AXONIUS

AXONIUS
WHITE PAPER

WHY ASSET MANAGEMENT FAILS FOR CYBERSECURITY

(AND HOW TO FIX IT)

YOU'D HAVE MULTIPLE SYSTEMS THAT KNOW SOMETHING ABOUT ALL YOUR ASSETS, LIKE AN ANTIVIRUS – OR AT LEAST WHAT YOU THOUGHT WAS ALL YOUR ASSETS... IT WAS TOUGH TO KNOW WHETHER OR NOT EVERYTHING WAS FULLY PROTECTED.

- MIKE CONROY

ASSISTANT MANAGER OF INFORMATION SECURITY RISK MANAGEMENT, DCU

We know asset management is foundational to cybersecurity. Without an accurate understanding of everything in your environment, all other initiatives suffer.

But as IT complexity rises – gaining visibility across diverse types of assets requires an approach that automatically and continuously discovers assets in their environment.

Many of the tools used today offer individual pieces of the asset puzzle. The information needed still lives in many different silos.

Plus, traditional asset inventory approaches are manual, error-prone, and time consuming. And as soon as an inventory is manually compiled, it quickly becomes outdated.

It doesn't have to be this way, though. All the data you need already exists – and the solutions that know about your assets have APIs. You just need a way to collect, correlate, and take action.

READ ON TO LEARN:

- Why asset management for cybersecurity is foundational to an array of security use cases
- The asset management challenges associated with these use cases and how they impact cybersecurity
- How to solve each use case with asset management for cybersecurity

86	***Hours of labor*** **needed to compile a manual asset inventory**	**64%**	***Organizations*** approaching asset inventory as a monthly or quarterly event
72%	***Organizations*** reporting increased IT complexity in the past two years	**82%**	***Organizations*** planning to increase asset inventory investment

Source: "Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-pandemic Security Priorities." Axonius and Enterprise Strategy Group. 2021.

USE CASE: DEVICE DISCOVERY

Device discovery is the process of discovering and collecting data on the assets (devices, users, software, and cloud instances) connected to a network for management, tracking, and security purposes.

But with so many connected devices both on a network and remote, gaining a credible and comprehensive asset inventory can quickly become a daunting task.

UNMANAGED DEVICES

Unmanaged devices are IP-connected devices that may or may not be known and accounted for in an asset inventory. They aren't being actively managed from an IT and security perspective and are only known to the network or network scanners.

Examples include IoT and smart devices, connected printers, and personal mobile devices.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Your security tools can only protect the assets they know about.

When it comes to finding the "unknown unknowns," asking Active Directory (AD) to show any unmanaged device doesn't work. Manually comparing AD data, network management, and endpoint security software is tedious and error-prone.

If a device is unmanaged, it's impossible to know if it's secure. Data from the network infrastructure or network scanners, often limited to just an IP address, doesn't yield adequate details.

The first step in securing, managing, segmenting, and controlling any device is understanding the nature of the device and its context.

HOW TO FIND UNMANAGED DEVICES

Finding unmanaged devices includes:

01 ***Gathering and comparing data*** from the network, IAM solutions, device management consoles, and endpoint security solutions

02 ***Mapping out the overlap and gaps*** between those devices that have accessed network resources and those that have an agent installed

03 For devices without an agent, ***identifying the device context*** and filtering out those that can't have an agent installed

04 ***Aggregating your list of unmanaged devices*** that should be managed, prioritizing agent and management system deployment and coverage

For more detailed information, read Finding Unmanaged Devices.

For ultimate efficiency, you'll need a process that continuously monitors for new, unmanaged devices.

EPHEMERAL DEVICES

Now let's look at ephemeral devices – or those that last for a short period of time. Many of these devices are authorized and a normal part of operational workflows. But that doesn't make them easy to manage.

It's usually tough for security, networking, and risk teams to identify their presence in real time. Examples include virtual machines, containers, cloud workloads, and certain unmanaged devices.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Given its transient nature, an ephemeral device is usually unaccounted for in asset inventories created using traditional methods.

Assessing the state of a past ephemeral asset is also a challenge for IT and security teams.

