Tanium Patch Management for ServiceNow IT Operations

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 Patch Management for ServiceNow IT Operations

This integration with ServiceNow IT Operations lets teams automate patch management orchestration through proper change controls with speed and scale

With Tanium Patch Management for ServiceNow IT Operations, organizations can proactively plan and execute automated patching programs and reduce the need for reactive and manual patch management. With full end-to-end patch lifecycle automation, organizations can meet their patching targets, increase compliance, and reduce risk, while no longer needing to spend days or weeks managing multiple disparate tools, manual processes, and people.

Today's patch lifecycle is too complex, slow, manual, and expensive, leading to increased risk and lower productivity.

Organizations today struggle to meet standard SLAs for patch management due to a variety of factors including lack of visibility, manual and complex processes, long cycle times to patch, and uncertainty about the efficacy of patching. These factors increase risk by delaying critical updates, decreasing team efficiency, and increasing cost.

As part of any organization's IT Operations program, a good patch management strategy with the ability to know what to patch, when to patch, and how to auto-patch on a schedule through a proper change control process is paramount to reducing risk. Unfortunately, organizations are limited by traditional patching tools because they:

- Fail to deliver comprehensive patch and OS visibility or compliance across enterprise and work-from-home environments.

- Require dozens or hundreds of staging servers, increasing overhead and points for failure.

- Threaten to crash the operating environment when run at scale.

- Force administrators to follow sub-optimal patching processes and accept insufficient patch coverage.

- Require multiple tools to operate, place strain on the network, and leave organizations unable to apply all required patches in a timely manner – if at all

- Do not enable change control or integration into the change management lifecycle

servicenow.

57.5
days to remediate a vulnerability, according to Edgescan – Slideshare

38,000
Tanium identified and fixed over 38,000 missing patches across thousands of endpoints. Tanium further reduced our patching update window from weeks to under 24 hours – University of Salford

Over 99%
of patches deployed at a first-pass success rate – Autonation

97%
of the company's endpoints are now compliant with a 30-day patching cycle. That's up sharply from just 13% before using Tanium. - ABB

150 days
required to patch a vulnerability on average

Tanium Patch Management for ServiceNow IT Operations enables organizations to proactively identify, organize, and deploy patches in real time, through automation and business workflows in ServiceNow. Imagine a world where Patch Tuesday is automated Tanium and ServiceNow make this a reality by ensuring end-to-end patch lifecycles that automate manual steps that directly impact teams and processes. All while mitigating risk at scale, meeting SLAs, and exceeding expectations

Understand current patch applicability and level of business risk with real-time patch information on CIs correlated with relationships through the CMDB

Understanding what to patch is extremely important. Tanium Patch Management for ServiceNow will enable organizations to:

- Scan, collect, and report on all applicable patches as records in ServiceNow

- Associate business risk criteria with current open patches by CI and CI Classes

- Determine upstream and downstream impact of breached SLAs by configuring simple dashboards

Automate patch lifecycle across either single endpoints or groups of devices using existing processes around sniper patching, monthly patching through change requests

Apply patches to endpoints based on patch applicability, monthly patching, and sniper patching scenarios. Associate patches with changes for planning and execution.

- Plan for and schedule patches based on risk calculations, so your most critical systems are always prioritized

- Schedule your monthly patching schedule automatically to avoid delays

- Use change request workflows to embed Tanium patching into existing processes seamlessly

- Meet and exceed SLAs on patch management providing executive KPIs

Future: Bringing autonomous patch management to life with auto ring-based patch deployment testing, and auto-risk scoring

With fully automated playbooks, Tanium Patch will enable organizations to create and learn from patch deployments.

- One-time playbook configuration using Tanium autonomous patching steps including ring-based patch testing

- Learning from previous deployments to make patching more efficient, fully automated, and zero-touch

- Intelligent use case-driven patch solutioning via AI, such as helping understand patterns of patch lifecycles to predict potential ring-based problems

Tanium Patch Management for ServiceNow IT Operations enables end-to-end patch orchestration lifecycle through change management increasing efficiency and reducing risk

- **Improved efficiency:** Know what to patch and when to patch faster with embedded single-click change control steps in ServiceNow. Reduce time by 75% from typical multi-tool, multi-team processes.

- **Reduced cost:** Consolidate legacy tools with strategic platform-to-platform integration and reduce tool licensing, maintenance, and support.

- **Reduced risk:** By ensuring Tanium can patch monthly on a schedule, we see a significant reduction in risk, allowing teams to focus on other high-priority items while meeting and exceeding SLAs.

With Tanium Patch Management for ServiceNow, employees and customers can:

- Proactively scan and understand all open patches against endpoints

- Automate patching to meet or exceed SLAs through change management

- Manage seamless workflow automation for patch teams in ServiceNow

- Assess business risk of missing SLAs

- Deploy a Patch at scale through the ServiceNow change process

- Uninstall a Patch (i.e., roll back) at scale through the ServiceNow change process

Tanium Patch Management for ServiceNow IT Operations empowers organizations to accelerate their patch management lifecycle by removing manual steps and augmenting ServiceNow processes with the speed and scale of Tanium. This provides a more unified interface, with related incident data that is meaningful and actionable. With Tanium Patch Management for ServiceNow IT Operations, organizations can reduce complexity, gain greater control, ensure audit and entitlement compliance, and increase operational resilience.

BUSINESS DIFFERENTIATORS:

- Near-real-time ability to patch at scale
- 100% visibility into all assets

TECHNICAL DIFFERENTIATORS:

- Fully integrated into ServiceNow's change-management process
- Compliant with the ServiceNow ITSM framework
- Fully certified integrations
- Tanium-patented communication architecture supporting real-time data and near-real-time remediation
- Uniquely supporting largest data sets for ServiceNow

TANIUM