TANIUM

Back to the basics: Cyber hygiene starts with asset management

A new approach to perform asset discovery and inventory, improve cyber hygiene and take the first step toward Zero Trust.

Back to the basics: Cyber hygiene starts with asset management

A new approach to perform asset discovery and inventory, improve cyber hygiene and take the first step toward Zero Trust.

Contents

The challenge of asset visibility in modern networks

Your challenge: how to manage millions of dynamic, distributed and diverse assets.

With globally distributed workforces and assets hiding in the shadows growing exponentially, maintaining a complete and accurate inventory of every IT asset and achieving real-time visibility at scale is more challenging than ever before. After all, to keep our doors and windows locked, we need to know how many there are, and where they are.

And yet the industry has failed to deliver a viable solution to the visibility problem, offering hub-and-spoke models that are slow and saturate networks that instead limit visibility in modern and complex environments.

It's no wonder that many organizations can't accurately report essential details about their environment.

To solve this problem, it's time to get back to basics.

To preserve and improve cyber hygiene, you first need to know what IT assets you have. Do you have 50,000, 100,000 or 500,000 computers and servers in your organization? Where are they? What are they? What's running on them? What services do they provide?

Answering those questions is what developing asset visibility — and following an **asset discovery and inventory process** — is all about. It's the foundation for creating and maintaining cyber hygiene. And we wrote this eBook to help develop the visibility you need to do just that.

In this eBook, we'll cover:

- Why you need asset visibility to maintain cyber hygiene
- How to build asset visibility in modern networks
- What tools you need to deliver these outcomes

Why cyber hygiene depends on asset visibility

You can't manage what you don't know you have

To manage your endpoints, you need three levels of knowledge:

1. What assets do you have, and where are they?
2. What software is running on them, and is it licensed? You need more than a hostname or an IP address.

All companies, regardless of size, need this information, which in modern IT changes constantly. Network assets come and go, especially with "bring your own device" (BYOD), a common and growing policy in many organizations. Some assets may appear on the network only occasionally. With more companies encouraging employees to work from home (WFH), complexity increases.

And as networks become more complex and change faster, it becomes harder to maintain visibility into them — and the consequences for losing sight of what assets there are and what those assets are doing becomes greater and greater.

The operational disadvantages of not knowing

To paraphrase former Eagle Don Henley, when you drive with your eyes closed, you're bound to hit something. When you don't know what assets are on your network, it's the IT equivalent of driving with your eyes closed.

One of the first things you're likely to "hit" is security vulnerabilities. If you can't manage an asset, you can't secure it. And you can't manage it if you don't know you have it. You won't know whether software is patched properly. So there may be attack vectors you're entirely unaware of.

How about financial implications? Do you have a general sense

of what you're spending money on? Take software licensing, say a popular productivity program like Microsoft Office. If you have a license for 10,000 copies, do you use 20,000 or only 5,000? Do you efficiently use the license you pay for? Or are you out of compliance where you may be subject to expensive legal action?

Moreover, compliance isn't just about software licensing. And it's another area of operations that's very dependent on knowing what assets are on your network.

Let's take healthcare as a use case. Healthcare organizations must prove compliance with HIPAA and PCI provisions that cover protected health information and credit card data. Do you know where that data lives? If not, you can't prove compliance. Inability to prove compliance has two significant downsides: regulatory sanctions and not being able to effectively provide your services.

The examples are endless. If you don't know what assets are in your network and what they are doing, you cannot secure them, you cannot manage them, and you can't maintain effective cyber hygiene for your environment as a whole.

And — unfortunately — many organizations are currently struggling to answer basic questions about the assets in their environment. Here's why.

Why organizations struggle to create asset visibility

There are two primary reasons why organizations struggle to answer basic questions about their assets to maintain cyber hygiene.

First, endpoint discovery has become a constantly moving target.

Not every endpoint on a network is a desktop computer, laptop or server. There are printers, phones, tablets and a growing number of consumer and industrial internet of things (IoT) devices. Mobile device management (MDM) is a growing application field.

But why should you have to worry about a consumer IoT device compromising the corporate network? Here's why: An employee of one of our customers was working from home. The company's security team was receiving alerts that someone was trying to break into her laptop. The source was a refrigerator with malware scanning her home network and trying to get into her device, which was temporarily on the corporate network. The same thing could occur with a smart light switch, thermostat, security camera — you name it.

This is also true of machines on the factory floor, many of which are equipped with sensors that communicate via wireless networks and the web with manufacturing applications.

It's a field called operational technology, and, in essence, it makes every machine on a factory floor a network device.

Every device type can create operational and/or security risks, and the number of these types will only continue to increase in the coming years.

Second, legacy tools struggle to create visibility in this new environment.

