Joint Solution Brief

How Oomnitza + Tanium Improves IT Security and Gives IT Teams Observability Superpowers

CONTENTS

Introduction

Core components of IT security for every enterprise are an endpoint management layer for IT asset discovery and tracking, and an enterprise technology management (ETM) layer to manage the broader scope of IT infrastructure. Endpoints are the most common way that users access enterprise networks and IT ecosystems, it is therefore crucial to possess both a detailed real-time understanding of the status and security of endpoint assets, as well as a contextual view of their use. This view includes what other resources (hardware, software, Cloud) are connected to the specific endpoint, who owns the endpoint and all connected systems, what key systems is an endpoint and its user able to access, and what key workflows or actions can an endpoint trigger.

This is why a holistic approach to Enterprise Technology Management (ETM), combined with detailed endpoint asset information (Tanium) is critical and becoming more so as global IT moves permanently into a hybrid model. When integrated together, ETM connects endpoint management to other systems and can create unified views, reports and automated workflows to streamline more complex processes and provide IT security and asset usage intelligence at enterprise scale. Integrating endpoint management and ETM is even more important when endpoints may be accessing networks and connecting with other systems via VPNs, over unsecured home WiFi routers or public access points, and operating from literally anywhere.

In many organizations, endpoint management is only loosely integrated with other sub-ITAM systems and no ETM aggregation and reconciliation layer exists. This leads to inefficient processes where IT help desks and security teams may be solving problems particular to siloed management systems, but those systems cannot talk to each other. The disconnect means that answering even basic questions, such as what are all the IT assets associated with a person, presents major challenges. In addition, the disconnect makes it difficult to automate manual processes for audit compliance and anomaly response, even when those processes are repeated frequently. For IT security teams, the lack of a complete picture and inability to easily update views across all assets poses a serious risk in terms of vulnerability assessment and response times. These challenges are only growing more significant as IT asset classes expand to include more non-traditional endpoints such as IoT and other connected devices, as well as cloud-based assets like SaaS, PaaS, and IaaS.

Oomnitza and Tanium are best-in-class solutions for ETM and unified endpoint management (UEM), respectively. Oomnitza integrates with Tanium via the Oomnitza omniconnector, a Python-based software module that integrates over 80 leading IT, security, HRIS and ERP solutions with the cloud-based Oomnitza ETM solution. Because Oomnitza supports bi-directional data management, Tanium admins can benefit from automated updates to endpoints or users under their management from other systems and also construct workflows that inform key systems to status changes and anomalies reported by Tanium.

The combined Oomnitza-Tanium solution helps teams in Security, Compliance and HR work together on complex problems: enterprises can set up complete views of all key technology asset activities and improve security posture as well as response mechanisms and vulnerability assessment. The two solutions can be integrated in minutes to manage laptops, mobile devices, SaaS, IaaS, PaaS, smart peripherals (monitors) and much more. The integration is intuitive and does not require any dedicated engineering time or additional coding; setting up a simple link from the Tanium API into Oomnitza delivers the full functionality and enables all the capabilities of integration.

How Oomnitza Addresses Dynamic IT Security and Asset Management Challenges

Oomnitza is an Enterprise Technology Management solution that provides a holistic view of all IT assets in a single system and empowers IT and security teams to manage the full lifecycle of assets and devices across all classes from a single integrated perspective. Oomnitza enables two-way data flows between siloed solutions, creating a unified view of the entire IT portfolio from a single, accurate database. Oomnitza improves security, increases compliance, streamlines and simplifies logistics, reduces costs, and supports the design and delivery of a superior employee experience.

An agentless solution with a REST API and extensible Python-based connector architecture, Oomnitza is pre-configured to connect directly with the Tanium API. Oomnitza acquires, cleans and reconciles data from other agents as well as from SSOs, employee directories, and other ITAM, SAM or CSB systems. This makes it simple for IT and security teams to create detailed, multi-step automated workflows and playbooks to execute in conjunction with Tanium workflows for asset management, vulnerability assessment, compliance and audit data handling, and policy enforcement. Using the Oomnitza multi-connector, IT security and management teams can link together multiple systems across IT management and support, IT security, and compliance and enforcement.

