CASE STUDY

Con Edison keeps New York City running with the power of Tanium

For many large organizations, ensuring compliance of all endpoints on a network can be a challenge.

That was the case for Consolidated Edison Inc. It's the parent company of four businesses, the largest being Consolidated Edison Company of New York (Con Edison), a utility that provides electricity, steam and natural gas service to more than 10 million people in New York City and Westchester County. Like many utilities, IT plays a major role in helping ensure continuity of service.

"If we have a major service outage," says Frank Santoro, a Con Edison Information Security Systems Specialist, "residential customers, businesses, hospitals, schools, subways, traffic lights, homes, can be severely impacted." To ensure residents of New York have proper continuity of service, the company employs nearly 14,000 people. In addition, Con Edison manages tens of thousands of endpoints in its network.

To gain visibility and manage endpoints on the network, Con Edison was utilizing different endpoint tools which provided different functionality. The challenge was that none of the existing tools were able to provide confirmation that other endpoint tools were installed and running properly on the endpoints.

"We had instances of clients and agents being broken and not reporting in," Santoro says. "For compliance reporting and many other security use cases, that was a concern. If your clients aren't reporting in, you're not getting the data you need. And if you don't have a tool to monitor and fix the other clients and agents you have deployed, it becomes a manual task of finding what's broken and remediating it."

> "Though we started out small with our Tanium use cases, over time, we've purchased more modules and expanded the number of groups utilizing it. Tanium's a massive ecosystem that offers valuable capabilities."

Frank Santoro
Information Security Systems Specialist, Con Edison

> "With multiple endpoint agents across our environment, our operations team uses Tanium to report on and ensure that our endpoints have the proper tools with everything configured correctly."

Frank Santoro
Information Security Systems Specialist, Con Edison

Results

- **Tanium beyond security**
  Though Con Edison's SOC team "owns" Tanium, many other groups that are not part of security use Tanium too.
- **Endpoint Assist**
  Tanium helps Con Edison determine when an endpoint agent is working properly, and when it needs help.
- **Device Compliance**
  Tanium is giving Con Edison's security team compliance assurance that devices in the network have the latest patches.

Making connections with Tanium

To address the issue, Con Edison's enterprise architecture group licensed Tanium in 2016. With Tanium, the utility knew where and when their other endpoint tools were deployed and running properly. The architecture group also used Tanium on devices that did not have all endpoint agents deployed, gaining additional visibility into their endpoints.

"We originally got Tanium primarily for the use case of being able to fix clients, having another agent on the endpoints to see whether our other tools, were running and, if so, whether they were healthy," Santoro says. "With Tanium, we are able to deploy and install agents on devices that potentially didn't have all tools installed but had Tanium running."

Tanium offers Con Edison a single platform that delivers complete, accurate endpoint data in real time, regardless of the scale or complexity. Tanium also offers asset discovery and inventory, client management, risk and compliance management, sensitive-data monitoring, and threat hunting. And the Tanium agent is lightweight, consuming minimal endpoint resources and bandwidth.

After deployment, Con Edison realized Tanium could be used for other projects, too. One use case involved detecting hashes on the company's endpoints. Some antivirus software relies on hash values to detect whether a file is dangerous. Because that's a security issue, the project was transferred to Santoro's group.

"We implemented Tanium and got a lot of value out of hash-detection on endpoints," Santoro says. "That was a win for us."

Since then, several groups at the utility have used Tanium for a growing list of use cases. The forensics group uses Tanium to capture information for analysis. Yet another group employs Tanium for patching use cases.

"Though we started out small with our Tanium use cases, over time, we've purchased more modules and expanded the number of groups utilizing it," Santoro says. "Other teams began using Tanium to supplement reporting received from other tools to ensure there was an accurate picture of the environment."

Santoro adds, "Tanium's a massive ecosystem that offers valuable capabilities."

Making way for cooperation

In an example of how Tanium is helping Con Edison ensure device compliance, they utilize the patch module to provide confirmation that endpoints are fully patched. They are also able to take action to patch any endpoint that's found to be out of compliance.

"We are able to take action and remediate very easily and quickly, making sure our endpoints have the proper patches, tools and that everything's configured correctly," Santoro says.

Looking ahead, Santoro and his colleagues want to automate the deployment of Tanium agents. That way, when Tanium discovers a Con Edison asset that doesn't have the Tanium agent, it will be able to install the agent automatically. It's yet another instance where Tanium can ensure that endpoints are visible to the company.