Since scans are performed in cycles, scanning tools fail to find many ephemeral devices. Agent-based approaches also fall short, as these devices never have an agent deployed to begin with. And network-based tools often lack the contextual data points needed to identify these devices.

The result? Massive ephemeral device visibility gaps.

Left unmanaged, ephemeral devices drive up an organization's attack surface. Security teams need to ensure that these devices have been patched, critical data is encrypted, and security agents have been deployed on the device, when possible.

HOW TO FIND EPHEMERAL DEVICES

To find ephemeral devices, you need to connect the sources of where devices are created and deprecated.

Tools built for cybersecurity asset management can offer continuous asset discovery capabilities to identify and manage ephemeral devices. This is done by connecting to the management consoles of platforms where these short-lived devices are created.

For more detailed information, read Finding Ephemeral Devices.

USE CASE: ENDPOINT PROTECTION

Your organization has likely implemented several endpoint protection tools. But endpoint detection and response consoles can't answer questions like:

- Which devices aren't protected but should be?
- Where are devices that have the agent installed, but the agent isn't sending back data to the console?

ENDPOINTS MISSING AGENTS

While organizations mandate that specified devices must be covered by a certain endpoint agent (example: Windows devices need CrowdStrike or Macs need Jamf), we've found that some customers have as many as **60% of devices that are missing the requisite agent.**

Agents generally run continuously and silently in the background, gathering data about the state of the device. Examples include security agents, configuration management agents, or other lightweight applications installed at the OS level on a corporate endpoint.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Accessing the admin console of the agent produces a list of covered devices. The real challenge lies in uncovering devices that should have the recommended agent, but don't.

Part of the challenge in knowing which assets are missing endpoint agents? Device discovery. *(How does an EPP/EDR solution identify a new device that exists and should be protected?)*

The other issue is based on the context of the security policy. *(If your security policy requires one endpoint agent for PCs and another for Macs, how can you find the device, understand its context, and ensure the right agent is installed to meet the policy?)*

Unmanaged devices can be difficult to pin down. But without knowing whether all relevant devices are covered, it's impossible to be confident that you're really protected.

HOW TO FIND DEVICES MISSING AGENTS

To find devices missing agents, you'll need to compare data from IAM, device management, and endpoint security solutions.

Using this data, you'll need to understand:

01 ***Which devices/types*** should have a certain agent installed

02 Which devices have the ***correct agent installed***

03 ***The delta*** between those

For more detailed information, read Finding Endpoints Missing Agents.

DEVICES WITH MALFUNCTIONING AGENTS

Now let's look at why it's necessary to find devices that have the required agent installed, but it's either inactive or not sending back data as expected.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Logging into the admin console of any agent-based solution gives you a list of devices on which the agent is installed. But you won't be able to see if the agent has been turned off, if it was uninstalled by the user, or if it's not functioning correctly.

And if you stop once you know which devices have an agent installed? You won't be able to account for cases where the agent is there, but isn't working properly.

HOW TO FIND DEVICES WITH MALFUNCTIONING AGENTS

To find devices with malfunctioning agents:

01 ***Look at the agent console*** to get the information on those devices with an agent installed

02 ***Get the subset of devices*** with a "stale" last seen date

If a device that has the agent installed hasn't transmitted data to the agent console in 30 days, but has been seen by AD or another agent console in the last week, it's safe to assume the device's agent is either off or malfunctioning.

For more detailed information, read Finding Endpoint Agents Not Functioning Correctly.

USE CASE: VULNERABILITY MANAGEMENT
USE CASE: VULNERABILITY MANAGEMENT

USE CASE: VULNERABILITY MANAGEMENT

Every system — even the most advanced and well protected — is inherently vulnerable. And most organizations have more vulnerabilities than they could possibly remediate.

The mismatch between vulnerabilities and resource capacity means that organizations have to prioritize which vulnerabilities to address.

And prioritization is a conscious decision about what you're willing to ignore.

DEVICES NOT BEING SCANNED FOR VULNERABILITIES

Vulnerability assessment tools do an incredible job of identifying known vulnerabilities present on devices they're aware of. But how can you ensure that all devices, including VMs and cloud instances, are being scanned?

