DATA SHEET

Tanium Configuration Compliance Integration for ServiceNow

Identify, prioritize, and remediate configuration issues in real time to reduce financial and security risk.

21+%

Last year, misconfigurations accounted for 21+% of error-related breaches.

https://www.verizon.com/business/en-gb/resources/2023-data-breach-investigations-report-dbir.pdf

Tanium Configuration Compliance Integration for ServiceNow provides up-to-date configuration compliance assessments against operating systems, applications, security configurations, and policies, enabling Security Operations (SecOps) teams to eliminate security exposures, improve overall IT hygiene, and prepare for audits.

Infrastructure and application vulnerabilities are only part of your attack surface

While the majority of breaches exploit known vulnerabilities, misconfigurations account for a significant number of breaches that could have been prevented with proper configuration. Additionally, non-compliant configurations can lead to financial and reputational risk from ever-changing regulatory laws and standards. To address this risk, IT, and security teams must continuously scan their endpoints for configuration compliance, and rapidly prioritize and remediate any issues found.

However, many configuration management tools are slow, siloed, inefficient, and limited in scope. Scanning may take days or weeks to complete, and the data returned is stale. Security and operations teams work in isolation, preventing collaboration and automation. Heavy bandwidth consumption severely impacts network performance. Point solutions produce blind spots and are unable to prioritize the risks they do find.

A new IT risk manager at a financial organization has been tasked with ensuring all endpoints are compliant with major regulatory standards – such as PCI, SOX, and GDPR – after several internal audits were failed. Various tools and point solutions are used to gather compliance data about operating systems, applications, and policies, but the data is often incomplete, difficult to prioritize, and resource-consuming to validate remediations. A single non-compliant endpoint can expose the organization to significant financial and security risk.

Tanium Configuration Compliance Integration for ServiceNow

Provide IT, vulnerability, and security teams with continuous, up-to-date configuration compliance assessments of their entire IT estate, enabling them to correlate, prioritize, remediate, and validate in real time.

Scan in minutes and report on non-compliant configurations across all endpoints

Eliminate the need for different monitoring tools and point solutions to cover all of your networks and operating systems.

- Fulfill configuration hardening to meet industry regulatory requirements – including PCI, HIPAA, and SOX – across all operating systems.

Automatically correlate configuration compliance exposures with configuration items in the ServiceNow CMDB

Prioritize and remediate the most important configuration gaps that lead to inaccurate data and increased risk exposure.

- Identify the specific endpoints detected in compliance assessments to automatically calculate risk based on criticality and configuration severity.

Quickly validate compliance remediations and gain insights to manage risk.

Automate the configuration compliance lifecycle and close risk issues without manual intervention based on test results.

- Re-scan known misconfigurations to validate remediation actions overall configuration compliance.

Tanium Configuration Compliance Integration

ServiceNow enables IT, vulnerability, and risk teams to continuously scan and identify configuration risks in real time for prioritization and remediation.

- Scan in minutes and report on non-compliant configurations across all endpoints.
- Automatically correlate configuration compliance exposures with configuration items in the ServiceNow CMDB.
- Quickly validate compliance remediations and gain insights to manage risk.

Key capabilities include the ability to:

- Leverage the Security Content Automation Protocol (SCAP) or use any Open Vulnerability and Assessment Language (OVAL) content in addition to the updated-daily Tanium Comply content library.
- Automatically correlate configuration risk with configuration items in the ServiceNow CMDB.
- Prepare for audits with the ability to run compliance scans on demand and report back in minutes.
- Eliminate time and effort of manual remediation validation with the ability to automatically rescan to confirm change outcomes and configurations.
- Collect real-time configuration compliance intelligence anytime with ServiceNow workflow actions.

DEMO OUR SOLUTION

Schedule a demonstration to see Tanium XEM live and to 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. Visit us at www.tanium.com.