

# NEC secures and manages endpoints at scale with Tanium

With over 260,000 endpoints worldwide, the IT services company needed help identifying, visualizing, patching, and managing its mix of Windows and Linux devices.



## ORGANIZATION

NEC Corporation

## LOCATION

Tokyo, Japan



While NEC Corp. was formed in 1899, the same year telephone service began between its headquarters city of Tokyo and Osaka, today the company's business is thoroughly modern. NEC offers cutting-edge cloud computing services, systems integration, telecom services, and much more. While that makes for a robust business, these modern operations also come with some equally modern cybersecurity challenges.

One source of security issues is NEC's sheer scale. The company employs some 120,000 people in every major continent. It operates more than 250 subsidiaries serving industries that include aerospace, agriculture, finance, manufacturing, retail, and transportation. And on the technology front, NEC manages a massive fleet of endpoint devices — over 260,000 in all, including both Windows clients and Linux servers.

"When managing over 260,000 devices, it's challenging to be continually up-to-date on the status of our IT assets and their vulnerabilities," says NEC's chief information security officer, Shinichi Fuchigami. "Yet endpoint management is critical to mitigating our business risk."

## Meeting Tanium

Though NEC launched its endpoint management program in 2002, the company didn't encounter Tanium until 2019. At the time, NEC sought a tool to manage its roughly 13,000 endpoints outside Japan in an integrated way. NEC also wanted the tool to help overcome three major challenges: ensuring thorough IT asset management, clarifying what endpoints existed and where they were located, and reducing the on-site workload of repetitive tasks such as applying patches

NEC selected Tanium and implemented it successfully in its branches outside Japan. And before long, CISO Fuchigami and his team realized that NEC faced similar challenges in Japan. With some 240,000 endpoints within Japan, those challenges loomed on a much larger scale

The team used the NIST Cybersecurity Framework — guidelines aimed at helping organizations understand, assess, prioritize, and communicate their cyber efforts — to inventory their issues and chart a way forward. In this way, they determined that Tanium Cloud was the optimal solution. Even better, deploying Tanium was quick. NEC installed the agent on over 200,000 endpoint devices in just four months.

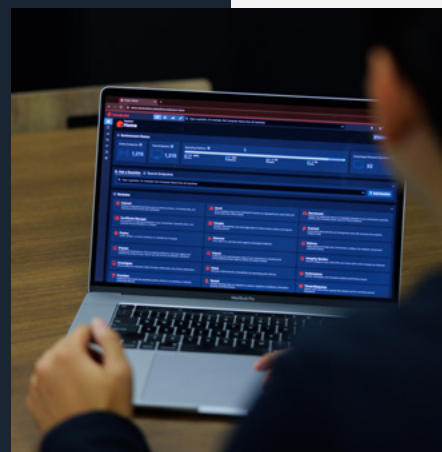
NEC realized Tanium could also help it manage “shadow IT” — computing devices acquired and installed without the central IT group's knowledge or oversight.

“With Tanium, any device on the network can be detected — even if Tanium is not installed on it,” says Anna Hayashi, a professional in NEC's CISO group. “Once the device's existence is identified, we can check who is managing it and bring it under proper management.”

NEC has also connected Tanium with ServiceNow. By linking critical asset and vulnerability information, this connection speeds NEC's detection of dangerous endpoint vulnerabilities.

The CISO team has also implemented a cybersecurity dashboard that uses Tanium data. The dashboard lets the team see the changing risk landscape, manage risk, and distinguish long-term issues from real-time emergencies.

“By obtaining information in near-real-time,” Fuchigami says, “Tanium has dramatically expanded what we can accomplish.”





## Gaining speed

For NEC, one big benefit of using Tanium is speed. That's important. When it comes to keeping systems and data secure, having real-time data can lead to speedy, effective responses.

Before using Tanium, investigating endpoint applications for specific vulnerabilities could take the NEC team more than 24 hours. Now, with Tanium, they can complete the same type of investigation in just five minutes.

Patching endpoint software is faster, too. Using Tanium has shortened the time NEC needs to deliver patches from 14 days to as few as four. NEC also patches with confidence; Tanium confirms a patch's deployment status, a task NEC's previous patching tool couldn't do.

