FORESCOUT

TANIUM

The Forescout-Tanium Solution

Automate Real-time 360-degree Asset Intelligence and Security Governance

Benefits

- Streamline enterprise-wide asset management, security governance, cross-team collaboration and audit readiness
- Increase threat defense via unified endpoint and network security controls
- Reduce manual labor and risk of cyber threat impact with automated, context-aware security workflows

Organizations of all sizes and sectors are facing the threat of a cyberattack every day. They are most vulnerable when they keep IT, Operational Technology (OT), security and networking teams in silos, rely on manual tasks, and lack real-time visibility and control of all technology assets – on or off the network.

The integrated Forescout-Tanium solution automates information sharing and orchestrates workflows that help unify IT, IoT and OT asset management, security and network operations, eliminating security gaps that put organizations at risk. The solution automates real-time, 360-degree, asset intelligence and security governance which enables organizations to increase operational resilience, asset protection and threat defense at enterprise scale.

Gain Comprehensive and Actionable Asset Intelligence

Continuous and actionable visibility of every endpoint is paramount to cybersecurity success. Tanium provides extensive real-time visibility and control of managed end-user, data center and cloud endpoints, including transient 'work-from-anywhere' endpoints located off the network. Forescout continuously discovers, identifies and assesses all network-connected IT, IoT and OT devices in real-time and without disruption. Tanium shares its extensive endpoint data with Forescout and Forescout provides Tanium with additional network data for managed endpoints as well as data about non-Tanium managed endpoints. The integrated solution provides comprehensive enterprise-wide asset intelligence to govern more effectively.

Automate Security Governance and Reduce Risk

Tanium and Forescout leverage their combined real-time asset intelligence to dynamically enforce granular security policies that apply targeted, context-aware actions against every connected device on both the endpoint and at the network layer, as needed. This enables organizations to continuously enforce compliance for every asset, automate remediation and automatically respond to threats to immediately limit any potential impact. These integrated capabilities empower organizations to address 'comply-to-connect' use cases that have grown increasingly important in a work-from-anywhere world in which endpoints frequently leave and join corporate networks. Based on real-time device state, Forescout can enact compliance enforcement polices at the network layer, such as those that control network access and segmentation. Forescout can also trigger policy-driven workflows that direct Tanium to perform actions on managed endpoints. For example, Forescout can detect corporate endpoints that need the Tanium agent and automatically orchestrate agent installation via Tanium.

Capability Highlights

- Gain comprehensive, real-time asset intelligence across all device types and locations
- Continuously assess all technology assets for compliance or compromise
- Centralize policy management and automate network access control, segmentation, compliance remediation and threat response workflows

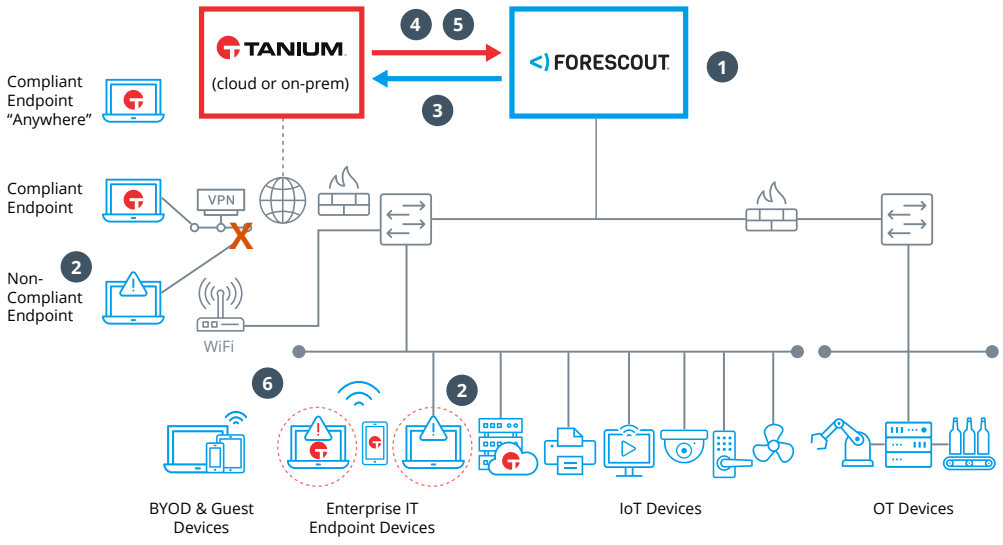
Forescout can also validate that every managed device connecting to the network has received a recent Tanium vulnerability scan and has installed all the patches Tanium has pushed. If devices are out of compliance, Forescout can direct Tanium to launch a vulnerability scan and will tag those devices that are unpatched so Tanium will patch them during the next deployment cycle.

Beyond the compliance remediation workflows described above, Forescout adds further protection by automatically containing non-compliant and compromised devices by applying policy-driven network controls that quarantine or block network access. Such policy-driven controls can occur immediately in response to severity of non-compliance, Tanium vulnerability scan and compliance check results as well as to live threats as they are detected by Tanium. This helps prevent or dramatically limit the impact of a cyberattack. Once incidents are remediated, Forescout will allow devices back on the network with each device's appropriate network access and segmentation policies continuously enforced.

Increase Cross-Team Collaboration and Audit Readiness

Collaboration across asset, security and network operations teams as well as among third-party vendors is key to reducing risk. The Forescout-Tanium solution helps close security gaps, streamline collaboration among teams and increase efficiency by unifying IT, IoT and OT asset intelligence and orchestrating workflows that foster organization-wide governance. As a result, organizations are equipped with greater threat defense, resiliency and audit readiness.

Forescout – Tanium Architecture Overview



1. Forescout discovers, identifies and assesses all connected assets/devices
2. Forescout detects non-compliant devices that need the Tanium agent, required patches, a vulnerability scan and/or compliance check and contains the at-risk device
3. Forescout facilitates remediation with Tanium to install the agent, run a scan, do a compliance check or push a patch
4. Tanium feeds Forescout managed endpoint data, including those off-network, for unified view and to apply policies against
5. Tanium alerts Forescout of vulnerabilities or threats detected
6. Forescout utilizes combined asset intelligence to enforce network access, segmentation and threat response policies to mitigate risk

For more information or to schedule a discussion, please contact: Forescout at alliances@forescout.com

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com