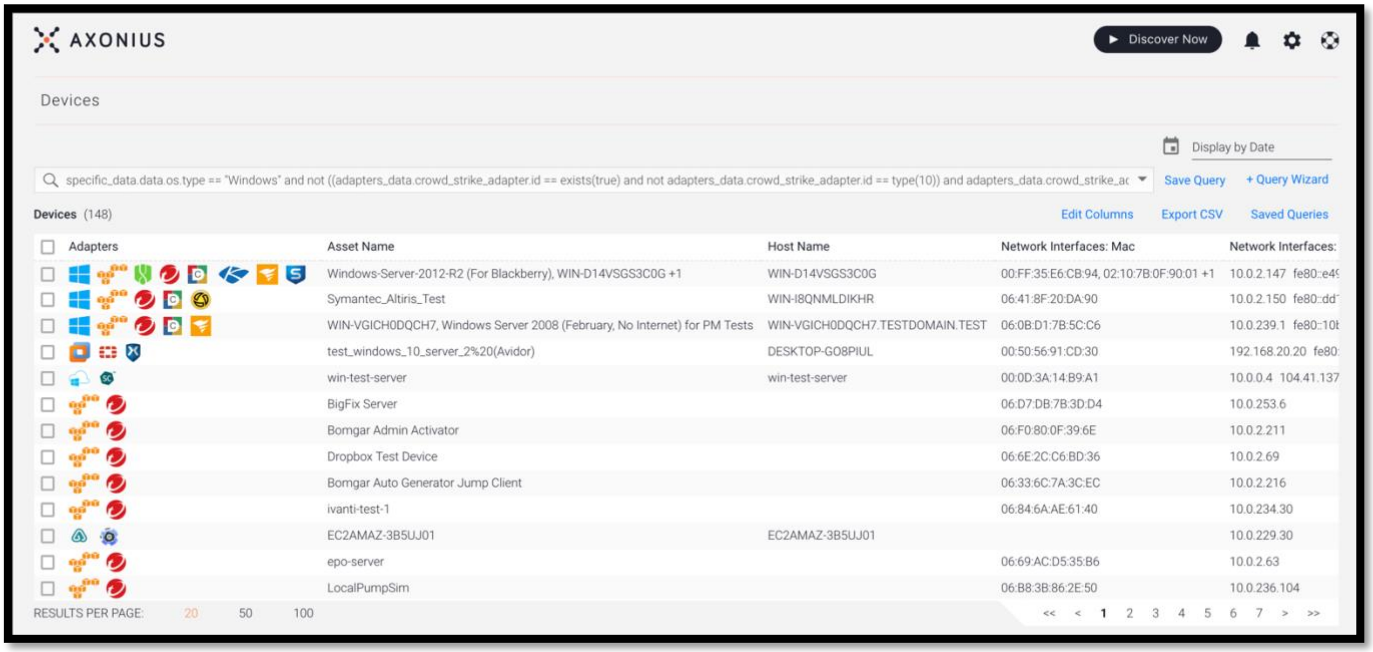
SECURITY IMPLICATIONS

Much like buying a home security system and not turning it on, going through the process of evaluating security vendors, rolling out the selected solution, and then having an asset fall victim to malware because it didn't have the endpoint agent would be a tragedy that shouldn't happen.

Knowing which assets are covered by each security solution should be easy but there are inherent challenges. Logging into the admin console of an EPP/EDR console, for instance, can tell you which assets have had the agent installed. Unfortunately, many of these solutions can't tell you whether the agent is currently running and functioning as expected.

The biggest security issue related to agent health and cyber hygiene is simply not knowing which of your assets isn't covered by what you're already paying for.

Example: A list of all Windows devices that do not have CrowdStrike installed:



```
specific_data.data.os.type == "Windows" and not ((adapters_data.crowd_strike_adapter.id == exists(true) and not adapters_data.crowd_strike_adapter.id == type(10)) and adapters_data.crowd_strike_ac
```

Devices (148)

