EBOOK

Why Does **Asset Management** Matter for Federal **Cybersecurity?**

AXONIUS

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.

Read on for a look at why asset management – once a pure IT play – matters for cybersecurity, and how federal IT and security teams can both benefit from cybersecurity asset management.

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 to support the agency's mission.

Some of the responsibilities of an IT asset management program would include:

ASSET INVENTORY – Getting a detailed inventory of all hardware, software, and network assets

LICENSE MANAGEMENT – Making sure that all assets are running properly licensed software

LIFECYCLE MANAGEMENT – Deciding which assets should be decommissioned, and managing the software licenses on these assets and updating the inventory

AXONIUS

Using the traditional definition, IT asset management would fall squarely in the hands of the IT service desk. But the process of gathering data about every asset and understanding what software is running is critical and foundational to cybersecurity in the government.

IN THIS EBOOK, WE'LL LOOK AT WHAT WE CALL "CYBERSECURITY ASSET MANAGEMENT" – OR THE PROCESS OF:

01 ***Gathering data*** from any source that provides detailed information about assets

02 Correlating that data to ***produce a view of every asset*** and what is on it

03 ***Continually validating*** every asset's adherence to the overall security policy

04 ***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 & 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 and can only be answered by asset management.

WHICH ASSETS ARE MISSING AN ENDPOINT AGENT?

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 by gathering data from multiple sources. Asking the agent console, **"Which devices are missing your agent?"** won't work, as EPP/EDR tools don't know which devices exist that should have the agent installed.

ASSET MANAGEMENT & 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:

THE VA SCANNER CONSOLE – to see all instances that are known and being scanned

IAM SOLUTIONS – Sources like AD or Azure AD that authenticate and authorize users and devices

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** and see any asset not being scanned by a VA tool.

AXONIUS

ASSET MANAGEMENT & CLOUD SECURITY

ASSET MANAGEMENT & CLOUD SECURITY
ASSET MANAGEMENT & 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.

ASSET MANAGEMENT & CLOUD SECURITY

VULNERABILITY ASSESSMENT & THE CLOUD

Unlike on-premise machines, 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:

01 ***The VA scanning console*** **-** To see all instances that are known and being scanned

02 ***The cloud infrastructure console*** **-** To see all instances in the environment

Now, with 50 percent of government organizations using the cloud [1], ***visibility into cloud security coverage gaps is needed more than ever before.***

Solving the cloud VA coverage gap relies on understanding every time a new instance is spawned, and letting the vulnerability scanner know that there's a new machine to add to its scan schedule.

1 Gartner via Hosting Tribunal: https://hostingtribunal.com/blog/cloud-adoption-statistics/#gref

ASSET MANAGEMENT & CLOUD SECURITY

ACCESS MISCONFIGURATION & THE CLOUD

Another common cloud asset management challenge is access misconfiguration.

Nearly every day, there's a new story about the latest breach or leak as a result of a misconfigured cloud instance. The nature of the cloud means that anything can be publicly available. One change to a configuration detail can make sensitive data available to sources like Shodan and Grey Hat Warfare.

To ensure all public cloud workloads are properly configured, security and IT teams must continuously monitor changes to configuration details and understand the context and risk of any change at scale.

ASSET MANAGEMENT & CLOUD SECURITY

ASSET MANAGEMENT & CLOUD SECURITY

CLOUD ASSET COMPLIANCE

Government cloud providers are held to FedRAMP and ITAR guidelines to ensure they meet security and compliance requirements. Agencies often look for additional guidance and frameworks on cloud security from NIST and CISA to understand their cybersecurity maturity and identify areas where they can strengthen their security posture. The Center for Internet Security (CIS) also provides objective, consensus-driven security guidelines and specific scored rules for public cloud infrastructure, including:

- ***CIS Amazon Web Services Foundations Benchmark 1.3.0***
- ***CIS Microsoft Azure Foundations Benchmark version 1.2.0***
- ***CIS Google Cloud Platform Foundation Benchmark version 1.1.0***
- ***CIS Oracle Cloud Infrastructure Foundations Benchmark version 1.1.0***

By comparing all public cloud workloads in their environments to the ***scored rules in the CIS benchmarks*** for individual cloud providers, security teams are able to understand any time an instance deviates from best practices.

ASSET MANAGEMENT & INCIDENT RESPONSE

When an **incident response (IR) analyst** receives an alert about an asset, several questions immediately come to mind.

1. IS THE ASSET "KNOWN" AND MANAGED?
2. WHERE IS IT?
3. WHAT IS IT?
1. IS THE CORE SOFTWARE UP-TO-DATE?
5. WHAT ADDITIONAL SOFTWARE IS INSTALLED?
6. DOES IT ADHERE TO MY SECURITY POLICY?

AXONIUS

ASSET MANAGEMENT & INCIDENT RESPONSE
ASSET MANAGEMENT & INCIDENT RESPONSE

ASSET MANAGEMENT & INCIDENT RESPONSE

Agencies can start by looking at all that's 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 and aid in incident response coordination efforts with NCCIC, the NCIRP, and other federal cyber organizations. They can get information on:

01 The OS and patch level

02 All other installed software

03 Known vulnerabilities

04 Agent coverage and health

05 Users and admins who have logged in

06 Available patches

07 Historical information and changes over time

ASSET MANAGEMENT & CONTINUOUS CONTROLS MONITORING
ASSET MANAGEMENT & CONTINUOUS CONTROLS MONITORING

ASSET MANAGEMENT & CONTINUOUS CONTROLS MONITORING

Along with the examples cited and in accordance with NIST SP 800-137, 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:

01 **AN ENDPOINT IS MISSING A SECURITY AGENT,** or the agent stops working

02 **AN ASSET ISN'T BEING SCANNED** by a VA tool

03 **A CLOUD INSTANCE ISN'T COVERED** or has become publicly accessible

04 An endpoint has known and/or **CRITICAL VULNERABILITIES**

05 A user has **IMPROPER ACCESS RIGHTS**

In a dynamic, ever-changing environment, quarterly audits simply aren't enough to catch these issues. 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.

AXONIUS

ASSET MANAGEMENT & 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.

IF AN ENDPOINT IS MISSING AN AGENT, you can use a solution like WMI or Crowdstrike to install the missing agent on any endpoint

IF AN ASSET IS MISSING FROM A CMDB or has inaccurate information, update the CMDB entry

IF AN ASSET OR CLOUD INSTANCE IS UNKNOWN to a VA scanner, tell the VA scanner to add it to the next scheduled scan

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.

AXONIUS

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 300 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

330 MADISON AVE., 39TH FLOOR
NEW YORK, NY 10017
INFO@AXONIUS.COM

See your assets in context, validate security policy compliance, and automate remediation with the Axonius Cybersecurity Asset Management Platform.

SEE IT FOR YOURSELF