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Understanding which devices are covered by a specific VA scanner is as simple as accessing the admin console, which offers a list of covered devices.

The problem lies in knowing which devices should be scanned but are not part of the VA scan schedule.

Put simply, devices not being scanned for vulnerabilities are at risk of being exploited.

HOW TO FIND DEVICES NOT BEING SCANNED FOR VULNERABILITIES

To find devices not being scanned for vulnerabilities:

01 ***Gather data from different sources,*** including VA scanner console, network, IAM solutions, and cloud infrastructure

02 ***Aggregate and correlate it*** to understand which of your devices, cloud instances, and VMs aren't part of the VA scan schedule

It's best to compare two or more trustworthy data sources to help identify gaps.

For more detailed information, read Finding Devices Not Being Scanned for Vulnerabilities. Then, watch "Building the Foundation for a Scalable Vulnerability Management Program" to understand how to prioritize vulnerabilities by CVEs.

USE CASE: CLOUD SECURITY AND CONFIGURATION
USE CASE: CLOUD SECURITY AND CONFIGURATION

USE CASE: CLOUD SECURITY AND CONFIGURATION

While the move to public cloud was already well under way, the pandemic further accelerated the use of cloud-delivered productivity and collaboration tools. In fact, 87% of organizations say that the pandemic has accelerated public cloud adoption.[1]

However, with cloud misconfigurations, overly permissive access rights, and publicly available data, many organizations struggle to secure all cloud instances.

CLOUD INSTANCES NOT BEING SCANNED FOR VULNERABILITIES

What do we mean by cloud instances not being scanned for vulnerabilities? We're referring to public cloud infrastructure services, like those from AWS, Google Cloud, and Microsoft Azure, that organizations want to scan for known vulnerabilities.

Cloud vulnerabilities are similar to those in traditional architectures. But the cloud characteristics of shared tenancy and potential ubiquitous access increases the risk of exploitation by threat actors.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Today's assessment tools do an excellent job of recognizing known vulnerabilities. But the elastic and ephemeral nature of cloud computing means cloud workloads can be spun up and down without security tools knowing about them.

This means tools like VA scanners are often unaware of any new instances to scan, making these instances prone to known vulnerabilities.

Cloud instances not being scanned are at risk of being exploited. Publicly accessible cloud instances not being scanned add another layer of risk.

[1] *"Cybersecurity Asset Management Trends 2021: How the Rapid Shift to Remote Work Impacted IT Complexity and Post-pandemic Security Priorities." Axonius and Enterprise Strategy Group. 2021.*

HOW TO FIND CLOUD INSTANCES NOT SCANNED FOR VULNERABILITIES

To find cloud instances not being scanned by a VA scanner:

01 ***Look to the public cloud infrastructure provider(s)*** to get the full list of all active instances

02 ***Review VA scanner coverage*** to find all IPs that are part of the scan schedule

03 ***Use that information*** to find active cloud instances unknown to your VA scanner

You'll need to repeat these same steps for every cloud provider and scan-based tool, and run the same process for every new cloud instance.

For more detailed information, read Discovering Cloud Instances Not Being Scanned for Vulnerabilities.

MISCONFIGURED CLOUD WORKLOADS

Now let's look at misconfigured cloud workloads or those not adhering to best practices. To ensure your cloud instances are properly secured, frameworks like the CIS Foundations Benchmarks provides a list of best practices against things like identity and access mangement logging, networking, and monitoring.

Misconfigured cloud workloads are those that fall short of these guidelines.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

Cloud workloads can be — and often are — publicly available. The many configuration customization options of public cloud workloads, coupled with their dynamic nature, makes it hard for security teams to discover when a new cloud instance arises that's also misconfigured and vulnerable.

Since the cloud is public, and cybercriminals can automatically scan for publicly accessible instances, poorly configured cloud instances are an easy target for commodity attacks.

HOW TO FIND MISCONFIGURED CLOUD WORKLOADS

To find cloud workloads not adhering to best practices:

01 ***Gather data*** from cloud infrastructure provider APIs, including settings and configuration options

02 ***Map each configuration setting*** to the scored rules within the CIS Foundations Benchmark for each cloud provider. This will help you see accounts and instances that adhere to or deviate from the mandated rules

For more detailed information, explore how Cloud Asset Compliance can help.

