TANIUM | servicenow

Tanium & ServiceNow

Delivering asset management peace of mind.

TANIUM

Tanium & ServiceNow

Delivering asset management peace of mind.

Contents

INTRODUCTION

Want to reduce costs, improve the security of your network and data, and better protect your entire operation?

This eBook will explain the benefits of a complete, accurate, and up-to-date view of your enterprise hardware, software, and virtual asset inventory in ServiceNow CMDB. It will also describe how, with Tanium Asset Integration for ServiceNow, your organization will have the insights you need to prioritize decisions about managing your devices and systems efficiently while reducing costs and lowering the risk of an attack.

These solutions will enable your business to reduce the complexity and strain on your IT asset management (ITAM) by delivering a single, reliable source of data to your configuration management database (CMDB).

Using this data, you can proactively identify what needs to be patched and secure assets while reducing total cost of ownership (TCO) associated with licensing and maintenance. You will also be able to protect against threats from ransomware and other common attacks by identifying compliance risks within your organization.

The challenges you're facing are complex, but the solution doesn't have to be.

CHAPTER 1

How reliable is your CMDB?

A configuration management database (CMDB) provides storage for data associated with IT assets such as applications, routers, servers, or other devices. Collecting data about these assets is done manually or by using various purpose-built tools. With the direct financial costs and the threats to overall business continuity on the rise, it becomes increasingly important for companies to have a reliable CMDB in order to have a successful IT asset management process.

Four good reasons for having a reliable CMDB

1. The number of organizational assets is increasing

To reap the benefits of additional productivity, more than 80% of organizations allow or promote a bring-your-own-device (BYOD) policy. The main concern for these organizations is data loss and data security, especially as 45% of employees do not change their device passwords following a breach.[1]

2. Security threats are evolving and increasing

Cybercriminals are exploiting systemic weaknesses with increasingly sophisticated methods. Ransomware and malware are being widely distributed over the dark web and, as cybercrime becomes more common, the associated costs are increasing. As many as 68% of organizations have experienced endpoint attacks that exposed data or compromised IT infrastructure.[2]

3. Regulatory compliance is becoming even more important

With increasing regulatory scrutiny and growing marketplace pressures following every high-profile breach, complying with IT security standards such as HIPAA protects critical data and helps protect a company's reputation and brand while ensuring business continuity.

4. Disparate tooling creates inefficiency and higher costs

In the absence of a unified approach for gathering asset data into a CMDB, the data can become fragmented, inaccurate, and difficult to identify. This can hinder workflows, increase costs, and put your entire operation at risk.

How can businesses react effectively to these asset-related challenges?

The first step is to increase overall visibility of every asset in the organization. An asset you're not aware of is more easily exploited by cybercriminals and represents a potentially devastating vulnerability. Once you have visibility of all your assets, you can manage licensing, patching, and maintenance while reducing the associated costs. And by using the appropriate tools to collect asset data, you can reduce risk and trust the CMDB as a single source of reliable information about all of your IT assets.

What should be the goal for your organization's CMDB?

To achieve the peace of mind that comes from having complete asset visibility and security, your goal should be to capture reliable, real-time data as you build a CMDB to reduce or eliminate:

- Stale or incomplete data
- Audit and compliance risk
- Difficulty prioritizing responses
- Lack of communication across silos
- Slow manual processes

Your ITAM needs help! To bring your endpoint ecosystem under control you must first ensure you are using the right tools and processes to build your CMDB.

Answer these questions below to determine the state of your CMDB:

- Do I know how many assets I have in my operational environment?
- Do I know what software is running on those endpoints?
- Are we using all the software we've paid for, or are redundant licenses making some devices essentially invisible and vulnerable to attack?
- Do all our assets meet the required audit and compliance rules?
- Am I at risk for known and zero-day vulnerabilities because of unknown assets?
- Can I trust the infrastructure that my business-critical services rely upon?

CHAPTER 2

It doesn't have to be this way

If the issues are not addressed, maintaining a reliable single source of truth in a CMDB and effectively managing CIs becomes expensive and exposes a business to unacceptable risk.

