



Building a Business Case for Cybersecurity Asset Management

Version 3.0, May 2019



OVERVIEW

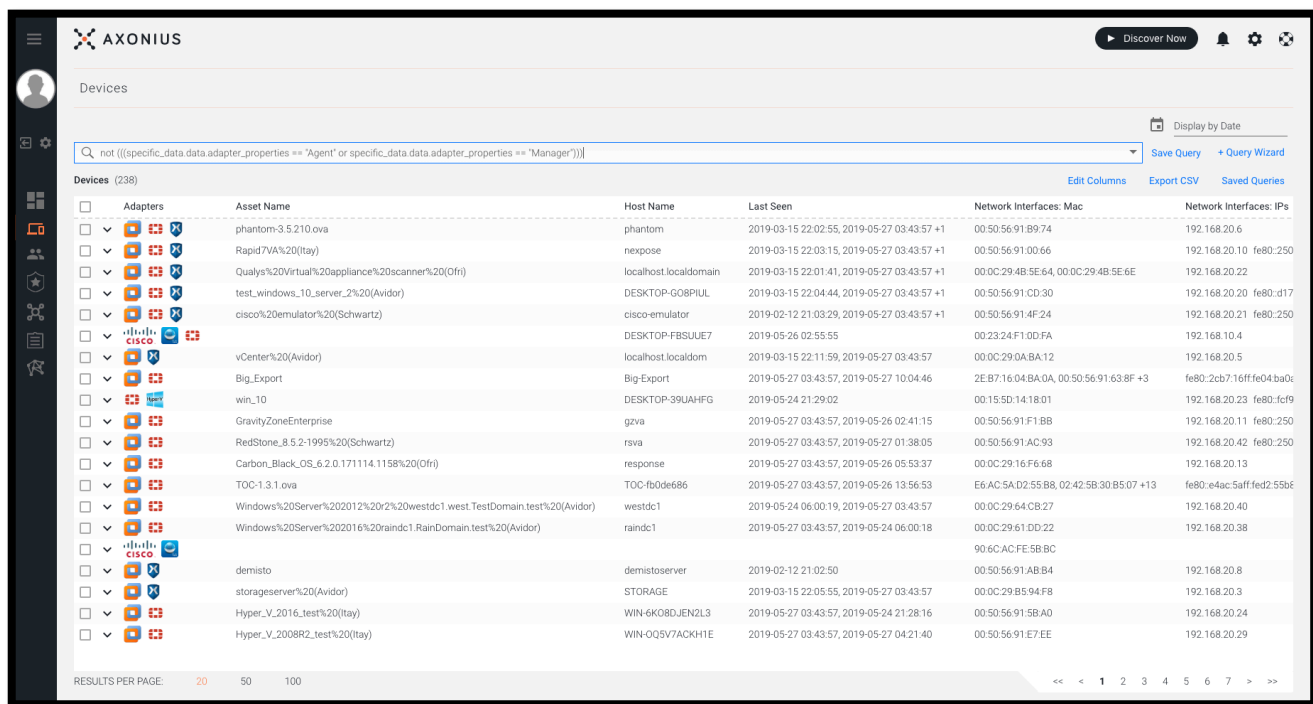
With many competing priorities facing information security teams, any new project must be prioritized against risk, net new capabilities, and ROI. The following document presents a business case for evaluating cybersecurity asset management solutions.

The Asset Management Challenge

The explosion in the number and types of devices on corporate networks has created three inextricably linked challenges: having comprehensive asset visibility and enforcing adherence to the security policy.

CHALLENGE ONE: ASSET VISIBILITY

- a. **Finding Unmanaged Devices** - You can't protect what you don't know you have. We've seen unmanaged devices account for between 10% and 18% of all devices in an average enterprise, and a full 100% of Axonius customers find devices they were not aware of.