USE CASE: INCIDENT RESPONSE MANAGEMENT

Finding devices that may be associated with an incident can be a daunting task. While security analysts often receive alerts that tell them what happened and how, analysts are forced to spend a lot of time tracking down assets to resolve security incidents.

Security analysts need rich, correlated data on devices, users, and cloud instances to accelerate incident response investigations.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

The analyst who gets the alert likely won't have access to the asset data that would offer valuable context. It can be both manual and time-consuming to:

01 ***Identify*** the data owners

02 ***Understand the systems*** and controls related to the asset

03 ***Get a full view*** of the asset, including its state and risk

An alert is often a harbinger of an incident or breach. The sooner it can be investigated and remediated, the lesser its impact.

HOW TO FIND CONTEXTUAL INFORMATION ABOUT AN ALERT

Finding contextual information about an alert involves:

01 ***Identifying the endpoint*** from the alert

02 ***Gathering data*** from security and management solutions, including agent-based tools, VA scanners, and IAM tools

03 ***Correlating the information*** to understand which tools cover which assets. This reveals patch status, known vulnerabilities, and the overall state of the asset at the time of the alert

Gaining this context helps analysts to accelerate incident response investigations.

For more detailed information, read Accelerate Incident Response Investigations.

USE CASE: GRV AND AUDIT
USE CASE: GRC AND AUDIT

USE CASE: GRC AND AUDIT

Organizations – especially those in regulated industries like finance, government, and healthcare – want to easily satisfy audit and reporting requirements and prove compliance. They need to meet and understand industry benchmarks and regulations while also protecting everything to the best of their ability.

Stale asset inventory information can adversely affect governance, risks, and compliance programs.

THE CHALLENGES AND IMPLICATIONS FOR CYBERSECURITY

One of the most common challenges for organizations when dealing with asset management for compliance and audits is accurately tracking and accounting for all in-scope assets in their environment.

Another challenge? Unifying and analyzing data from disparate sources across the organization.

Many companies today rely on manual processes and spreadsheets to track assets. This trickles down to additional issues around policy validation and enforcement.

A lack of visibility into all assets and how they're configured means it's harder to track and secure these assets, opening organizations to risks and consequences of non-compliance.

Organizations also waste numerous, expensive person-hours of expert resources in preparation and remediation of compliance audits. When the device inventory isn't up-to-date, it affects GRC and audit preparation – and audits tend to have negative results.

HOW ASSET MANAGEMENT FOR CYBERSECURITY CAN HELP

Asset management platforms for cybersecurity can continuously gather an inventory of in-scope assets and help you understand the configuration of each asset.

This is done by aggregating data from different data sources, discovering which devices are unmanaged or misconfigured, and understanding whether every asset adheres to or deviates from security policies.

It provides a single source of truth into all your assets, allowing GRC teams to:

01 ***Streamline*** audits, pen tests, and assessments

02 ***Identify the results*** of compliance initiatives, such as CIS Top 20, NIST, PCI, HIPAA, NDAA, and more

03 ***Continuously monitor*** risks presented from IT assets before, during, and post audits

For more detailed information, read How Asset Management platform can help evaluate compliance with HIPAA and PCI DSS.

SOLVING THE ASSET MANAGEMENT CHALLENGE FOR CYBERSECURITY

For cybersecurity asset management to deliver its full potential, it needs to be automated, continuous, and easy to implement.

A cybersecurity asset management platform integrates with customers' existing security and management tools to get asset details from a variety of data sources. This creates a complete inventory of all assets – whether managed or unmanaged, in the cloud or on premise.