Asset discovery tools built 10 years ago preceded many of the things modern IT environments operate with daily. Two examples: containers and hybrid clouds.

These tools can't handle the rate of change we see now. Yet organizations often remain attached to the tools they're comfortable with, many of which are not easy to use.

In fact, they may take pride in mastering hard-to-use tools. Maybe they wrote custom scripts to make them work more effectively. Not only that, an entire partner ecosystem has grown up around helping IT departments do just that.

The unintended — and unfortunate — consequences of that are IT policies and processes crafted not because they're the best way to address an issue but because they fit the capabilities of the tools in use. It's the IT version of "if you have a hammer, everything must be a nail." The policies are: "We must nail things." Entrenched tools become part of the IT ecosystem. But the best IT policies should be tool-agnostic. A tool built in 1993 — or 2010 — can't offer that flexibility.

The result of these two problems

When organizations try to create asset visibility in modern environments using older tools, their asset discovery and inventory process becomes:

- **Complex:** They need to add more and more tools just to identify their assets, and each of these tools must be integrated with the others.
- **Expensive:** They pay for expensive software — and supporting teams and infrastructure — that no one uses, is likely outdated, and consumes resources.
- **Stale:** They produce data that is incomplete and often days, weeks or even months late and does not reflect the current state of the network.

In sum: Organizations need a new way to build asset visibility in modern networks.

How to build asset visibility in modern networks

Rethink your legacy asset visibility tools

First, you must decide if your legacy asset visibility tools are still serving you. If you struggle to create visibility across your entire estate, then you may need to decommission one or more of your tools and replace them with modern options.

What features are important for a modern toolset intended for asset management?

The tools or platform you use for your asset discovery and inventory should possess:

- Accuracy
- Speed
- Scale
- Ease of use

Accuracy, speed and scale are closely related. If it takes two weeks or a month to do an inventory, by the time you're finished, the network has changed, and you've undoubtedly missed something.

It's no longer accurate, no matter how diligent you were. The bigger the network, the more of a problem this presents. That's why scale matters. Ease of use comes into play because a tool that's hard to configure produces errors, and over time, people won't want to use it.

To create effective asset visibility, and to drive a modern asset discovery and inventory process, your tools must possess all four qualities.

Drive toward the right asset visibility outcomes

Second, you must target the right outcomes for your asset visibility capabilities. "Asset visibility" can be a broad topic, and it's easy to get lost trying to achieve too many outcomes at once. To start, focus on building visibility for a few key outcomes.

What outcomes are important for a modern asset visibility capability?

You must develop the asset visibility required to:

1. **Gain insight into endpoints you don't know you have to reduce risk.** If you can't see your endpoints, you can't manage them. Yet today's diverse, dynamic and distributed infrastructure creates an environment where endpoints can easily hide and are always changing, increasing security risks. You must be able to:
   - Discover every endpoint in your environment in minutes — not days or weeks — including hard-to-find endpoints in remote subnets.
   - Build a real-time inventory that continuously discovers and categorizes new assets and enables you to bring them under your management.
2. **Increase the value of your CMDB with accurate, real-time data.** Most legacy tools can answer only a single question for a single-asset class, forcing organizations to deploy dozens of complex point tools. IT teams then try to integrate, centralize and normalize data provided by these point solutions in their configuration management database (CMDB). This leads to inaccurate, and insufficient asset data. Instead, you must be able to:
   - Connect to your CMDB with the confidence that endpoint and usage data are fresh and accurate.
   - Export your asset data into your CMDB regularly on a schedule based on your needs for consistent reporting, better collaboration and informed decision-making.
   - Create a single source of truth used by security, operations, risk, procurement, finance, and leadership teams.
3. **Avoid unnecessary hardware and software costs.** Organizations today struggle to identify what software is installed on their machines and how much it is being used. They can't precisely assess their software either for audits or reclamation purposes. This leads to high software expenditures in both audit fees and recurring license costs. You must be able to:
   - Have a complete list of software by product or vendor in your environment available at any time.
   - Easily find unauthorized or underutilized software to reclaim or redistribute licenses.
   - Use out-of-the-box reporting to understand usage statistics at a glance.

Perform the 4-step cycle of asset visibility to maintain cyber hygiene

Next, recognize that creating asset visibility and cyber hygiene is not a one-time project. Your environment is constantly changing, and it requires a continuous process to maintain a clear picture and fundamental security over its present state.

Many of our customers use the following process to maintain effective visibility and cyber hygiene over their assets:

STEP 1

Establish visibility by performing a comprehensive initial scan of their entire environment.

STEP 2

Find issues by discovering unknown, unmanaged and vulnerable assets in the environment.

STEP 3

Secure your devices and other endpoints by closing vulnerabilities and bringing unknown and unmanaged endpoints into as much control as possible.