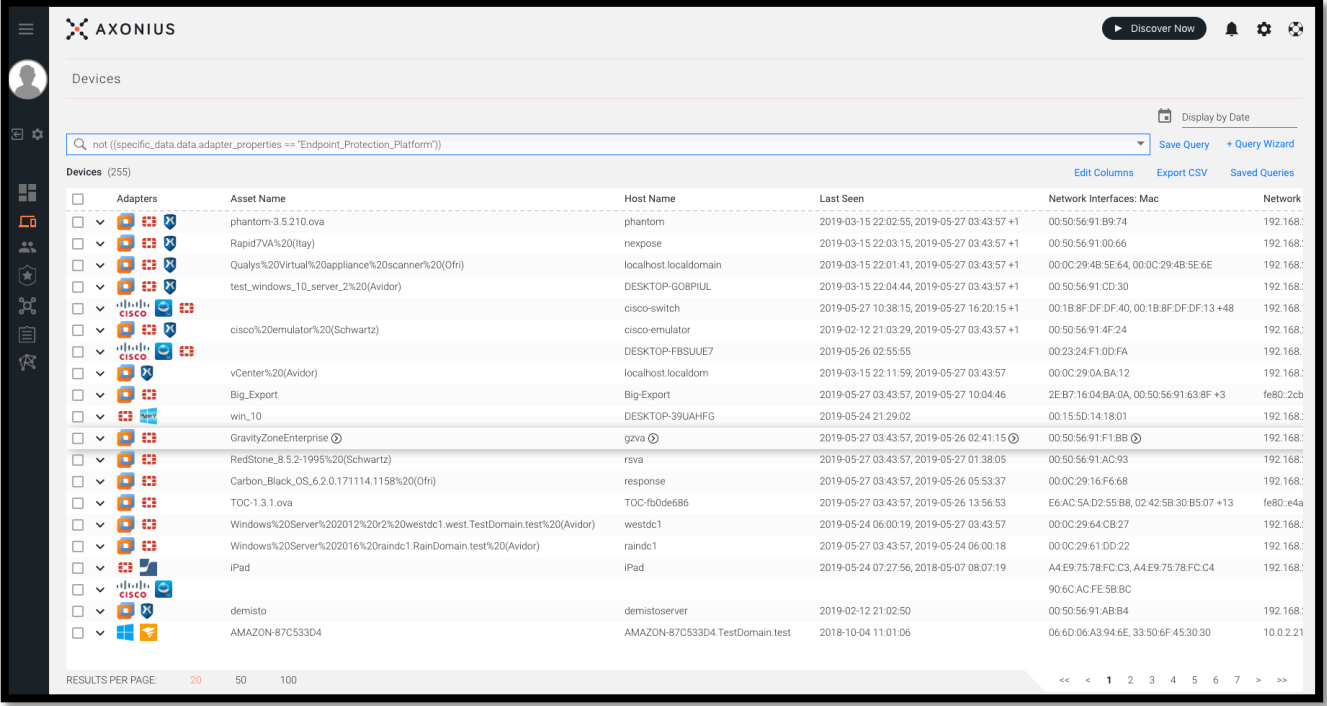


| Adapters | Asset Name | Host Name | Last Seen | Network Interfaces: Mac | Network Interfaces: IPs |
|----------|---|-----------------------|---|--|--------------------------|
| | phantom-3.5.210.ova | phantom | 2019-03-15 22:02:55, 2019-05-27 03:43:57 +1 | 00:50:56:91:89:74 | 192.168.20.6 |
| | Rapid7VA%20(tay) | nexpose | 2019-03-15 22:03:15, 2019-05-27 03:43:57 +1 | 00:50:56:91:00:66 | 192.168.20.10 fe80:250 |
| | Qualys%20Virtual%20Appliance%20(scanner%20(Offr) | localhost.localdomain | 2019-03-15 22:01:41, 2019-05-27 03:43:57 +1 | 00:0C:29:4B:5E:64, 00:0C:29:4B:5E:6E | 192.168.20.22 |
| | test_windows_10_server_2%20(Avidor) | DESKTOP-G08PIUL | 2019-03-15 22:04:44, 2019-05-27 03:43:57 +1 | 00:50:56:91:CD:30 | 192.168.20.20 fe80:d17 |
| | cisco%20emulator%20(Schwartz) | cisco-emulator | 2019-02-12 21:03:29, 2019-05-27 03:43:57 +1 | 00:50:56:91:4F:24 | 192.168.20.21 fe80:250 |
| | DESKTOP-FBSUUE7 | DESKTOP-FBSUUE7 | 2019-05-26 02:55:55 | 00:23:24:F1:00:FA | 192.168.10.4 |
| | vCenter%20(Avidor) | localhost.localdom | 2019-03-15 22:11:59, 2019-05-27 03:43:57 | 00:0C:29:0A:BA:12 | 192.168.20.5 |
| | Big_Export | Big-Export | 2019-05-27 03:43:57, 2019-05-27 10:04:46 | 2E:87:16:04:BA:0A, 00:50:56:91:63:8F +3 | fe80:2cb7:16ff:fe04:ba0c |
| | win_10 | DESKTOP-39UAHFG | 2019-05-24 21:29:02 | 00:15:5D:14:18:01 | 192.168.20.23 fe80:fcf9 |
| | GravityZoneEnterprise | gzva | 2019-05-27 03:43:57, 2019-05-26 02:41:15 | 00:50:56:91:F1:B8 | 192.168.20.11 fe80:250 |
| | RedStone_8.5.2-1995%20(Schwartz) | rsva | 2019-05-27 03:43:57, 2019-05-27 01:38:05 | 00:50:56:91:AC:93 | 192.168.20.42 fe80:250 |
| | Carbon_Black_OS_6.2.0.171114.1158%20(Offr) | response | 2019-05-27 03:43:57, 2019-05-26 05:53:37 | 00:0C:29:16:F6:68 | 192.168.20.13 |
| | TOC-1.3.1.ova | TOC-fb0de686 | 2019-05-27 03:43:57, 2019-05-26 13:56:53 | E6:AC:5A:D2:55:B8, 02:42:5B:30:B5:07 +13 | fe80:e4ac:5aff:fed2:55b8 |
| | Windows%20Server%202012%202%20westdc1.west.TestDomain.test%20(Avidor) | westdc1 | 2019-05-24 06:00:19, 2019-05-27 03:43:57 | 00:0C:29:64:CB:27 | 192.168.20.40 |
| | Windows%20Server%202016%20raindc1.RainDomain.test%20(Avidor) | raindc1 | 2019-05-27 03:43:57, 2019-05-24 06:00:18 | 00:0C:29:61:DD:22 | 192.168.20.38 |
| | demisto | demistoserver | 2019-02-12 21:02:50 | 00:50:56:91:AB:B4 | 192.168.20.8 |
| | storage%20(Avidor) | STORAGE | 2019-03-15 22:05:55, 2019-05-27 03:43:57 | 00:0C:29:B5:94:F8 | 192.168.20.3 |
| | Hyper_V_2016_test%20(tay) | WIN-6K08DJEN2L3 | 2019-05-27 03:43:57, 2019-05-24 21:28:16 | 00:50:56:91:5B:A0 | 192.168.20.24 |
| | Hyper_V_2008R2_test%20(tay) | WIN-OQ5V7ACKH1E | 2019-05-27 03:43:57, 2019-05-27 04:21:40 | 00:50:56:91:E7:EE | 192.168.20.29 |

A query showing unmanaged devices.

