

Pluxee, a Sodexo company, improves IT hygiene with Tanium



pluxee

Industry

Employee benefits

Size

5,000 employees

Headquarters

Issy-les-Moulineaux, France

“For us, Tanium is a proven accelerator, it’s fast-tracking a lot of the activities of our security roadmap.”

Joseph Boudara

Head of IT security for Pluxee

When an organization’s business changes, its IT needs to change too

That was the case at Pluxee, a Sodexo company, that provides some 250 employee-program products and services to roughly 36 million consumers and beneficiaries in over 30 countries.

Within Sodexo, Pluxee’s contribution to global revenue is disproportionately large. Despite employing just 1% of the company’s total workforce, Pluxee generates 4% of its total annual revenue. For Sodexo’s fiscal 2021, revenue from Pluxee totaled €745 million (approx. \$847 million).

Pluxee’s business, like that of many, is being disrupted by digital transformation. In response, Pluxee is doing some transforming of its own. That includes offering new personalized and simplified work-experience services for today’s hybrid work environment. It also includes forming partnerships with Uber Eats and Just Eat Takeaway that let holders of Pluxee meal plans order and pay for meal deliveries with a smartphone or other digital device. It also includes developing new digital payment technologies in markets such as Brazil and India.

However, supporting Pluxee’s IT is complex. While some of its entities have tiny IT departments — in one case, just a couple of people — others boast as many as 200 IT staff. Their skill sets vary widely, too. The company’s entrepreneurial culture has also had a big impact. Historically, entities were pushed to create their own local solutions to adapt to local needs. But now, with the business shapeshifting from paper vouchers to payment cards and now mobile payments solutions, there was a need to work differently.

“We believed Tanium could help infrastructure teams gaining efficiency to focus their time on more value-added activities. That meant Tanium wasn’t just another security solution, it was really one team working together to improve both efficiency and security.”

Joseph Boudara

Head of IT security for Pluxee

In addition, Joseph identified three main IT challenges

The first was a lack of visibility into all IT assets. Pluxee didn’t know how many endpoints it had, meaning it also didn’t know if all the endpoints were properly secured. The second was poor IT hygiene practices. Patching was inconsistent, and much of it was done manually. The third was a strong security roadmap that was hard to execute and follow across all 30+ markets, mainly due to inconsistent skills and tools on the field to push the activities forward, particularly in remote work conditions.

To overcome some of those challenges, Pluxee launched an initiative around asset patching. The Security and Infrastructure groups teamed up to find and build a global patching solution.

“To accelerate the adoption of our Global Security Solutions, we needed a solution not just for patching, but also for software deployments” Joseph says. “But as the initiative came into life during first COVID lockdown, we wanted remote functionality, too.” That’s where Pluxee met with Tanium, which Joseph had discovered few months before at an industry conference.

“I knew the solution and its capacities,” he says. “But we needed to check if it could work in our complex IT environment, and how we could operate it.”

In mid-2020, work got underway with a three-month live proof-of-concept (PoC) project with Tanium, involving a mix of 380 workstations and servers spread across three regional markets. Leveraging a detailed evaluation grid, Pluxee understood that Tanium ticked most of the boxes and could help overcome most of their challenges. In November 2020, Pluxee went live with its Tanium Platform built upon the Asset, Patch and Deploy modules. The main objectives were to regain visibility across all endpoints and support the deployment of Security solutions — a rising challenge with so many employees working from home during the pandemic.

In 2021 Joseph and his colleagues expanded Tanium’s use cases to tackle the Windows patching challenge, always working on gaining visibility first, to facilitate efficient remediation activities. Uptake by Pluxee entities was accelerated by the emergence of three complex Microsoft critical security vulnerabilities during the summer of 2021: PrintNightmare, HiveNightmare and MSHTML.

Indeed, Pluxee’s Security Operations Center (SOC) issued security alerts, mandating entities to implement several workarounds across all vulnerable assets before the patches were finally available. That’s where Tanium really helped.

“This is where Tanium became a game-changer,” says Joseph. “It helped us detect and monitor our vulnerabilities, efficiently deploy workarounds and later push security patches. It really fostered the adoption of our solution across all [our] markets.”

Impressive results came quickly. Using Tanium, the Pluxee team implemented workarounds on their domain controllers in just four days. The workstations rollout was just as quick, and compliance promptly exceeded the 90% mark within same timeline.

Upon Patch release on the server side, the Pluxee team used Tanium to improve patching from just 17% of all systems to 83%, and in only two weeks. For workstations, the results were even more efficient, moving from 24% to 95% patched within just a week.

One key to success, Joseph says, is how the security teams have worked hand-in-hand with Pluxee’s infrastructure team.