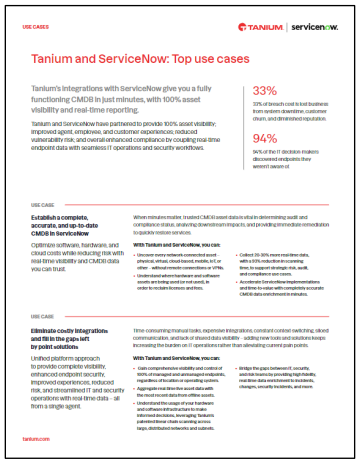


USE CASES

TANIUM | servicenow.

Tanium and ServiceNow: Top use cases

Tanium's integrations with ServiceNow give you a fully functioning CMDB in just minutes, with 100% asset visibility and real-time reporting.

Tanium and ServiceNow have partnered to provide 100% asset visibility; improved agent, employee, and customer experiences; reduced vulnerability risk; and overall enhanced compliance by coupling real-time endpoint data with seamless IT operations and security workflows.

33%

33% of breach cost is lost business from system downtime, customer churn, and diminished reputation.

94%

94% of the IT decision makers discovered endpoints they weren't aware of.

USE CASE

Establish a complete, accurate, and up-to-date CMDB in ServiceNow

Optimize software, hardware, and cloud costs while reducing risk with real-time visibility and CMDB data you can trust.

When minutes matter, trusted CMDB asset data is vital in determining audit and compliance status, analyzing downstream impacts, and providing immediate remediation to quickly restore services.

With Tanium and ServiceNow, you can:

- Uncover every network-connected asset – physical, virtual, cloud-based, mobile, IoT or other – without remote connections or VPNs.
- Understand where hardware and software assets are being used (or not used), in order to reclaim licenses and fees.
- Collect 20–30% more real-time data, with a 10% reduction in scanning time, to support strategic risk, audit, and compliance use cases.
- Accelerate ServiceNow implementations and time-to-value with completely accurate CMDB data enrichment in minutes.

USE CASE

Eliminate costly integrations and fill in the gaps left by point solutions

Unified platform approach to provide complete visibility, enhanced endpoint security, improved experiences, reduced risk, and streamlined IT and security operations with real-time data – all from a single agent.

Time-consuming manual tasks, expensive integrations, constant context switching, siloed communication, and lack of shared data visibility – adding new tools and solutions keeps increasing the burden on IT operations rather than alleviating current pain points.

With Tanium and ServiceNow, you can:

- Gain comprehensive visibility and control of 100% of managed and unmanaged endpoints, regardless of location or operating system.
- Aggregate real-time live asset data with the most recent data from offline assets.
- Understand the usage of your hardware and software infrastructure to make informed decisions, leveraging Tanium's patented linear-chain scanning across large, distributed networks and subnets.
- Bridge the gaps between IT, security, and risk teams by providing high-fidelity, real-time data environment to incidents, changes, security incidents, and more.

tanium.com

Tanium and ServiceNow: Top use cases

Thank you for downloading this Tanium resource. Carahsoft is the official government distributor for Tanium cybersecurity solutions available via GSA, NASA SEWP V, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Tanium's solutions, please check out the following resources and information:

For additional resources:
carah.io/taniumresources

For upcoming events:
carah.io/taniumevents

For additional Tanium solutions:
carah.io/taniumsolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
tanium@carahsoft.com
703-673-3560

To purchase, check out the contract vehicles available for procurement:
carah.io/taniumcontracts

Tanium and ServiceNow: Top use cases

Tanium's integrations with ServiceNow give you a fully functioning CMDB in just minutes, with 100% asset visibility and real-time reporting.

Tanium and ServiceNow have partnered to provide 100% asset visibility; improved agent, employee, and customer experiences; reduced vulnerability risk; and overall enhanced compliance by coupling real-time endpoint data with seamless IT operations and security workflows.

33%

33% of breach cost is lost business from system downtime, customer churn, and diminished reputation.

94%

94% of the IT decision-makers discovered endpoints they weren't aware of.

USE CASE

Establish a complete, accurate, and up-to-date CMDB in ServiceNow

Optimize software, hardware, and cloud costs while reducing risk with real-time visibility and CMDB data you can trust.

When minutes matter, trusted CMDB asset data is vital in determining audit and compliance status, analyzing downstream impacts, and providing immediate remediation to quickly restore services.