When a device is unmanaged, you don't know its security state or risk profile, and without that information, it cannot be updated.

- b. **Finding Managed Devices Missing an Agent** – Even with devices that are managed, there is no simple way to cross-correlate to understand gaps in coverage. At an average deployment, we see between 16% and 24% of devices are missing a security solution that has already been purchased and is required by the corporate security policy.



The screenshot shows the Axonius interface with a search query: `not (specific_data.data.adapter_properties == "Endpoint_Protection_Platform")`. The results table lists 255 devices, including various operating systems and network devices, all of which are missing the endpoint protection agent.

| Adapters | Asset Name | Host Name | Last Seen | Network Interfaces: Mac | Network |
|----------|--|---------------------------------|---|--|-----------|
| | phantom-3.5.210.oiva | phantom | 2019-03-15 22:02:55, 2019-05-27 03:43:57 +1 | 00:50:56:91:B9:74 | 192.168. |
| | Rapid7VA%20(Italy) | nexpose | 2019-03-15 22:03:15, 2019-05-27 03:43:57 +1 | 00:50:56:91:00:66 | 192.168. |
| | Qualys%20Virtual%20Appliance%20Scanner%20(Offr) | localhost.localdomain | 2019-03-15 22:01:41, 2019-05-27 03:43:57 +1 | 00:0C:29:4B:5E:64, 00:0C:29:4B:5E:6E | 192.168. |
| | test_windows_10_server_2%20(Avidor) | DESKTOP-GOBIUUL | 2019-03-15 22:04:44, 2019-05-27 03:43:57 +1 | 00:50:56:91:CD:30 | 192.168. |
| | cisco%20emulator%20(Schwartz) | cisco-switch | 2019-05-27 10:38:15, 2019-05-27 16:20:15 +1 | 00:1B:8F:DF:DF:00, 00:1B:8F:DF:DF:13 +48 | 192.168. |
| | cisco%20emulator%20(Schwartz) | cisco-emulator | 2019-02-12 21:03:29, 2019-05-27 03:43:57 +1 | 00:50:56:91:4F:24 | 192.168. |
| | DESKTOP-FBSUUE7 | DESKTOP-FBSUUE7 | 2019-05-26 02:55:55 | 00:23:24:F1:0D:FA | 192.168. |
| | vCenter%20(Avidor) | localhost.localdom | 2019-03-15 22:11:59, 2019-05-27 03:43:57 | 00:0C:29:0A:BA:12 | 192.168. |
| | Big_Export | Big-Export | 2019-05-27 03:43:57, 2019-05-27 10:04:46 | 2E:B7:16:04:BA:DA, 00:50:56:91:63:8F +3 | fe80:2cb |
| | win_10 | DESKTOP-39UAHFG | 2019-05-24 21:29:02 | 00:15:5D:14:18:01 | 192.168. |
| | GravityZoneEnterprise | gzva | 2019-05-27 03:43:57, 2019-05-26 02:41:15 | 00:50:56:91:F1:B8 | 192.168. |
| | RedStone_8.5.2-1995%20(Schwartz) | rsva | 2019-05-27 03:43:57, 2019-05-27 01:38:05 | 00:50:56:91:AC:93 | 192.168. |
| | Carbon_Black_OS_6.2.0.171114.1158%20(Offr) | response | 2019-05-27 03:43:57, 2019-05-26 05:53:37 | 00:0C:29:16:F6:68 | 192.168. |
| | TOC-1.3.1.oiva | TOC-fb0de686 | 2019-05-27 03:43:57, 2019-05-26 13:56:53 | E6AC:5A:D2:55:B8, 02:42:5B:30:B5:07 +13 | fe80:e4a |
| | Windows%20Server%202012%20%20westdc1.west.TestDomain.test%20(Avidor) | westdc1 | 2019-05-24 06:00:19, 2019-05-27 03:43:57 | 00:0C:29:64:CB:27 | 192.168. |
| | Windows%20Server%202016%20raindc1.RainDomain.test%20(Avidor) | raindc1 | 2019-05-27 03:43:57, 2019-05-24 06:00:18 | 00:0C:29:61:DD:22 | 192.168. |
| | iPad | iPad | 2019-05-24 07:27:56, 2018-05-07 08:07:19 | A4:E9:75:78:FC:C3, A4:E9:75:78:FC:C4 | 192.168. |
| | demisto | demistosever | 2019-02-12 21:02:50 | 90:6C:AC:FE:5B:BC | 192.168. |
| | AMAZON-87C533D4 | AMAZON-87C533D4.TestDomain.test | 2018-10-04 11:01:06 | 06:6D:06:A3:94:6E, 33:50:6F:45:30:30 | 10.0.2.21 |

A query showing devices missing an endpoint agent.

