Toyota Financial Services: Secure, up-to-date IT

Profile: Situated in about 40 countries, Toyota Financial Services provides Toyota and Lexus customers a range of financial and associated services through its network of partnered dealers.

Location: Vaucresson (Hauts-de-Seine, France)

Industry: Financial

Website: toyota-financement.fr

Solutions:
- Ivanti® Patch for Endpoint Manager
- Ivanti® Application Control
- Ivanti® Device Control

Benefits:
- Greatly reduced time spent patching
- Reduced risk of update errors and corrected past errors
- Helped secure removable devices (USB flash drives, etc.) and bring them into compliance with GDPR
- Helped ensure compliance with annual safety audits
- Context-based whitelisting/blacklisting and privilege management

The Challenge

As an international company, Toyota Financial Services provides a global IT strategy with a level of customization for each country that factors in local challenges, regulations, and limitations. So, while all offices comply with global objectives—especially when it comes to security—networks, remote access facilities, links and inter-site connections, and email systems are unique, and the core network, storage and virtualization systems, office automation tools, and some professional solutions rely on local IT expertise.

To comply with the security directives from the Japanese parent company, for example, the IT team in France has for many years dealt with patching manually, using whatever tools were available. Unfortunately, when corrections are applied manually, malfunctions can occur, preventing some components from being updated. "This was an issue we found with VMware Tools," recalls Pierre Ng, Chief Information Security Officer at Toyota Financial Services. It led him to consider other solutions.

In addition, recurring security audits and General Data Protection Regulation (GDPR) obligations made better application control essential, and the company needed the ability to identify and encrypt removable devices like USB flash drives as well.

The Solution

"In autumn 2017 Ivanti requested the opportunity to present its range of solutions to us," Pierre Ng noted. "We were immediately attracted by the automated patch management solution."

From the launch of the Proof of Concept (POC) in early 2018, Pierre Ng was convinced by Patch for Endpoint Manager's automatic inventory function and patch testing ahead of deployment: "The automatic inventory allowed us to build up a map of our environment very quickly. Now, as soon as a patch is released, I'm confident Patch for Endpoint Manager will run smoothly and take care of everything, because it's tested beforehand by Ivanti."

In March the solution was deployed to 400 machines across two sites in France, including 20 physical servers, 150 virtual servers, 20 laptops, 100 virtual workstations, and so on.

Toyota Financial Services France also uses Ivanti Application Control to protect against zero-day exploits and block the applications that can't be patched with tools like application whitelisting and privilege management. With Ivanti Device Control they can quickly identify and enforce security policies on removable devices—flash drives in particular. Device Control helps keep unknown apps from being installed and executed on those devices, further reducing the attack surface. It can also encrypt the data they store to help protect against loss of confidential information.

The Results

From the start, the results have been spectacular for Toyota Financial Services, especially in terms of time spent on patching: "Previously, managing manual patching throughout France took up 60 percent of my time," explained Pierre Ng. "Now, just one day a week—not three—gets the job done."

"Thanks to the wide range of Ivanti solutions available, we are now in reach of the dream of so many IT team members: a fully automated information system."

— Pierre Ng
CISO

This time saving results from the elimination of certain tests on new updates, as this process is done beforehand by Ivanti teams, and because equipment is always kept up-to-date and thus secure, with less risk.

Ivanti Patch for Endpoint Manager also provides convenience: Where an individual connection to each server used to be essential, the company now needs simply to check off the devices to be updated directly in the product interface. And Patch for Endpoint Manager offers the largest patch catalog on the market.

For its part, Ivanti Application Control helps keep unauthorized applications from executing, helping the company comply with annual audits without requiring the IT team in France to manage extensive lists manually. It manages user privileges and policy just as easily, at a granular level, while allowing for self-elevation when exceptions occur.

It takes into account full admin privileges down to a regular user, and provides escalation of privileges where and when needed, from access to install applications, install a printer, use PowerShell, or whatever the user may need, but nothing more than what that user should have. And it can take a full administrator and strip away the things they may not need access to. Ivanti makes it simple for the IT team in France to give users just the privileges they need to fulfil their roles—no more, no less.

Flash drives, regularly used by employees, also no longer pose a threat to the company's network. Ivanti Device Control also helps the company trace all data that transits from the PC to a USB for GDPR compliance.

Just a few weeks after deploying all three Ivanti endpoint security solutions, Toyota Financial Services uncovered new opportunities to add more of the Ivanti solutions portfolio, including IT Service Management (ITSM). They are eager to define, implement, and automate workflows for the business, including onboarding/offboarding employees.

Learn More

↖ **ivanti.com**

☎ **1 800 982 2130**

✉ **sales@ivanti.com**