□	Adapters	Asset Name	Host Name	Network Interfaces: Mac	Network Interfaces:
□		Windows-Server-2012-R2 (For Blackberry), WIN-D14VSGS3C0G +1	WIN-D14VSGS3C0G	00:FF:35:E6:CB:94, 02:10:7B:0F:90:01 +1	10.0.2.147 fe80::e4
□		Symantec_Altiris_Test	WIN-I8QNMLDIKHR	06:41:8F:20:DA:90	10.0.2.150 fe80::dd
□		WIN-VGICH0DQCH7, Windows Server 2008 (February, No Internet) for PM Tests	WIN-VGICH0DQCH7.TESTDOMAIN.TEST	06:0B:D1:7B:5C:C6	10.0.239.1 fe80::10
□		test_windows_10_server_2%20(Avidor)	DESKTOP-GO8PIUL	00:50:56:91:CD:30	192.168.20.20 fe80
□		win-test-server	win-test-server	00:0D:3A:14:B9:A1	10.0.0.4 104.41.137
□		BigFix Server		06:D7:DB:7B:3D:D4	10.0.253.6
□		Bomgar Admin Activator		06:F0:80:0F:39:6E	10.0.2.211
□		Dropbox Test Device		06:6E:2C:C6:BD:36	10.0.2.69
□		Bomgar Auto Generator Jump Client		06:33:6C:7A:3C:EC	10.0.2.216
□		ivanti-test-1		06:84:6A:AE:61:40	10.0.234.30
□		EC2AMAZ-3B5UJ01	EC2AMAZ-3B5UJ01		10.0.229.30
□		epo-server		06:69:AC:D5:35:B6	10.0.2.63
□		LocalPumpSim		06:B8:3B:86:2E:50	10.0.236.104

Unmanaged Assets

WHAT IT MEANS

Unmanaged assets are those devices that are only known to the network and have no management or security agents installed. These could be laptops that are plugged into the corporate network, cloud instances without any security solution coverage, or an IoT device only seen by a vulnerability assessment tool.

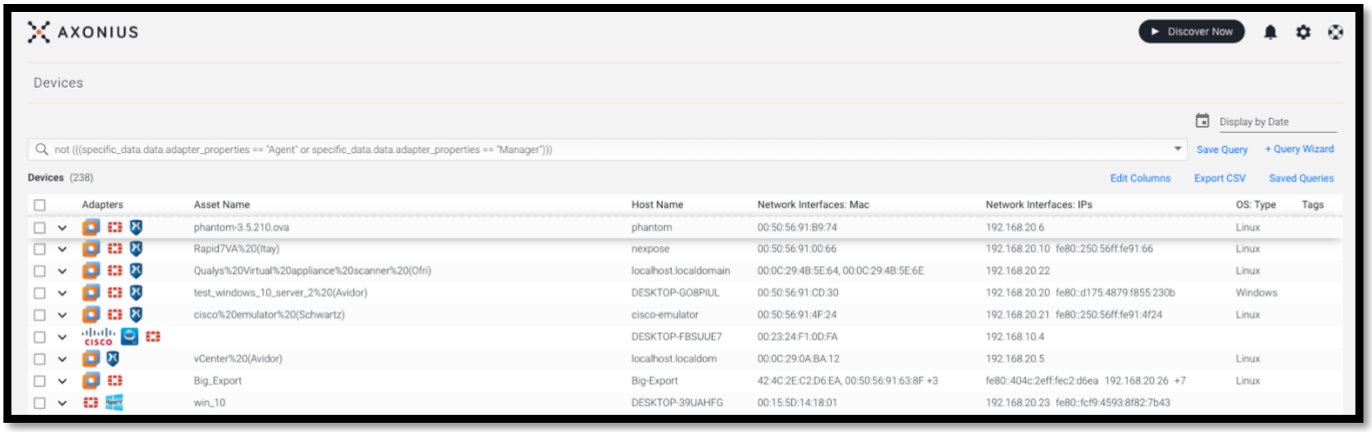
By the Numbers

Axonius customers find that between 10% and 18% of assets are unmanaged and only seen by the network.

SECURITY IMPLICATIONS

By definition, unmanaged devices are only known to the network or network scanners, and that means very little is known about them. In some cases, that's okay; the smart TV in the conference room isn't going to be part of a patch schedule and doesn't need to have an EPP/EDR agent installed. However, 100% of Axonius customers find unmanaged assets that should be managed.

Example: A list of assets that do not have an agent installed and are not part of a management system (for example: Active Directory).



