SOLUTION BRIEF

Tanium + ServiceNow: Better Together

Integrating Tanium with ServiceNow enhances your data, workflows, and outcomes with maximum visibility, control, and remediation.

ServiceNow customers face many challenges, including asset visibility, customer and employee experiences, and the ability to identify, prioritize, and respond to vulnerabilities and threats. These challenges can have a significant impact financially as well as operationally if a breach occurs.

Tanium's powerful solutions enhance ServiceNow

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.

WITH TANIUM AND SERVICENOW TOGETHER, CUSTOMERS CAN:

- Establish a complete, accurate, and up-to-date configuration management database (CMDB) providing full visibility of your hardware and software inventory data.
- Increase productivity and accelerate growth by delivering superior digital experiences for employees and customers.
- Enable organizations to identify, prioritize, and respond to vulnerability risks with end-to-end vulnerability response lifecycle automation.
- Enhance overall compliance through real-time endpoint data coupled with seamless IT operations and security workflows.

Ultimately, by maximizing the capabilities from both the Tanium and ServiceNow platforms working in synchrony, customers can remove costly integrations from a multitude of point solutions and benefit from a single endpoint agent all through the Tanium XEM platform.

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.

YOUR CHALLENGE

Ensure total asset visibility, provide excellent customer and employee experiences, and quickly identify and respond to all vulnerabilities and threats.

ServiceNow can centralize and normalize data from your mix of legacy and new management tools to create a consolidated Configuration Management Database (CMDB). However, unless you directly address any underlying visibility gaps, your investment could fall short. Incomplete, inaccurate, and out-of-date CMDB data can impede processes and workflows that IT, operations, and security teams leverage to support customer and employee experiences, triage and remediate incidents, and ensure infrastructure is secure and up to date.

Lack of IT visibility can lead to multiple problems

- Maintaining accurate and complete asset data can be challenging, especially for organizations with large, diverse IT environments.
- If internal issues degrade the agent and employee experience, this can have a compounding effect, slowing an organization's deliveries to customers.
- Integrating and maintaining multiple tools and point solutions can lead to inefficiencies and complexities in overall spend, administration, and usage.
- Quickly identifying vulnerabilities across the IT infrastructure can be a challenge. Patching at scale to close the loops on those vulnerabilities can be difficult, too.
- Many organizations lack the vulnerability scoring, risk assessments, and IT-to-operations communications needed to prioritize remediation.

These challenges can negatively impact your business

- Only 30% of IT operations and security teams feel confident that they have visibility into 85% to 95% of their network-connected endpoints.
- 94% of the IT decision-makers discovered endpoints they weren't aware of.
- 33% of breach cost is lost business from system downtime, customer churn, and diminished reputation.

YOUR SOLUTION

Deliver full value from your ServiceNow investment with the Tanium XEM platform

Take advantage of Tanium's integrations with ServiceNow to get a fully functioning CMDB up and running in just minutes, with 100% asset visibility and real-time reporting.

You'll also improve agent, employee, and customer experiences, reduce vulnerability risk, and enhance overall compliance through real-time endpoint data coupled with seamless IT operations and security workflows.

> 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

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 importantly, 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.

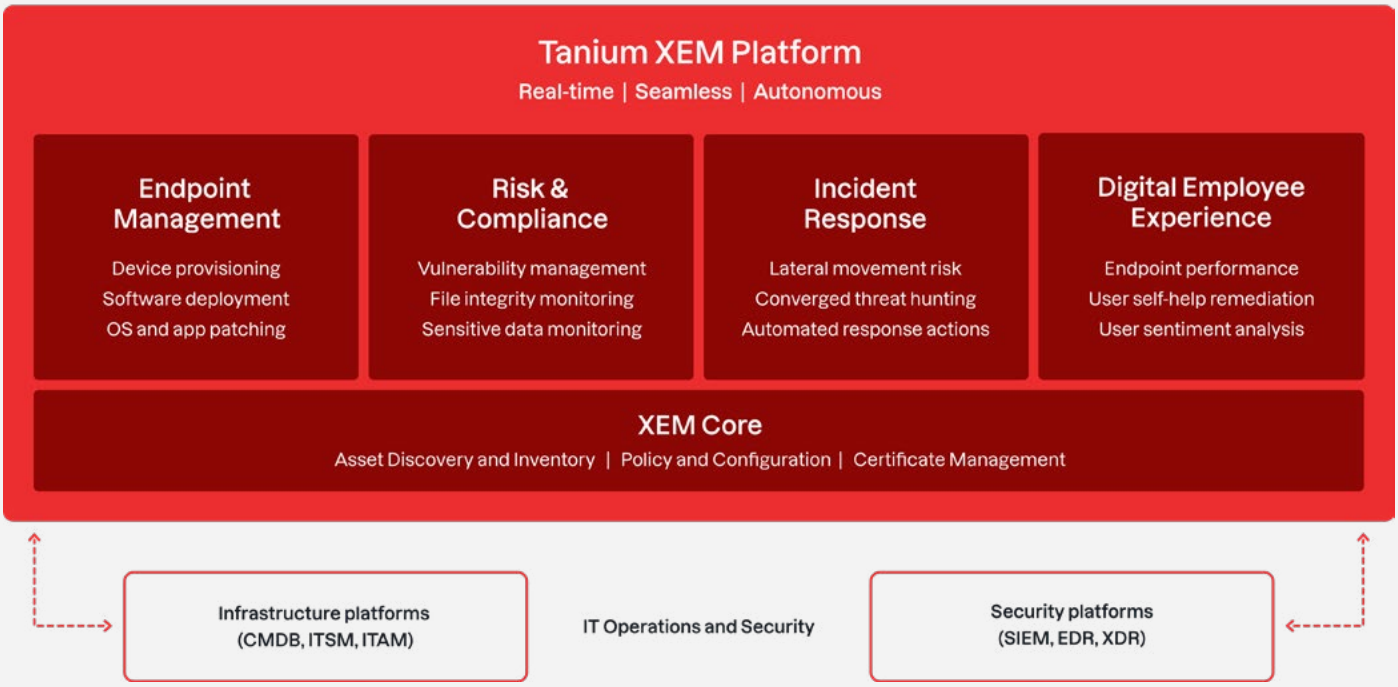
Remediation

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.