More speed comes from NEC's Tanium-ServiceNow integration. According to CISO Fuchigami, this integration enables the early detection of critical vulnerabilities. This, in turn, has cut the time from detection to notifying the appropriate administrator by a massive 85 percent.

Also, by automating some tasks, Tanium has also helped NEC lower the workload of select on-premises employees to less than 7 percent of the previous level. That has freed them to work on more strategic projects.

NEC has also developed its own applications that integrate with Tanium. Under the Unified Endpoint Management brand, the NEC team offers a proprietary tool that works with Tanium.

"This makes it easy for us to manage and associate IT assets with their administrators," CISO Fuchigami says. "With Tanium, we have achieved quicker response times, improved efficiency, and increased productivity."

**"Tanium lets us detect any device on the network – even if Tanium is not installed on it. Once the device's existence is identified, we can check who is managing it and bring it under proper management."**

**Anna Hayashi**

Professional in the Office of the CISO  
NEC Corporation



# Results

## Fast answers

Before, investigating endpoint applications for specific vulnerabilities could take NEC more than 24 hours. Now, using Tanium, the same type of investigation gets completed in just five minutes.

## Fast patching

Using Tanium has shortened the time needed to deliver patches from 14 days to as few as four.

## Fast deployment

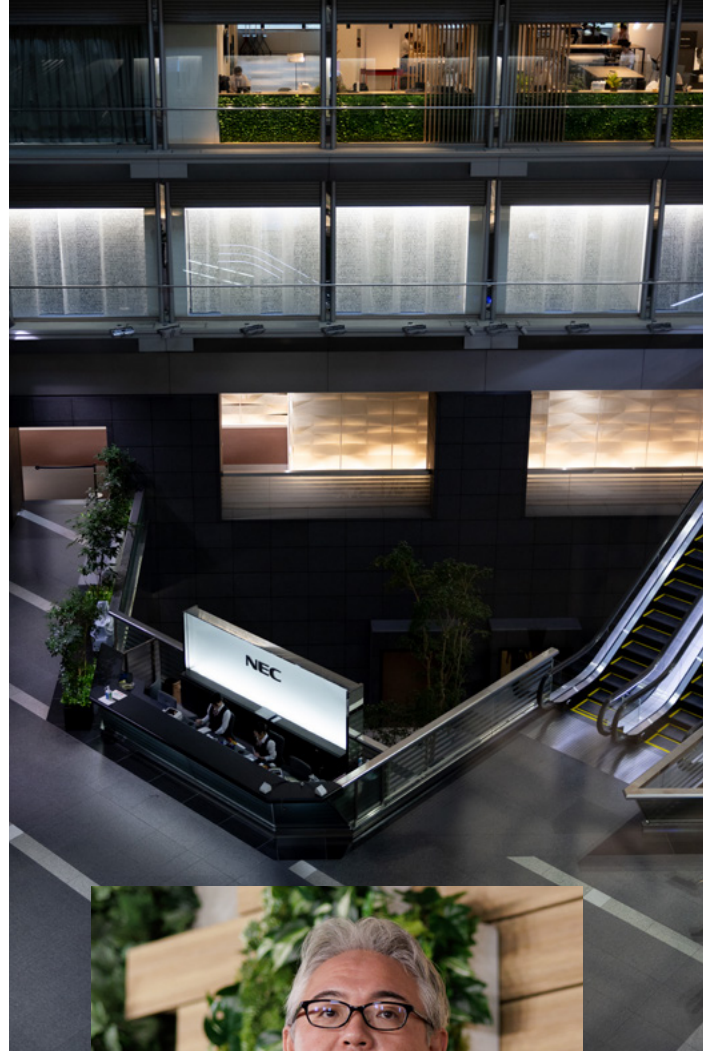
Deploying Tanium to some 220,000 endpoint devices took NEC only four months.

## Fast alerts

Integrating Tanium with ServiceNow empowers NEC to detect critical vulnerabilities early, cutting the time needed to move from detection to notifying an administrator by 85 percent.

“With Tanium, we’ve achieved quicker response times, improved efficiency, and increased productivity.”

**Shinichi Fuchigami**  
Chief Information Security Officer  
NEC Corporation



The Power of Certainty.™

Visit us at [www.tanium.com](http://www.tanium.com) and follow us on [LinkedIn](#) and [X](#).

© Tanium 2025