SOLUTION BRIEF

Tanium Security Operations for ServiceNow

Act on real-time vulnerability and threat intelligence—so security teams can detect, prioritize, and remediate with certainty.

Tanium Security Operations for ServiceNow brings the power of Tanium's Autonomous Endpoint Management (AEM) and real-time endpoint threat intelligence into ServiceNow. From eliminating data silos and enabling IT and security teams to act faster and smarter, to gaining full visibility and control over automated response, organizations can achieve proactive security operations—all from within the workflows they already trust.

Security teams can't act on what they can't see

In an era of accelerating threats and growing complexity, traditional security operations tools can't keep up. Without real-time visibility into endpoint vulnerabilities and configuration drift, teams are stuck reacting to stale data—delaying response, increasing risk, and escalating costs.

Compatibility issues, resource constraints, and manual processes all slow teams' efforts to close these critical gaps. What holds teams back?

- **Slow detection:** Vulnerability scans take too long, and data is outdated before action can be taken.
- **Fragmented tooling:** Disconnected systems create blind spots, slow handoffs, and missed signals.
- **Limited automation:** Manual steps introduce risk, waste time, and increase the burden on overextended teams.
- **Lack of context:** Incidents lack the data needed to prioritize and act with confidence, making containment reactive and costly.
- **Inaccurate recommendations:** Stale and incomplete data leads to inability to take action.

Tanium Security Operations for ServiceNow enables proactive vulnerability response and real-time threat mitigation, powered by Tanium's AEM platform. Security and IT teams no longer wait for scans or switch between tools, instead, they respond at the speed of risk—correlating vulnerabilities and threat signals with CMDB assets, triggering automated patching through change workflows, and containing security incidents with live endpoint data directly within ServiceNow.

43%

of risk managers have experienced 3+ critical risk events this past year, according to Forrester

$600B

Cybercrimes cost $600 billion a year worldwide, says Mordor Intelligence

33%

of total breach costs are due to lost business, finds Ponemon Institute

> "Organizations worldwide are facing sophisticated ransomware, attacks on the digital supply chain and deeply embedded vulnerabilities. The pandemic accelerated hybrid work and the shift to the cloud, challenging CISOs to secure an increasingly distributed enterprise – all while dealing with a shortage of skilled security staff."

Peter Firstbrook
Research Vice President, Gartner

Collect real-time vulnerability data to proactively identify and investigate risk

Automatically correlate vulnerabilities with configuration items in the ServiceNow CMDB to prioritize remediation based on risk calculations.

- Scan and report on real-time vulnerability data – in minutes, not days – to find gaps that lead to inaccurate data and increased financial and security risk exposure.
- Eliminate the time and manual effort of remediation validation with the ability to automatically rescan endpoints and confirm change outcomes.

Leverage workflows and automate patch orchestration based on applicability, detected vulnerabilities through planned change management processes

Plan for, schedule, and deliver patches at scale through risk calculations, configuration item grouping, and change management processes– so your most critical systems are always prioritized.

- Proactively mitigate risk, maintain compliance, and reduce disruption caused by gaps in outdated endpoints missing critical patches.
- Confidently plan patch deployments through the change lifecycle in ServiceNow – with test and deployment plans, approval processes, and scheduled workflows.

Provide IT, security, and risk teams in ServiceNow with real-time endpoint data, remediation actions, and threat occurrence searches

Enrich security incidents in ServiceNow with the most important, real-time data about associated configuration items.

- Expedite the investigation, prioritization, response, and remediation of security incidents – without context switching between tools.
- Uncover the actual prevalence of threats across all endpoints, enabling security incidents to be resolved at scale.

Tanium solutions for ServiceNow

Tanium AEM for ServiceNow gives security teams the intelligence and automation they need to act fast—with confidence. No guesswork, no silos—just real-time visibility and AI-powered control embedded directly in ServiceNow.

By integrating Tanium's real-time endpoint insights with ServiceNow Security Operations, organizations move beyond reactive containment to proactive control. Whether it's patching vulnerable systems at scale or investigating and containing threats—Tanium fuels every SecOps decision with data and actions you can trust.

Discover how Tanium and ServiceNow SecOps deliver proactive security and automated control.

Tanium has embedded its real-time endpoint intelligence directly into ServiceNow Security Operations—transforming how teams detect, investigate, and respond to risk. With Tanium's Autonomous Endpoint Management (AEM) capabilities powering SecOps workflows, security teams get more than visibility—they gain continuous, actionable insight delivered at speed and scale. Whether responding to threats, remediating vulnerabilities, or enforcing policy, Tanium AEM for ServiceNow ensures every action is informed by live data, executed within the workflows teams already trust, and reinforced by AI-driven automation across the platform. The result is faster response, stronger resilience, and greater confidence in every decision.

Integrations that comprise Tanium Security Operations for ServiceNow are:

Vulnerability Management for ServiceNow

- Required Tanium platform features: Tanium Core, Tanium Comply
- Required ServiceNow platform features: SecOps (Vulnerability Response)

Patch Management for Vulnerability Response

- Required Tanium platform features: Tanium Core, Tanium Patch
- Required ServiceNow platform features: SecOps (Vulnerability Response and Vulnerability Response Patch Orchestration)

Security Incident Response

- Required Tanium platform features: Tanium Core, Tanium Threat Response
- Required ServiceNow platform features: SecOps (Security Incident Response)

With Tanium Security Operations for ServiceNow, security teams can

- Prioritize threats based on real-time risk and business impact
- Proactively identify endpoint vulnerabilities
- Automate patching to eliminate vulnerability gaps through change management processes
- Shrink investigation and resolution times—at enterprise scale
- Enrich security incidents with real-time intelligence to significantly reduce response and remediation times
- Minimize the impact and cost of breaches

Tanium Security Operations for ServiceNow also empowers organizations to accelerate their security-incident lifecycle by removing the number of manual investigation steps and augmenting ServiceNow processes with the speed and scale of Tanium. This provides a more unified interface, with related incident data being presented in ways that are both meaningful and actionable. With Tanium and ServiceNow, organizations can reduce complexity, gain greater control, ensure audit and entitlement compliance, and increase operational resilience.

Business Differentiators

- End-to-end vulnerability management in ServiceNow
- Security risk identification and remediation tied to the ServiceNow CMDB and change management processes
- Proactively mitigate risk and reduce disruption due to vulnerability gaps
- Expedite the investigation, response, and remediation of security incidents through automated workflows in ServiceNow

Technical Differentiators

- Fully certified ServiceNow integrations leveraging Tanium's patented linear chain architecture for real-time data and remediation
- Collect and correlate real-time vulnerability data with configuration items in the ServiceNow CMDB
- Automated patching based on calculated risk and tied to change management processes
- Enriched security incidents with real-time endpoint data and actions

TANIUM & SERVICENOW

Discover how Tanium and ServiceNow can help your organization reduce cyber risks and increase control.

Learn more →

TANIUM

The Power of Certainty.™

Visit us at www.tanium.com and follow us on LinkedIn and X.