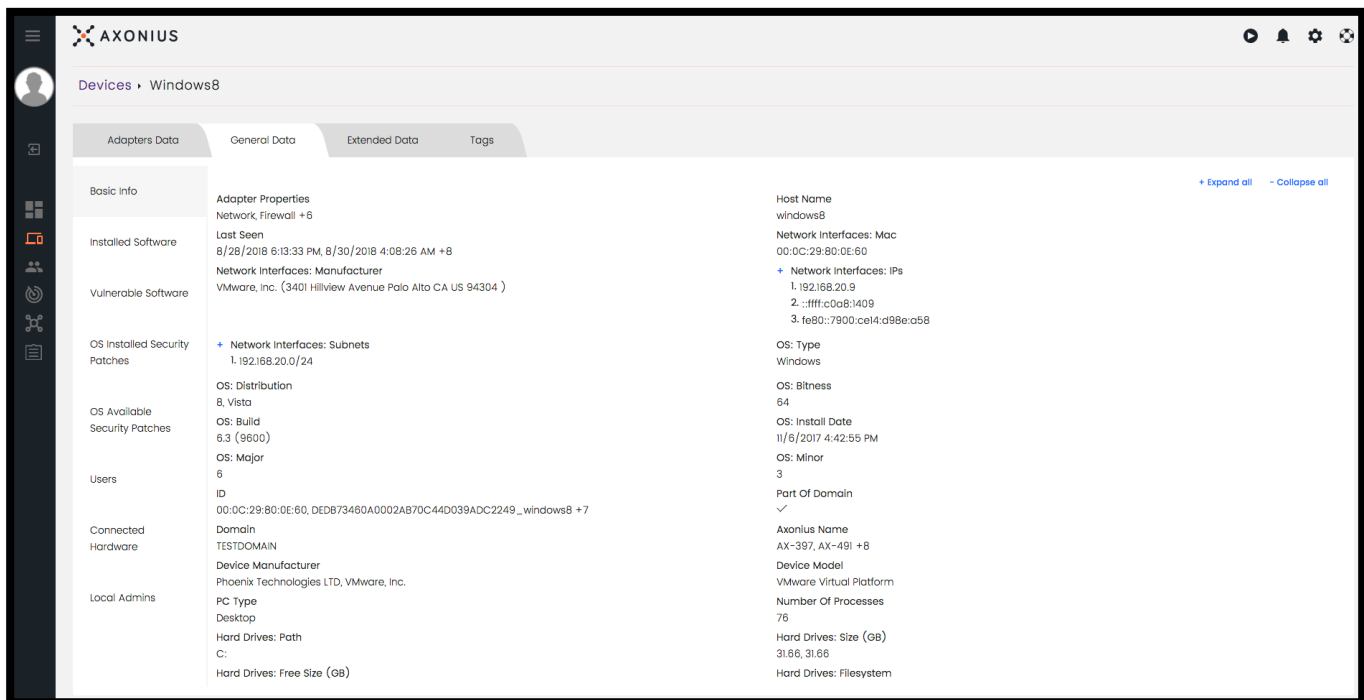
Devices that are managed but missing coverage by a security solution represent two unique issues:

- Risk** – These are devices that are corporate assets and are required to be covered by the security policy but are unnecessarily at risk.
- Waste** – Dollars are wasted when a license has already been purchased but is not in use.

- c. **Understanding Asset Context** - With many different solutions to secure devices and users, all of the information exists to ensure that assets are adhering to policy. The challenge is that the data lives in different silos.

For example, when an alert from a SIEM solution comes in to a SOC, an incident responder must look to many different sources to understand:

1. What device is the alert referring to?
2. What user(s) had access or were logged in?
3. Was the core software up-to-date?
4. What vulnerabilities are present?
5. What other devices share the same vulnerabilities and may be impacted?



The screenshot displays the Axonius web interface for a device named 'Windows8'. The interface is organized into several sections:

- Adapters Data:**
 - Basic Info: Adapter Properties (Network, Firewall +6)
 - Installed Software: Last Seen (8/28/2018 6:13:33 PM, 8/30/2018 4:08:26 AM +8)
 - Vulnerable Software: Network Interfaces: Manufacturer (VMware, Inc. (3401 Hillview Avenue Palo Alto CA US 94304))
 - OS Installed Security Patches: Network Interfaces: Subnets (1. 192.168.20.0/24)
 - OS Available Security Patches: OS: Distribution (8, Vista); OS: Build (6.3 (9600)); OS: Major (6)
 - Users: ID (00:0C:29:80:0E:60, DEDB73460A0002AB70C44D039ADC2249_windows8 +7)
 - Connected Hardware: Domain (TESTDOMAIN); Device Manufacturer (Phoenix Technologies LTD, VMware, Inc.); PC Type (Desktop); Hard Drives: Path (C:); Hard Drives: Free Size (GB)
 - Local Admins: PC Type (Desktop); Hard Drives: Path (C:); Hard Drives: Free Size (GB)
- General Data:**
 - Host Name: windows8
 - Network Interfaces: Mac (00:0C:29:80:0E:60)
 - Network Interfaces: IPs (1. 192.168.20.9; 2. ::ffff:c0a8:1409; 3. fe80::7900:ce14:d98e:a58)
 - OS: Type (Windows)
 - OS: Bitness (64)
 - OS: Install Date (11/6/2017 4:42:55 PM)
 - OS: Minor (3)
 - Part Of Domain (✓)
 - Axonius Name (AX-397, AX-491 +8)
 - Device Model (VMware Virtual Platform)
 - Number Of Processes (76)
 - Hard Drives: Size (GB) (31.66, 31.66)
 - Hard Drives: Filesystem

