Tanium with IBM Automation

Automate app performance across your IT stack while mitigating security risks

Highlights

Automate from a single point of context across your IT stack

Manage endpoints in concert with application performance

Create harmony between ITOps and security teams

In today's world, applications are a key aspect of business; yet they remain the most common attack vector.[1] Traditional siloed priorities and tools force IT teams to manage application performance and security separately, which can unexpectedly slow applications and affect customer experience. Due to the siloed relationships between security and ITOps teams, it takes an average of 38 business days[2] for enterprises to patch IT vulnerabilities. With an average cost of USD 4.35 million per data breach[3], you can't allow performance issues to prevent security operations. At the same time, you can't let necessary operations halt business processes, cause downtime and jeopardize customer experience. Application performance and endpoints must be jointly managed.

Don't let necessary security operations limit application performance. The integration between IBM® Turbonomic® and Tanium with IBM Automation unifies IT and security teams to enable continuous application performance and assure security and compliance at a low cost.

Tanium with IBM Automation delivers real-time endpoint data that allows IT teams to discover new assets and analyze known vulnerabilities. This decreases risk and enables IT teams to gain complete visibility into their OS, applications and resources with endpoint management. IBM Turbonomic Application Resource Management (ARM) enables you to automate critical actions that proactively deliver the most efficient use of computing, storage and network resources to your apps at every layer of the stack. The solution does this continuously, in real time and without human intervention.

The integration between the two solutions enables IBM Turbonomic to make API calls to Tanium with IBM Automation. These calls pull high-fidelity endpoint data from Tanium with IBM Automation to ensure IBM Turbonomic has the most up-to-date grouping when executing resourcing actions to confidently accelerate automation for proactive performance and security. IBM's unique approach to full-stack visibility combines with dynamic resource management to provide complete context and automation across application and security operations for proactive performance and security. With this solution, your endpoint management practices (scanning, patching, and updating) never put application performance at risk and business-critical applications are automatically isolated from known vulnerabilities.

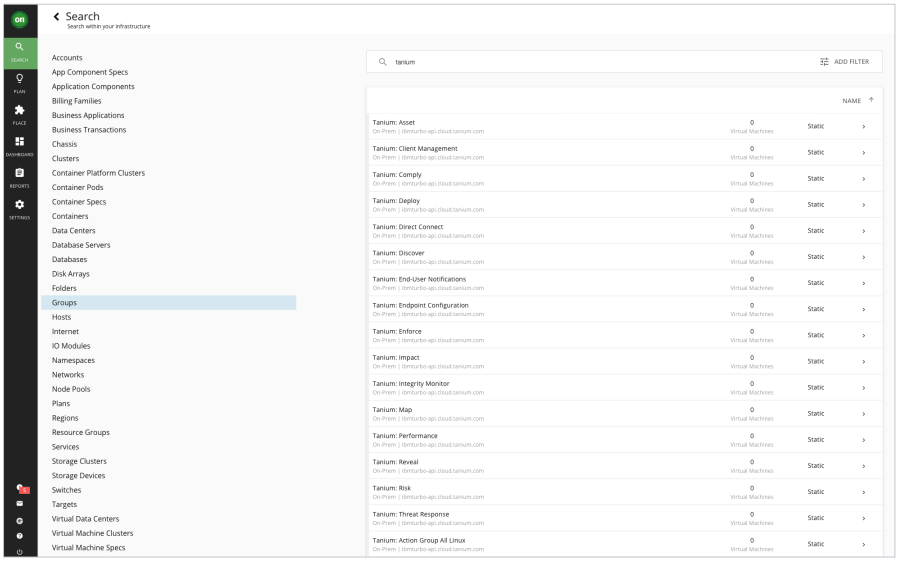

Figure 1. IBM Turbonomic uses data on endpoint groups to dynamically resource your endpoints.

Automate from a single point of context to ensure app performance while mitigating security risks

With data on endpoint groups with known vulnerabilities, IT teams can automate from a unified system of context. Using Tanium's data, IBM Turbonomic automatically sequesters workloads to secure systems, minimizing both security and performance risks. The solution combines full-stack visibility with dynamic resource management to provide complete context and automation across all your application and security operations for proactive performance and security.

Ensure business continuity and app uptime with performance-first endpoint management

Performance-first endpoint management assures business continuity while routine maintenance activities are underway. With endpoint data from Tanium, IBM Turbonomic determines when and how to best roll out patches and upgrades so maintenance never affects user experience. Thanks to the integration of Tanium with IBM Automation, your endpoint management processes (scanning, patching, and updating) never put application performance at risk and business-critical applications are automatically isolated from known vulnerabilities.

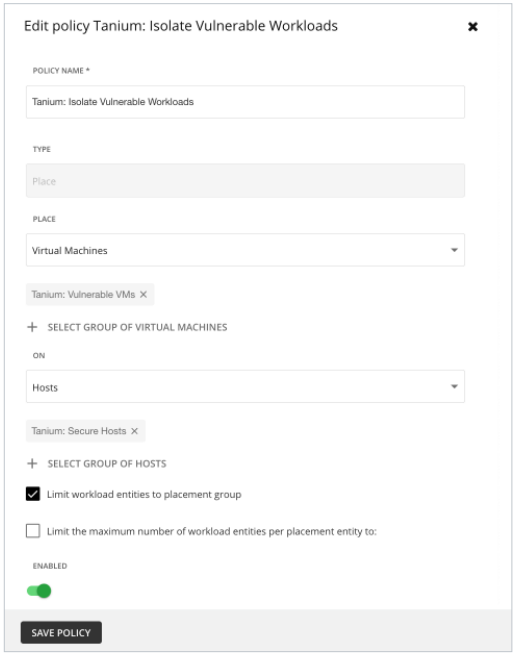

Figure 2. IBM Turbonomic uses Tanium's data to automatically sequester workloads.

Create harmony between ITOps and security teams for operational excellence and reduced costs

Silos between ITOps and security tools and manual integration efforts can lead to unnecessary costs and inaccurate data. Dynamic resourcing-based endpoint management enables organizations to empower their existing staff to automate the time-intensive work of performance assurance and deliver applications that are secure and always on. The integration between IBM Turbonomic and Tanium with IBM Automation enables IT and security teams to work together to eliminate downtime, ensure continuous application performance, and run necessary security operations at a low cost.

Conclusion: Automate app performance while mitigating security risks

Together, IBM Turbonomic and Tanium with IBM Automation eliminate downtime, ensure continuous application performance, and run necessary security operations at a low cost. This enables IT and security teams to work together to accelerate ITOps automation confidently for proactive performance and security.

Why IBM?

IBM Cloud® offers the most open and secure public cloud for business with a next-generation hybrid cloud platform, advanced data and AI capabilities, and deep enterprise expertise across 20 industries. IBM offers a full stack cloud platform with over 170 products and services covering data, containers, AI, the Internet of Things (IoT) and blockchain. To learn more, visit ibm.com/cloud.

For more information

To learn more about Tanium with IBM Automation, please contact your IBM representative or IBM Business Partner, or visit ibm.com/products/tanium.

Notes

1. The State Of Application Security, 2022, Forrester, 9 May 2022.
2. Security Report for In-Production Web Applications, Rapid7, 2018.
3. The Cost of a Data Breach Report 2022, IBM, July 2022.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2022