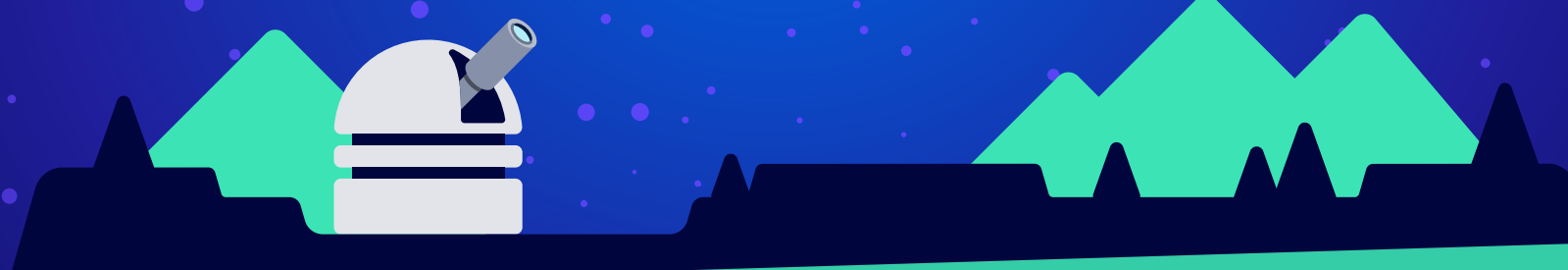


WHITEPAPER

# Modern 'Visibility' for Cybersecurity and IT Asset Management



It's no longer enough to just know where all your assets are. Where it used to be simple, businesses must now reinvent how they track, monitor, and govern a new "cyber asset" collection in order to step up their game to survive in the new, digital world. There is no point in gaining 'visibility' into the asset monster when you don't have the ability to tame it.

The continued adoption of cloud-first and digital transformation strategies has fundamentally changed the way businesses operate. Companies are migrating to new tools, systems, and processes to not only propel their businesses forward, but simply survive in a rapidly changing world, a shift that the recent global pandemic has only exacerbated.

This change presents a unique problem for cybersecurity. As IT assets proliferate beyond devices and increase in both scale and complexity, companies quickly realize that they have created asset monsters within their organizations, ones that are simply too cumbersome to manage.

**Because of this, the security team is having trouble defining what ‘asset visibility’ even means.**

It's no longer enough to just know where all your assets are. Simply seeing the signs doesn't tell us enough of the story. For example, take the 9/11 attacks - all the signals were there. But the dots didn't connect. There was no throughline to understand what those signals represented as risk to our country.

Simply having visibility into the asset monster when you don't have the ability to tame it doesn't help. Companies today don't understand the relationships between assets or how one asset interacts with the broader ecosystem making the asset monster even more powerful and potentially destructive.

Incremental improvements offered by traditional IT asset management (ITAM) are only short term fixes to a fundamental problem. The entire approach to traditional IT asset management needs to evolve to address the ‘visibility’ problem -- enter Modern Cyber Asset Management.

**As IT assets proliferate and increase in both scale and complexity, companies quickly realize that they have created asset monsters within their organizations.**

## The Importance of Traditional IT Asset Management & Its Limitations

[Gartner](#) defines traditional ITAM as “a process that provides an accurate account of technology asset lifecycle costs and risks to maximize the business value of technology strategy, architecture, funding, contractual and sourcing decisions”. In essence, ITAM is a process and/ or tool that helps organizations optimize and track how their assets are deployed, maintained, and used.

Key aspects of ITAM programs often include:

- **Hardware asset management:** managing and optimizing company devices - e.g. laptops, mobile devices, workstations, monitors, servers, and more
- **Software asset management:** managing and optimizing purchase, deployment, maintenance, utilization, and ultimately removal of all software applications within a company
- **Third-party licensing and compliance:** ensuring that the licensing of all hardware and software assets align with set company policies and limit risk exposure

Understanding your asset inventory is a fundamental component of an effective long-term business strategy. However, keeping track of your IT assets is usually a manual, error-prone



process that consumes time and resources with limited upside. **It's not scalable or dynamic**, two attributes that are table stakes to transition from a cost-savings operation to a strategic value-add for the business. Disconnected, inaccurate asset inventory systems inadvertently hide the context of how assets interoperate, giving attackers the advantage to exploit the attack vectors that lurk in the dark.