STEP 4

Establish ongoing asset monitoring; repeat this cycle as new assets enter and known assets change their status.

Think past cyber hygiene and lay the foundation for Zero Trust

Finally, recognize that cyber hygiene is just the first step toward creating a more secure organization. The right asset visibility capability will also lay the foundation for nearly any Zero Trust strategy or solution you choose to bring to life.

When everything is a network device, everything is a potential security vulnerability. So you need policies and procedures that break endpoints into three categories: managed, unmanaged and unmanageable.

Endpoint discovery is the first crucial step in the trend toward Zero Trust solutions. CSO Online describes Zero Trust[1] as "a security concept centered on the belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access."

Threat response and remediation tools are only as good as the breadth of endpoints they're running on. And with the endpoint acting as the new perimeter, endpoint discovery really is where cyber hygiene and security begin, and implementing a Zero Trust practice is the next meaningful step on that journey.

[1] https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

How Tanium creates asset visibility and drives cyber hygiene

Meet Tanium: Asset visibility for modern environments

Tanium is a converged platform that delivers visibility and control over diverse, dynamic and distributed assets within modern environments.

Tanium's *Asset Discovery and Inventory* solution provides a comprehensive, reliable and actionable picture of your endpoint environment. Its technology efficiently investigates areas of the network where common endpoint tools may not know how or where to look for "hidden" devices — including endpoints that don't report properly via traditional methods.

Tanium also offers additional contextual detail on each endpoint — including hardware configurations, installed software, and how that software was used over 30-, 60-, and 90-day intervals.

With Tanium, you will answer fundamental questions about your environment with accurate, complete, and up-to-date data about all endpoints across your estate, in seconds — not hours, days or weeks.

Using Tanium, many of our customers have:

- Reduced their weekly scan time by 93%
- Discovered 35% more endpoints than they knew they had
- Discovered 20% more unmanaged assets than they were aware of

Here's how.

What you get with Tanium: visibility, control and truth

Tanium corrects the problems with legacy tools and leverages a modern architecture that was built to create asset visibility across modern networks. Tanium leverages:

- **An extensible data model** that lets you collect new, ad hoc data from your endpoints at will.
- **A distributed communications protocol** that gathers and distributes data to millions of endpoints with zero intermediate infrastructure in seconds.
- **A single, lightweight agent** with minimal endpoint performance impact that can fit on the smallest chips.

By taking this fundamentally different approach, Tanium gives you:

- **Speed.** You will discover every endpoint in your environment and build a comprehensive inventory in minutes. You will generate real-time visibility for thousands, perhaps hundreds of thousands of assets, ask fundamental questions and receive answers in seconds, and integrate this real-time data with third-party tools like CMDBs and SIEMs.
- **Control.** You will categorize your entire environment in minutes and see how your hardware, software and infrastructure assets are being used. You will reduce costs by reclaiming or redistributing software based on accurate data. You will quickly find unauthorized software and assets, allowing you to reduce risks.
- **Truth.** You will build a central and trusted view of your IT assets and unify your IT operations, security and risk teams around one accurate dataset. You will create a single source of truth and an accurate system of record for all your assets and make confident decisions that impact multiple teams.

Nine ways Tanium improves asset discovery and inventory

None of this is theory. Tanium can meaningfully improve your asset discovery and inventory process and give you tangible results. With Tanium, you will:

1

Find unknown endpoints. Identify 10–20 percent more endpoints in your environment than you're currently aware of. If you can't see it, you can't secure it.

2

Collect data consistently. Develop a single source of truth that provides a current and reliable picture of your entire environment.

3

Catalog lost assets. Maintain an accurate inventory of remote assets anywhere, anytime — while understanding the state of those assets.

4

Increase the percentage of endpoints under management. Reduce risk by securing and managing more of your endpoints using flexible discovery and automation.

5

Decrease mean-time-to-manage. Rapidly identify new endpoints entering your environment and bring them under control.

6

Track software usage and coverage percent. Track usage and percentage of unused installed software on each of your endpoints.

7

Reallocate resources. Stop allocating 90 percent of your time collecting data and instead put that data to work.

8

Optimize investments. Analyze usage data across hardware and software assets to rationalize your spend and derive additional value from existing solutions through robust integrations.

9

Mitigate risk and inefficiency. Centralize visibility and control for managed and unmanaged assets. Drive consistency and eliminate variability and guesswork.

Improve your asset visibility and cyber hygiene — starting today

The difference is clear. With traditional tools, you will collect stale, inaccurate and incomplete data from your assets and struggle to maintain cyber hygiene. With Tanium, you will collect fresh, accurate comprehensive data from every asset in your environment and confidently maintain cyber hygiene.

Learn more about **Tanium's Asset Discovery and Inventory solution** and contact us to **schedule a demo and consultation.**

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.