Devices

not (((specific_data.data.adapter_properties == "Agent" or specific_data.data.adapter_properties == "Manager")))

Devices (238)

☐	Adapters	Asset Name	Host Name	Network Interfaces: Mac	Network Interfaces: IPs	OS: Type	Tags
☐		phantom-3.5.210.ova	phantom	00:50:56:91:B9:74	192.168.20.6	Linux	
☐		Rapid7VA%20(Itay)	nexpose	00:50:56:91:00:66	192.168.20.10 fe80::250:56ff:fe91:66	Linux	
☐		Qualys%20Virtual%20appliance%20scanner%20(Ofri)	localhost.localdomain	00:0C:29:4B:5E:64, 00:0C:29:4B:5E:6E	192.168.20.22	Linux	
☐		test_windows_10_server_2%20(Avidor)	DESKTOP-GO8PIUL	00:50:56:91:CD:30	192.168.20.20 fe80::d175:4879:f855:230b	Windows	
☐		cisco%20emulator%20(Schwartz)	cisco-emulator	00:50:56:91:4F:24	192.168.20.21 fe80::250:56ff:fe91:4f24	Linux	
☐	CISCO		DESKTOP-FBSUUE7	00:23:24:F1:0D:FA	192.168.10.4		
☐		vCenter%20(Avidor)	localhost.localdom	00:0C:29:0A:BA:12	192.168.20.5	Linux	
☐		Big_Export	Big-Export	42:4C:2E:C2:D6:EA, 00:50:56:91:63:8F +3	fe80::404c:2eff:fec2:d6ea 192.168.20.26 +7	Linux	
☐		win_10	DESKTOP-39UAHFG	00:15:5D:14:18:01	192.168.20.23 fe80::fcf9:4593:8f82:7b43		

Cloud Instances Not Being Scanned by a Vulnerability Assessment Tool

WHAT IT MEANS

The elastic, on-demand nature of the cloud coupled with the speed of DevOps have driven organizations to move more and more to the cloud. However, the security solutions that organizations have implemented to protect their on-premises assets don't necessarily work for the cloud.

Vulnerability assessment tools do an amazing job of scanning a network to discover devices with known vulnerabilities, but they can only scan what they know about. The dynamic nature of the cloud can cause a gap whereby VA tools simply don't know that there are new instances to scan.

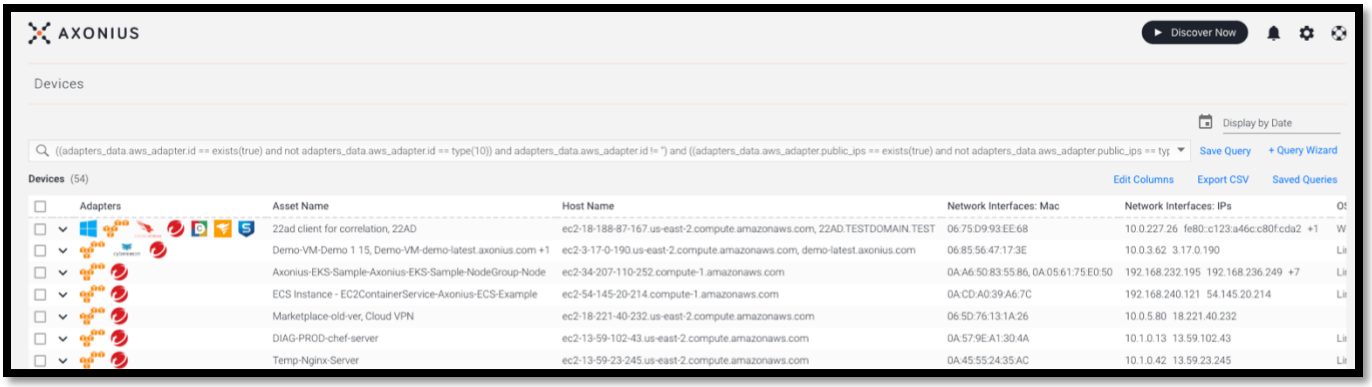
By the Numbers

Axonius customers find that between 7% and 20% of cloud instances have not been scanned by their vulnerability assessment tool.

SECURITY IMPLICATIONS

You'll need to go no further than a Google search to see just how often breaches occur based on publicly accessible cloud instances. And most recently, attackers have found a way to exploit a zero-day to install ransomware on cloud servers without requiring end-users to click on anything.

