SOLUTION BRIEF

Tanium Vulnerability Risk and Compliance for ServiceNow

Reduce risks and increase control with Tanium Vulnerability Risk and Compliance for ServiceNow.

With Tanium Vulnerability Risk and Compliance for ServiceNow, organizations can proactively identify endpoint vulnerabilities and compliance risk, automate patching to eliminate vulnerability gaps, enrich security incidents with real-time intelligence, and identify unauthorized changes and configurations.

Too slow. Too siloed. Too limited.

CISOs today need complete visibility and control of all assets across their expanding and distributed landscapes. CISOs must also be able to complete impromptu audits, meet ever-changing compliance and regulatory requirements, stay up to date on the latest vulnerabilities, and respond to security incidents quickly.

Most cyber breaches exploit known asset vulnerabilities or simple application misconfigurations. To close these risks, organizations must continuously scan their endpoints for vulnerabilities and misconfigurations, then rapidly prioritize and remediate any problems they find. Unfortunately, existing vulnerability management tools are often:

- **Slow:** They can take days, even weeks, to complete scans, meaning the data they serve is often stale.
- **Siloed:** They can't work together, further isolating the security and operations teams.
- **Inefficient:** They consume heavy bandwidth, hurting overall network performance.
- **Limited:** They suffer from blind spots. And the risks they do find, they fail to prioritize.

Tanium Vulnerability Risk and Compliance (VRC) for ServiceNow enables organizations to proactively identify, correlate and calculate risk of endpoint vulnerabilities and compliance gaps in real time, through automated searches of known vulnerable assets, activities, and traffic on networks. This integration facilitates IT, security, and risk teams to find, prioritize and proactively fix critical gaps that otherwise lead to inaccurate data, increased financial and security risk exposure, through Tanium's VRC and automated patch orchestration.

43%

of enterprise risk management (ERM) decision-makers report having experienced three or more discrete critical risk events over the past 12 months, 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 for prioritization and investigation

Automatically search for known vulnerable assets, activities, and traffic on your network. Correlate vulnerabilities and compliance assessments with configuration items in the ServiceNow CMDB.

- Scan, collect and report on vulnerabilities, not in days, but minutes.
- Find and fix compliance gaps that lead to inaccurate data and increased financial and security risk exposure.
- Validate remediations across vulnerability items and vulnerability groups to confirm successful changes.

Automate patch orchestration across either single endpoints or groups of devices, based on known compliance issues and detected vulnerabilities

Apply patches to endpoints based on patch applicability, detected vulnerabilities, and compliance gaps. 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.
- Close the loop on detected vulnerabilities with patch orchestration tied to planned and unplanned changes.

Bridge the gaps between IT, security, and risk teams and quickly identify the true scope of security incidents

Enrich security incidents with the most important real-time data about associated configuration items, including logged-in users, network statistics, and running processes. Then search across all endpoints for risk occurrences.

- 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 integration with ServiceNow

Seamlessly integrate real-time visibility and risk detection with unified tools and data supporting ServiceNow Security Operations, IT Service Management, and IT Operations Management.

Tanium has integrated its industry leading 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, real-time data. The capabilities extend beyond just funneling data into ServiceNow. With ServiceNow as the brains of an organization's IT processes and Tanium acting as the eyes and hands, you can increase productivity and maximize your investment.

Integrations that comprise the Tanium Vulnerability Risk and Compliance solution are:

Vulnerability Response Integration

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

Configuration Compliance Integration

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

Security Operations Integration

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

File Integrity and Unauthorized Change Monitoring

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

With Tanium Vulnerability Risk and Compliance for ServiceNow, employees and customers can:

- Proactively identify endpoint vulnerabilities
- Automate patching to eliminate vulnerability gaps through change management
- Eliminate risk exposure and prepare for audits
- Identify and alert on unauthorized changes
- Enrich security incidents' response times with real-time intelligence
- Minimize the impact and cost of breaches

Tanium Vulnerability Risk and Compliance 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 VRC for ServiceNow, organizations can reduce complexity, gain greater control, ensure audit and entitlement compliance, and increase operational resilience.

Business differentiators

- Near-real-time ability to patch vulnerabilities at scale
- 100% visibility into all assets
- Linear chain architecture

Technical differentiators

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

LEARN MORE ABOUT TANIUM SERVICENOW INTEGRATION

Discover how Tanium Vulnerability Risk and Compliance for ServiceNow can help your organization reduce cyber risks and increase control.

Learn more →

Tanium, the industry's only provider of converged endpoint management (XEM), is the reference platform of choice to manage complex security and technology environments. Only Tanium protects every endpoint from cyber threats by integrating workflows across IT, Risk, Compliance, and Security into a single platform that delivers comprehensive visibility across devices, a unified set of controls, real-time remediation, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Tanium has been named to the Forbes Cloud 100 list for seven consecutive years and ranks for the second consecutive year on the Fortune 100 Best Companies to Work For. In fact, 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.