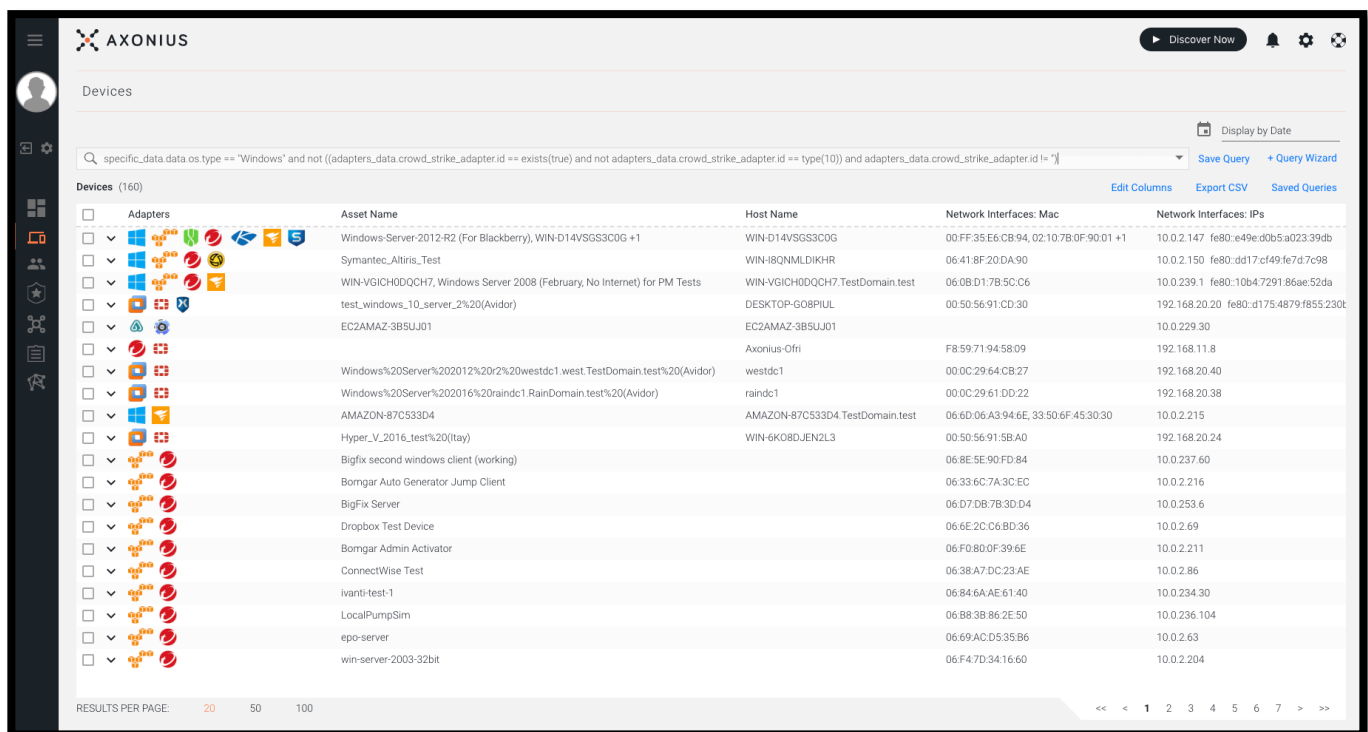
A list of all known asset properties for a single device.

The time it takes to track down the essential contextual information to make an alert actionable can easily extend to hours.

CHALLENGE TWO: ENFORCING SECURITY POLICIES

Understanding which assets you have and whether or not every device and user meets the overall security policy is an incredibly valuable first step (see [CIS Controls 1&2](#)). However, just knowing which assets are out of policy doesn't fix the issue.

For example, if your policy states that every Windows device needs to have a CrowdStrike agent installed, if you had full asset inventory, you could end up with a candidate list:



| Adapters | Asset Name | Host Name | Network Interfaces: Mac | Network Interfaces: IPs |
|--------------------------|---|---------------------------------|---|--|
| <input type="checkbox"/> | 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:e49e:d0b5:a023:39db |
| <input type="checkbox"/> | Symantec_Altiris_Test | WIN-I8QNMLDIKHR | 06:41:8F:20:DA:90 | 10.0.2.150 fe80:dd17:cf49:fe7d:7c98 |
| <input type="checkbox"/> | WIN-VGICH0DQCH7, Windows Server 2008 (February, No Internet) for PM Tests | WIN-VGICH0DQCH7.TestDomain.test | 06:08:D1:7B:5C:C6 | 10.0.2.39.1 fe80:10b4:7291:86ae:52da |
| <input type="checkbox"/> | test_windows_10_server_2%20(Avidor) | DESKTOP-G08PIUL | 00:50:56:91:CD:30 | 192.168.20.20 fe80:d175:4879:f855:230t |
| <input type="checkbox"/> | EC2AMAZ-3B5UJ01 | EC2AMAZ-3B5UJ01 | | 10.0.2.29.30 |
| <input type="checkbox"/> | | Axonius-Ofri | F8:59:71:94:58:09 | 192.168.11.8 |
| <input type="checkbox"/> | Windows%20Server%202012%20r2%20westdc1.west.TestDomain.test%20(Avidor) | westdc1 | 00:0C:29:64:CB:27 | 192.168.20.40 |
| <input type="checkbox"/> | Windows%20Server%202016%20raindc1.RainDomain.test%20(Avidor) | raindc1 | 00:0C:29:61:DD:22 | 192.168.20.38 |
| <input type="checkbox"/> | AMAZON-87C533D4 | AMAZON-87C533D4.TestDomain.test | 06:6D:06:A3:94:6E, 33:50:6F:45:30:30 | 10.0.2.215 |
| <input type="checkbox"/> | Hyper_V_2016_test%20(Itay) | WIN-6K08DJEN2L3 | 00:50:56:91:5B:A0 | 192.168.20.24 |
| <input type="checkbox"/> | Bigfix second windows client (working) | | 06:8E:5E:90:FD:84 | 10.0.2.237.60 |
| <input type="checkbox"/> | Bomgar Auto Generator Jump Client | | 06:33:6C:7A:3C:EC | 10.0.2.216 |
| <input type="checkbox"/> | BigFix Server | | 06:D7:D8:7B:3D:D4 | 10.0.2.253.6 |
| <input type="checkbox"/> | Dropbox Test Device | | 06:6E:2C:C6:BD:36 | 10.0.2.69 |
| <input type="checkbox"/> | Bomgar Admin Activator | | 06:F0:80:0F:39:6E | 10.0.2.211 |
| <input type="checkbox"/> | ConnectWise Test | | 06:38:A7:DC:23:AE | 10.0.2.86 |
| <input type="checkbox"/> | ivanti-test-1 | | 06:84:6A:AE:61:40 | 10.0.2.234.30 |
| <input type="checkbox"/> | LocalPumpSim | | 06:B8:38:86:2E:50 | 10.0.2.236.104 |
| <input type="checkbox"/> | epo-server | | 06:69:AC:D5:35:B6 | 10.0.2.63 |
| <input type="checkbox"/> | win-server-2003-32bit | | 06:F4:7D:34:16:60 | 10.0.2.204 |

