CASE STUDY

TANIUM

Aptiv drives faster remediation and enhanced security with Tanium

APTIV

Industry
Automotive

Size
30,000 employees

Headquarters
Dublin, Ireland

Managed endpoints
65,000

Results

Quickly identify vulnerabilities

Aptiv needed to identify its vulnerabilities around Log4j – and fast. With Tanium, Aptiv gained full visibility in less than five minutes.

Bridge the gap between security and IT operations

Tanium helps Aptiv's security and IT operations teams collaborate to keep endpoints safe and secure. Security staff uses Tanium to quickly identify vulnerabilities. Then IT operations can use Tanium to rapidly remediate at-risk systems.

Quickly secure WFH devices

During the early days of the pandemic, Aptiv had some 30,000 of its employees working from home. Tanium helped Aptiv implement a speedy new approach to keeping its devices secure.

The maker of automotive 'brains and nervous systems' needed an approach to endpoint security that was flat-out fast. With help from Tanium, Aptiv now moves from endpoint vulnerability to remediation with a speed even a Ferrari might envy.

A fast-moving industry demands fast-moving security

In the fast-moving auto industry, it pays to be speedy. That's been the case for Aptiv PLC, a company focused on what its CEO recently described as "the brain and nervous system of the vehicles."

Since 2017, when Aptiv emerged from the ashes of the former Delphi Automotive Systems, the company has risen phoenix-like to become a profitable, multibillion-dollar player. Aptiv's fast moves include developing the Smart Vehicle Architecture, creating a cloud-native DevOps platform, and acquiring edge-to-cloud software provider Wind River.

But one area where Aptiv needed greater speed was at the juncture of IT operations and security.

"If I find a vulnerability, I need to make sure the team that's going to do the remediation does it at speed," says Luis Cunha, Aptiv's director of security architecture and engineering. "But most of the time, because the priorities of our teams were different, that wasn't true."

> "Wow! That was my first impression of Tanium. The amount of things I can see with this tool, the amount of information the tool is giving me, and all the actions I can do to fix stuff. Wow."

Luis Cunha
Director, Security Architecture and Engineering, Aptiv

That was a serious issue. "The bad actors don't have this problem," Cunha says. "They work together very well."

Given Aptiv's scale and distribution, managing and securing endpoint devices at speed is a big deal. The company operates over 125 manufacturing plants and 12 major technical centers, giving it a presence in over 45 countries. And connected to the company's IT infrastructure are some 300,000 endpoints, each of which offers a potential entryway for hackers, thieves, and other criminals.

"Sometimes," Cunha adds, "we need to react very fast."

Tanium delivers visibility, breaks down security and IT operations silos

Fortunately for Cunha and his colleagues, that kind of speed is possible with Tanium. Cunha first encountered Tanium in 2018, the year he joined Aptiv, as the company was already using Tanium.