With Tanium and ServiceNow, you can:

- Uncover every network-connected asset – physical, virtual, cloud-based, mobile, IoT, or other – without remote connections or VPNs.
- Understand where hardware and software assets are being used (or not used), in order to reclaim licenses and fees.
- Collect 20-30% more real-time data, with a 93% reduction in scanning time, to support strategic risk, audit, and compliance use cases.
- Accelerate ServiceNow implementations and time-to-value with completely accurate CMDB data enrichment in minutes.

USE CASE

Eliminate costly integrations and fill in the gaps left by point solutions

Unified platform approach to provide complete visibility, enhanced endpoint security, improved experiences, reduced risk, and streamlined IT and security operations with real-time data – all from a single agent.

Time-consuming manual tasks, expensive integrations, constant context-switching, siloed communication, and lack of shared data visibility – adding new tools and solutions keeps increasing the burden on IT operations rather than alleviating current pain points.

With Tanium and ServiceNow, you can:

- Gain comprehensive visibility and control of 100% of managed and unmanaged endpoints, regardless of location or operating system.
- Aggregate real-time live asset data with the most recent data from offline assets.
- Understand the usage of your hardware and software infrastructure to make informed decisions, leveraging Tanium's patented linear chain scanning across large, distributed networks and subnets.
- Bridge the gaps between IT, security, and risk teams by providing high fidelity, real-time data enrichment to incidents, changes, security incidents, and more.

> By plugging Tanium into ServiceNow and Sentinel, our operations team can achieve total visibility across all three core platforms without any data silos.

Mark Wantling
CIO, University of Salford

USE CASE

Maximize productivity and elevate experiences

Improve the user experience through unparalleled visibility into IT Infrastructure and endpoints, reduced costs and complexity of point solutions, and increased transparency and efficiency.

Internal issues that affect employees and their ability to work without disruption have a compounding effect on an organization's capacity to deliver to their customers, and vice versa.

With Tanium and ServiceNow, you can:

- Gain visibility into every endpoint powering an organization's IT infrastructure, including real-time monitoring and advanced reporting.
- View and remediate performance events, terminate processes, and restart services – all without remote control or interruption of end-user workflows.
- Proactively identify and remediate incidents before they become a problem, through automated and integrated alerts in workflows
- Minimize IT service ticket creation by empowering end users to take actions proactively and independently of IT agents using simple, automated workflows that remediate and optimize their experience before they run into issues.
- Reduce ticket loads to refocus your IT agents' time on tasks that better leverage their expertise and provide more value to the business.

USE CASE

Mitigate risk, raise compliance, reduce disruptions, cut complexity

Identify financial and security risk from vulnerabilities and non-compliant configurations, prioritize remediation based on the criticality of threats and endpoints, and close the loop with automated patch orchestration.

Today's CISOs need to have complete visibility and control of all assets across an expanding and distributed landscape, while being secure and agile enough to complete impromptu audits, meet ever-changing compliance requirements, keep up to date on the latest vulnerabilities, and respond to security incidents quickly.

With Tanium and ServiceNow, you can:

- Scan, collect, and report on real-time vulnerability and compliance data – across all networks and operating systems, in just minutes – to find gaps that lead to inaccurate data and increased financial and security risk exposure.
- Automatically correlate vulnerabilities and compliance assessments with configuration items in the ServiceNow CMDB to prioritize remediation based on risk calculations, ensuring your most critical systems and highest risks are resolved first.
- Eliminate the time and manual effort of remediation validation with the ability to automatically rescan endpoints and confirm change outcomes.
- Confidently plan patch deployments at scale through the change lifecycle in ServiceNow – with test and deployment plans, approval processes, and scheduled workflows.

By integrating Tanium with ServiceNow, you can provide 100% asset visibility, reduce your vulnerability risk, enhance overall compliance, consolidate tools and point solutions, and eliminate data and communication siloes between teams.

Tanium has built ServiceNow integration solutions aligned with a Value Realization Framework. This ensures that organizations can adopt Tanium's integration solutions in a structured approach, empowering them to achieve their business outcomes at the desired pace. Also, the framework organizes capabilities and outcomes to effectively realize increasing value as additional capabilities are adopted.

Visibility

Optimize software, hardware, and cloud costs with real-time visibility and CMDB data you can trust.

- Physical, virtual, software, cloud-based, mobile, IoT, or other. Hardware, software, and virtual assets are automatically mapped to the appropriate object structure in ServiceNow.
- Leverage automatic object mapping and Tanium's ability to stream real-time, high-fidelity data with the power of ServiceNow workflows.
- Access live, actionable endpoint performance data directly inside of ServiceNow, without any remote control or interruption of end-user workflows.

Control

Automatically correlate configuration items with real-time vulnerability, configuration compliance, and change authorization assessments.