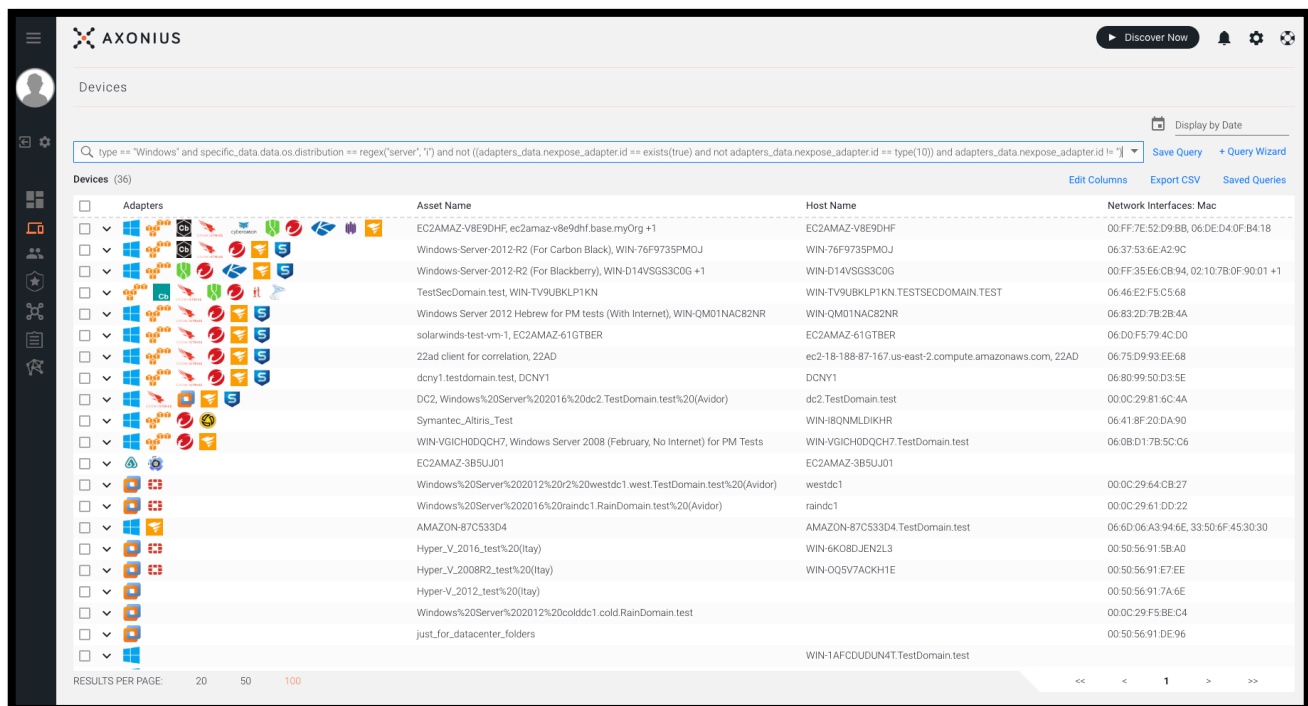
But you would then need to alert a person to deploy the missing agent on each machine. At larger organizations, this is just too much manual work.

The Solution: Cybersecurity Asset Management

By connecting to the different solutions that manage devices and users and correlating information, a cybersecurity asset management solution provides ongoing security policy validation and enforcement.

ONGOING SECURITY POLICY VALIDATION

1. **Creating a comprehensive asset inventory** - With a comprehensive and always up-to-date asset inventory, customers have a complete picture of the intersection of devices, users, and security solutions.
 - a. **Devices** - For example, show me any unmanaged devices or devices missing an agent.
 - b. **Users** - Show me all AD-enabled users with passwords set to never expire.
 - c. **Security Solutions** - Give me a list of all assets not being scanned by my VA tool