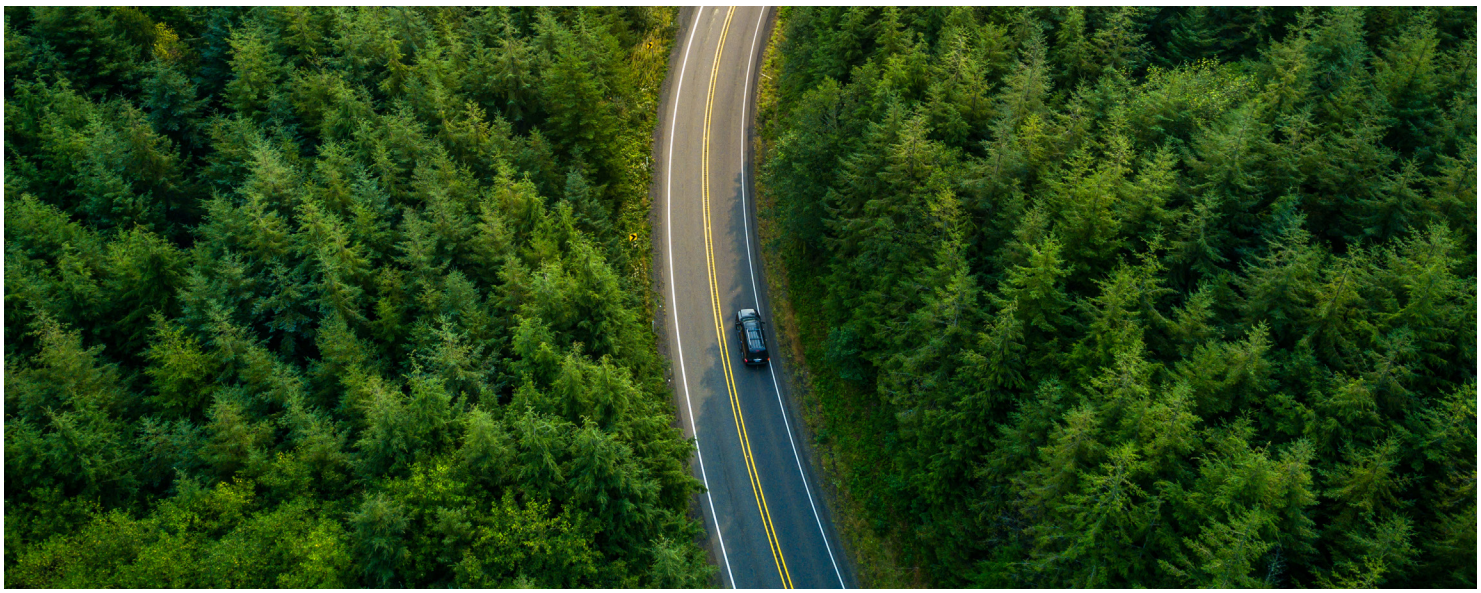
"Wow! That was my first impression of Tanium," Cunha says. "The amount of things I can see with this tool, the amount of information the tool is giving me, and all the actions I can do to fix stuff. Wow."

Cunha especially appreciated the way Tanium provides not only visibility into endpoints, but also what he calls observability. "I like to think of devices as living things connected to our infrastructure," he explains. "To keep things safe, I need to understand their behavior."

More specifically, Aptiv is now using Tanium for patch management, risk management, vulnerability management and deployment. It's a big job, as about 70,000 of the company's endpoints can be managed by Tanium, according to Cunha.

Tanium also helped Aptiv during the early days of the COVID-19 pandemic, when about 30,000 of the company's formerly office-bound employees were suddenly working from home. "We basically had to readapt the way we do security," Cunha recounts. "Mainly, by looking more at the devices and less at the perimeter and infrastructure. And we had to do it fast." Tanium helped, empowering Cunha and his colleagues to respond quickly and keep Aptiv's devices secure.

Tanium is also helping Aptiv to bridge the gap between its IT operations and security teams. Tanium helps by empowering the two teams to collaborate when vulnerabilities are discovered and require fast remediation. The security crew can use Tanium to quickly find vulnerabilities. And the IT operations staff can then use Tanium to remediate the systems with the required speed.



Open roads ahead

> "Tanium gives us not only visibility but also observability, which is the ability to understand our devices."
>
> **Luis Cunha**
> Director, Security Architecture and Engineering, Aptiv

As much as Aptiv has enjoyed big benefits from using Tanium, in some ways it's just getting started. Looking ahead, Cunha sees several opportunities where Aptiv could harness Tanium for new use cases.

One such area is Tanium's Microsoft integration. While the work is still exploratory, one possible area is using Tanium to help secure Microsoft email and prevent unauthorized use. For example, Tanium with Microsoft Entra AD integration could help Aptiv verify the identity of an end user trying to check email, understand what device they're using, and whether the user-device combination is authorized to connect with the corporate email account.

"Tanium together with Microsoft will make our life simpler," Cunha says. "We'll get there with both."

Another feature that has caught Aptiv's interest is Tanium's Software Bill of Materials (SBOM) feature, which gives users real-time visibility into their complex software environments, to make betterinformed decisions and lower their endpoint risk. For Aptiv, that could help provide fast visibility into potential exposures.

Aptiv has already used Tanium to do just that with the recent Log4j vulnerabilities. Using Tanium to gain visibility around Log4j took Aptiv less than five minutes, Cunha says. Tanium then gave him all the information Aptiv needed for a remediation strategy. The work went so quickly and smoothly, Cunha says, affected staff never even realized they had dangerous software vulnerabilities — another benefit of Tanium-powered speed.