AXONIUS

Why Does Asset Management Matter for Cybersecurity?

November 2019

OVERVIEW

The line between IT and Security is blurring. What was once a simple delineation between keeping information safe and providing the tools necessary to get work done is no longer clear. In this short paper, we'll look at why asset management – once a pure IT play – matters for cybersecurity, and how both IT and security teams can benefit from cybersecurity asset management.

Table of Contents.

What Do We Mean by "IT Asset Management"?

When we look at what has been traditionally called "IT Asset Management", we're referring to a set of practices surrounding the financial, inventory, contractual, and lifecycle management of an IT asset. In this case, an "IT asset" is really any device or cloud instance that is used for business purposes. Some of the responsibilities of an IT Asset Management program would include:

1. Inventory – Getting a detailed inventory of all hardware, software, and network assets
2. License Management – Making sure that all assets are running properly licensed software
3. Lifecycle Management – Deciding which assets should be decommissioned and managing the software licenses on these assets and updating the inventory

Using the traditional definition, IT Asset Management would fall squarely in the hands of the IT and Desktop Support teams. However, the process of gathering data about every asset and understanding what software is running is critical and foundational to cybersecurity.

In this paper, we'll look at what we call "Cybersecurity Asset Management" or the process of:

1. Gathering data from any source that provides detailed information about assets
2. Correlating that data to produce a view of every asset and what is on it
3. Continually validating every asset's adherence to the overall security policy
4. Creating automatic, triggered actions whenever an asset deviates from the policy

In this context, Cybersecurity Asset Management or "Modern Asset Management" becomes the nexus for cybersecurity projects and decisions.

Asset Management and Endpoint Protection.

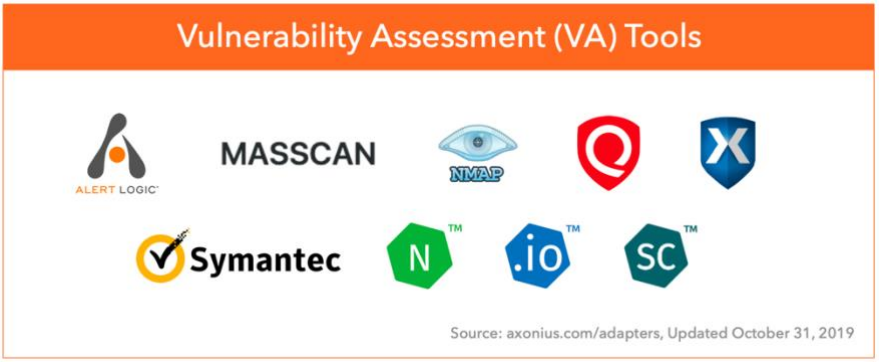
When it comes to endpoint security, we have access to an amazing array of tools. From next-generation AV to cloud and AI-based EPP/EDR products, there are a staggering number of tools to choose from, and organizations spend millions to protect their endpoints.

Despite how effective these endpoint protection tools can be, there are fundamental challenges that arise which can only be answered by asset management:

1. Which assets are missing an endpoint agent?
2. Which assets have the agent installed, but the agent isn't functioning properly?

The only way to find assets missing an agent or with an agent *not working* is through gathering data from multiple sources. Asking the agent console "which devices are missing your agent?" won't work, as EPP/EDR tools do not know which devices exist that should have the agent installed.

Asset Management and Vulnerability Management.



Today's vulnerability assessment tools do an incredible job of identifying known vulnerabilities present in the devices they're aware of. But how can we ensure that all assets — including workstations, laptops, virtual machines, and other IT assets — are being scanned?

To understand which assets are not covered by VA tools, we must gather data from:

1. The VA Scanner Console – To see all assets that are known and being scanned
2. IAM Solutions – Sources like AD or Azure AD that authenticate and authorize users and devices
3. Network/Infrastructure Data – To see all assets known to the network but aren't being scanned

Only when you can understand all assets, and compare all to those being scanned, can you uncover the difference to see any asset *not* being scanned by a VA tool.

Asset Management and Cloud Security.

When it comes to cloud workloads, many of the tools we use to secure our on-premise devices don't apply. The dynamic, ephemeral nature of the cloud makes it difficult for some security tools to know when a new instance has been spawned that needs attention.

Like the example on the right, VA scanners face challenges with cloud instances. With dynamic IPs, VA tools can't predict where a new instance will pop up, and they can't scan what they don't know. Instead, we must gather data from:

1. The VA Scanner Console – To see all instances that are known and being scanned
2. The Cloud Infrastructure Console – To see all instances in the environment

Another example is finding cloud instances with public IPs and known to sources like Shodan. Again, only by collecting and correlating data from multiple sources can we understand which cloud instances are not being covered by our VA tools and what is known publicly about them.

#	Bucket
1	016.s3-eu-west-1.amazonaws.com
2	storage.test.s3-eu-west-1.amazonaws.com
3	image.lalaegitim.com.s3.eu-central-1.amazonaws.com
4	tempdev.s3-us-west-2.amazonaws.com
5	01501.s3-us-west-2.amazonaws.com
6	01862.s3-us-west-2.amazonaws.com
7	svn.s3-ap-southeast-1.amazonaws.com
8	website-bot.s3-eu-west-1.amazonaws.com
9	screenshotstest.s3.us-east-2.amazonaws.com

Example of exposed S3 buckets on GrayHatWarFare.com

Asset Management and Incident Response.

