Complete visibility and control of your IT landscape

- The needs of the modern IT environment are becoming increasingly complex and extensive. Many companies have a mountain of tools to manage that seldom integrate well, can be slow, lack accuracy, or are based on outdated architecture.

- The risks are far from negligible, including security problems, silos, and downtime, creating unnecessarily high costs. For both companies and government organizations, it is more important than ever to take a holistic view of your IT landscape.

- And that is exactly how Tanium is making a difference for customers around the world, thanks to an integrated endpoint management platform with a single agent that can achieve hundreds of operations and security use cases for IT teams.

- Its unique architecture makes it possible to generate real-time insight and visibility of the IT landscape to enable faster action and improve an organization's resilience.

REFERENCE

1. https://www.tanium.com/blog/10-ways-tanium-improves-patch-management/

10 challenges Tanium can solve

Here are ten common challenges Tanium helps its customers solve through heightened visibility and control.

1. An incomplete and outdated configuration management database (CMDB)

Tool variation and infrastructure complexities mean that the information in your CMDB is often inaccurate or out of date. That creates risks since you can't take action on incomplete data.

2. Software noncompliance

Due to a lack of visibility, unknown and legacy licenses can be running, which limits your control. The cost of this can be very high when audited.

3. Unidentified vulnerabilities

As there is no complete picture of all endpoints and applications, some vulnerabilities are not identified.

4. Incomplete patch management

Regular patches should be sent to all endpoints that access your network. However, Tanium research suggests 80% of IT managers find that their patch efficacy is much lower than they would like to achieve.[1]

5. Data leakage

It is important to prevent sensitive data leaks by monitoring for risky behavior. For example, when network users deploy unauthorized software.

6. Blind spots in the IT landscape

Many organizations have far more endpoints connected to their network than they think. This lack of visibility into the IT landscape makes them vulnerable.

7. No control over admin accounts

Since it is not clear which endpoints are present in the organization, it is impossible to maintain control over admin accounts.

8. Disruptions due to change management

Without an up-to-date CMDB, nobody knows which services are running on which server. As a result, services may suddenly be unavailable for long periods of time.

9. No visibility into the application chain

In a chain, different applications often depend on each other. Therefore, it is important to quickly see which components a server is communicating with.

10. Lack of clarity about tools

In the absence of visibility into the tools used, it is not possible to quickly consult the right tool when a question needs to be answered urgently.

> "With employees increasingly working from home, we need a solution that maps out our entire IT landscape more than ever. Working from home is becoming the new normal, so it is important to be ready for the future and mitigate security risks."

Lourens Visser
CIO, Rijk

We also solve governance challenges

Tanium users enjoy a true sense of security. Thanks to Tanium, organizations know that all tasks have actually been performed. They are sure that their tools have indeed been installed and that all patches or updates are active. This is useful for government organizations that decentralize IT management or work with outsourced partners. Tanium reports on the quality of its services on an objective basis. Distributed discovery also ensures 100% coverage. The due diligence by Tanium increases the quality of services and improves deficiency.

Thanks to Tanium's unified endpoint management and security solution, customers have a holistic view of their IT landscape, making it possible to fix vulnerabilities in just a few hours, whereas using other methods could take days or even weeks. Thanks to Tanium, not only is time saved but also significant costs.

How Tanium helps save costs

You can't protect what you can't see. Based on a recent **Total Economic Impact™** study that used a composite organization to represent the average Tanium customer, Forrester Consulting determined that investing in Tanium Converged Endpoint Management (XEM) could allow organizations to realize $18.07 million in savings over three years. The following factors play a crucial role in this:

Better management of existing hardware and software

- Discovering unused assets, claiming them, or giving them a new purpose
- Reduced spending on service providers
- Avoiding costs by optimizing applications on endpoints

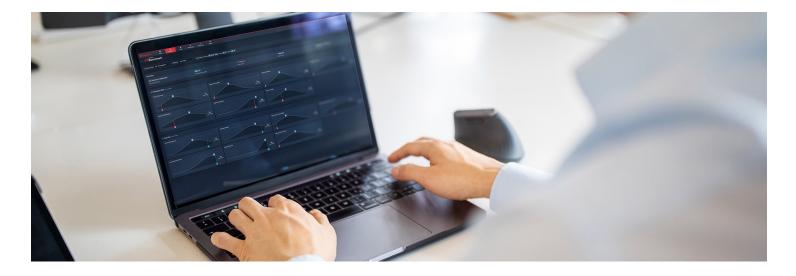### Fewer operational interruptions and security issues

- Systems become less vulnerable to cyber threats
- Lower costs due to security problems, data leakage, and associated fines and penalties
- Better visibility allows data centers to migrate to the public cloud with more confidence

Replace and reduce the number of tools in the IT landscape

- Patches can be rolled out much faster and more effectively
- Avoid fragmented approach and duplicate licensing

Optimize processes and the role of people

- More time to deploy people and resources where they can really generate value

More benefits of Tanium

The Tanium platform helps any organization adapt to the high demands of the current times in the following ways:

- Tanium is great for discovering and managing unknown workstations in an organization's domain or network. Consider the many home offices of employees who work from home.

- Tanium simplifies compliance issues. When software vendors or auditors need to check whether the software is compliant, it takes only seconds or minutes to gather all the information. With other systems, this can be very time-consuming and can take days or weeks.

- The number of cyber incidents and the mean time to resolution (MTTR) decrease significantly. This is often a key KPI for a C-level role in the organization, such as the CISO.

- IT architecture is simplified and optimized. Tanium helps to turn off servers and replace and disable tools.

WANT TO LEARN MORE?

Interested in the many benefits Tanium has to offer? We'd love to hear what your key challenges are, so let's meet up so we can show you why your organization will also benefit from working with Tanium.

Yes, I want to make an appointment!

Tanium delivers the industry's only true real-time cloud-based endpoint management and security offering. Its converged endpoint management (XEM) platform is real-time, seamless, and autonomous, allowing security-conscious organizations to break down silos and reduce complexity, cost, and risk. Securing more than 32M endpoints around the world, Tanium's customers include more than 40% of the Fortune 100, 7 of the top 10 U.S. retailers, 9 of the top 10 U.S. commercial banks, all 6 branches of the U.S. military, and MODs and DODs around the world. It also partners with the world's biggest technology companies, system integrators, and managed service providers to help customers realize the full potential of their IT investments. Tanium has been named to the Forbes Cloud 100 list for eight consecutive years and ranks on the Fortune 100 Best Companies to Work For.

Visit us at www.tanium.com and follow us on LinkedIn and X.

© Tanium 2024