SOLUTION BRIEF

Tanium Security Operations for ServiceNow

Identify, correlate, prioritize, and remediate risk of endpoint vulnerabilities and security incidents in real time

Tanium Security Operations for ServiceNow unifies IT, security, and risk teams in ServiceNow to proactively identify, prioritize, and remediate risk from vulnerabilities, unauthorized changes, non-compliant configurations, and security incidents.

Too slow. Too siloed. Too limited.

Maintaining your cyber resilience and vulnerability management while responding to security incidents faster gets harder every day. Expanding physical and virtual infrastructure and a proliferation of software and end-user devices make it ever more difficult to identify, correlate, and prioritize vulnerabilities and risk exposers.

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

IT and security operations teams need to be able to work together quickly. Unfortunately, existing security operations tools are often:

- **Slow:** They can take days, even weeks, to complete scans, meaning the data they serve is often stale, which leads to reactive – rather than proactive – response.
- **Siloed:** They can't work together, further isolating the security and operations teams. Disconnected platforms and tools make it difficult to properly identify risk and prioritize based on non-hardware or software factors, such as business impact and service dependencies.
- **Inefficient:** They consume heavy bandwidth, rely on manual processes, and fail to scale, which hurts overall network performance.
- **Limited:** They suffer from blind spots. And the risks they do find, they fail to prioritize, which leads to difficulties in correlating, prioritizing, and assessing the true impact of risk to the business.

Tanium Security Operations for ServiceNow enables organizations to proactively identify, correlate, and calculate risk through automated searches of known vulnerable assets and activities – facilitating IT, security, and risk teams in ServiceNow to find, prioritize, and fix critical gaps through automated patch orchestration. When security incidents are detected, real-time actionable data about all affected endpoints expedites remediation at scale without context switching between tools.

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 and compliance data to proactively identify and investigate risk

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

- Scan and report on real-time vulnerability and compliance 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, and compliance gaps 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, unapproved change alerts, remediation actions, and threat occurrence searches

Enrich security incidents in ServiceNow with the most important, real-time data about associated configuration items and alert on unapproved changes to files and registries.

- 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

ServiceNow brings organizations of every size and in every industry smarter, faster, and better ways to work. With Tanium's ServiceNow solutions, these organizations can maximize their investment in ServiceNow by leveraging real-time endpoint data that is accurate at any scale, no matter if the endpoint is physical, virtual, cloud-based, or IoT.

Tanium has integrated its industry-leading Converged Endpoint Mangement (XEM) platform with ServiceNow, the leader in Gartner Magic Quadrant for IT Service Management (ITSM) platforms for nine consecutive years. Tanium integration brings unparalleled visibility, real-time data, and proactive remediation to improve overall agent and user experiences.

Combining Tanium and ServiceNow can empower your IT and security operations workflows with accurate, near-real-time data. The capabilities extend beyond just funneling data into ServiceNow. With With ServiceNow as the brains of an organization's IT and Security operations, and Tanium's visibility and actionability acting as the eyes and hands, you can increase productivity and maximize your joint-platform investments.

Integrations that comprise Tanium Security Operations for ServiceNow are:

Vulnerability Response Integration

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

Patch Orchestration for Vulnerability Response

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

Configuration Compliance Integration

- Required Tanium platform features: Tanium XEM Core, Tanium Comply
- Required ServiceNow platform features: SecOps (Vulnerability Response and Configuration Compliance)

File Integrity and Unauthorized Change Monitoring

- Required Tanium platform features: Tanium XEM Core, Tanium Integrity Monitor
- Required ServiceNow platform features: ITSM

Security Operations Integration

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

With Tanium Security Operations for ServiceNow, security teams can

- Proactively identify and correlate endpoint vulnerabilities and configuration gaps with ServiceNow CMDB configuration items
- Automate patching to eliminate vulnerability risk through planned change management processes
- Eliminate risk exposure and prepare for audits
- Identify and alert on unauthorized changes to files and registries
- 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 response in ServiceNow
- Security risk identification and remediation tied to the ServiceNow CMDB and change management processes
- Proactively mitigate risk, maintain compliance, 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 and compliance 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 →