Example: A list of every Amazon instance with a public IP that isn't being scanned by a VA Scanner:



((adapters_data.aws_adapter.id == exists(true) and not adapters_data.aws_adapter.id == type(10)) and adapters_data.aws_adapter.id != ") and ((adapters_data.aws_adapter.public_ips == exists(true) and not adapters_data.aws_adapter.public_ips == typ

Devices (54)

☐	Adapters	Asset Name	Host Name	Network Interfaces: Mac	Network Interfaces: IPs	O
☐		22ad client for correlation, 22AD	ec2-18-188-87-167.us-east-2.compute.amazonaws.com, 22AD.TESTDOMAIN.TEST	06:75:D9:93:EE:68	10.0.227.26 fe80::c123:a46c:c80f:cda2 +1	W
☐		Demo-VM-Demo 1 15, Demo-VM-demo-latest.axonius.com +1	ec2-3-17-0-190.us-east-2.compute.amazonaws.com, demo-latest.axonius.com	06:85:56:47:17:3E	10.0.3.62 3.17.0.190	Li
☐		Axonius-EKS-Sample-Axonius-EKS-Sample-NodeGroup-Node	ec2-34-207-110-252.compute-1.amazonaws.com	0A:A6:50:83:55:86, 0A:05:61:75:E0:50	192.168.232.195 192.168.236.249 +7	Li
☐		ECS Instance - EC2ContainerService-Axonius-ECS-Example	ec2-54-145-20-214.compute-1.amazonaws.com	0A:CD:A0:39:A6:7C	192.168.240.121 54.145.20.214	Li
☐		Marketplace-old-ver, Cloud VPN	ec2-18-221-40-232.us-east-2.compute.amazonaws.com	06:5D:76:13:1A:26	10.0.5.80 18.221.40.232	
☐		DIAG-PROD-chef-server	ec2-13-59-102-43.us-east-2.compute.amazonaws.com	0A:57:9E:A1:30:4A	10.1.0.13 13.59.102.43	Li
☐		Temp-Nginx-Server	ec2-13-59-23-245.us-east-2.compute.amazonaws.com	0A:45:55:24:35:AC	10.1.0.42 13.59.23.245	Li

Users with Bad Permissions

WHAT IT MEANS

Microsoft lists several Active Directory permissions that should not be set for users, but here we'll look at three:

1. AD Password Never Expires
2. AD Password Not Required
3. AD No Pre-Authentication Required

By the Numbers

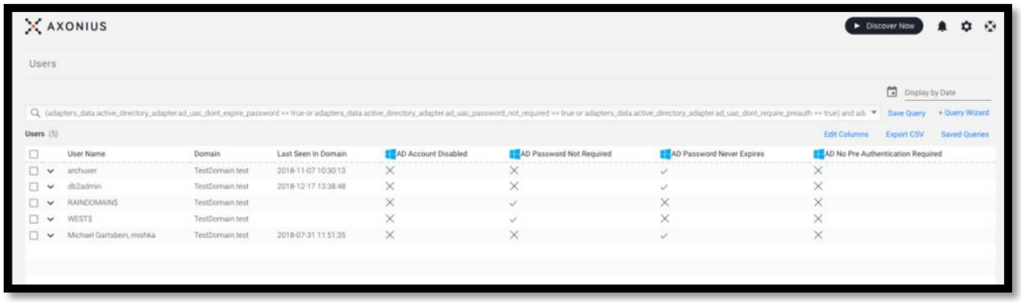
100% of Axonius customers find accounts with bad permissions, mostly from service accounts that haven't been changed in more than one year.

SECURITY IMPLICATIONS

Having a user account in AD with the password not required flag set can create a security risk, especially when this is a domain admin account login on a domain controller. Additionally, the user is not subject to any existing policy regarding the length of password and may have a shorter password than is required or may even have no password at all, even if empty passwords are not allowed.

With no pre-authentication set, a malicious attacker can directly send a dummy request for authentication, and the Key Distribution Center (KDC) will return an encrypted TGT and the attacker can brute force it offline. Upon checking the KDC logs, nothing will be seen except a single request for a TGT. When Kerberos timestamp pre-authentication is enforced, the attacker cannot directly ask the KDCs for the encrypted material to brute force offline. The attacker has to encrypt a timestamp with a password and offer it to the KDC. The attacker can repeat this over and over. However, the KDC log will record the entry every time the pre-authentication fails.