| Adapters | Asset Name | Host Name | Network Interfaces: Mac |
|----------|---|---|---|
| | EC2AMAZ-V8E9DHF; ec2amaz-v8e9dhf.base.myOrg +1 | EC2AMAZ-V8E9DHF | 00:FF:7E:52:D9:8B, 06:DE:D4:0F:B4:18 |
| | Windows-Server-2012-R2 (For Carbon Black), WIN-76F9735PMOJ | WIN-76F9735PMOJ | 06:37:53:6E:A2:9C |
| | Windows-Server-2012-R2 (For BlackBerry), WIN-D14VSGS3C0G +1 | WIN-D14VSGS3C0G | 00:FF:35:E6:C8:94, 02:10:7B:0F:90:01 +1 |
| | TestSecDomain.test, WIN-TV9UBKLP1KN | WIN-TV9UBKLP1KN.TESTSECDOMAIN.TEST | 06:46:E2:F5:C5:68 |
| | Windows Server 2012 Hebrew for PM tests (With Internet), WIN-QM01NAC82NR | WIN-QM01NAC82NR | 06:83:2D:7B:2B:4A |
| | solarwinds-test-vm-1, EC2AMAZ-61GTBER | EC2AMAZ-61GTBER | 06:D0:F5:79:4C:D0 |
| | 22ad client for correlation, 22AD | ec2-18-188-87-167.us-east-2.compute.amazonaws.com, 22AD | 06:75:D9:93:EE:68 |
| | dcny1.testdomain.test, DCNY1 | DCNY1 | 06:80:99:50:D3:5E |
| | DC2, Windows%20Server%202016%20dc2.TestDomain.test%20(Avidor) | dc2.TestDomain.test | 00:0C:29:81:6C:4A |
| | Symantec_Altiris_Test | WIN-18QNMLDIK1HR | 06:41:8F:20:DA:90 |
| | WIN-VGICH0DQCH7, Windows Server 2008 (February, No Internet) for PM Tests | WIN-VGICH0DQCH7.TestDomain.test | 06:0B:D1:7B:5C:C6 |
| | EC2AMAZ-3BSUJ01 | EC2AMAZ-3BSUJ01 | |
| | Windows%20Server%202012%20r2%20westdc1.west.TestDomain.test%20(Avidor) | westdc1 | 00:0C:29:64:C8:27 |
| | Windows%20Server%202016%20raindc1.RainDomain.test%20(Avidor) | raindc1 | 00:0C:29:61:DD:22 |
| | AMAZON-87C533D4 | AMAZON-87C533D4.TestDomain.test | 06:6D:06:A3:94:6E, 33:50:6F:45:30:30 |
| | Hyper_V_2016_test%20(Itay) | WIN-6K08DUJEN2L3 | 00:50:56:91:5B:A0 |
| | Hyper_V_2008R2_test%20(Itay) | WIN-OQSV7ACKH1E | 00:50:56:91:E7:EE |
| | Hyper_V_2012_test%20(Itay) | | 00:50:56:91:7A:6E |
| | Windows%20Server%202012%20coldcd1.cold.RainDomain.test | | 00:0C:29:F5:BE:C4 |
| | just_for_datacenter_folders | | 00:50:56:91:DE:96 |
| | | WIN-1AFCDUDUN4T.TestDomain.test | |

A list of assets not scanned by a VA tool

Customer Example: 100% of Axonius customers find unknown devices in the initial deployment phase and are able to identify assets that do not adhere to their security policy as they come online.



2. **Alert when assets do not adhere to policy** – An asset inventory is valuable, but security teams want to know when a change takes place where a user or device no longer adheres to the security policy.

For example:

- A. **Devices** – Tell me any time a new IoT devices is connected to the network.
- B. **Users** – Let me know any time a user has been granted admin privileges.
- C. **Security Solutions** – Tell me when an EPP agent has stopped sending back data.

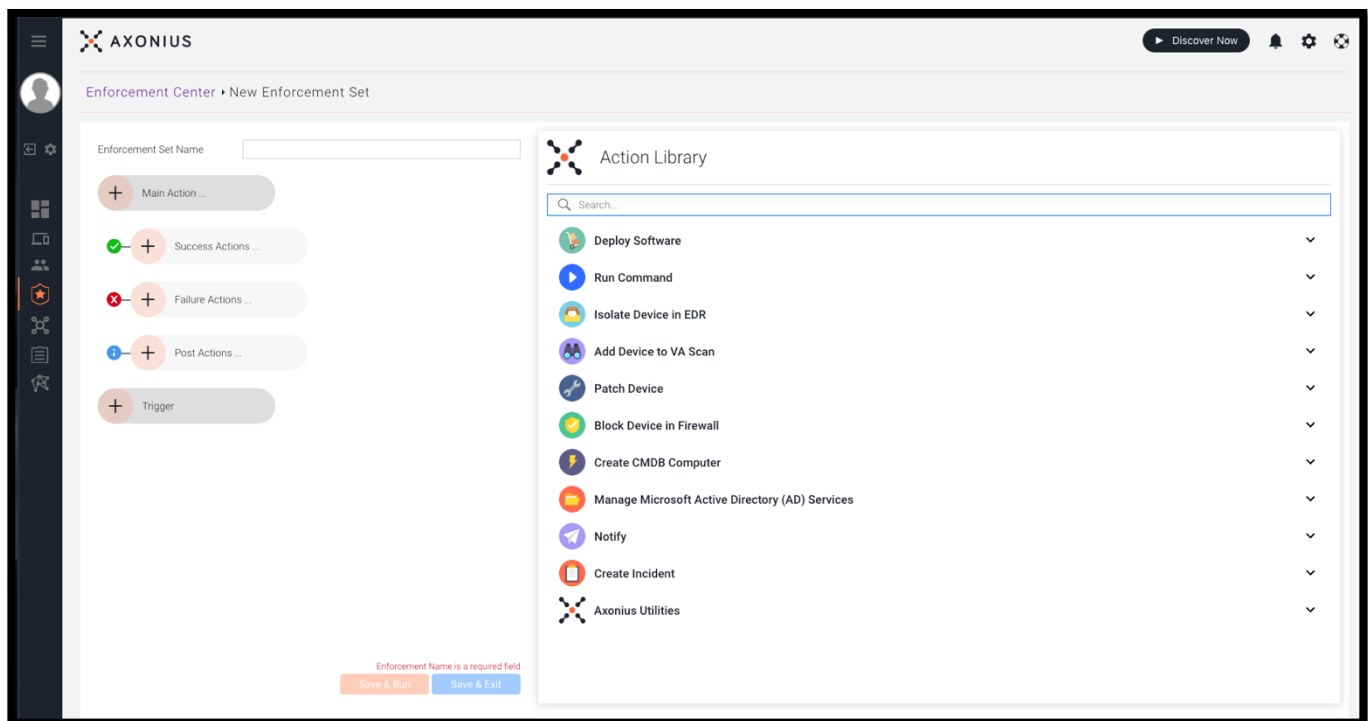
The screenshot shows a web interface for creating a ServiceNow incident. The title bar reads 'Action Library / Create ServiceNow Incident per Entity'. Below the title, there is a text input field for 'Action Name:'. A 'Configuration' section follows, containing several optional fields: 'Use ServiceNow Adapter' (checkbox), 'ServiceNow Domain', 'User Name', 'Password', 'Verify SSL' (checked checkbox), and 'HTTPS Proxy'. Below these is an 'Incident Short Description' text area and a 'Message Severity' dropdown menu currently set to 'info'. A red error message 'Action Name is a required field' is visible near the bottom right. A blue 'Save' button is at the bottom right corner of the form.