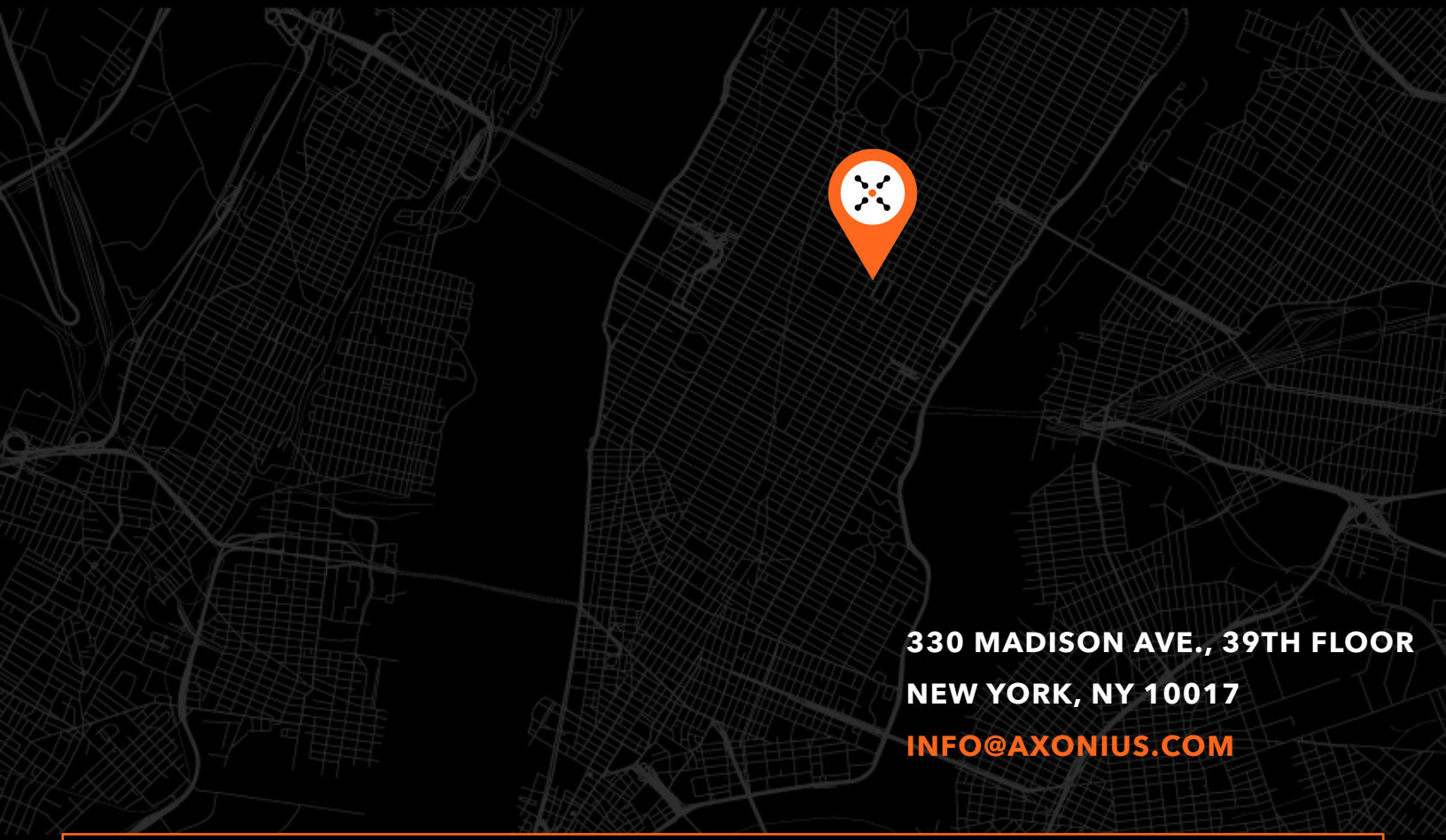
It also helps you take steps to validate security compliance and automate remediation.

Whether you're implementing a cybersecurity asset management solution or building something in-house, the asset management challenges for cybersecurity can be solved by:

- **Gathering data** from sources that know about assets
- **Correlating the data** to ensure that the sources are referring to the same unique device
- **Understanding the relationship** between the asset and the solutions in place to secure and manage them
- **Querying across all data sources** to get answers to questions
- **Running continuous queries** to know any time a new asset appears or changes

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 how you can correlate asset data from existing solutions to provide an always up-to-date inventory, uncover gaps, and automate action with the Axonius Cybersecurity Asset Management Platform.

SEE IT FOR YOURSELF