Many organizations find themselves trying to operate with a patchwork of manual or unnecessarily complex tools, automated processes, and inadequate procedures to build and maintain a CMDB. In fact, 99% of organizations using CMDB tooling that do not confront configuration item data quality gaps will experience visible business disruptions – through 2024, according to a 2022 Gartner® report, *3 Steps to Improve IT Service View CMDB Data Quality.* This can result in:

- Inaccurate and incomplete asset visibility
- High TCO in IT operations
- IT/SecOps silos which, combined with inaccurate endpoint data, create increased risk

Operating with an incomplete or inaccurate inventory of hardware and software asset data can lead to increased costs and inefficiencies associated with:

- High change failure rates
- Patch and vulnerability issues

Businesses that attempt to integrate disparate operations and security tools can experience costly and sometimes catastrophic outcomes. These can include:

- Incomplete data
- Resource-intensive
- manual effort
- Frustrated customers and employees who will inevitably require support related to the systemic issues

These disjointed workflows trigger delays in identifying risk and in acting to implement the necessary remediation. Many IT asset-related changes can occur, causing:

- Slow response times and SLA impact
- Data breaches and attacks by bad actors
- Major delays in repairing vulnerabilities and resolving high priority incidents

Where does it hurt?

Use the table below to see how Tanium and ServiceNow can address each pain point and the benefits you can achieve.

What are your pain points?	What the Tanium/ServiceNow partnership delivers	How can you benefit? *varies by industry, complexity, and organizational size
No real-time, accurate, and complete CMDB that can be trusted	One reliable method for feeding real-time updates into the CMDB from all endpoints and applications	20–30% more real-time data
Inability to conduct a proper software asset, license, and cost management assessment	Accurate software inventory in the CMDB	35% reduction in software license costs
Inability to right-size and optimize cloud resources and business applications due to lack of insights	Data on current hardware and software performance and utilization to help make insightful business decisions	Millions in savings from reclaiming unused software and decommissioning legacy apps
High TCO and low value from tool investments due to numerous incompatible point solutions and integrations	Complete, accurate, real-time information to populate your CMDB	40% lower TCO from reducing the number of disparate asset point solutions
Inability to proactively prevent business failures and a slow Mean Time to Recover (MTTR)	The ability to monitor real-time performance of endpoints for proactive safeguarding and real-time remediation	60% reduction in MTTR

> Integrating Tanium Asset with ServiceNow will fill the gaps that are limiting visibility, accuracy, and a real-time reliable CMDB. Resolving these issues will help simplify IT asset management, improve your overall security, and significantly reduce costs.

CHAPTER 3

The Tanium and ServiceNow difference

Using the Tanium Asset integration for ServiceNow allows organizations to reduce the complexity of IT and operational environments, reduce costs, improve security, and proactively manage their estates.

Tanium delivers a single source of accurate and real-time data to ServiceNow's CMDB. Combining Tanium and ServiceNow means that any workflow created in ServiceNow is based on information that is up to date and accurate, whether the asset is physical, virtual, cloud-based, or IoT. ServiceNow can create automation workflows that put Tanium to work when incidents occur, or thresholds are reached.