An example of an incident, which can be sent to a ticketing system.

Customer Example: Many Axonius customers use the alerting features to both enhance a CMDB and to enhance alerts generated from other systems.

AUTOMATED SECURITY POLICY ENFORCEMENT

In addition to the inventory and alerting capabilities, customers using a cybersecurity asset management platform are able to turn queries into action, letting them decide the level of automation that makes sense in their environments.



The Security Policy Enforcement Center in Axonius

1. [Create trigger-based policy enforcement sets](#) – Enforcement actions are triggered by any saved query, and can perform actions like:
 - a. Deploy Software – If a device is missing an agent, deploy the missing agent
 - b. Run a Command – Tell a Windows machine to fetch an update
 - c. Isolate Devices in EDR – If a device isn't meeting policy (for example, a laptop with a critical vulnerability), use the installed EDR to isolate it from a production network
 - d. Add Device to a VA Scan – If an Amazon instance isn't being scanned by a VA scanner, add it to the next scheduled scan
 - e. Patch Device – Patch a machine that has an update available
 - f. Block Device in Firewall – Use the firewall as the mechanism to keep a vulnerable device out of a critical VLAN
 - g. Create a CMDB Entry – Add detailed device info to a CMDB
 - h. Manage AD Services – Add or edit AD Services
 - i. Notify – Send an email or slack message
 - j. Create an Incident – File a ticket for someone to act on



AXONIUS

Customer Example: To enhance SOC investigations, Axonius provides contextual information to enhance alerts, drastically decreasing the time spent trying to understand the meaning behind alerts. One customer was able to quantify the value from just a single use case: Dramatically decreasing the time spent getting device context from SIEM alerts.

Mean Time to Inventory Value

To understand the value of decreased MTTI, we use the following calculation:

(Minutes spent gathering contextual information * # of incidents) * pay rate = MTTI Cost

For example, if it takes 10 minutes/incident to gather context, and there are 10 incidents a day, with an analyst making \$100,000 per year:

$10 \times 10 = 100$ minutes or 1 hour and 40 minutes per day

\$100,000 at 8 hours/day 5 days/week for 50 weeks per year = \$50/hour

\$83/day spent on gathering context or \$93,750 per year

If you were to decrease MTTI from 15 to 3 minutes:

$3 \times 20 = 60$ minutes or 1 hour per day

\$75/day spent on gathering context or \$18,750

Dollars Saved: \$75,000

Ultimate Value: Decreased Risk

Any security solution must be judged by decreased risk. By enabling ongoing security policy validation and decreasing mean time to inventory, customers decrease their risk profile by:

- 1. Understanding what they have**
- 2. Understanding the coverage gaps and addressing solutions that have been purchased but not fully deployed**
- 3. Validating what is properly protected**
- 4. Getting alerted when anything changes**
- 5. Creating automated action sets to ensure security policy adherence**
- 6. Lowering mean time to inventory and subsequently resolving incidents faster**

We hope that this document has presented a clear business case for evaluating a cybersecurity asset management solution like Axonius. We believe that our platform can provide tremendous value today, and it will only continue to grow as we invest in its functionality. We encourage any and all questions and comments, as our mission is to create a product that can significantly increase the productivity and security of our customers. Simply selling a product that sits on the shelf doesn't get us excited to go to work in the morning.

About Axonius

Axonius is the only [cybersecurity asset management platform](#) that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with more than 120 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately. Covering millions of devices at customers like the New York Times, Schneider Electric, and AppsFlyer, Axonius was named the Most Innovative Startup of 2019 at the prestigious RSAC Innovation Sandbox and was named Rookie Security Company of the Year by SC Magazine. For more visit [Axonius.com](#)

Get Started

Because it integrates natively with [over 120 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 here](#).

Support and Questions

We are committed to helping our customers deploy, configure, and start seeing value immediately. You can view our [getting started documentation here](#). Should you have any questions, concerns, or product feedback, please do not hesitate to [contact Axonius](#) 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.