DATA SHEET

Tanium Patch Orchestration for Vulnerability Response Integration for ServiceNow

Automated patching of endpoints associated with change records, based on vulnerability and compliance risk

21%

21% of surveyed security teams indicated that patching vulnerabilities in a timely manner was the most challenging aspect of their vulnerability management processes.

22%

22% of surveyed security teams indicated that vulnerabilities are most often prioritized and patched based on vulnerabilities that have been exploited.

Tanium Patch Orchestration for Vulnerability Response Integration for ServiceNow enables organizations to mitigate risk, maintain compliance, reduce disruption, and minimize complexity through patch orchestration associated with changes – closing the loop on detected vulnerabilities and compliance issues.

Patching known vulnerabilities shouldn't be so painful

One of the most critical IT operations tasks is to ensure that all systems are running and up to date with the latest patches. Stale systems are prone to failure and incompatibilities, and missed patches expose organizations to breaches and severe vulnerabilities that expose expand the attack surface.

But current patching solutions don't provide IT teams with the comprehensive visibility required to ensure successful patching at scale, making even simple patch updates difficult to manage. Organizations also continue to fear downtime or outages caused by patching processes, leading to delays and off-peak hour deliveries – which often miss endpoints that are offline – further exposing risk from vulnerabilities and attacks.

An organization's security team recently ran vulnerability assessments and determined that a large number of endpoints are outdated and non-compliant due to missing and failed patches. Several of the affected endpoints are servers that are critical to maintaining business services for both employees and customers, and many affected laptops are assigned to executives and other employees with highly sensitive data.

The security and IT teams have been tasked with prioritizing, planning, scheduling, and applying patches for the organization's most vulnerable assets – a process that has been difficult due to manual efforts and inefficient point solutions.

Tanium Patch Orchestration for Vulnerability Response Integration for ServiceNow enables IT and security teams to apply patches – based on applicability, detected vulnerabilities, and compliance gaps – through planned change management processes.

Prevent security breaches and keep endpoints up to date.

- Proactively mitigate risk, maintain compliance, and reduce disruption caused by outdated endpoints missing critical patches.
- Apply patches to one device or all applicable devices – all through correlation with scheduled changes.

Close the loop on vulnerable items and vulnerable groups.

- Patch at scale while ensuring the most critical vulnerabilities are resolved first, to reduce financial and security risk.
- Classify and prioritize patch initiatives based on known vulnerabilities and their calculated risk.

Coordinate and plan for patches at scale.

- Confidently plan patch deployments through the change lifecycle, with test and deployment plans, approvals, and scheduled workflows.
- Associate patches with change records to prioritize tasks, affected configuration items, and solution options.

Tanium File Integrity and Unauthorized Change Monitoring Integration for ServiceNow enables IT and security teams to close the loop on identified vulnerabilities and known risk through automated patch orchestration tied to planned change processes.

- Apply patches to one device or all applicable devices – all through correlation with scheduled changes.
- Classify and prioritize patch initiatives based on known vulnerabilities and their calculated risk.
- Confidently plan patch deployments through the change lifecycle, with test and deployment plans, approvals, and scheduled workflows.

Key capabilities include the ability to:

- Detect and view missing and installed patches across all endpoints.
- Prioritize patch initiatives based on calculated risk from known vulnerabilities and endpoint criticality.
- Automate patching of all applicable configuration items at once, eliminating the need for sniper patching of select devices.
- Initiate patches through planned change lifecycle processes in ServiceNow.

Combining the Tanium XEM platform capabilities with the ITSM capabilities in ServiceNow provides a better total experience for the IT agent, employee, and customer.

The Tanium Converged Endpoint Management (XEM) platform offers comprehensive IT operations and security management from a single agent. It delivers complete, accurate, and real-time endpoint data, regardless of scale or IT complexity, and uses minimal infrastructure. Tanium XEM provides visibility, control, and remediation needed to help you continuously manage your organization's endpoint risk.

DEMO OUR SOLUTION

Schedule a demonstration to see Tanium XEM live and visualize exactly how our solution can transform your endpoint management and security.

SEE TANIUM LIVE

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.