Oomnitza allows Tanium admins to tag and update assets and status in the Tanium asset or user view, or in the Oomnitza dashboard. This makes it easier to manage processes without forcing changes in workflows while increasing accuracy. This also allows IT admins to gain a holistic view of users, business units, geographic locations and functions across all asset types (mobile, Cloud, physical) and across SaaS, IaaS, PaaS and other modalities. For IT security teams using Tanium and Oomnitza, the integration empowers faster time-to-resolution, better anomaly detection and management, and an improved security posture.

Oomnitza + Tanium Integration Benefits

With Oomnitza and Tanium, IT and security teams can manage, configure, monitor and secure their entire IT estate with real-time visibility into changes and anomalies. This is critical for today's IT leaders who facilitate the operation and management of millions of globally distributed and increasingly diverse assets, while ensuring minimal downtime and maintaining a strong security posture. With the integration between Oomnitza and Tanium, you can:

Know what software and hardware you have at all times.
Oomnitza can combine information from other sub-systems such as SAM or CMDBs with endpoint data and data from Tanium, SSOs and authentication systems. Procurement data from ERPs or from VARs such as SHI and CDW can also be included. Building on this rich set of data, the combination of Oomnitza and Tanium provides IT security and management teams global visibility into software and hardware running on an enterprise's systems, as well as procured IT assets, whether or not they have been deployed.

Pull information from ticketing and other systems to create a 360-degree view of the status of every IT asset.
Bi-directional data integrations between Oomnitza and Tanium and other systems such as Jira, ZenDesk, InTune and JAMF allow for Oomnitza to generate a complete view of asset status that includes upgrade cycle, repair history, and proximity or exposure to compromised assets and accounts.

Perform compliance checks and vulnerability scans on demand.
Oomnitza allows teams to create detailed workflows and playbooks that can tap into Tanium endpoint information and feed that information into other systems for managing compliance or vulnerabilities.

Take control of unmanaged endpoints and rogue devices.
Tanium can identify unmanaged endpoints and Oomnitza can map those endpoints back to specific IT records to identify the most recent owner, or notify IT teams to take control of those endpoints. For rogue devices, Tanium can identify those assets and Oomnitza can subsequently ensure that those devices are purged or banned from access directories and authentication systems.

Simplify regulatory compliance and file integrity monitoring.
Using bi-directional workflows, Oomnitza can pull multiple types of data to automatically verify compliance status. For file integrity, Oomnitza can combine Tanium endpoint data with data from system configuration and management tools to create a holistic and more accurate view of system and file integrity.

Distribute and report on operating system updates quickly and reliably.
Working together, Oomnitza and Tanium can rapidly generate reports on the status and progress of operating system updates across an entire enterprise and update all other related systems with OS-level status and version number.

Improve the end user experience by managing performance of all network-connected devices.
By pulling in Tanium endpoint data and combining it with ticketing data and support data and other system data focused on device performance, Oomnitza and Tanium can create a unified performance dashboard for network-connected devices and highlight those that require additional attention due to poor performance.

Oomnitza + Tanium Improves Security, Efficiency and Compliance

Alone, Oomnitza and Tanium offer IT security, compliance and operations teams strong value. Together, the two systems can exert a dramatic positive impact on many key IT metrics including:

- Reducing instances of data loss and exposure
- Reducing time-to-response and time-to-remediation in case of breaches or vulnerabilities
- Improving software license compliance with legal terms to avoid painful "true-up" penalties
- Reducing time required to initiate and complete an IT audit
- Reducing the exposed attack surface of an enterprise
- Cutting IT off-boarding duration for departing employees
- Improving the accuracy and reliability of IT asset security data and status

Overall, implementing an Oomnitza-Tanium integration saves IT teams money, time and hassles, while improving security and asset reliability. Setting up the integration takes minutes but rewards are nearly immediate.

About Oomnitza

Oomnitza offers the industry's most versatile Enterprise Technology Management platform that delivers key business process automation for IT. Our SaaS solution, featuring agentless integrations, best practices and low-code workflows, enables enterprises to quickly achieve operational, security and financial efficiency leveraging their existing endpoint, application, network infrastructure and cloud infrastructure systems. We help some of the most well-known and innovative companies to optimize resources, mitigate cyber risk, expedite audits and fortify digital experience.

Learn more at Oomnitza.com.

oomnitza