Existing ITAM tools such as ServiceNow Asset Management, Snipe-IT, AssetCloud, and Blissfully have a limited ability to solve the asset monster problem. And if organizations ignore the fundamentals of ITAM, they'll never reach the more critical goals of their business like optimizing the security of their IT investments.

## The Rise of Software-Defined Cyber Assets

Companies are still trying to segment data across the "Types of IT Assets" you manage or own including:

- On-Premise Software Tools
- Cloud-Based Software Apps
- Employee Hardware
- IT Hardware
- Virtual IT Assets
- Bespoke IT Assets
- Serverless Platform Assets (containers, functions, message queues, etc.)
- Valuable Data or Personal Information (user information, etc)
- Development Resources (code repos, pull requests, commits)

Cloud adoption, digital transformation, and API based infrastructure and security tooling are fundamentally changing how we build, manage, govern, and secure the enterprise. These three shifts in technology necessitate a transition to an modernized definition of cyber asset. Where it used to be simple, businesses must now reinvent how they track, monitor, and govern a new "cyber asset" collection in order to step up their game to survive in the new, digital world.

**In the age of cloud, assets have becoming increasingly more complex; instead, we should redefine all assets as:**

- **Anything you can draw a box around**, specifically any asset that can be software defined. Everything from identities to cloud configurations and repositories fall under this category.
- **More than just IP-based devices**. Limiting assets to those things that are addressable by IP severely limits the depth of understanding that can be built with interconnected relationships.
- **Software defined and ephemeral**. Cyber assets in a modern world don't last long. Actually, if designed properly you want them to come and go as scale dictates.
- **Highly complex relationships that connect people, process, and technology**. The most important part about cyber assets isn't the asset itself, but it's the asset's relationship to every other asset in the collection. This is where the value really resides.

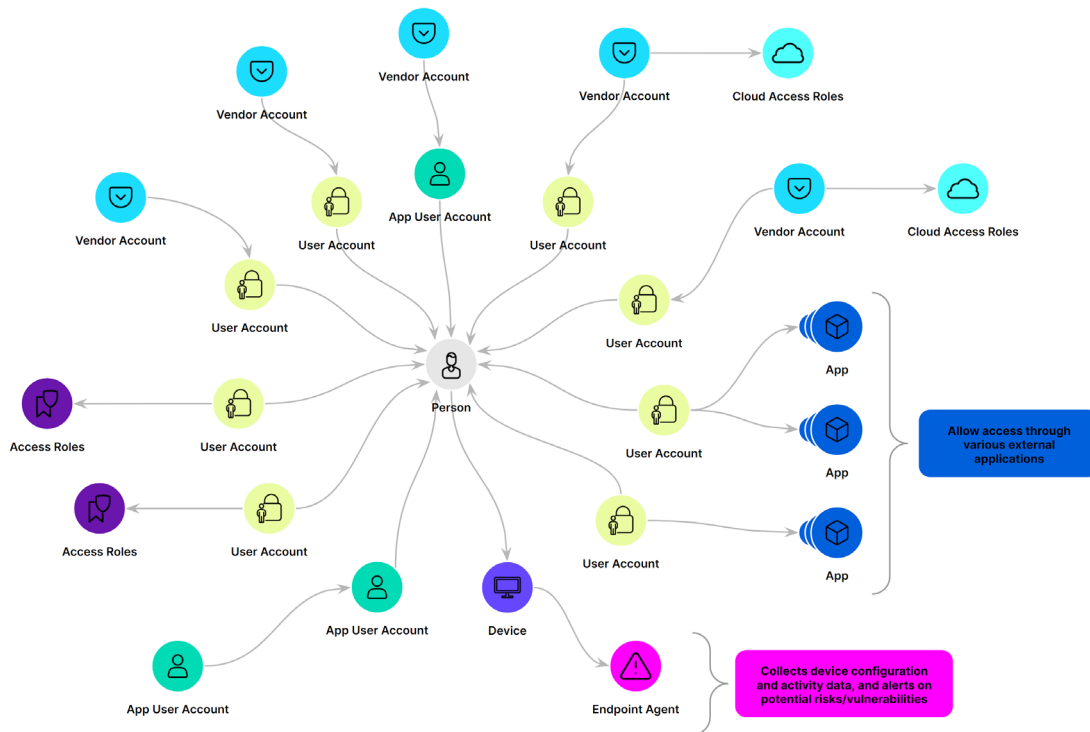
It's time to move on from static lists of asset inventory. Let's start understanding the web of relationships and context of your dynamically changing software-defined cyber assets.