When an Incident Response (IR) analyst receives an alert about an asset, several questions immediately come to mind:

By looking at all that is known about the asset in question – with information from many different data sources – security analysts can quickly gather the context and detail needed to inform their investigation. They can get information on:

1. The OS and patch level
2. All other installed software
3. Known vulnerabilities
4. Agent coverage and health
5. Users and admins that have logged in
6. Available patches
7. Historical information and changes over time

Asset Management and Continuous Controls Monitoring.

In addition to the examples cited, it's essential to know any time an asset stops adhering to the overall security policy. Security teams need an automated way to learn when:

1. An endpoint is missing a security agent, or the agent stops working
2. An asset isn't being scanned by a VA tool
3. A cloud instance isn't covered and is publicly accessible
4. An endpoint has known and/or critical vulnerabilities
5. A user has improper access rights

Quarterly audits simply aren't enough to catch these issues in a dynamic, ever-changing environment. Only by having an automated process to detect changes that bring assets out of policy can you truly know that the security policy is being adhered to at any given moment.

Asset Management and Security Policy Enforcement.

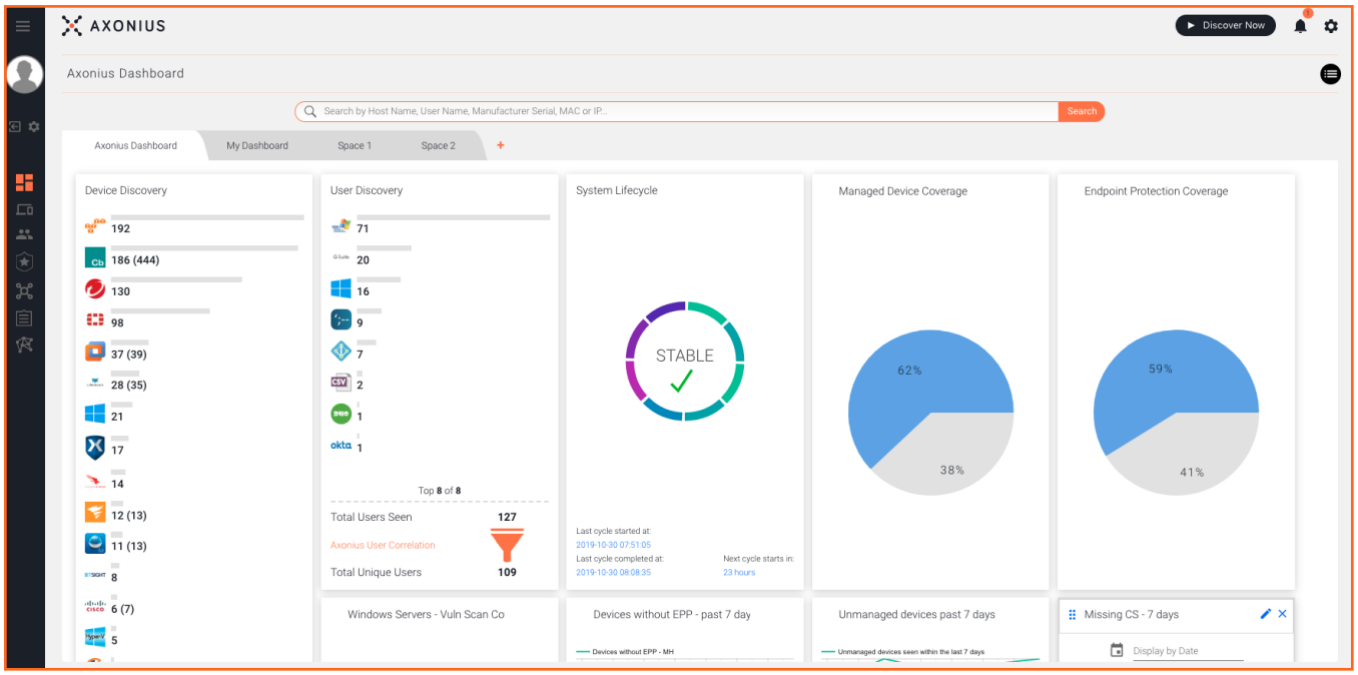
Finally, knowing when an asset is out of policy is important, but this only matters if you have the resources to do something about it. Since cybersecurity asset management works by connecting to all the security and management solutions that know about assets, you can then use those same sources to remediate issues.

For example:

1. If an endpoint is missing an agent, you can use a solution like WMI or Tanium to install the missing agent on any endpoint
2. If an asset or cloud instance is unknown to a VA scanner, tell the VA scanner to add it to the next scheduled scan
3. If an asset has a critical vulnerability, apply the patch automatically

These are just a few examples of the automated actions that can be triggered using the tools that already exist in your environment.

About Axonius.



Axonius is the 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 over 200 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, Landmark Health, AppsFlyer, and many more, Axonius was named the Most Innovative Startup of 2019 at the prestigious RSAC Innovation Sandbox and was named to the CNBC Upstart 100 list and Forbes 20 Rising Stars.

For more information, please visit Axonius.com.

Get a Demo.