- Automatically search for known vulnerable assets, configurations, activities, and traffic on your network – whether you leverage the Security Content Automation Protocol (SCAP), Open Vulnerability and Assessment Language (OVAL) content, or any industry regulatory requirements such as PCI, HIPAA, and SOX.
- Enrich security incidents with the most important, real-time data about associated configuration items – including logged-in users, network statistics, and running processes – and the ability to search across all endpoints for risk occurrences.

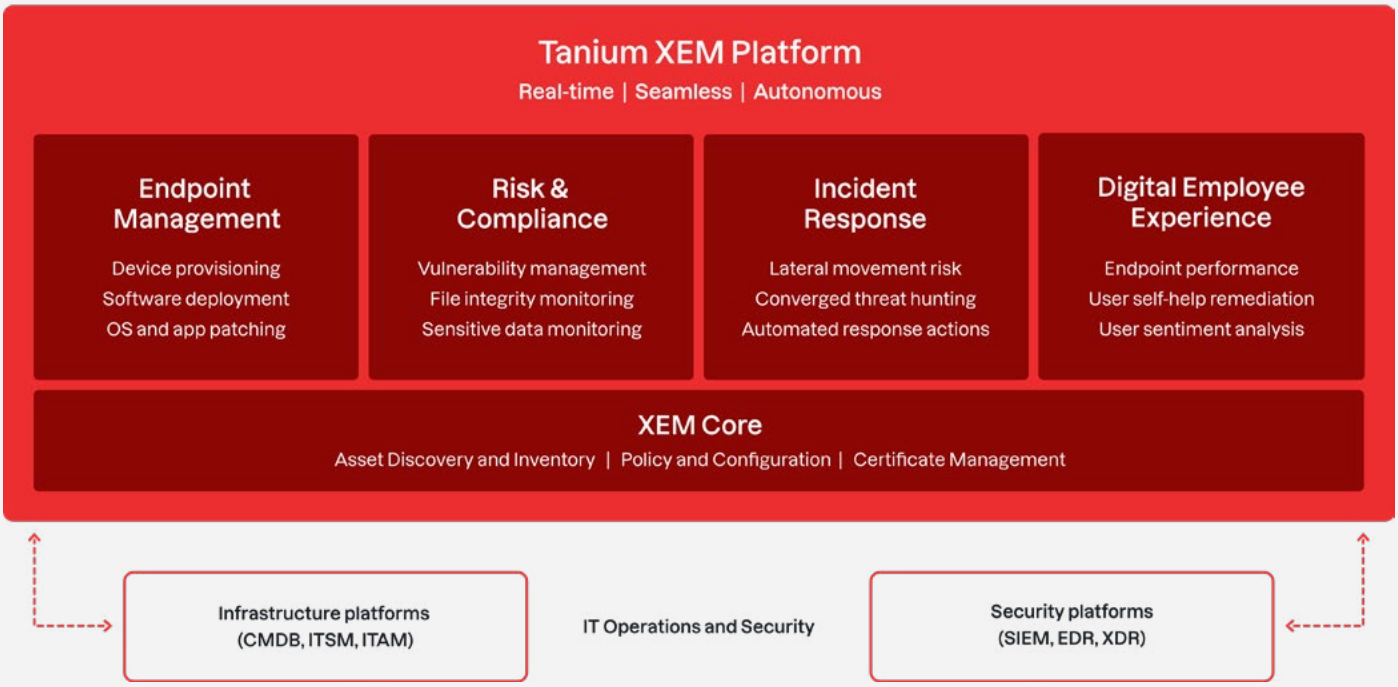
Remediation

Prioritize, remediate, and validate change outcomes with patch orchestration at scale.

- Classify and prioritize patch initiatives at scale, based on known vulnerabilities and their calculated risk, ensuring the most critical risks are resolved first.
- Confidently plan patch deployments through the change lifecycle in ServiceNow, with test and deployment plans, approval processes, and scheduled workflows.
- Eliminate the time and manual effort of remediation validation with the ability to rescan and confirm change outcomes automatically.

Converged Endpoint Management (XEM)

Visibility, control, and remediation for all endpoints



OUR PLATFORM

Transform IT visibility, control, and remediation with ServiceNow and Tanium.

Tanium ITX for ServiceNow →

Optimize software, hardware, and virtual asset inventory and reduce risk with real-time asset visibility.

Tanium Security Operations for ServiceNow →

Identify, correlate, and prioritize risk of endpoint vulnerabilities and compliance gaps in real time.

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. Visit us at www.tanium.com.

© Tanium 2024