Example: A list of accounts with one of these flags set to true:



(adapters_data.active_directory_adapter.ad_uac_dont_expire_password == true or adapters_data.active_directory_adapter.ad_uac_password_not_required == true or adapters_data.active_directory_adapter.ad_uac_dont_require_preauth == true) and adı

Users (5)

User Name	Domain	Last Seen In Domain	AD Account Disabled	AD Password Not Required	AD Password Never Expires	AD No Pre Authentication Required
archuser	TestDomain.test	2018-11-07 10:30:13	✕	✕	✓	✕
db2admin	TestDomain.test	2018-12-17 13:38:48	✕	✕	✓	✕
RAINDOMAIN$	TestDomain.test		✕	✓	✕	✕
WEST$	TestDomain.test		✕	✓	✕	✕
Michael Gartsbein, mishka	TestDomain.test	2018-07-31 11:51:35	✕	✕	✓	✕

Assets with Critical Vulnerabilities

WHAT IT MEANS

Assets with critical vulnerabilities are based on a CVE classification, defined as deficient or vulnerable to direct or indirect attack that will create decisive or significant effects.

By the Numbers

Axonius customers report a more than 50% decrease in time spent searching for assets with critical vulnerabilities.

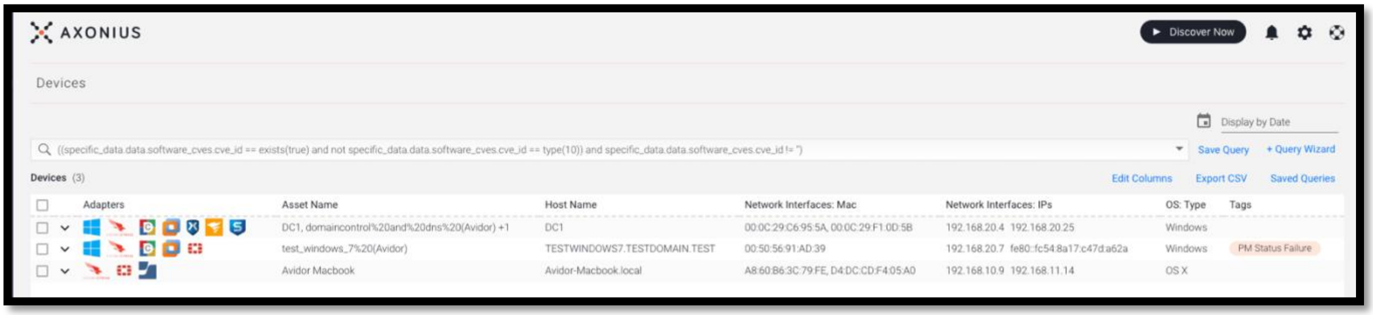
SECURITY IMPLICATIONS

Devices with critical vulnerabilities are the most prone to attack, as published vulnerabilities are those that are proven to be exploitable and are the most likely to be targets of malicious actors. Any time a critical vulnerability is published, security teams should prioritize patching and updating any assets found to have the critical vulnerability present.

FINDING ASSETS WITH CRITICAL VULNERABILITIES

As Axonius integrates with several vulnerability assessment tools as well as the NIST database, customers can either run a query with the parameters “Vulnerable Software: CVE ID Exists” or they can run a query using the information from their VA tool. For example:

Example: A list of devices with a CVE ID:



```
((specific_data.data.software_cves.cve_id == exists(true) and not specific_data.data.software_cves.cve_id == type(10)) and specific_data.data.software_cves.cve_id != '')
```

Devices (3)

□	Adapters	Asset Name	Host Name	Network Interfaces: Mac	Network Interfaces: IPs	OS: Type	Tags
□		DC1, domaincontrol%20and%20dns%20(Avidor) +1	DC1	00:0C:29:C6:95:5A, 00:0C:29:F1:0D:5B	192.168.20.4 192.168.20.25	Windows	
□		test_windows_7%20(Avidor)	TESTWINDOWS7.TESTDOMAIN.TEST	00:50:56:91:AD:39	192.168.20.7 fe80::fc54:8a17:c47d:a62a	Windows	PM Status Failure
□		Avidor Macbook	Avidor-Macbook.local	A8:60:B6:3C:79:FE, D4:DC:CD:F4:05:A0	192.168.10.9 192.168.11.14	OS X	

About Axonius

Axonius is the only cybersecurity asset management platform providing actionable visibility and security policy enforcement for all assets and users by aggregating existing business data from 100+ management and security solutions. Axonius manages and secures millions of assets for a wide range of public and private companies, including The New York Times, AppsFlyer, Natera and more. 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.

Get Started

Because it integrates natively with the Security and IT solutions customers already have, getting started is painless and fast. To get a demo and to see what you can do with a unified view of all assets, click the button below.

Try It Now.

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.