**Where it used to be simple, businesses must now reinvent how they track, monitor, and govern a new "cyber asset" collection in order to step up their game to survive in the new, digital world.**

## Reimagine ITAM - Enter Cyber Asset Management

Asset discovery and management is the foundation to a strong IT program – not only for managing infrastructure costs, but also leading cyber governance, compliance, and engineering efforts within your organization. Assets are what help your business and teams effectively function and best serve your customers.

ITAM has historically focused on managing assets to optimize spend and efficiency. However, with the advent of software-defined cyber assets and the rise of cyber security as a business accelerator, we need a new way to manage cyber assets.



**Cyber asset management is about understanding all of your assets and the context of how they interoperate to strengthen your company’s cyber risk posture and security program.**

Security, compliance, and engineering teams must have access to continuously and dynamically updated views of their entire cyber asset universe and go beyond lists, rows, and columns. Using a single source of truth allows teams to build a graph-based system to explore relationships and make understanding their assets much easier.

By reimagining how we look at the fundamentals, modern cyber asset management helps you:

1. Continuously discover and update an accurate inventory of all cyber assets
2. Understand the context and relationships, and how they interoperate across your asset universe.
3. Understand the true impact and risk of compromised assets
4. Discover security gaps related to the any asset’s configuration or management
5. Automate and continuously govern security policies and compliance to identify gaps in security posture

## Dynamic, Scalable, Cloud-Native Cyber Asset Management

**Cyber asset knowledge gives you power.** In order to secure your enterprise, you need to start with understanding your environment and your asset universe. Visibility is not just about observability, but about complete understanding. This means that your teams should be able to answer questions that matter the most to your business — not just the “What” but also the “So what”.

JupiterOne can help you achieve better cybersecurity asset management with our cloud-native cyber asset management platform by helping you:

**1. Discover all of your software-defined assets.**

*Problem:* Most companies have no visibility into the cyber assets within their environment. You can't secure what you don't know about.

*Solution:* Gain complete visibility so you can truly secure the unknown. JupiterOne gives you visibility in addition to providing your teams with a unified asset inventory and management solution.

**2. Understand your assets through contextual relationships.**

*Problem:* Most companies have no idea how their cyber assets are connected or interoperate with each other. Some solutions can collect data and define and track your assets, but most can't put the relationships and impact of those connections into context, as part of a broader security and IT strategy.

*Solution:* Understanding the relationships between all of your assets forms the fabric for understanding your entire environment. JupiterOne helps you gain deep context via visual graphs and mapping relationships across your entire infrastructure.

**3. Monitor your asset compliance through automated security enforcement.**

*Problem:* In order to create a highly functioning security program, organizations need an automated way to discover and manage cyber assets while aligning the data with their security policies.

*Solution:* Reduce complexity by automating security policy enforcement and avoiding compliance drift. With JupiterOne you can automate with purpose and context. Close the security gap. And stay ahead of the curve in managing your assets.

**4. Proactively act through continuous governance and security programs.**

*Problem:* To be proactive, you must automate the collection of cyber asset data, analyze and alert on issues, and integrate these results with optimized workflows. Building your own source of truth is often resource-intensive causing you to struggle to see the forest through the trees.

*Solution:* Instead of thinking in lists, JupiterOne offers a graph-based view to understanding the relationships between assets and an integrated way to orchestrate remediation, all at the speed of your business. Quickly switch from the big picture impact to the metadata to prioritize efforts and right-size resource commits.

Visibility of your assets is meaningless if you can't do anything about the problem. You can't build a security program without deeper insights into how assets interact with one another in an increasingly volatile and complex asset universe. You can succeed with JupiterOne.

**Start your journey with JupiterOne today.**

**Your cyber assets - like you've never seen them before.**

**Get Started**