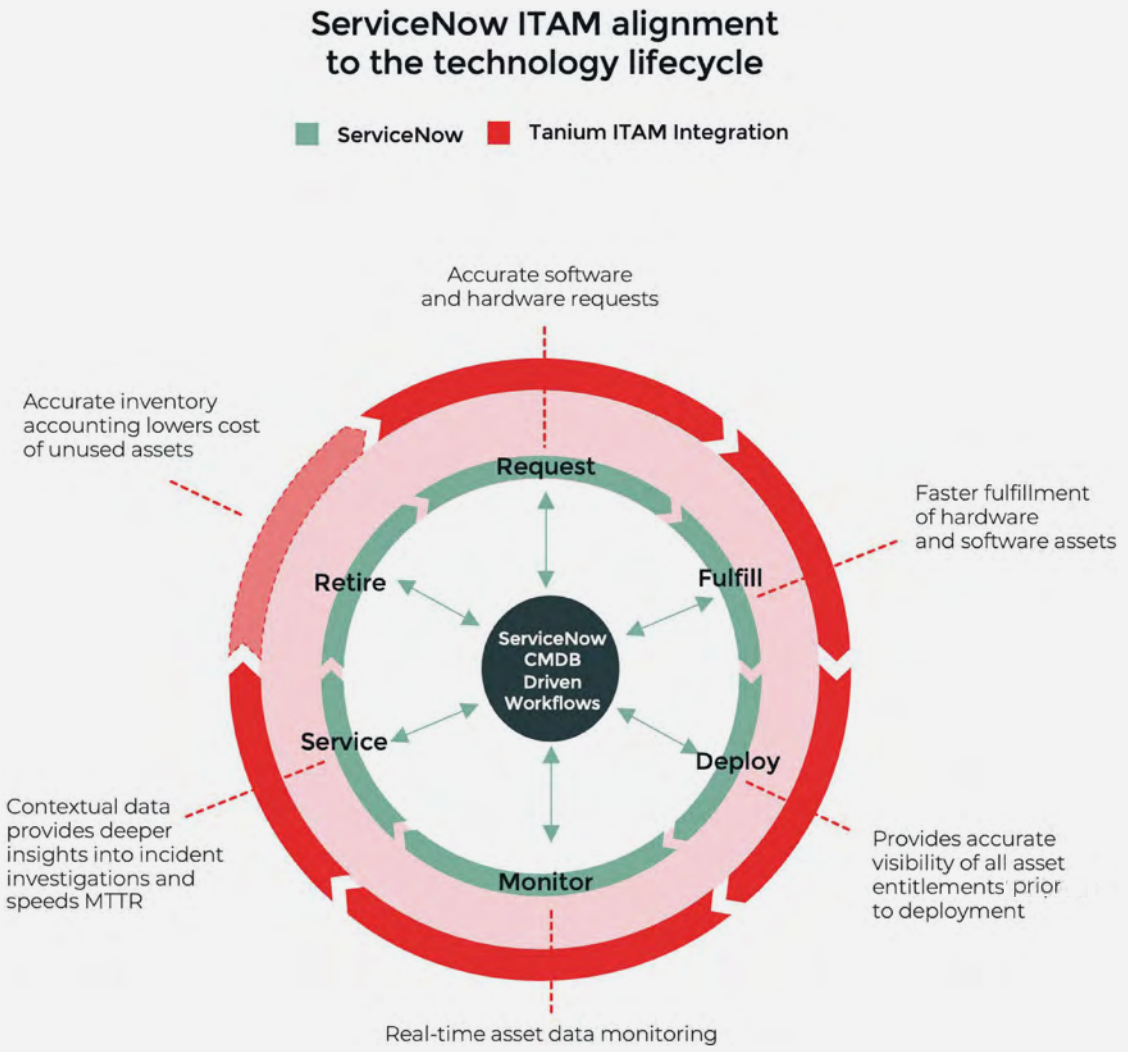
Tanium/ServiceNow partnership

Tanium acts as the eyes and ears to detect all endpoints, monitor in real time, and gather data to populate the ServiceNow CMDB. As the brain, the CMDB leverages the data harvested by Tanium in order to take action and orchestrate what is required to support the infrastructure and the end-user experience.

With Tanium and ServiceNow solutions in place, ITAM processes and CMDB maintenance are integrated to help streamline, automate, and simplify endpoint management activities.

Now you can:

- Immediately onboard and offload steps to be automated for real-time hardware and software inventory, such as when something goes out of stock.
- Pull real-time data concerning software usage into ServiceNow to optimize use, mitigate risk, and create a single source of truth for asset and software insights.
- Keep your employees and your network safe from threats by using complete visibility of your assets and software to remediate vulnerabilities and ensure compliance across your entire environment.
- Optimize resources and business applications while planning for future cloud initiatives with accurate, real-time, data-driven decisions.



Every moment counts

With costly, inefficient tools and processes feeding data into your CMDB, your assets are at risk. With each passing moment that risk, and the associated cost, increases.

Make today the day you take action to bolster your IT asset management process, enrich your CMDB with real-time information you can trust, and turn your assets from potential vulnerabilities into trusted, productive, and secure operational assets.

Learn more about the Tanium and ServiceNow complementary solution offerings and how it can deliver cost-effective, real-time peace of mind.

Visibility

Bring all assets under control while you build a real-time inventory of every new or legacy asset in your environment.

Inventory compliance

Deliver complete and near-real-time HAM/SAM inventory compliance to enable granular visibility of the assets themselves, along with detailed information about usage and optimization.

Risk reduction

With Tanium Asset integration for ServiceNow, organizations can reduce the risk and lower the severity of attacks. With enhanced contextual data in real time, you can significantly reduce your mean time to both investigate and remediate an incident.

Cost savings

By identifying unused licenses, out-of-compliance applications, and unused or underutilized software and hardware, organizations can significantly reduce costs and increase efficiency by focusing on the most important assets. Typically, with Tanium Asset Integration for ServiceNow, customers can consolidate the number of platforms used for similar tasks and achieve a more desirable outcome.

Schedule a demo with Tanium

Let us show you how Tanium's Asset Discovery and Inventory solution provides a comprehensive, real-time view of assets across your organization.

See the Tanium Asset demo in action or **request a personalized demo** today.

Endnotes

1 https://explodingtopics.com/blog/byod-stats

2 https://expertinsights.com/insights/50-endpoint-security-stats-you-should-know/

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.